MIS Quarterly

RESEARCH ARTICLE

WHEN DO IT SECURITY INVESTMENTS MATTER? ACCOUNTING FOR THE INFLUENCE OF INSTITUTIONAL FACTORS IN THE CONTEXT OF HEALTHCARE DATA BREACHES[1]

Corey M. Angst
IT, Analytics, and Operations Department, University of Notre Dame, 348 Mendoza College of Business, Notre Dame, IN 46556 U.S.A. {cangst@nd.edu}

Emily S. Block
Department of Strategic Management and Organization, University of Alberta, 4-21 F Alberta School of Business, Edmonton, AB T6G 2R6 CANADA {eblock@ualberta.ca}

John D'Arcy
Department of Accounting and MIS, University of Delaware, 356 Purnell Hall, Newark, DE 19716 U.S.A. {jdarcy@udel.edu}

Ken Kelley
IT, Analytics, and Operations Department, University of Notre Dame, 363 Mendoza College of Business, Notre Dame, IN 46556 U.S.A. {kkelley@nd.edu}

In this study, we argue that institutional factors determine the extent to which hospitals are symbolic or substantive adopters of information technology (IT) specific organizational practices. We then propose that symbolic and substantive adoption will moderate the effect that IT security investments have on reducing the incidence of data security breaches over time. Using data from three different sources, we create a matched panel of over 5,000 U.S. hospitals and 938 breaches over the 2005–2013 time frame. Using a growth mixture model approach to model the heterogeneity in likelihood of breach, we use a two class solution in which hospitals that (1) belong to smaller health systems, (2) are older, (3) smaller in size, (4) for-profit, (5) non-academic, (6) faith-based, and (7) less entrepreneurial with IT are classified as symbolic adopters. We find that symbolic adoption diminishes the effectiveness of IT security investments, resulting in an increased likelihood of breach. Contrary to our theorizing, the use of more IT security is not directly responsible for reducing breaches, but instead, institutional factors create the conditions under which IT security investments can be more effective. Implications of these findings are significant for policy and practice, the most important of which may be the discovery that firms need to consider how adoption is influenced by institutional factors and how this should be balanced with technological solutions. In particular, our results support the notion that deeper integration of security into IT-related processes and routines leads to fewer breaches, with the caveat that it takes time for these benefits to be realized.

Keywords: Data security breach, institutional theory, firm characteristics, IT security, health IT, panel data, growth mixture model, longitudinal

[1]F. Mariam Zahedi was the accepting senior editor for this paper. Merrill Warkentin served as the associate editor.

The appendices for this paper are located in the "Online Supplements" section of the *MIS Quarterly*'s website (http://www.misq.org).

Introduction

A recent criminological report investigates the motivation and decision making of burglars by interviewing offenders. It found that offenders are deterred from burglarizing a target home when they see a sticker on the window or a sign posted indicating that there is either an alarm system or a dog on the premises (Blevins et al. 2012). These stickers or signs are types of signals. Many organizations deploy signals in an attempt to convince stakeholders they are complying with the laws, rules, norms, and values expected within their domain (e.g., DiMaggio and Powell 1983; Scott 2008). In the context of information technology (IT) security, researchers have advanced various deterrent mechanisms (e.g., policies; security education, training, and awareness (SETA) programs; and monitoring and detection technologies) that signal to both rogue employees and external hackers that an organization's information and technology assets are well protected (Png et al. 2008; Straub and Welke 1998). Whether the recipient of organizational information is an employee, hacker, analyst, regulator, investor, or other stakeholder, signals are often the best way for them to infer an organization's intent when more specific information is either unavailable or too costly to obtain (e.g., Bromley and Powell 2012; Fombrun and Shanley 1990; Stiglitz 2000; Weigelt and Camerer 1988). However, in the example above, the burglars are deterred from criminal behavior based on symbols that signal the existence of an alarm system or dog, regardless of whether an alarm system or dog is actually present. Given that these symbols may be detached from actual security practices, the question remains as to whether they maintain their deterrent effectiveness over time. Similarly, organizational signals only provide a surface level indication of a firm's endeavors, and thus the extent to which these signals are indicative of *actual* activities that achieve their intended outcomes over time is a topic of research and debate.

Neo-institutional theory[2] (hereafter institutional theory) distinguishes between *symbolic* and *substantive* adoption in order to account for the degree to which the activities of a firm are accurately reflected in the signals they communicate to relevant stakeholders (Lounsbury 2001; Thompson 2003). Substantive adoption represents one extreme, where signals are accurate representations of adopted practices and are tightly integrated with the organization's core operations. In contrast, symbolic adoption, such as the house with an alarm sticker but no security system, is intended to enhance a firm's external validation or legitimacy rather than achieve a specific technical benefit. Within the institutional literature, symbolic and substantive adoption are synonymous with loosely and tightly coupled organizational practices (Boxenbaum and Jonsson 2008; Bromley and Powell 2012). Accordingly, when we use the terms symbolic and substantive adoption, we are referring to the likelihood that practices are loosely or tightly coupled with actions.

One area in which the concepts of symbolic and substantive adoption would seem particularly consequential is the IT security function in a firm. A combination of high profile data breach incidents and increasing regulatory requirements (e.g., Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX)) have put IT security at the forefront of many firms' strategic agendas. The result has been a fairly consistent increase in IT security expenditures over the past decade or so across almost all industry sectors (Gartner 2015; PricewaterhouseCoopers 2016). Paradoxically, while firms have become more committed to IT security and have allocated higher budgets for it, data breach incidents have become more frequent and severe (Sen and Borle 2015). We submit that at least some explanation for this predicament is that firms vary with respect to how they integrate security into their IT-specific organizational practices. That is, some firms adopt IT practices more symbolically (as opposed to substantively, or vice versa) and this influences the extent to which they reap the benefits of their IT security investments.

We explore this phenomenon in the U.S. healthcare sector, where legislation mandates a baseline level of IT security expenditures and where detailed data on these expenditures are available. The healthcare setting is ideal for our research because hospitals exist in a complex environmental and social milieu where a multitude of internally and externally driven institutional pressures exist (Angst et al. 2010). These pressures are ripe for variance with respect to symbolic versus substantive adoption of IT practices. For instance, IT has long been viewed as an enabler of improved patient care in hospitals and thus there have been institutional pressures to incorporate IT into both clinical and administrative processes (Angst et al. 2012; Mishra et al. 2012). More recently, electronic health records (EHRs) have been identified as conduits to both healthcare quality improvements and cost reductions, which has led to a push toward technologies that support the digitization of health information (Bhargava and Mishra 2014). To this end, legislation (i.e., the Health Information Technology for Economic and Clinical Health Act (HITECH) and HIPAA) provides financial incentives for hospitals that adopt EHRs as well as mandatory guidelines for the security of patient data.

[2]The term *neo-institutional theory* emerged to distinguish DiMaggio and Powell's (1983) view of institutions, which consider an organization's social environment and its quest for legitimacy within this environment, from the tradition of historical institutionalism (i.e., formal institutions of government and the modern state) forwarded by Philip Selznick and others. For a review of the distinction please see Selznick (1996).

Even with these pressures, hospitals have discretion as to the degree to which they adopt IT practices. Institutional theory, and perspectives on firms' decoupling practices in particular, would suggest that hospitals are incentivized to temper such adoption to maintain internal flexibility (Meyer and Rowan 1977). Specifically, if hospitals can communicate their legitimacy through signals, by adopting practices symbolically and avoiding the costs of full implementation by decoupling those practices from core activities, it seems probable that many will do so. The heterogeneity with respect to hospitals' IT adoptions, including those related to security, lends credence to this point (Angst et al. 2010; Bhargava and Mishra 2014; Kwon and Johnson 2014). An unfortunate consequence of symbolic adoption, however, is that actual performance benefits may not be realized. This is because symbolically adopted practices are often superficial "window dressing" and typically do not substantially influence organizational activities (Bromley and Powell 2012).

Against this backdrop, we investigate the role that symbolic versus substantive adoption of IT practices plays in the effectiveness of IT security by means of reducing the likelihood of data security breaches. A key point that distinguishes our study from prior literature is that we assume the existence of different subgroups (i.e., symbolic and substantive classes) of hospitals in terms of how they adopt IT practices. We contend that these distinct classes can help explain why IT security investments have not been universally effective in reducing data breaches, and we hypothesize on this in the hospital context. Our results indicate that, over time, IT security investments are effective in preventing data breaches for substantive adopters only, and that this effect is masked when not accounting for the symbolic and substantive subgroups.

To uncover these subgroups, we used advanced statistical methods (i.e., latent class growth mixture models) to examine the growth curves of data breaches relative to time (from 2005 to 2013) and found evidence of a two-class *latent*[3] solution that fit both empirically and theoretically. Theoretical support for the latent classes as being representative of symbolic and substantive adoption comes from a set of factors rooted in hospitals' institutional environment, which we model as predictors of class membership. That is, we theorize that symbolic versus substantive adoption of IT practices is driven by the institutional environments in which firms, in this case hospitals, are embedded. Here, we define *IT practice* as a broad concept that includes clinical, administrative, and security IT functions, but also the amount of training, support, and investment in the IT function. While some of these variables can be measured directly, the degree of substantive or symbolic adoption cannot, thus the need for latent classes to represent the unobservable heterogeneity that we attribute to differing adoption strategies.

There are three key objectives of this study: (1) provide a context-specific extension of institutional theory by modeling the cluster of characteristics that are associated with symbolic or substantive adoption of IT practices in hospitals, with possible extensions to a broader range of firms; (2) investigate how symbolic and substantive adoption influences the relationship between IT security investments and the likelihood of data security breaches over time; and (3) propose a new concept—the IT value point—that draws from institutional theory and empirically validates one reason why it takes time for firms to yield benefits from IT security investments.

We contribute to the IT security literature by adding to the small number of studies exploring the macro-level factors that influence data breaches (e.g., Kankanhalli et al. 2003; Kwon and Johnson 2014; Straub 1990; Straub and Welke 1998). In particular, we delineate conditions under which IT security investments lead to improved performance, and we advance the limited research that has explored IT security effectiveness in the healthcare sector (Kwon and Johnson 2013, 2014), an area where security is a growing public concern.[4] Our findings also contribute to the IT adoption literature and research on institutional theory by considering the context of the adoption of an IT practice in terms of organizations that adopt substantively (and thus derive benefits from the technology) and those that adopt symbolically (and hope the action alone will result in benefits). We further contribute to institutional theory by proposing and empirically modeling a set of characteristics of hospitals that, when combined, can predict symbolic or substantive adoption. To do this, we utilize a latent classification method to categorize symbolic and substantive adopters based on their trajectory of likelihood of breach over time, providing a theoretically grounded empirical classification of these adoption patterns. Finally, as a departure from most extant studies that consider only immediate outcomes of symbolic and substantive adoptions, we investigate enduring effects of these adoption strategies within our nine-year study time frame.

The remainder of the paper proceeds as follows. In the next section we draw on institutional theory and develop hypotheses that classify hospitals as symbolic or substantive

[3]It is important to note that these classes are not directly measurable, akin to latent factors that are determined by a set of indicators in factor models.

[4]An analysis of recent data showed that the healthcare industry suffered more data breaches and more stolen records than any other industry (Gemalto 2015). Security experts expect this trend to continue due to the increasing value of personal health information (Experian 2015). For example, the "street value" of a stolen medical record has been estimated at 50 dollars compared to 1 dollar for a stolen social security number (AT&T 2015).

adopters. We then discuss our conceptual model relating IT security investments to data security breaches over time and the moderating role that a symbolic or substantive approach to adoption plays in this relationship. We follow this discussion with a description of our methods, data, and analysis techniques. We conclude with a discussion of our results, theoretical and practical implications, limitations, and opportunities for future research.

Literature Review and Hypotheses

Institutional Theory and Symbolic and Substantive Adoption

Institutional theory (DiMaggio and Powell 1983; Greenwood et al. 2011; Meyer and Rowan 1977) focuses on the influence of an organization's social environment on its activities. Institutions are higher order social structures that define what structures and behaviors are appropriate and necessary for organizations to operate. Institutional "rules" (i.e., shared beliefs that become instilled with value and social meaning) are established and reinforced over time such that they become taken for granted as appropriate behavior for firms (DiMaggio and Powell 1983). Institutions drive firm behavior, not necessarily because they improve firm performance, but because they provide legitimacy from the various social environments in which they operate (Boxenbaum and Jonsson 2008). In this institutional sense, legitimacy refers to the degree to which an organization's actions are endorsed and accepted by its stakeholders (Scott 2008). In the case of hospitals, there are a number of different stakeholder groups that can confer legitimacy. For example, teaching hospitals may wish to be viewed by peers as top-tier research and training institutions; Catholic hospitals follow their faith-based doctrine to maintain their standing with the Catholic Church; and for-profit hospitals seek legitimacy from owners and investors and compare themselves against other for-profit hospitals.

Given the tenets of institutional theory, the motivation to adopt a practice is only partially driven by actual performance benefits. But when organizations are embedded in social structures that value technical benefits, they are more apt to adopt a practice substantively, integrating it into their core routines and processes so that it can have the maximum amount of impact (i.e., tightly coupled) (Boxenbaum and Jonsson 2008). However, other firms, in an effort to seek legitimacy, may adopt practices symbolically, decoupling those practices from their technical core in an effort to derive legitimacy benefits of standardization, but avoiding the disruptions of day-to-day activities (Boxenbaum and Jonsson 2008). Studies of various symbolic adoptions, including pro-environment/sustainability programs (Berrone et al. 2009; Kim and Lyon 2013; Perez-Batres et al. 2012; Rodrigue et al. 2013; Westphal et al. 1997; Westphal and Zajac 2001), long-term incentive plans for CEOs (Westphal and Zajac 1998), recycling programs (Lounsbury 2001), stock repurchase plans (Westphal and Zajac 2001), codes of ethics (Stevens et al. 2005), and total quality management programs (TQM) (Levin 2006; Westphal et al. 1997) have demonstrated how firms realize the legitimacy benefits of adoption without incurring the full implementation costs when faced with pressures from stakeholders (e.g., regulatory agencies, customers, the community, employees, shareholders). Similarly, the healthcare context is not immune from pressures to adopt practices; as noted, there has been a push to adopt EHRs and other forms of IT, and the extent to which these technologies have been adopted varies greatly across hospitals (Angst et al. 2010; Bhargava and Mishra 2014; Mishra et al. 2012).

Discerning whether an organization is adopting symbolically or substantively is a formidable challenge, as we are often only able to observe implications of such adoption strategies. For example, if environmental protection mechanisms are only undertaken symbolically, they are less likely to have any long-term impact on reducing emissions and protecting the ecosystem (Kim and Lyon 2013; Rodrigue et al. 2013). Similarly, symbolic adoption of an IT practice—such as a weak and outdated wireless encryption protocol (e.g., wired equivalent privacy (WEP)), a technology that is implemented but not integrated with other systems, or employees that are not properly trained on its use—may allow for vulnerabilities in an organization's IT security that increase the likelihood of a data breach. As there is no measure that quantifies the degree to which (a numeric value) or whether or not (dichotomous outcome) symbolic versus substantive adoption is taking place, we employ methods that are designed to disentangle unobservable classes based on the different trajectories of change (in our case, the likelihood of a data breach over time). We draw upon institutional theory to designate these classes as either symbolic or substantive adoption of IT practices.[5] In this manner, institutional theory provides certain characteristics of the institutional environment of hospitals that are *predictive* of each type of adoption, and we elaborate on these in the following section.

[5]At later points in the paper, we explicitly note that symbolic and substantive adoption are not absolutes, but rather they lie on a continuum of the degree of adoption, with lower values suggesting symbolic adoption and higher values being substantive (Kim and Lyon 2013).

The Characteristics of Symbolic and Substantive Adopters

Institutional theory suggests that firms often look to their peers to determine appropriate behavior, including adoption decisions (DiMaggio and Powell 1983; Kraatz and Zajac 1996; Meyer and Rowan 1977; Rogers 1995; Scott 2008). In the U.S. healthcare context, many hospitals belong to a health system, suggesting a clear set of peers that serve as referents (Angst et al. 2012; Westphal et al. 1997). There are several advantages of belonging to a health system, ranging from economies of scale associated with system wide adoption, to sharing of resources, to reputational benefits, and many others. Health systems can range in size from single-hospital systems to hundreds of hospitals (Punke and Rosin 2015).

We argue that hospitals that are members of smaller health systems are more likely to be symbolic adopters of IT practices, whereas those that are members of larger systems will be more likely to be substantive adopters. First, larger systems are more likely to be under the watchful eyes of regulators and the press and, therefore, may not have the luxury of symbolic adoption. Research has shown that highly visible firms are more prone to substantive adoption whereas those that are able to evade such scrutiny are more likely to symbolically adopt (Delmas and Montes Sancho 2010; Kim and Lyon 2013). Even though it is difficult for an external entity to ascertain whether a hospital is adopting symbolically or substantively when viewing them superficially, the fear of more in-depth monitoring, based on hospitals' high visibility (Bansal and Roth 2000), suggests that they will err on the side of meaningful adoption. In this vein, Levin (2006) found that U.S. hospitals that were subject to active inspections and enforcement from an accreditation body were more likely to substantively adopt TQM programs.

Second, a hospital that belongs to a smaller health system may not have the resources to devote to substantive adoption. Institutional theory suggests that, all things being equal, firms with limited resources will pursue a symbolic adoption strategy as a means to avoid the full costs of implementation and maintain organizational efficiency (Bromley and Powell 2012). Conversely, members of larger health systems have slack resources that enable substantive adoption (Margolis and Walsh 2001; Orlitzky et al. 2003). In addition to having more resources, larger health systems may have a number of requirements for their members, including IT training, rules regarding the use of innovations, and technical support. As a result, we believe centralization increases the likelihood that an individual hospital will have the support and resources necessary to adopt practices substantively.

A counterargument might suggest that hospitals that are members of larger systems are more likely to become symbolic adopters because there is "strength in numbers"[6] that shields them from potential detection and penalties (either from regulatory bodies or due to public backlash) for symbolic adoption. While acknowledging this point, we contend that in the highly pressurized healthcare context where IT issues are matters of public policy and discourse (Appari and Johnson 2010), institutional constituents will demand substantive adoption and thus the increased visibility that comes with being a member of a larger health system will make substantive adoption more likely. Hence, we hypothesize:

> *Hypothesis 1a: Hospitals that are members of smaller health systems are more likely to be symbolic adopters.*

Other characteristics that are likely to distinguish between symbolic and substantive adopters are age and size of the hospital (Tolbert and Zucker 1983). The formal structure of a firm reflects the historical era in which it was founded, and the influence of the founding institutions are thought to persevere even as employees turn over (Johnson 2007). The imprinting of founding institutions also makes organizations less likely to change and evolve with the conditions in their environments (Johnson 2007; Sydow et al. 2009). Organizational scholars have maintained that older organizations seek to preserve informal routines that have evolved over time, whereas younger organizations are more receptive to new ideas (Westphal and Zajac 2001). As evidence to this point, Tolbert and Zucker (1983) found that younger cities were more likely to substantively adopt reforms than older cities whose municipal structures were already accepted as established practice by constituents. Reform, by definition, is the process of making changes to something in order to improve it, thus it should be viewed as substantive adoption. An additional perspective is that older firms have become more adept at symbolic adoption (i.e., decoupling), and given that this is a desirable strategy for maintaining organizational efficiency, older firms tend to employ such practices more often.

Turning to the healthcare context, older hospitals were founded in periods in which data was largely collected on paper and stored in filing cabinets, rather than in digital form. Older hospitals are also likely to be burdened with a much higher percentage of legacy systems. Indeed, the rate of new IT adoptions in the healthcare sector has historically trailed that of most other industries by a wide margin (Kwon and Johnson 2014). Imprinted by these institutional conditions, the integration of IT practices into hospitals' operations will be more difficult for those that were not founded in the age of technology (Johnson 2007). Angst et al. (2010) articulate a

[6]We thank an anonymous reviewer for raising this point.

similar view in their study of EHR adoptions in U.S. hospitals: "younger organizations are less likely to be fettered by legacy and are more willing to adopt and experiment with new technological innovations" (p. 1226). Given the above points, younger hospitals would seem to have stronger tendencies toward substantive adoption, whereas older hospitals, due to imprinting, would lean toward symbolic adoption. Hence,

Hypothesis 1b: Older hospitals are more likely to be symbolic adopters.

Prior research is somewhat mixed relative to the influence of size on the extent of adoption. While larger firms have the resources needed to acquire and implement practices in a substantive way, they also have organizational inertia (Huang et al. 2013; Stinchcombe 1965), which can make it more difficult to enact substantive change (note that here we are referring to size of the hospital itself, and not that of its hospital system). It is also administratively challenging to make organizational changes in larger firms because the increased complexity creates decision-making and communication delays (Kelly and Amburgey 1991). Yet the implications of failure are far greater in larger firms assuming that, similar to our arguments for H1a, larger firms are more visible entities and thus face greater scrutiny from stakeholders (e.g., regulators, press, customers). In other words, larger firms are more likely to get called out for their symbolic adoption practices. Again, we argue that this visibility effect is particularly acute in the healthcare sector where there are strong institutional pressures to meaningfully adopt IT practices. Conversely, we posit that smaller hospitals are more likely to resist the changes required to adopt IT substantively, and given the finite resources available to them, instead will adopt symbolically in order to gain legitimacy. Empirical studies provide some evidence to support these assertions. For example, Lounsbury (2001) found that smaller universities were more likely to symbolically adopt recycling programs (as compared to substantive adoptions at larger universities), while, in the hospital context, Levin (2006) found that symbolic adoption of a mandated TQM program was more likely in smaller hospitals. Accordingly, we hypothesize

Hypothesis 1c: Smaller hospitals are more likely to be symbolic adopters.

Institutional logics are coherent sets of institutional practices, values, norms, and identities that combine to drive the behavior of organizations (Thornton 2004). Research has emphasized that the degree to which firms are subject to multiple institutional logics influences the extent of symbolic and substantive adoption (Bromley and Powell 2012; Greenwood et al. 2011; Kraatz and Block 2008). The primary institutional logic that historically has governed hospitals is that of patient care (Anthony et al. 2014; Scott 2001; Scott and Meyer 1983; Scott et al. 2000). However, all hospitals, regardless of the extent to which they prioritize patient care, must deal with the *business* logic of funding, insurance, lawsuits, personnel management, and other issues associated with managing an enterprise (Anthony et al. 2014). Not all hospitals are equally embedded in business and patient care logics, therefore they are likely to face differential pressures associated with each, depending on the centrality of the influence of each logic (Besharov and Smith 2014).

Three hospital characteristics that indicate the degree of embeddedness in patient care or business logic are the business model utilized (for-profit/not-for-profit), organizational type (teaching/non-teaching), and mission (faith-based/non-faith-based) (Seo and Creed 2002; Thornton 2004). We argue that not-for-profit (NFP) hospitals have a stronger patient care logic whereas hospitals that are for-profit (FP) are more apt to prioritize elements of a business logic (Burgess and Wilson 1996). This view is supported by the features of FP hospitals that align with a business logic, including a more hierarchical organizational structure, a higher percentage of business professionals in leadership, and a more traditional governance structure (Caronna 2004; Sloan and Vraciu 1983). FP hospitals must prioritize shareholder and/or owner needs in addition to providing patient care. This business logic begets a greater emphasis on issues of efficiency and profitability (Anthony et al. 2014), both of which have the potential to lead to symbolic adoption (Campbell 2007). Furthermore, U.S. hospitals have for some time been under intense pressure to decrease spending while improving patient outcomes (Mindel and Mathiassen 2015), and this pressure is likely even more acute for FP hospitals. Although IT has been identified as a means to reduce healthcare costs, empirical studies have demonstrated that it takes time for hospitals to realize the benefits of these investments (Bhargava and Mishra 2014; Devaraj and Kohli 2003). Hence, under pressure to demonstrate immediate value for shareholders, it can be expected that FP hospitals are more likely to pursue a symbolic adoption strategy rather than incur the costs of full-scale integration of IT practices into core processes. This is because, from a business logic standpoint, such investments (e.g., transactional and security technologies that are required by HIPAA), would not demonstrate strong enough performance benefits (i.e., return-on-investment) in the short-term to justify substantive adoption. Thus, we predict that with competing priorities and limited resources, it is likely that FP hospitals will see less value in substantively investing in practices that offer speculative benefits, which leads to the following:

Hypothesis 1d: For-profit hospitals are more likely to be symbolic adopters.

Similar points regarding competing logics can be used to distinguish the adoption practices of teaching versus non-teaching hospitals and faith-based versus non-faith-based hospitals. Not only are these types of hospitals likely to vary from their counterparts in terms of staffing requirements, performance goals, and cost structures (Goldstein and Naor 2005), but, more importantly, they are known to have different strategic foci (Caronna 2004). For example, teaching hospitals tend to be more concerned with their goal of educating future physicians and conducting research. Faith-based hospitals face a similar dilemma in that their mission is often rooted in serving the poor and underprivileged. This is not to say that IT practices are unimportant in teaching or faith-based hospitals; however, for firms to survive, they must choose and develop core competencies in the presence of resource constraints (Barney 1991). By definition, teaching and faith-based hospitals have chosen their "primary" institutional affiliation and will likely only substantively adopt practices aligned with those institutions (Brickson 2005, 2007; Christmann and Taylor 2006). Other practices, less closely aligned with their core institutions, will be relegated to symbolic adoption. We argue that IT practices would fall into this category. Additionally, in terms of the security portion of IT practices, academic environments are generally regarded as "soft" in this area due to a culture that encourages openness and sharing, and the pragmatic issue of supporting a diverse set of users that includes students, faculty, and staff (Burd et al. 2005).[7] Teaching hospitals function in a similar institutional environment, and thus should be more likely to adopt security practices symbolically, rather than in a manner that is potentially disruptive to established culture and routines. Hence, the following hypotheses:

Hypothesis 1e: Teaching hospitals are more likely to be symbolic adopters.

Hypothesis 1f: Faith-based hospitals are more likely to be symbolic adopters.

Our last hypothesis regarding the classification of symbolic and substantive adoption of IT practices involves the entrepreneurial mindset of the hospital. Entrepreneurship involves the presence of lucrative opportunities, combined with individuals or firms that are willing to exploit these opportunities (Shane and Venkataraman 2000). Hospitals themselves have limited options when it comes to entrepreneurial actions. For example, hospitals cannot diversify or expand their geographic footprint, unlike health systems, which have the option to purchase other hospitals. However, a hospital's entrepreneurial nature can be evidenced by its choice of IT investments. Hospitals have a great deal of discretion in this area, as it is not uncommon for a given hospital to have more than 100 distinct IT systems that serve a variety of needs within the hospital, ranging from clinical treatment to administrative functions (Angst et al. 2012; Queenan et al. 2011). Entrepreneurially minded hospitals can be expected to proactively seek out new IT systems, test their efficacy, and set the standard for what laggard hospitals will adopt later (Lounsbury and Glynn 2001; Lumpkin and Dess 1996; Pérez-Luño et al. 2011). As a result, entrepreneurial hospitals would be early adopters of IT and related practices.

Institutional theory has long considered the implications of being an early or late adopter of organizational practices. For example, in their seminal work, DiMaggio and Powell (1983) argued that laggard firms adopt practices not for performance reasons but instead to be perceived as legitimate by their peers. This stance has been borne out by a number of empirical studies, which found early adopters more likely to reap the benefits of adoption, while later adopters did not realize the same value (Boxenbaum and Jonsson 2008; Bromley and Powell 2012). Hence, early adoption is generally viewed as substantive whereas late adoption is considered symbolic (Delmas and Montes Sancho 2010). We combine this view with the notion that late IT adopters are less likely to be entrepreneurs who substantively adopt these technologies and related practices, and predict the following in the hospital context:

Hypothesis 1g: Less entrepreneurial hospitals are more likely to be symbolic adopters.

Table 1 provides a summary of the main theoretical arguments used to support the preceding hypotheses. The conceptual model describing these and the other study relationships is shown in Figure 1. The top portion of the figure depicts the drivers of symbolic or substantive adoption (H1a through H1g) and the bottom portion depicts the role that symbolic or substantive adoption plays in moderating the relationship between IT security investment and data breaches over time, which we describe in the next section and later evaluate with a growth mixture model. As a point of clarification, we use the term *moderation* here because we are positing that the relationship between IT security investment and data breach depends on the group (i.e., different effects across groups; thus, group is a categorical moderator). A difficulty, as already noted, is that group membership is not observed; hence, the group is an unobserved variable that is theorized to exist and thus we use the term *latent class* to refer to symbolic or substantive approaches to adoption.

[7]We thank an anonymous reviewer for raising this point.

Table 1. Institutional Drivers of Symbolic or Substantive Adoption

Institutional Driver	Theoretical Arguments	References in the Institutional Literature
Size of Health System	Greater visibility makes substantive adoption more likely; Larger systems have slack resources that enable substantive adoption	Delmas and Montes Sancho (2010); Margolis and Walsh (2001); (Orlitzky et al. 2003)
Hospital Age	Due to imprinting, older organizations take on elements present in the environment upon their founding, and resist substantive adoption of new technologies	Johnson (2007); Sydow et al. (2009)
Hospital Size	Greater visibility makes substantive adoption more likely; More resources make substantive adoption more likely	Campbell (2007); Delmas and Montes Sancho (2010); Lounsbury (2001)
For-Profit or Not-for-Profit	Focus on short term returns due to business logic; Shareholder monitoring emphasizes efficiency and profits, thus symbolic adoption of non-revenue-generating activities	Campbell (2007); Christmann and Taylor (2006); Westphal and Zajac (2001); Westphal and Zajac (1998)
Teaching or Faith-Based Orientation	Consumer preferences and core identity drive priorities, resulting in the deprioritizing of non-core features of the organization by means of symbolic adoption	Brickson (2005); Brickson (2007); Christmann and Taylor (2006)
Entrepreneurial Orientation	Proactiveness, risk taking, innovation, and early adoption make firms with greater entrepreneurial orientation more likely to adopt technology substantively	Lounsbury and Glynn (2001); Lumpkin and Dess (1996); Pérez-Luño et al. (2011)

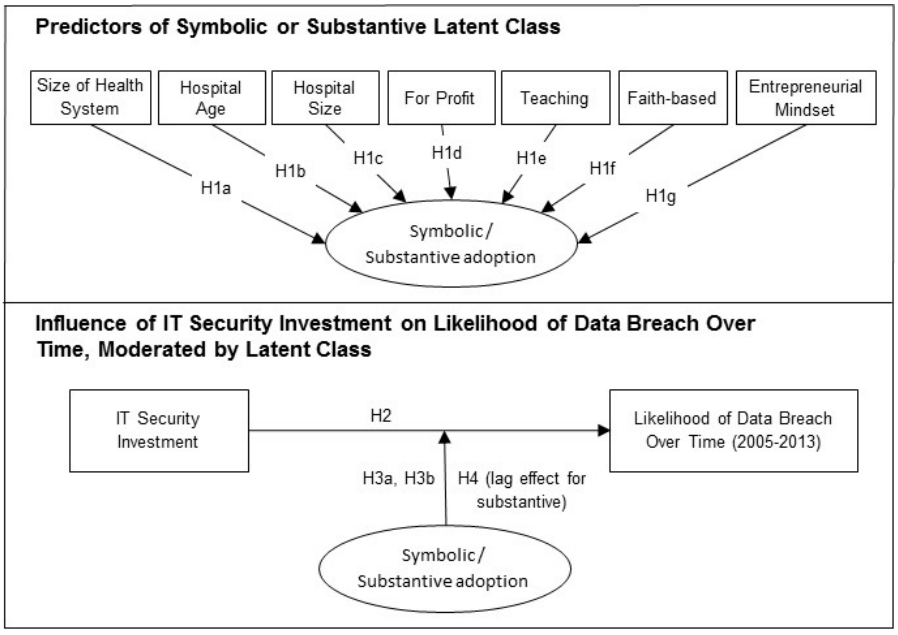


Figure 1. Conceptual Model

Symbolic and Substantive Adoption and IT Security Effectiveness

Before discussing the moderating influence of a symbolic or substantive adoption classification on the effectiveness of IT security investments, we begin with a baseline hypothesis regarding the efficacy of IT security investments on breaches. The HIPAA Security Rule (HIPAAPrivacy 2004) defines baseline levels of technical, physical, and administrative security controls that must be implemented to safeguard sensitive patient data,[8] and the HITECH Act (Freedman 2009)

[8]The HIPAA Security Rule is based on the fundamental concepts of flexibility, scalability, and technology neutrality. Therefore, no specific requirements for types of technology to implement are identified. The rule allows a covered entity to use any security measures that allow it reasonably and appropriately to implement the standards and implementation specifications. A covered entity must determine which security measures and specific

added additional security and privacy requirements for healthcare organizations and increased the penalties for noncompliance (Johnson and Willey 2011). The emergence of these regulations is predicated on the fact that taking steps to protect hospitals' information and technology assets, through the adoption of IT security, will be effective in reducing the likelihood of breach. However, and that which is central to our study, hospitals have a great deal of discretion in the adoption of specific technologies that fulfill their legal requirements, and the manner and extent to which these technologies are integrated into their core processes. With respect to IT security investments, hospitals may choose among a suite of technologies of which only some must be adopted by legal mandate. Interestingly, although some empirical studies found that increased IT security resources were associated with fewer security incidents in both hospital (Kwon and Johnson 2013, 2014) and non-hospital contexts (Straub 1990), as noted earlier, there is also anecdotal evidence that IT security investments have not been universally effective in reducing data breaches. However, as a baseline for our study, we predict that hospitals making larger investments in IT security will experience fewer breaches. Hence,

> *Hypothesis 2: Greater IT security investment will have a negative effect on the likelihood of security breaches over time (i.e., more IT security investment will reduce breaches).*

Even among hospitals that adopt identical technologies, the conditions under which adoption occurs should be important in predicting the efficacy of those technologies in preventing breaches. Research has demonstrated that *how* firms adopt IT security is vital to understanding the impact of those technologies and related practices. Much of this research has been considered from the perspective of the end user. For example, studies by Bulgurcu et al. (2010) and Puhakainen and Siponen (2010) found that organizations with a pro-security posture emphasizing security awareness increased compliance with security policies. Likewise, in the healthcare setting, Warkentin et al. (2011) found that informal learning environments that encourage attention to security and privacy issues increased employees' compliance with HIPAA privacy policies. Other IT security research suggests that developing a punitive posture toward IT security reduces breaches due to the anticipation of sanctions (D'Arcy and Herath 2011; D'Arcy et al. 2009; Herath and Rao 2009). This resonates with the IT appropriation and co-specialized assets literature in that IT alone is insufficient to gain competitive advantage, but when coupled with certain organizational practices, it can yield improved performance (Dos Santos and Peffers 1995; Duliba et al. 2001).

Deep integration of IT into a process is one of the defining features of substantive adoption, where practices are tightly coupled with an organization's other activities, values, systems, and processes (Lounsbury 2001; Meyer and Rowan 1977; Thompson 2003). We posit that the benefits of the adoption of IT security will be greater for hospitals that adopt substantively than those that adopt symbolically, due to the ongoing learning and process improvements that accrue to substantive adopters. Symbolic adoption, by definition, will not be accompanied with efforts to integrate the technology with existing organizational knowledge (Argote and Miron-Spektor 2011). As a result, substantive adoption should positively impact security performance over time (i.e., lower likelihood of breach) but we do not expect symbolic adoption to have the same effect. To the extent that internal and external hackers become more adept at attacking firms and the legitimacy attached to symbolic security efforts diminishes in the minds of these potential attackers over time, we posit that the likelihood of security breaches will increase in hospitals that have symbolically adopted. There is evidence to support this position, particularly the legitimacy perspective, as Berrone et al. (2009) found that symbolic adoption of pro-environmental practices had only a short-term impact on environmental legitimacy whereas substantive adoption had both short- and long-term effects. We also expect that from a pragmatic perspective, because IT practices are adopted only on the surface in symbolic firms and not tightly woven into core processes, IT security investments will not benefit from the same integrative efforts that accrue to substantive adopters of IT practices, and thus attackers will exploit these weaknesses given time. Hence, we hypothesize

> *Hypothesis 3a: Over time, the benefit of* substantive *adoption on the relationship between IT security investment and breaches will increase (i.e., the likelihood of breach will decrease, thus the slope will be negative).*

> *Hypothesis 3b: Over time, the negative consequences of symbolic adoption on the relationship between IT security investment and breaches will increase (i.e., the likelihood of breach will increase, thus the slope will be positive).*

Finally, prior literature demonstrates that the positive effects of technology adoptions, including those in hospitals, are often not immediately realized (Bhargava and Mishra 2014; Devaraj and Kohli 2003; Pisano et al. 2001). Like other firms that implement IT, hospitals presumably require time to adequately train employees, integrate technologies into their processes, achieve organizational learning, and ultimately

---

technologies are reasonable and appropriate for implementation in its organization (as specified in §164.306(b) the Security Standards: General Rules, Flexibility of Approach (*HIPAA Security Series: Basics of Risk Analysis and Risk Management*, available at www.cms.hhs.gov).

extract value from the implementation. Some hospitals have even demonstrated that IT investments can have negative performance effects in the short term, but will improve over time (Bhargava and Mishra 2014). As a consequence, the benefits of substantive adoption may not be realized immediately, but should continue to improve as the IT security technologies get more deeply integrated into the organizational framework. Collectively, prior literature leads us to predict that hospitals that substantively adopt and deeply integrate IT security into their processes and structures will be more successful in preventing breaches, but the amount of time the hospital is exposed to the technology will be an important predictor of success. We refer to this phenomenon as the *IT value point* and suggest that it is likely to vary depending on whether adoption is substantive or symbolic, such that there will be lag for substantive adoptions. Hence, the following:

> *Hypothesis 4: The benefits of* substantive *adoption will take time to be realized (i.e., there will be an IT value point at which substantive adoption becomes more effective than symbolic adoption).*

Methods

Hospital IT Security Context

There are several IT security technologies that are relevant to the hospital context and, similar to extant work (Anthony et al. 2014; Kwon and Johnson 2014), we focus on the following: biometrics (fingerprint and iris scan), identity (ID) management, intrusion detection system, antivirus software, user authentication systems (non-biometric), data encryption, Internet firewall, spyware filter, and single sign-on technology (see Appendix A for descriptions). Although these technologies have varying degrees of sophistication, apart from antivirus software, Internet firewall, and spyware filters, each would generally be considered beyond *basic* security measures. To this point, industry research demonstrates varying adoption patterns for several of these technologies during the timeframe of our study (e.g., Richardson 2008), and they were not fully deployed among U.S. hospitals during this period (HIMSS 2014).

Data and Operationalization of Constructs

We constructed a panel dataset from 2005 to 2013 including all U.S. hospitals in the HIMSS Analytics™ Database. The number of hospitals with complete data ranged from 3,998 in 2005 to 5,882 in 2013, which is approximately 80% of the entire population of U.S. hospitals. Using Medicare ID (a unique identifier assigned by the Centers for Medicare and Medicaid Services (CMS)) as the matching variable, we merged data from the HIMSS database, which includes IT adoption data (security applications and other technologies) and several hospital characteristics, with data acquired from the HospitalCompare database (data.medicare.gov). HospitalCompare includes hospitals' teaching and for-profit status, among other information.

We conducted a detailed search for data security breaches[9] that affected hospitals over the nine years of our panel. The majority of the breaches in our sample were obtained from the Privacy Rights Clearinghouse website (www.privacyrights.org). This website provides a comprehensive list of publicly announced data breaches and has served as the single source of this information in recent research (Sen and Borle 2015). However, for completeness sake, and similar to Kwon and Johnson (2014), we conducted an additional search for hospital data breaches using the LexisNexis database, Health & Human Services website (www.hhs.gov), and the Identity Theft Resource Center (www.idtheftcenter.org). We found no additional breaches in these databases but were able to glean more complete information on several reported breaches, such as the specific location of the breach. We then manually matched our breach data to our data from the HIMSS and HospitalCompare databases using the hospital's name and location. We identified 938 data breaches[10] over the nine-year time frame of our study. Descriptive statistics for all of the study variables are included in Table 2.

[9]Following Sen and Borle (2015), we define a data security breach as an incident that "involves unauthorized access to sensitive, protected, or confidential data resulting in the compromise or potential compromise of confidentiality, integrity, and availability of the affected data. Sensitive, protected, or confidential data may include personal health information, personal identifiable information, trade secrets or intellectual property, and/or personal financial data" (p. 315). Not only does this definition include both internal and external breaches but it also encompasses those motivated by either malicious or non-malicious (e.g., bypassing security protocols to improve job efficiency) intent (Willison and Warkentin 2013).

[10]Using the same databases, Kwon and Johnson (2014) identified 234 hospitals that had at least one breach during the 2005–2010 time frame, which is markedly different than what we found during the same time period (515 hospitals). One explanation is that Kwon and Johnson (2014) did not assume that when a parent (health system) had a breach, that it impacted all of the member hospitals; yet they did account for individual reactive investment in IT security by all member hospitals when any hospital in the system had a breach, suggesting they considered network effects. We felt it was imperative to include all hospitals in a "breached" health system. To support this claim, we point to the existence of the Enterprise Master Person Index system (EMPI), an electronic database that identifies all patients within the health system. The vast majority of hospitals in our sample (over 77% per HIMSS database) utilize an EMPI, thus the likelihood of a breach in a health system having ramifications for member hospitals is very high and, therefore, we accounted for this when coding our data.

Table 2. Descriptive Statistics

Year	Variable / Statistic	Size Health System	Hospital Size (staffed beds)	Hospital Age (years)	For Profit	Teaching	Faith Based	Entrepre-neurial Mindset (Saidin)	IT Security Investment	Breach
2005 n = 3998	Median/[Total]	6	136	22	[707]	[331]	[909]	8.87	1	[9]
	Mean	33.0	183.4	38.4	0.18	0.08	0.23	9.67	1.04	0.002
	Std. Dev	56.8	165.0	32.9	0.38	0.28	0.42	5.20	1.62	0.047
2006 n = 4071	Median/[Total]	5	133	21	[727]	[324]	[923]	15.31	2	[202]
	Mean	21.7	180.7	38.0	0.15	0.08	0.23	16.11	2.49	0.050
	Std. Dev	39.5	166.2	33.5	0.36	0.27	0.42	8.09	2.50	0.219
2007 n = 5214	Median/[Total]	2	92	21	[935]	[310]	[989]	16.94	2	[37]
	Mean	19.3	149.0	38.1	0.18	0.06	0.19	17.35	2.21	0.007
	Std. Dev	39.2	159.6	33.6	0.39	0.24	0.39	8.39	2.30	0.085
2008 n = 5384	Median/[Total]	3	87	21	[954]	[299]	[1005]	18.12	3	[150]
	Mean	19.7	146.5	38.1	0.18	0.06	0.19	17.29	2.81	0.029
	Std. Dev	37.7	160.3	33.7	0.39	0.23	0.39	7.85	2.53	0.168
2009 n = 5477	Median/[Total]	3	86	21	[1003]	[297]	[1026]	18.52	3	[65]
	Mean	19.9	145.6	38.1	0.19	0.06	0.19	18.01	2.92	0.013
	Std. Dev	37.7	160.4	33.6	0.39	0.23	0.39	7.66	1.76	0.111
2010 n = 5532	Median/[Total]	3	84	21	[1074]	[261]	[1031]	19.02	4	[52]
	Mean	19.3	144.4	38.0	0.20	0.05	0.19	18.52	4.42	0.010
	Std. Dev	36.3	161.0	33.7	0.40	0.22	0.39	7.54	1.76	0.099
2011 n = 5613	Median/[Total]	3	80	21	[1141]	[220]	[1047]	19.14	4	[135]
	Mean	20.7	142.8	38.1	0.21	0.04	0.19	18.81	4.40	0.026
	Std. Dev	37.6	160.8	33.6	0.41	0.20	0.39	6.28	1.97	0.158
2012 n = 5827	Median/[Total]	4	78	21	[1218]	[209]	[1067]	20.38	4	[167]
	Mean	23.3	141.4	38.2	0.22	0.04	0.18	20.56	4.62	0.031
	Std. Dev	40.8	161.4	33.6	0.42	0.19	0.39	6.00	2.01	0.174
2013 n = 5882	Median/[Total]	5	76.5	22	[707]	[207]	[1079]	19.37	4	[121]
	Mean	26.4	140.0	38.4	0.18	0.04	0.18	18.77	3.86	0.021
	Std. Dev	43.0	161.3	32.9	0.38	0.18	0.39	7.97	2.31	0.142

Data security breach (*Breach*) is coded as 1 (had a breach) or 0 (did not have a breach) in each year for each hospital. IT security investment (*ITSec*) is a count of the number of security systems (those listed in Appendix A) in service in each year and ranged from 1 to 10 per year. Kwon and Johnson (2014) used the count of a similar set of technologies, but their measure did not include fingerprint, iris scan, spyware filters, or single sign-on. We use mean *ITSec* (over the available years, up to nine years for hospitals with complete data) to quantify each hospital's IT security investment in our analysis. The institutional variables were measured as follows: size of health system (*SystemSize)* is the number of hospitals in the focal hospital's health system; hospital size (*HospitalSize)* is the natural log of the number of staffed beds; hospital age (*Age)* is the natural log of the length of time (in years) that the hospital has been operating (we log-transformed *HospitalSize* and *Age* due to skewed distributions; e.g., Dranove et al. 2014); for profit (*BusinessModel)* is coded as 1 if the hospital is FP and 0 if it is NFP;[11] teaching (*Teaching)* is coded as 1 if the hospital is a teaching/academic hospital and 0 if not; faith based (*Mission)* is coded as 1 if the hospital has a religious affiliation and 0 if not.[12] Finally, entrepreneurial mindset (*EntrepMindset*) is calculated using the Saidin Index (Spetz and Maiuro 2004), which is a weighted metric of IT adoption that takes into account the

[11]There are rare instances in which a hospital changed from FP to NFP, or vice versa, during the time frame under investigation. In these situations we used the proportion of time they were FP (e.g., if a hospital was FP for six of the nine years, it received a score of 6/9 =.67). The same method was used for *Teaching* and *Mission* variables.

[12]An exhaustive web and literature search did not yield a database that identified hospitals as faith-based, and this information was not contained in the HIMSS or HospitalCompare databases. We found a list of Catholic hospitals and supplemented that list by counting hospitals that had faith-related words in their title, such as Methodist, Lutheran, Jewish, Baptist, Presbyterian, etc.

rarity of the IT relative to its adoption by other hospitals. As described in Queenan et al. (2011), the index works by "summing across all hospital technologies the product of a technology's weight and a 0,1 indicator variable signifying whether or not a hospital has adopted a given technology" (p. 643).

The complete formula, as specified in Spetz and Maiuro (2004), is as follows:

$$a_{k,t} = 1 - \left(\frac{1}{N_t}\right)\sum_{i=1}^{N_t} \tau_{i,k,t} \quad \text{and} \quad S_{i,t} = \sum_{k=1}^{K} a_{k,t}\tau_{i,k,t}$$

where k is the number of technologies available in a given year and indexed by all $k = 1, \ldots, K$; t is year; $a_{k,t}$ is the weight for a given technology across all hospitals; N_t is the number of hospitals in year t; $\tau_{i,k,t}$ is 1 if hospital i has technology k in year t, 0 otherwise. We used the list of 88 technologies available to hospitals in the HIMSS database and calculated the number of technologies adopted per hospital per year, minus the technologies that make up our *ITSec* variable. Table 3 describes our study variables and their correlations are reported in Appendix B.

Analysis Strategy

We used a growth mixture model (GMM) for dichotomous outcomes in the context of a general latent variable modeling framework to map our conceptual model (Figure 1) onto a statistical model (Appendix C) to test of our hypotheses (for a detailed discussion of this type of statistical model, see Muthén 2002, 2004; Muthén and Shedden 1999).[13] Consistent with our theorizing regarding symbolic and substantive adoption of IT practices, we fit a two-class model for the binary outcome variable (i.e., *Breach*) over time to account for heterogeneity in change trajectories in the likelihood of breach over the nine occasions (i.e., nine years) of measurement.

A mixture model assumes that a population is heterogeneous in that different classes (within the population) have different parameters (Jung and Wickrama 2008). In our case, the theorized symbolic and substantive adoption types are the two latent classes that influence the likelihood of a data breach over time and, as we have earlier noted, this grouping variable is not directly observable and is thus latent.[14] In a theoretical argument for incorporating latent classes into statistical models, Muthén (1989) argues that "data are frequently analyzed as if they were obtained from a single population, although it is often unlikely that all individuals [or entities more generally] in a sample have the same set of parameter values" (p. 558). This line of reasoning was also argued by Nagin (1999), who developed an early model of heterogeneous change that incorporated latent classes under the auspices that the population was composed of a mixture of groups where, as in the GMM, group membership was unknown. One can regard mixture models as a missing variable problem, in which the grouping variable is unknown (and often unknowable). For example, the model proposed by Nagin was motivated in part by delinquent development, in which there were different trajectories in the number of convictions of young males; some of the participants rarely were convicted of criminal offenses, others were convicted a few times, whereas a third group were convicted multiple times (particularly between ages 16 and 20). Nagin's approach was not to presuppose a single trajectory style that governs delinquency (i.e., homogeneous change across individuals), but rather to use the developmental trajectories to estimate the *class specific* parameter estimates (i.e., intercepts and slopes) for the three hypothesized types of delinquency. That is to say, such latent class models in the context of change, such as the GMM, presume that there are different sets of change parameters for different groups, where the difficulty is that the group membership is unknown. Ignoring the possibility of latent classes actually imposes a rather restrictive assumption: all entities conform to the same model. Again, in our context, we believe that there are two distinct classes of adopters and, unfortunately, obtaining a direct measure of "type of adopter" is not possible. Sterba (2013) provides a review of this rich methodological framework on mixture models and the interconnections among many related models.

GMMs are flexible in that they include several important features that allow us to map to our conceptual model, which

[13]GMM is an advanced statistical technique that, to our knowledge, has not previously been used in information systems (IS) research and, therefore, the statistical model in Appendix C may look unfamiliar to some readers. On this point, it is important to differentiate between our conceptual model (Figure 1) and this statistical model. This statistical model is akin to the complete model that is tested in covariance-based structural equation modeling (SEM), where there are error terms included, with possible correlations between variables, model constraints, etc.

[14]This interpretation of a mixture model is sometimes called the "direct" interpretation, in that mixtures are regarded as latent classes that exist, whereas another interpretation of mixture models is called "indirect," where the component distributions are used to model an unknown distributional form from multiple other distributions (see Sterba 2013). The former interpretation is consistent with our theoretical arguments of unobservable groups, whereas the latter is a way of parsing data to arrive at an approximation of a particular distribution.

Table 3. Study Variables and Their Definitions

Variable	Description	References in the Literature
Size of health system (*SystemSize*)	Number of hospitals in the focal hospital's health system	Angst et al. (2012); Bazzoli et al. (2000)
Hospital size (*HospitalSize*)	Number of beds that are staffed in the hospital (natural log)	Angst et al. (2010); Angst et al. (2012); Kwon and Johnson (2014); Queenan et al. (2011); Westphal et al. (1997)
Hospital age (*Age*)	Age of hospital in years (natural log)	Angst et al. (2010); Angst et al. (2012); Kwon and Johnson (2014); Queenan et al. (2011); Westphal et al. (1997)
For profit (*BusinessModel*)	Dummy variable to differentiate between for-profit and not-for-profit hospital; Value = 1 for-profit; 0 for not-for-profit	Angst et al. (2010); Angst et al. (2012); Kwon and Johnson (2014); Anthony et al. (2014)
Teaching (*Teaching*)	Dummy variable to differentiate between teaching (academic) and non-teaching hospital; Value = 1 for teaching hospital; 0 for a non-teaching hospital	Angst et al. (2010); Angst et al. (2012); Kwon and Johnson (2014); Queenan et al. (2011)
Faith based (*Mission*)	Dummy variable to indicate whether the hospital's description includes faith orientation; Value = 1 faith based; 0 for not faith based	Hagland (2009); Dranove et al. (2014)
Entrepreneurial mindset (*EntrepMindset*)	The extent to which the hospital adopts innovative technologies, as assessed by the Saidin index	Queenan et al. (2011); Spetz and Maiuro (2004)
IT security investment (*ITSec*)	Number of IT security technologies adopted by the hospital in the given year (range from 1 to 10)	Anthony et al. (2014); Kwon and Johnson (2014)
Breach (*Breach*)	Dummy variable to indicate whether the hospital had a breach in the given year; Value = 1 breach; 0 for no breach	Kwon and Johnson (2013; 2014); Sen and Borle (2015)

we now describe. First, we use the logit link function, that is, a logistic regression model, because the outcome variable *Breach* is binary each year. As in traditional logistic regression, the logit (i.e., log odds) can be converted into the probability scale with the following transformation: probability = exp(logit)/(1 + exp(logit)), where exp(.) is the antilogarithm function. Second, the values of the change coefficients (i.e., the intercepts and slopes) are specific to each class, thus making up the mixture portion of the model (which allows for different trajectories of change for each latent class, and for *ITSec* to have differential impact across classes). Third, we did not specify prior probabilities of group membership but rather allowed the latent class probabilities to be estimated from the breach data. Fourth, as we later elaborate, we use a recently developed auxiliary variable three-step approach that (1) first fits the GMM and (2) then models the latent class as a logistic regression model based on our predictors (H1a through H1g) of class membership (Asparouhov and Muthén 2014). Fifth, similar to Nagin, our GMM assumes that each class follows the same growth model (i.e., there is no within-class variability on the intercepts or slopes). Taken together, this is a rich model for understanding heterogeneous change as well as predictors of class membership.

Specifics of Model Implementation

We utilize full information maximum likelihood in Mplus (Muthén and Muthén 2015) to fit the specific GMM discussed in the previous section. Appendix D provides additional details about the analysis and the Mplus syntax used to fit the structural and measurement part of the GMM. Note that we scaled time such that time 0 represents 2005, so that the intercept term is the estimated logit in the first year. Thus, the timescale can be interpreted as "years since 2005" (i.e., the outset of our study period), which is a common way to parameterize change models.

An important point is that our model for the latent class does not affect the latent change (growth) model parameters that are implemented first, as is typical with traditional GMMs that simultaneously estimate all parameters (i.e., "single step" approaches). Our model is a GMM that has an additional model in a second stage that is used to assess the estimated class membership (symbolic or substantive) by the covariates of interest (i.e., *SystemSize*, *HospitalSize*, *Age*, *Business Model*, *Teaching*, *Mission*, *EntrepMindset*). This auxiliary variable three-step approach was recently developed and has

been implemented in Mplus. It differs from a typical GMM in that the covariates of interest are used to model class membership *after* the GMM itself has been implemented (Asparouhov and Muthén 2014; Muthén and Muthén 2015; Vermunt 2010).[15, 16]

While a relatively small number of hospitals in our study experienced a data breach (just over 2% over the nine-year time period), the empirical method we use considers all hospitals at all time points (i.e., 5,882 total hospitals in the final year, see Table 1), even those with missing breach data (i.e., full data for the *Breach* variable is not necessary, under the standard assumption of missing at random; Curran et al. 2010). Most analytical methods, including regression, require that censored data be eliminated or that these cases be assigned the event time associated with the end of the data collection, both of which bias the results (Frank and Keith 1984; Tuma and Hannan 1984). Although our data is left-censored in that the hospitals existed and were engaging in IT security practices prior to 2005, the first year of our sample coincides with the first year that breaches were listed at www.privacyrights.org and thus became a public issue for hospitals. Hence, our data and the timeframe in which it is collected are relevant and appropriate.

Results

We begin our discussion of results by addressing the adequacy of our two-class model for latent classification. The literature on the "best" or "most appropriate" number of classes to extract in GMMs is unclear and often nuanced to a particular type of model, and recommendations typically let theory be the guide (e.g., Tofighi and Enders 2008). Hence, theory guided our selection of two classes, but as a robustness check, we also conducted model comparisons with both one- and three-class solutions. We report these results in Appendix E; in short, based on the evidence, the two-class solution fits better than the alternatives.[17] Additional considerations for the adequacy of latent classifications are entropy (range of 0–1.0, where 1.0 indicates perfect classification) and posterior probabilities (mean probability for belonging to a particular class, near 1.0 is ideal although not typical because distributions will tend to have some nontrivial overlap) (Jung and Wickrama 2008).[18] Our model showed satisfactory results based on these criteria, with a relatively high entropy score (.87) and high average posterior probabilities (.80 for symbolic and .98 for substantive).[19]

Turning to our hypothesized relationships, the coefficients in Table 4 represent the relationship between each firm-specific institutional factor and *symbolic* adoption (H1a through H1g). For ease of interpretation, consider the symbolic class to be coded as 1 and the substantive to be 0; hence, a positive (negative) coefficient for the covariates predicting class is the increase (decrease) in the log odds of being in the symbolic versus the substantive class for each unit increase in the covariates. The results show that, with the exception of *Teaching*, each institutional factor is significantly related to symbolic adoption, as hypothesized. *Teaching* is significant but opposite to its predicted direction, suggesting that teaching hospitals are more likely to be substantive adopters. Note that although we have conceptualized symbolic adopters as being fundamentally different than substantive adopters (i.e., the opposite), the reality is more nuanced (e.g., Kim and Lyon 2013), and our model explicitly accounts for this in terms

[15]Vermunt (2010) notes the disadvantages of a single-step (i.e., simultaneous) approach, where "each time a covariate is added or removed not only the prediction model but also the measurement model needs to be re-estimated" (p. 451). In our case the measurement model is the change model of breaches across time (i.e., the intercept and slope of the logit). Further, Vermunt argues that a simultaneous estimation approach is at odds with the "logic of most applied researchers, who view introduction of covariates as a step that comes after the classification model has been built" (p. 451). This logic is exactly why we use the newly implemented three-step approach, because we are interested in first the growth model by class and then understanding what factors predict the classes (i.e., symbolic and substantive adoption).

[16]There is an additional point regarding our model that warrants elaboration. In estimating the probability of class membership for each hospital (based on the hospital's breach data), the estimated change parameters are weighted according to the estimated probability of membership into each class. In that sense, classification is probabilistic (i.e., "fuzzy"), meaning that estimates from each unit of analysis (i.e., hospital) influence the estimates within each class. This approach is in contrast to a "crisp" classification approach, in which the units influence only the class in which they were most likely to belong. In general, a crisp classification approach has the disadvantage of weighting each of the unknown classifications the same, when in reality it is likely that some units are very likely in one class, and not the other, but others are more ambiguous (Kelley 2008).

[17]An anonymous reviewer requested this robustness check, thus it was not part of an exploratory process to empirically discover the optimal number. Our two-class solution was theory driven.

[18]Entropy is a measure of class separation, which is akin to the concept of discriminant validity in factor analysis. Posterior probability is used to measure the precision of class assignments based on the probability that (in our case) each hospital belongs to that particular class (Muthén 2004). The results for our model compare favorably with those reported in the literature on GMM (e.g., Asparouhov and Muthén 2014; Muthén 2004).

[19]In order to test our hypotheses, we ran two models. Both were two-class models for the latent classification portion but in one model the influence of *ITSec* was held constant across classes (to test H2) while in the second model *ITSec* was allowed to vary across classes (to test H3a and H3b; shown in Table 5). For both model runs, the fit indices were the same as those reported above, except that entropy was .85 in the second model.

Table 4. Coefficients for Predictors (Covariates) of Symbolic Latent Class

Predictor	Coefficient (β) Log Odds	Standard Error	*p*-value*
SystemSize	-0.02	0.01	0.03
HospitalSize	-0.48	0.17	0.01
Age	0.54	0.14	0.00
BusinessModel	4.42	1.31	0.00
Teaching	-1.88	0.38	0.00
Mission	0.68	0.35	0.05
EntrepMindset	-0.07	0.03	0.03

Notes: N = 5,882; *$p < 0.05$, two-tailed tests; the coefficients for the predictors represent their relationship to *symbolic* adoption. Only the sign of the coefficients would change in the prediction of *substantive* adoption.

of the probability of a hospital being in each of the two classes (where the two probabilities sum to 1). From these probabilities, the model we use weights the parameter estimates by the estimated probability that each hospital belongs in one of the two latent classes. This information can be found in aggregate form in the aforementioned average posterior probabilities, which indicate the mean assignment probability for each class. Hence, our results in Table 4 account for the uncertainty in the estimated classes with regard to how the parameter estimates are weighted.

The next point of discussion for our analysis focuses on the impact of *ITSec* on the change parameters for likelihood of breach. These results are shown in Table 5.

The results were counter to our baseline hypothesis (H2) regarding the benefit of *ITSec* on the change coefficients when *ITSec* was held constant across classes. Referring to Panel 1 in the top portion of Table 5, the coefficients indicate that for the relationship between *ITSec* and *Breach*, the intercept and slope are statistically significant (albeit marginally in the case of the slope), but in a positive direction (Intercept .34, $p < .01$; Slope .02, $p \leq .10$). What this suggests is that across both symbolic and substantive adopters, at the onset of our measurement period (time 0 in the year 2005), the likelihood of a breach is higher in hospitals with higher levels of mean *ITSec* and the likelihood of breach *increases* over time with higher mean *ITSec*, thus rejecting H2. However, this finding should be considered in the broader context of substantive and symbolic adoption, as we now discuss.

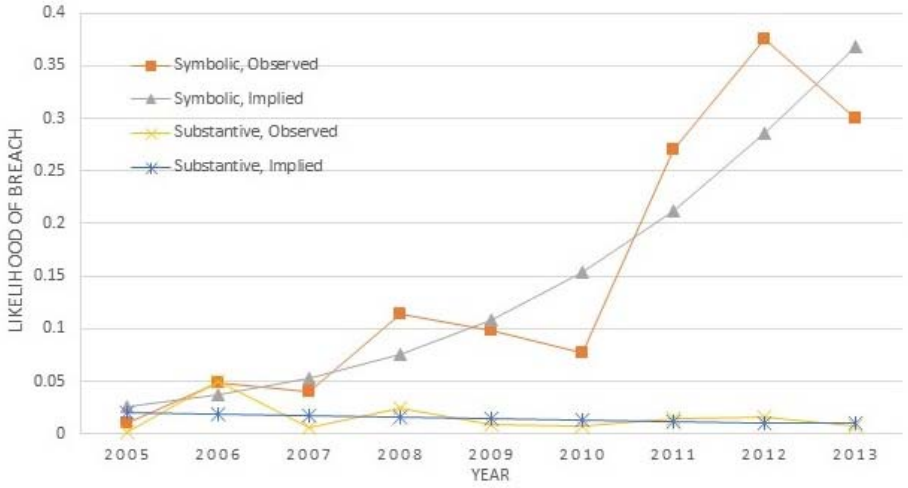
Next, we focus on the change in likelihood of breach over time for the two classes, with *ITSec* allowed to vary across the two classes—that is, the model of the moderating influence of class on the relationship between *ITSec* and *Breach*. In particular, the results in the middle and lower portions of Table 5 (see Panels 2 and 3 for substantive and symbolic, respectively) show that *ITSec* is predictive of the intercept of *Breach* in the substantive class but not the symbolic class, and that the likelihood of breach in 2005 starts out statistically significantly *higher* for the substantive class (.38, $p < .01$; -.12, $p = .52$, for substantive and symbolic, respectively). Regarding the slopes that model the likelihood of breach over time, we see that in the symbolic class (Panel 3), the relationship between *ITSec* and *Breach* is positive and significant (.06, $p \leq .05$), indicating that over time the likelihood of breach increases. For substantive adopters (Panel 2), the likelihood of breach is positive, but not statistically significant (.02, $p = .15$). This does not provide definitive support for H3a in that the likelihood of breach is not decreasing as we hypothesized; however, when considered in the broader context in relation to symbolic adoption, the benefits become more apparent. To that end, the combination of the intercept and slope results for the symbolic class support H3b in that *ITSec* is associated with greater likelihood of breach over time. To better understand these relationships, we graphed the results (see Figure 2). The graph shows that, over time, the combination of *ITSec* and symbolic adoption increases breach likelihood (note the drastically increasing trajectory) whereas for substantive adoption the likelihood of breach is relatively flat, particularly after 2006.

In H4, we argued that it takes time for the benefits of a substantive adoption strategy to be realized, and we termed this the *IT Value Point*. The results in Figure 2 show that beginning in 2006, the likelihood of breach becomes greater in the symbolic class and this trend continues throughout the remainder of the study period. Conversely, the likelihood of breach in the substantive class increases from 2005 to 2006, and then generally flattens out. This suggests that the substantive class realizes improved performance post 2006, in terms of preventing additional breaches, and thereby H4 is supported. To confirm this statistically, we tested for significant differences between the model-implied (i.e., predicted

Table 5. Coefficients of the Growth Mixture Model (GMM)

	Effect on *Intercept* of Breach			Effect on *Slope* of Breach		
Panel 1: Influence of ITSec Across Both Classes (H2)						
	Coefficient	**Standard Error**	***p*-value**	**Coefficient**	**Standard Error**	***p*-value**
ITSec	0.34	0.05	0.00**	0.02	0.01	0.10†
Panel 2: *Substantive* Class (H3a)						
	Effect on *Intercept* of Breach			**Effect on *Slope* of Breach**		
	Coefficient	**Standard Error**	***p*-value**	**Coefficient**	**Standard Error**	***p*-value**
ITSec	.38	0.05	0.00**	0.02	0.01	0.15
Panel 3: *Symbolic* Class (H3b)						
	Effect on *Intercept* of Breach			**Effect on *Slope* of Breach**		
	Coefficient	**Standard Error**	***p*-value**	**Coefficient**	**Standard Error**	***p*-value**
ITSec	-.12	0.19	0.52	0.06	0.03	0.05*

Notes: N = 5,882; **$p < 0.01$, *$p \leq 0.05$, †$p \leq 0.10$, two-tailed tests.



Note: We show the likelihood of breach per year for the two estimated latent classes, while providing the model implied values. The model implied values are the values that the model predicted, here for the probability of *Breach* each year within each latent class based on the maximum likelihood parameter estimates. For context, the model implied value in a simple regression is the predicted value (often denoted $\hat{y}$) of the dependent variable for a given value of an independent variable based on the estimated coefficients. The drastically different class trajectories illustrate the value of using a GMM framework, in that (1) there is change over time, and (2) the parameters of change differ across the latent classes, which in our case represent symbolic and substantive adoption. Note that hospitals cannot switch classes based on our model.

Figure 2. Graph of Likelihood of Breach by Latent Class

Table 6. Differences in Coefficients for ITSec by Latent Class

Year	Δ Coefficient	Standard Error	*p*-value
2005	.003	.006	0.60
2006	.015	.008	0.04*
2007	.033	.009	0.00*
2008	.057	.012	0.00*
2009	.092	.015	0.00*
2010	.139	.020	0.00*
2011	.202	.028	0.00*
2012	.283	.040	0.00*
2013	.378	.054	0.00*

Notes: Δ Coefficient is the difference in the model implied values for the symbolic versus substantive class in each year (the model implied values are the values that the model predicted with *ITSec* as a predictor of *Breach*); *$p < 0.05$.

Table 7. Summary of Results

Hypothesis	Result
H1a: Hospitals that are members of smaller health systems are more likely to be symbolic adopters.	Supported
H1b: Older hospitals are more likely to be symbolic adopters.	Supported
H1c: Smaller hospitals are more likely to be symbolic adopters.	Supported
H1d: For-profit hospitals are more likely to be symbolic adopters.	Supported
H1e: Teaching hospitals are more likely to be symbolic adopters.	Not Supported (opposite)
H1f: Faith-based hospitals are more likely to be symbolic adopters.	Supported
H1g: Less entrepreneurial hospitals are more likely to be symbolic adopters.	Supported
H2: Greater IT security investment will have a negative effect on the likelihood of security breaches.	Not Supported (opposite)
H3a: Over time, the benefit of *substantive* adoption on the relationship between IT security investment and breaches will increase.	Not Supported
H3b: Over time, the negative consequences of *symbolic* adoption on the relationship between IT security investment and breaches will increase.	Supported
H4: The benefits of substantive adoption will take time to be realized.	Supported

values based on our model) probability of *Breach* values for symbolic and substantive adopters at the mean of *ITSec* for each year, yielding the results shown in Table 6. Table 7 provides a full summary of our hypotheses tests.

Interpretation of Results and Discussion

We used a GMM to model heterogeneity in hospitals' likelihood of data breach over time and found empirical evidence to support two distinct classes of hospitals based on drastically different class trajectories. We argued for and found evidence to support the distinction of classes into symbolic and substantive adopters of IT practices. Somewhat surprisingly, one of our findings falls counter to our hypothesizing, in that we theorized that teaching hospitals would be symbolic, not substantive adopters. The opposite was true, and we attribute this discrepancy to not completely understanding the motives of hospitals that fall into this category. We expected that teaching hospitals would prioritize training and research far more than IT practices. In hindsight, it seems logical that the need to conduct research and train clinicians requires that teaching hospitals have more comprehensive systems and practices, especially as it relates to IT. Without the substantive adoption of these practices, the educators and researchers cannot perform their duties as effectively. From

a practical standpoint, because teaching hospitals are more likely in the substantive class, they should experience fewer breaches over time as compared to their symbolic counterparts.

On the whole, we can state that institutional factors are predictive of the symbolic and substantive classification of IT practices. Our theorizing and empirical results on this matter are a departure from prior institutional research which infers symbolic or substantive adoption based on either the timing of an adoption or its outcome (e.g., Delmas and Montes Sancho 2010; Rodrigue et al. 2013; Tolbert and Zucker 1983). We likewise infer symbolic or substantive adoption but we do so with arguably a more comprehensive approach that first distinguishes these adoption strategies empirically, and then validates this distinction based on a set of predictive factors that are rooted in hospitals' institutional environment. Notably, the theoretical logic that underlies these predictors is typically not hospital-specific and the predictors themselves would seem generalizable to the broader study of symbolic and substantive practices within firms. We leave these possible extensions of our work to future research.

We also set out to investigate whether symbolic or substantive adoption influences the relationship between IT security investment and the likelihood of breaches over time. This inquiry was motivated in part by the frequency with which firms (and hospitals in particular) have experienced data breaches even as institutional pressures have yielded increased IT security expenditures. We theorized and found evidence to suggest that at least some explanation for this disconcerting situation is the manner in which hospitals integrate security into their IT-related processes and routines. In particular, hospitals that were classified as symbolic adopters showed weaker security performance (as compared to substantive adopters) in terms of the effectiveness of their IT security investments in reducing the likelihood of breaches. Hence, a lack of cohesion and deep integration of security into IT practices appears to make hospitals susceptible to ever growing and changing security threats. Our results indicate a "cost" for symbolic adoption in that IT security investment is associated with an increased likelihood of breach that worsens over time. This is a powerful finding because prior institutional research has focused primarily on the benefits of symbolic adoption, from a legitimacy perspective, and if a cost was considered, it was mainly in terms of a lack of meaningful performance gain (i.e., status quo) (Boxenbaum and Jonsson 2008; Bromley and Powell 2012). It appears that in the IT security context, and specifically as it relates to thwarting data breaches, the cost of symbolic adoption is far greater than maintaining the status quo. The takeaway for practitioners is that while symbolic adoption of IT practices may engender legitimacy from certain stakeholders (e.g., the media, regulators), there are longer term consequences that can weaken IT security.

In contrast to symbolic adopters, while hospitals that were classified as substantive adopters did not show improvements in the effectiveness of their IT security investments, there was not a statistically significant increase in the likelihood of breaches over time (i.e., the trajectory (slope) showed that the likelihood of breach flat-lines over time). Hence, our results do not suggest a performance gain for substantive adopters, but when considered in conjunction with the cost that symbolic adopters incur, the real benefit of substantive adoption may be that it enables a fairly steady level of performance from IT security investments. Practically speaking, the value of substantive adoption appears to be more of loss prevention than performance gains. However, the data for the combined classes does suggest that there is an increasing trend of likelihood of breach over time, so we do not want to discount the fact that while substantive adoption does not show a significant decrease (as we hypothesized), it also does not statistically increase, even in the presence of this increasing overall trend.

Consistent with our notion of an IT value point, we also found evidence that the benefits of substantive adoption are not immediate. Specifically, our results suggest that it takes at least one year from when substantive adopters are exposed to their IT security technologies before the likelihood of breach begins to flatten out; before then, IT security investment appears to increase the likelihood of breach. These findings are consistent with prior health IT literature that found lagged effects for extracting value from IT implementations (e.g., Bhargava and Mishra 2014; Devaraj and Kohli 2003). IT implementations are known to be disruptive to organizational processes (Adner 2002) and it is plausible that internal personnel struggle in early time periods adapting to the system needs, resulting in accidental breaches and temporary openings for those with malicious intent. From a practical perspective, organizations need to realize that the value proposition for deep integration of IT security into core processes and routines is not short-term; a short-term focus might therefore suggest a symbolic adoption strategy, which, as our results suggest, can be detrimental to long-term security performance.

We also hypothesized that IT security investment would have a negative effect on the likelihood of breach irrespective of whether a symbolic or substantive class was considered. This prediction is based on the straightforward rationale that more IT security resources lead to fewer breaches and certain empirical studies that support this relationship. Counter to our hypothesis, we found that IT security investment was associated with a slightly increasing pattern of breaches over time,

after taken into account the increasing breach trend. Beyond the moderating influence of symbolic or substantive adoption, we have several thoughts on the findings for our baseline hypothesis. One thing we wanted to rule out was a reverse-causality problem in which breaches are causing additional IT security investments. We conducted several lead and lagged dependent variable tests, varying the relationships across years, (i.e., 2005 *ITSec* predicting 2006 breaches, 2005 *ITSec* predicting 2007 breaches, 2006 breaches predicting 2007 *ITSec*, etc.), and surprisingly, our results remained largely unchanged, with the temporal prediction mattering little to the relationships. Kwon and Johnson (2014) suggest that the differential effect of IT security investment may be a function of proactive and reactive investment and they create an elegant model to test this. While our model differed on several characteristics from theirs, our lagged model suggests that proactively adopting IT security investments only benefits substantive adopters. With symbolic adopters, benefits of proactive IT security investments are not realized, and the effect worsens over time.

Proceeding on the assumption that increasing levels of IT security investment are associated with greater probabilities of breaches, we believe one explanation relates to reputation-seeking activities and the negative implications that can result from these actions (Pfarrer et al. 2010). When hospitals adopt innovative IT security solutions, not only are they likely to seek attention, but vendors of these systems are also likely to release information to the press. To the extent that hospitals highlight the fact that they have adopted state-of-the-art IT security, hackers may target these firms to boast about their accomplishments (Kolbasuk McGee 2014). We also surmise that the adoption of more IT security technologies may signal that a hospital has more information assets to protect, again drawing the attention of hackers. All of this suggests that adopting more IT security, as long as it becomes known to the public, may in fact draw unwanted attention and more attacks. Although this topic is beyond the scope of the current study, we believe it is an important area for future research.

It is also important to note that our findings do not suggest the irrelevance of IT security investments. Indeed, basic security technologies, which make up only a small portion of our *ITSec* measure, are part and parcel to any organizational IT security management program and necessary for a firm's survival. An Internet firewall, for example, is needed to repel the constant deluge of illegitimate connection-opening attempts, presumably from hackers, that are precursors to more sophisticated attacks. Moreover, legislation requires organizations in almost every industry to have a baseline level of IT security that includes technical controls. That being said, our results suggest that hospitals need to rethink their approach to IT security because they appear to be falling behind the "bad guys." A strategy in which security is tightly woven into IT practices appears necessary to at least halt the trend of escalating breaches.

Taken together, our findings have significant implications for the study of IT security. By and large, extant literature focuses specifically on the IT posture of the firm or the characteristics of individuals within firms in order to explain why some firms are more susceptible to security breaches than others. Our research indicates that beyond these direct effects, the context in which organizations operate and the structure of firms plays an important role in the way these practices are deployed. In particular, our findings delineate institutional conditions under which hospitals' IT security investments lead to improved performance, and we believe that these findings are applicable beyond the healthcare context. Scholars and practitioners are urged to look beyond the direct features of IT security and consider the organization more broadly and how its core features and environmental interface may influence how practices are deployed with differential effectiveness. Clearly, mandated IT security practices appear insufficient to deter and prevent many data security breaches. A takeaway from this is that organizations are much less likely to experience breaches when they are more responsive to their organizational characteristics and embedded in environments that place inherent value on substantive adoption. Therefore, policymakers need to branch out beyond investments in IT security and consider institutional factors when developing directives for securing personally identifiable information and other forms of sensitive data.

Because of the nature and scope of our data, we were able to identify wide variation in the hospitals' embeddedness in institutions and test their effects. Our study implicitly assumes there will be heterogeneous learning processes taking place with respect to IT security investments, and that the institutional environment has a further influence. This extends prior research that highlights the importance of *how* organizations learn, but which did not account for the role of institutions (Edmondson et al. 2001). This finding is important for practitioners as well because the nature of adoption may be able to be predicted by embeddedness in institutions and this may allow particularly proactive hospitals to combat their baseline tendencies. For example, knowing that there are specific characteristics of older hospitals that make symbolic adoption more likely suggests that those traits could be identified and possibly altered. Benchmarking against young, larger, teaching, or NFP hospitals might help them understand their shortcomings.

From a theoretical perspective, our findings suggest that theories of adoption need to consider not only whether the act

of adoption occurs, but also the nature or type of adoption that is occurring as well the length of time the adopted practices have been in place. Researchers have long theorized that organizations will seek ways to minimize the disruption of adopted practices to their core activities by symbolically adopting while decoupling those practices from their core (Bromley and Powell 2012). The implication is that the mere adoption of a practice may not differentiate those organizations that truly derive benefits from those adopted practices from those that are unlikely to see any positive impact.

A second theoretical contribution resides at the intersection of IS and institutional theory. The majority of institutional studies in the IS domain consider adoption to be the outcome of interest (Mignerat and Rivard 2009), whereas our study focuses on the interplay between IT and institutions and how this affects breakdowns in organizational practices. Our work is not focused on an outward act (adoption) but instead it considers the negative result (a data security breach) of institutions, while acknowledging that the right combination of characteristics can greatly minimize risk. We believe institutional theory provides an insightful lens through which to explore this phenomenon.

Limitations

This study has certain limitations that should be taken into account, and which provide a basis for future research. First, our measure of IT security investment is one of adoption, and although this is a common approach (e.g., Brynjolfsson and Hitt 2000), we acknowledge it to be a coarse assessment. In particular, we measure IT security investment by the number of security technologies in place, and weight them equally. Further, similar to other firm-level health IT studies, we are limited to using publicly available data in the HIMSS database. Yet our measure is broader and more inclusive than in prior work (Kwon and Johnson 2014), and our panel dataset extends across a longer time period. We provide justification for the selection of these variables, but we acknowledge that different measures of IT security may produce different results. It is also possible that our hospital level data may not be granular enough in that it does not specify if the IT is deployed across the hospital or only in certain departments.

Second, our context is specific to the U.S. healthcare industry, which inherently suggests that the institutional factors and their effects may not be relevant in other industries or countries. In particular, a single-payer context in economically advanced or economically disadvantaged countries may have drastically different institutional factors. It would also be interesting to investigate whether our results hold in other highly regulated industries, such as the financial sector, where there are similar institutional pressures to adopt IT security controls.

Finally, similar to recent IT security research (Kwon and Johnson 2014; Sen and Borle 2015), we relied on reported breaches and thus we cannot determine the extent to which hospitals were targeted yet able to thwart attacks. By some estimates, only 1 in 10 breaches is discovered (HIPAABreach 2014), but we did not feel any empirical method could appropriately address this problem. Hence, we are limited to our secondary data sources. Related to this point is the low number of reported breaches in 2005, relative to the other years in our study. We ran our models with and without the 2005 data and the results did not change in any meaningful way.

Conclusion

In conclusion, organizational scholars have long made the distinction between different classifications of adoption and have argued that organizations can gain legitimacy by adopting mandated practices but avoid the costs of implementation by decoupling those practices from core activities (e.g., Thompson 2003). Although this approach might be effective in garnering social praise in some contexts, such as equal opportunity hiring practices (Tolbert and Zucker 1983) or university recycling programs (Lounsbury 2001), our research suggests that when the consequences are more tangible, such as the case of data security breaches, symbolic and decoupled adoption may not be sufficient. Our findings also lend credence to the recent HITECH Act which calls for "meaningful use," specifying both the type of system to be used and also mandating the percentage of time it needs to be used to qualify for incentives.

The investigation of determinants of data security breaches is an important phenomenon not simply because of the immediate or short-term effects of loss, but more importantly because of the long-lasting effects on society. If people begin to doubt the security of IT infrastructures and the ability of organizations to ensure that personal information will not be breached, it could cripple our financial markets, healthcare system, global food and goods distribution, and virtually every industry that operates in developed markets. While others have led the way in research investigating firm-level determinants of IT security (e.g., Cavusoglu et al. 2005), ours is one of the few to identify firm-level institutional factors that contribute to IT security performance. We believe this is a step toward identifying the key factors that must be considered to secure personal data in the healthcare context and beyond.

References

Adner, R. 2002. "When Are Technologies Disruptive? A Demand-Based View of the Emergence of Competition," *Strategic Management Journal* (23:8), pp. 667-688.

Angst, C. M., Agarwal, R., Sambamurthy, V., and Kelley, K. 2010. "Social Contagion and Information Technology Diffusion: The Adoption of Electronic Medical Records in U.S. Hospitals," *Management Science* (56:8), pp. 1219-1241.

Angst, C. M., Devaraj, S., and D'Arcy, J. 2012. "Dual Role of IT-Assisted Communication in Patient Care: A Validated Structure-Process-Outcome Framework," *Journal of Management Information Systems* (29:2), pp. 255-291.

Anthony, D. L., Appari, A., and Johnson, M. E. 2014. "Institutionalizing HIPAA Compliance Organizations and Competing Logics in US Health Care," *Journal of Health and Social Behavior* (55:1), pp. 108-124.

Appari, A., and Johnson, M. E. 2010. "Information Security and Privacy in Healthcare: Current State of Research," *International Journal of Internet and Enterprise Management* (6:4), pp. 279-314.

Argote, L., and Miron-Spektor, E. 2011. "Organizational Learning: From Experience to Knowledge," *Organization Science* (22:5), pp. 1123-1137.

Asparouhov, T., and Muthén, B. O. 2014. "Auxiliary Variables in Mixture Modeling: Three-Step Approaches Using Mplus," *Structural Equation Modeling* (21:3), pp. 329-341.

AT&T. 2015. "What Every CEO Needs to Know About Cybersecurity" (available at http://www.business.att.com/content/src/csi/decodingtheadversary.pdf).

Bansal, P., and Roth, K. 2000. "Why Companies Go Green: A Model of Ecological Responsiveness," *Academy of Management Journal* (43:4), pp. 717-736.

Barney, J. B. 1991. "Firm Resources and Sustained Competitive Advantage," *Journal of Management* (17:1), pp. 99-121.

Bazzoli, G. J., Chan, B., Shortell, S. M., and D'Aunno, T. 2000. "The Financial Performance of Hospitals Belonging to Health Networks and Systems," *Inquiry* (37:3), pp. 234-252.

Berrone, P., Gelabert, L., and Fosfuri, A. 2009. "The Impact of Symbolic and Substantive Actions on Environmental Legitimacy," IESE Business School, Working Paper Series, WP-778, University of Navarra (available at http://www.iese.edu/research/pdfs/di-0778-e.pdf).

Besharov, M. L., and Smith, W. K. 2014. "Multiple Institutional Logics in Organizations: Explaining Their Varied Nature and Implications," *Academy of Management Review* (39:3), pp. 364-381.

Bhargava, H. K., and Mishra, A. N. 2014. "Electronic Medical Records and Physician Productivity: Evidence from Panel Data Analysis," *Management Science* (60:10), pp. 2543-2562.

Blevins, K. R., Kuhns, J. B., and Lee, S. 2012. "Understanding Decisions to Burglarize From the Offender's Perspective," The University of North Carolina at Charlotte, Department of Criminal Justice & Criminology (available at http://airef.org/research/BurglarSurveyStudyFinalReport.pdf).

Boxenbaum, E., and Jonsson, S. 2008. "Isomorphism, Diffusion, and Decoupling," in *The Sage Handbook of Organizational Institutionalism,* R. Greenwood, C. Oliver, K. Sahlin and R. Suddaby (eds.), London: Sage, pp. 299-323.

Brickson, S. L. 2005. "Organizational Identity Orientation: Forging a Link Between Organizational Identity and Organizations' Relations with Stakeholders," *Administrative Science Quarterly* (50:4), pp. 576-609.

Brickson, S. L. 2007. "Organizational Identity Orientation: The Genesis of the Role of the Firm and Distinct Forms of Social Value," *Academy of Management Review* (32:3), pp. 864-888.

Bromley, P., and Powell, W. W. 2012. "From Smoke and Mirrors to Walking the Talk: Decoupling in the Contemporary World," *Academy of Management Annals* (6:1), pp. 482-530.

Brynjolfsson, E., and Hitt, L. M. 2000. "Beyond Computation: Information Technology, Organizational Transformation and Business Performance," *The Journal of Economic Perspectives* (14:4), pp. 23-48.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523-548.

Burd, S. A., Cherkin, S. S., and Concannon, J. 2005. "Information Security in Academic Institutions: Emerging Issues and Remediation Strategies," *Journal of Security Education* (1:2-3), pp. 55-68.

Burgess, Jr., J. F., and Wilson, P. W. 1996. "Hospital Ownership and Technical Inefficiency," *Management Science* (42:1), pp. 110-123.

Campbell, J. L. 2007. "Why Would Corporations Behave in Socially Responsible Ways? An Institutional Theory of Corporate Social Responsibility," *Academy of Management Review* (32:3), pp. 946-967.

Caronna, C. A. 2004. "The Misalignment of Institutional 'Pillars': Consequences for the U.S. Health Care Field," *Journal of Health and Social Behavior* (45:Extra Issue), pp. 45-58.

Cavusoglu, H., Mishra, B., and Raghunatham, S. 2005. "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research* (16:1), pp. 28-46.

Christmann, P., and Taylor, G. 2006. "Firm Self-Regulation Through International Certifiable Standards: Determinants of Symbolic Versus Substantive Implementation," *Journal of International Business Studies* (37:6), pp. 863-878.

Curran, P. J., Obeidat, K., and Losardo, D. 2010. "Twelve Frequently Asked Questions About Growth Curve Modeling," *Journal of Cognition and Development* (11:2), pp. 121-136.

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643-658.

D'Arcy, J., Hovav, A., and Galletta, D. F. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Delmas, M. A., and Montes Sancho, M. J. 2010. "Voluntary Agreements to Improve Environmental Quality: Symbolic and Substantive Cooperation," *Strategic Management Journal* (31:6), pp. 575-601.

Devaraj, S., and Kohli, R. 2003. "Performance Impacts of Information Technology: Is Actual Usage the Missing Link?," *Management Science* (49:3), pp. 273-299.

DiMaggio, P., and Powell, W. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational fields," *American Sociological Review* (48:2), pp. 147-160.

Dos Santos, B. L., and Peffers, K. 1995. "Rewards to Investors in Innovative Information Technology Applications: First Movers and Early Followers in ATMs," *Organization Science* (6:3), pp. 241-259.

Dranove, D., Forman, C., Goldfarb, A., and Greenstein, S. 2014. "The Trillion Dollar Conundrum: Complementarities and Health Information Technology," *American Economic Journal: Economic Policy* (6:4), pp. 239-270.

Duliba, K. A., Kauffman, R. J., and Lucas, H. C. 2001. "Appropriating Value from Computerized Reservation Systems Ownership in the Airline Industry," *Organization Science* (12:6), pp. 702-728.

Edmondson, A. C., Bohmer, R. M., and Pisano, G. P. 2001. "Disrupted Routines: Team Learning and New Technology Implementation in Hospitals," *Administrative Science Quarterly* (46:4), pp. 685-716.

Experian. 2015. "Second Annual Data Breach Industry Forecast" (available at https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf).

Fombrun, C., and Shanley, M. 1990. "What's in a Name? Reputation Building and Corporate Strategy," *Academy of Management Journal* (33:2), pp. 233-258.

Frank, A. R., and Keith, T. Z. 1984. "Academic Abilities of Person Entering and Remaining in Special Education," *Exceptional Children* (51:1), pp. 76-77.

Freedman, L. F. 2009. "The Health Information Technology for Economic and Clinical Health Act (HITECH Act): Implications for the Adoption of Health Information Technology, HIPAA, and Privacy and Security Issues," Nixon Peabody LLP, (available at https://www.nixonpeabody.com/en/ideas/articles/2009/02/23/the-health-information-technology-for-economic-and-clinical-health-act-hitech-act-impli).

Gartner. 2015. "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 percent to Reach $75.4 Billion in 2015," Gartner, Inc., Stamford, CT (available at http://www.gartner.com/newsroom/id/3135617).

Gemalto. 2015. "2015 First Half Review: Findings from the Breach Level Index," Gemalto NV, (available at http://www.gemalto.com/brochures-site/download-site/Documents/Gemalto_H1_2015_BLI_Report.pdf).

Goldstein, S. M., and Naor, M. 2005. "Linking Publicness to Operations Management Practices: A Study of Quality Management Practices in Hospitals," *Journal of Operations Management* (23:2), pp. 209-228.

Greenwood, R., Raynard, M., Kodeih, F., Micelotta, E. R., and Lounsbury, M. 2011. "Institutional Complexity and Organizational Responses," *The Academy of Management Annals* (5:1), pp. 317-371.

Hagland, M. 2009. "Faith-Based Health Systems Point the Way: Mission-Driven Quality of Care Combined with Cost-Effectiveness Offer New Model for Hard Economic Times," *Health Progress* (91:1), pp. 16-20.

Herath, T., and Rao, H. G. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

HIMSS. 2014. "6th Annual HIMSS Security Survey, sponsored by Experian® Data Breach Resolution," Healthcare Information and Management Systems Society, Chicago, IL (available at http://www.himss.org/).

HIPAABreach. 2014. "HIPAA Breach Notification Tool," U. S. Department of Health & Human Services, Washington, DC.

HIPAAPrivacy. 2004. "Summary of the HIPAA Privacy Rule,"U. S. Department of Health & Human Services, Washington, DC.

Huang, H.-C., Lai, M.-C., Lin, L.-H., and Chen, C.-T. 2013. "Overcoming Organizational Inertia to Strengthen Business Model Innovation: An Open Innovation Perspective," *Journal of Organizational Change Management* (26:6), pp. 977-1002.

Johnson, M. E., and Willey, N. D. 2011. "Usability Failures and Data Hemorrhages?," *IEEE Security & Privacy* (9:2), pp. 18-25.

Johnson, V. 2007. "What Is Organizational Imprinting? Cultural Entrepreneurship in the Founding of the Paris Opera," *American Journal of Sociology* (113:1), pp. 97-127.

Jung, T., and Wickrama, K. A. S. 2008. "An Introduction to Latent Class Growth Analysis and Growth Mixture Modeling," *Social and Personality Psychology Compass* (2:1), pp. 302-317.

Kankanhalli, A. M., Teo, H. H., Tan, B. C. Y., and Wei, K. K. 2003. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2), pp. 139-154.

Kelley, K. 2008. "Nonlinear Change Models in Populations with Unobserved Heterogeneity," *Methodology: European Journal of Research Methods for the Behavioral and Social Sciences* (4:3), pp. 97-112.

Kelly, D., and Amburgey, T. L. 1991. "Organizational Inertia and Momentum: A Dynamic Model of Strategic Change," *Academy of Management Journal* (34:3), pp. 591-612.

Kim, E.-H., and Lyon, T. P. 2013. "Beyond the Dichotomy of Symbolic versus Substantive Actions," Academy of Management Proceedings, Academy of Management, Orlando, FL.

Kolbasuk McGee, M. 2014. "Why Hackers Are Targeting Health Data," Healthcare Info Security (available at http://www.healthcareinfosecurity.com/hackers-are-targeting-health-data-a-7024).

Kraatz, M. S., and Block, E. S. 2008. "Organizational Implications of Institutional Pluralism," in *Handbook of Organizational Institutionalism,* R. Greenwood, C. Oliver, R. Suddaby, and K. Sahlin-Andersson (eds.), London: Sage, pp. 243-275.

Kraatz, M. S., and Zajac, E. J. 1996. "Exploring the Limits of New Institutionalism: The Causes and Consequences of Illegitimate Organizational Change," *American Sociological Review* (61:5), pp. 812-836.

Kwon, J., and Johnson, M. E. 2013. "Health-Care Security Strategies for Data Protection and Regulatory Compliance," *Journal of Management Information Systems* (30:2), pp. 41-66.

Kwon, J., and Johnson, M. E. 2014. "Proactive Versus Reactive Security Investments in the Healthcare Sector," *MIS Quarterly* (38:2), pp. 451-471.

Levin, D. Z. 2006. "Institutionalism, Learning, and Patterns of Decoupling: The Case of Total Quality Management," Working Paper, Rutgers University (available at https://www.

researchgate.net/profile/Daniel_Levin4/publication/228474707_Institutionalism_learning_and_patterns_of_selective_decoupling_The_case_of_total_quality_management/links/00b7d52c8576445cb3000000.pdf).

Lounsbury, M. 2001. "Institutional Sources of Practice Variation: Staffing College and University Recycling Programs," *Administrative Science Quarterly* (46:1), pp. 29-56.

Lounsbury, M., and Glynn, M. A. 2001. "Cultural Entrepreneurship: Stories, Legitimacy, and the Acquisition of Resources," *Strategic Management Journal* (22:6-7), pp. 545-564.

Lumpkin, G. T., and Dess, G. G. 1996. "Clarifying the Entrepreneurial Orientation Construct and Linking it to Performance," *Academy of Management Review* (21:1), pp. 135-172.

Margolis, J. D., and Walsh, J. P. 2001. *People and Profits? The Search for a Link between a Company's Social and Financial Performance*, Mahwah, NJ: Lawrence Erlbaum Associates.

Meyer, J. W., and Rowan, B. 1977. "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American Journal of Sociology* (83), pp. 440-463.

Mignerat, M., and Rivard, S. 2009. "Positioning the Institutional Perspective in Information Systems Research," *Journal of Information Technology* (24:4), pp. 369-391.

Mindel, V., and Mathiassen, L. 2015. "Contextualist Inquiry into IT-Enabled Hospital Revenue Cycle Management: Bridging Research and Practice," *Journal of the Association for Information Systems* (16:12), pp. 1016-1057.

Mishra, A. K., Anderson, C., Angst, C. M., and Agarwal, R. 2012. "Electronic Health Records Assimilation and Physician Identity Evolution: An Identity Theory Perspective," *Information Systems Research* (23:3, Part 1 of 2), pp. 738-760.

Muthén, B. O. 1989. "Latent Variable Modeling in Heterogeneous Populations," *Psychometrika* (54:4), pp. 557-585.

Muthén, B. O. 2002. "Beyond SEM: General Latent Variable Modeling," *Behaviormetrika* (29:1), pp. 81-117.

Muthén, B. O. 2004. "Latent Variable Analysis: Growth Mixture Modeling and Related Techniques for Longitudinal Data," in *Handbook of Quantitative Methodology for the Social Sciences,* D. Kaplan (ed.), Newbury Park, CA: Sage, pp. 345-368.

Muthén, B. O., and Shedden, K. 1999. "Finite Mixture Modeling with Mixture Outcomes Using the EM Algorithm," *Biometrics* (55:2), pp. 463-469.

Muthén, L. K., and Muthén, B. O. 2015. *Mplus User's Guide* (7th ed.), Los Angeles: Muthén & Muthén.

Nagin, D. S. 1999. "Analyzing Developmental Trajectories: A Semiparametric, Group-Based Approach," *Psychological Methods* (4:2), pp. 139-157.

Orlitzky, M., Schmidt, F. L., and Rynes, S. L. 2003. "Corporate Social and Financial Performance: A Meta-Analysis," *Organization Studies* (24:3), pp. 403-441.

Perez-Batres, L. A., Doh, J. P., Miller, V. V., and Pisani, M. J. 2012. "Stakeholder Pressures as Determinants of CSR Strategic Choice: Why Do Firms Choose Symbolic Versus Substantive Self-Regulatory Codes of Conduct?," *Journal of Business Ethics* (110:2), pp. 157-172.

Pérez-Luño, A., Wiklund, J., and Cabrera, R. V. 2011. "The Dual Nature of Innovative Activity: How Entrepreneurial Orientation Influences Innovation Generation and Adoption," *Journal of Business Venturing* (26:5), pp. 555-571.

Pfarrer, M. D., Pollock, T. G., and Rindova, V. P. 2010. "A Tale of Two Assets: the Effects of Firm Reputation and Celebrity on Earnings Surprises and Investors' Reactions," *Academy of Management Journal* (53:5), pp. 1131-1152.

Pisano, G. P., Bohmer, R. M. J., and Edmondson, A. C. 2001. "Organizational Differences in Rates of Learning: Evidence from the Adoption of Minimally Invasive Cardiac Surgery," *Management Science* (47:6), pp. 752-768.

Png, I. P., Wang, C.-Y., and Wang, Q.-H. 2008. "The Deterrent and Displacement Effects of Information Security Enforcement: International Evidence," *Journal of Management Information Systems* (25:2), pp. 125-144.

PricewaterhouseCoopers. 2016. "The Global State of Information Security® Survey," PricewaterhouseCoopers (available at http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html).

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

Punke, H., and Rosin, T. 2015. "50 Great Health Systems to Know 2015," *Becker's Hospital Review* (http://www.beckershospitalreview.com/lists/50-great-health-systems-to-know-2015.html).

Queenan, C., Angst, C. M., and Devaraj, S. 2011. "Doctors' Orders—If They're Electronic, Do They Improve Patient Satisfaction? A Complements/substitutes Perspective," *Journal of Operations Management* (29:7-8), pp. 639-649.

Richardson, R. 2008. "CSI/FBI Computer Crime and Security Survey," Computer Security Institute, San Francisco, CA.

Rodrigue, M., Magnan, M., and Cho, C. H. 2013. "Is Environmental Governance Substantive or Symbolic? An Empirical Investigation," *Journal of Business Ethics* (114:1), pp. 107-129.

Rogers, E. M. 1995. *Diffusion of Innovations* (4th ed.), New York: The Free Press.

Scott, W. R. 2001. *Institutions and Organizations* (2nd ed.), Thousand Oaks, CA: Sage Publications.

Scott, W. R. 2008. *Institutions and Organizations: Ideas and Interests* (3rd ed.), Thousand Oaks, CA: Sage Publications, Inc.

Scott, W. R., and Meyer, J. W. 1983. "The Organization of Societal Sectors," in *Organizational Environments: Ritual and rationality,* J. W. Meyer and W. R. Scott (eds.), Beverly Hills, CA: Sage, pp. 129-153.

Scott, W. R., Ruef, M., Mendel, P., and Caronna, C. 2000. *Institutional Change and Healthcare Organizations: From Professional Dominance to Managed Care* (1st ed.), Chicago: University of Chicago Press.

Selznick, P. 1996. "Institutionalism 'Old' and 'New'," *Administrative Science Quarterly* (41:2), pp. 270-277.

Sen, R., and Borle, S. 2015. "Estimating the Contextual Risk of Data Breach: An Empirical Approach," *Journal of Management Information Systems* (32:2), pp. 314-341.

Seo, M.-G., and Creed, W. E. D. 2002. "Institutional Contradictions, Praxis, and Institutional Change: A Dialectical Perspective," *Academy of Management Review* (27:2), pp. 222-247.

Shane, S., and Venkataraman, S. 2000. "The Promise of Entrepreneurship as a Field of Research," *Academy of Management Review* (25:1), pp. 217-226.

Sloan, F. A., and Vraciu, R. A. 1983. "Investor-Owned and Not-for-Profit Hospitals: Addressing Some Issues," *Health Affairs* (2:1), pp. 25-37.

Spetz, J., and Maiuro, L. 2004. "Measuring Levels of Technology in Hospitals," *Quarterly Review of Economics and Finance* (44:3), pp. 430-447.

Sterba, S. K. 2013. "Understanding Linkages Among Mixture Models," *Multivariate Behavioral Research* (48:6), pp. 775-815.
Stevens, J. M., Steensma, H. K., Harrison, D. A., and Cochran, P. L. 2005. "Symbolic or Substantive Document? The Influence of Ethics Codes on Financial Executives' Decisions," *Strategic Management Journal* (26:2), pp. 181-195.
Stiglitz, J. E. 2000. "The Contributions of the Economics of Information to Twentieth Century Economics," *Quarterly Journal of Economics* (115:4), pp. 1441-1478.
Stinchcombe, A. L. 1965. "Organizations and Social Structure," in *Handbook of Organizations,* J. G. March (ed.), Chicago: Rand McNally, pp. 153-193.
Straub, D. W. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.
Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision-Making," *MIS Quarterly* (22:4), pp. 441-469.
Sydow, J., Schreyögg, G., and Koch, J. 2009. "Organizational Path Dependence: Opening the Black Box," *Academy of Management Review* (34:4), pp. 689-709.
Thompson, J. D. 2003. *Organizations in Action: Social Science Bases of Administrative Theory* (1st ed.), New Brunswick, NJ: Transaction Publishers.
Thornton, P. H. 2004. *Markets from Culture: Institutional Logics and Organizational Decisions in Higher Education Publishing*, Stanford, CA: Stanford University Press.
Tofighi, D., and Enders, C. K. 2008. "Identifying the Correct Number of Classes in Growth Mixture Models," in *Advances in Latent Variable Mixture Models,* G. R. Hancock and K. M. Samuelson (eds.), Charlotte, NC: Information Age Publishing, pp. 317-341.
Tolbert, P. S., and Zucker, L. G. 1983. "Institutional Sources of Change in the Formal Structure of Organizations: The Diffusion of Civil Service Reform, 1880-1935," *Administrative Science Quarterly* (28:1), pp. 22-39.
Tuma, N. B., and Hannan, M. T. 1984. *Social Dynamics: Models and Methods* (1st ed.), Orlando, FL: Academic Press,
Vermunt, J. K. 2010. "Latent Class Modeling with Covariates: Two Improved Three-Step Approaches," *Political Analysis* (18:4), pp. 450-469.
Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention," *European Journal of Information Systems* (20:3), pp. 267-284.
Weigelt, K., and Camerer, C. 1988. "Reputation and Corporate Strategy: A Review of Recent Theory and Applications," *Strategic Management Journal* (9:5), pp. 443-454.
Westphal, J. D., Gulati, R., and Shortell, S. M. 1997. "Customization or Conformity? An Institutional and Network Perspective on the Content and Consequences of TQM Adoption," *Administrative Science Quarterly* (42:2), pp. 366-394.
Westphal, J. D., and Zajac, E. J. 1998. "The Symbolic Management of Stockholders: Corporate Governance Reforms and Shareholder Reactions," *Administrative Science Quarterly* (43:1), pp. 127-153.
Westphal, J. D., and Zajac, E. J. 2001. "Decoupling Policy from Practice: The Case of Stock Pepurchase Programs," *Administrative Science Quarterly* (46:2), pp. 202-228.
Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer abuse," *MIS Quarterly* (37:1), pp. 1-20.

About the Authors

Corey M. Angst is the Viola D. Hank Associate Professor in the IT, Analytics, and Operations Department at the Mendoza College of Business, University of Notre Dame. His research interests are in the transformational effect of IT, technology usage, IT value, and privacy of information. Corey has held various editorial roles and his research has been published in top journals across diverse disciplines including information systems, healthcare informatics, policy, operations, and strategy. He received his Ph.D. from the Smith School of Business, University of Maryland.

Emily S. Block is an associate professor of Strategic Management and Organization at the Alberta Business School. She received her Ph.D. from the University of Illinois at Urbana-Champaign. Her research focuses on the generation (by organizations), and interpretation (by stakeholders), of formal and informal organization structures, language, and practices. Just as nonverbal communication provides valuable information about individuals beyond their spoken words, symbols do the same for organizations. Symbols may be purposefully or unintentionally generated by organizations, and the ways that they are interpreted may have significant consequences. Her research, focusing on these consequences, can be found in *Academy of Management Journal* and *Strategic Management Journal*.

John D'Arcy is an associate professor in the Department of Accounting & MIS, Lerner College of Business and Economics, at the University of Delaware. He received his Ph.D. in Management Information Systems from Temple University. His research interests include information assurance and security, IT risk management, and computer ethics. His work appears in journals such as *Information Systems Research*, *Decision Sciences Journal*, *European Journal of Information Systems*, *Journal of Management Information Systems*, *MIT Sloan Management Review*, and *Decision Support Systems*.

Ken Kelley is a professor of Information Technology, Analytics, and Operations (ITAO), and the Associate Dean for Faculty and Research in the Mendoza College of Business at the University of Notre Dame. Ken's work is on quantitative methodology, where he focuses on the development, improvement, and evaluation of statistical methods and measurement issues. His specialties are in the areas of research design, effect size estimation and confidence interval formation, longitudinal data analysis, and statistical computing. In addition to his methodological work, Ken collaborates with colleagues on a variety of important topics applying methods. He is an Accredited Professional Statistician™ (PStat®) by the American Statistical Association, associate editor of *Psychological Methods*, recipient of the Anne Anastasi early career award by the American Psychological Association's Division of Evaluation, Measurement, & Statistics, and a fellow of the American Psychological Association.

MIS Quarterly

RESEARCH ARTICLE

WHEN DO IT SECURITY INVESTMENTS MATTER? ACCOUNTING FOR THE INFLUENCE OF INSTITUTIONAL FACTORS IN THE CONTEXT OF HEALTHCARE DATA BREACHES

Corey M. Angst
IT, Analytics, and Operations Department, University of Notre Dame, 348 Mendoza College of Business, Notre Dame, IN 46556 U.S.A. {cangst@nd.edu}

Emily S. Block
Department of Strategic Management and Organization, University of Alberta, 4-21 F Alberta School of Business, Edmonton, AB T6G 2R6 CANADA {eblock@ualberta.ca}

John D'Arcy
Department of Accounting and MIS, University of Delaware, 356 Purnell Hall, Newark, DE 19716 U.S.A. {jdarcy@udel.edu}

Ken Kelley
IT, Analytics, and Operations Department, University of Notre Dame, 363 Mendoza College of Business, Notre Dame, IN 46556 U.S.A. {kkelley@nd.edu}

Appendix A

IT Security Included in this Study

Technology	Description
Biometric systems	Authentication mechanisms that determine whether a user is authorized to access a particular IT system based on his/her physical characteristics.
ID management	Used to electronically identify users and control their access to IT resources based on certain access privileges.
Intrusion detection	Monitoring systems designed to detect an attack on a network or computer system.
Anti-virus software	Software programs used to detect and remove computer viruses.
Single sign-on technology	Software authentication that enables a user to authenticate once and gain access to the resources of multiple systems, reducing the need to track and manage multiple passwords.
Non-biometric user authentication systems	Used to verify the identity of a user through non-physical means (e.g., user ID and password, electronic tokens or smart cards, responses to short questions, or some combination).
Data encryption	Technologies that encode electronic data in such a way that non-authorized users cannot read it but authorized parties can.
Internet firewalls	Hardware and/or software technologies that control incoming and outgoing network traffic by analyzing data packets.
Spyware filters	Software programs used to detect and deter unwanted spyware programs that monitor internal systems.

Appendix B

Correlation Table

Variable	1	2	3	4	5	6	7	8	9
(1) SystemSize	1.00								
(2) HospitalSize	-0.02	1.00							
(3) Age	**-0.34**	0.01	1.00						
(4) BusinessModel	**0.62**	**-0.11**	**-0.29**	1.00					
(5) Teaching	**-0.13**	**0.51**	**0.04**	**-0.12**	1.00				
(6) Mission	**0.03**	**0.17**	**-0.16**	**-0.18**	**-0.04**	1.00			
(7) EntrepMindset	**0.03**	**0.39**	**-0.07**	**-0.27**	**0.23**	**0.15**	1.00		
(8) ITSec	**-0.04**	**0.19**	**0.01**	**-0.10**	**0.07**	**0.07**	**0.46**	1.00	
(9) Breach	**0.21**	**0.28**	**-0.07**	**0.10**	**0.22**	0.02	**0.25**	**0.15**	1.00

Note: Bold represents statistically significant coefficients at $p < 0.05$.

Appendix C

Statistical Specification of Our GMM Model

In the path diagram below (Figure C1), squares are measured variables and circles are latent variables. Arrows represent a presumed causal relationship. The triangle on the left of the model represents the intercept and the one on the right, the fixed effects of the predictors. The 1's along the paths for the intercept are the constant effect the intercept has on each time point, and the numbers along the paths for the slope denote the particular value of time. Zero is used for the first time point so that the intercept can be more easily interpreted as the "baseline," in which the intercept term represents the logit (or probability if rescaled) of breach in 2005.

In terms of mapping this diagram to our conceptual model (Figure 1 in the paper), the squares on the left side represent the firm-specific institutional factors (covariates) that predict latent class (specifically the symbolic latent class, as per H1a through H1g). Moving to the right, the arrows from IT Security Investment (*ITSec*) to Intercept of Breach and Slope of Breach represent the influence of *ITSec* on these growth factors (which are derived from the repeated measures of *Breach* from 2005–2013). Note that *ITSec* is held constant for testing H2 (as described in footnote 19) to assess its influence on the combined classes. The arrows from Latent Class to the Intercept of Breach and Slope of Breach indicate that the influence of *ITSec* on these growth factors varies by Latent Class, as tested in H3a and H3b (also described in footnote 19). This corresponds to the regressions of the Intercept of Breach and Slope of Breach on a dummy variable representing the latent class categories (symbolic and substantive adoption, in our case).

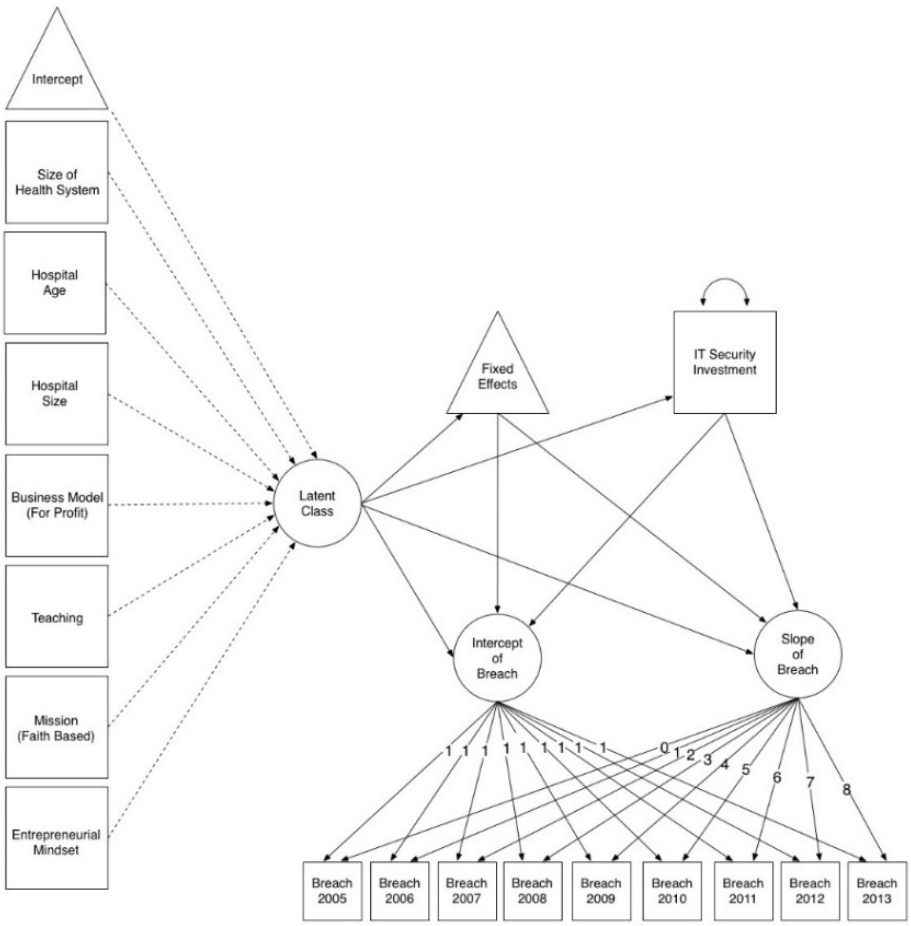


Figure C1. Path Model Showing Statistical Specifications of Our GMM Model

Appendix D

Detailed Description of Analysis Including Mplus Syntax

The Mplus syntax below fits the measurement (intercept and slope) and structural model (effect of *ITSec*). Note that an exclamation point denotes a commented line. As noted earlier, we scaled time such that 0 represents 2005. The value of time can be seen in the Mplus model statement below (Part 2; note that this model statement is for the model in which *ITSec* is held constant across classes) where, for example, *Breach* at 2005 is denoted as BrchY_05@0, *Breach* at 2006 is denoted as BrchY_06@1, *Breach* at 2007 is denoted as BrchY_07@2 and so forth up until 2013. Also, M_ITS is the mean of our *ITSec* variable; other variable names are self-explanatory. The R3STEP labeling on the variables listed under the AUXILIARY heading (Part 1) indicates that these variables will be treated as latent class predictors per the three-step method described earlier (in the Mplus program, AUXILIARY is an option of the VARIABLE command and for the three-step method, a variable is specified as R3STEP if it is to be included in this procedure).

As recommended (e.g., Jung and Wickrama 2008), we use multiple random starts (1,000) and multiple optimization attempts (250). This can be seen in the ANALYSIS section of the Mplus syntax below (Part 3). We took these steps to help ensure that our solutions yield the global minimum log likelihood discrepancy function rather than (as can happen in nontrivial models) the optimization procedure converging at a local minimum log likelihood discrepancy function. The global log likelihood minimum discrepancy function is what produces the estimates that maximize the likelihood (i.e., that yield the maximum likelihood solution).

Part 1: Specifying the Variables

```
VARIABLE:  NAMES ARE
   SeqID
   ln_HosAg
   FaithBsd
   P_Acad
   ln_StBed
   P_Prof
   M_SysSz
   M_SaidT
   M_ITS
   ;
   AUXILIARY ARE
   M_SaidT(R3STEP)
   M_SysSz(R3STEP)
   ln_StBed(R3STEP)
   ln_HosAg(R3STEP)
   FaithBsd(R3STEP)
   P_Prof(R3STEP)
   P_Acad(R3STEP)
   ;
   USEVARIABLES ARE
   BrchY_05 BrchY_06 BrchY_07 BrchY_08 BrchY_09 BrchY_10 BrchY_11 BrchY_12  BrchY_13
   M_ITS
   ;
   CATEGORICAL ARE
   BrchY_05 BrchY_06 BrchY_07 BrchY_08 BrchY_09 BrchY_10 BrchY_11 BrchY_12 BrchY_13;

   IDVARIABLE is SeqID;
   MISSING ARE all (9999);
   CLASSES = C(2);
```

Part 2: Mplus Model Statement

```
Model:   %OVERALL%
   i s | BrchY_05@0 BrchY_06@1 BrchY_07@2
      BrchY_08@3 BrchY_09@4 BrchY_10@5
      BrchY_11@6 BrchY_12@7 BrchY_13@8;

   i on M_ITS(I_MITS);
   s on M_ITS(S_MITS);

   [
   i@0
   s(Slope1)
   BrchY_05$1(Thres)
   BrchY_06$1(Thres)
   BrchY_07$1(Thres)
   BrchY_08$1(Thres)
   BrchY_09$1(Thres)
   BrchY_10$1(Thres)
   BrchY_11$1(Thres)
   BrchY_12$1(Thres)
   BrchY_13$1(Thres)
   ];
```

! Model differences for Class 2, in which differences are between the overall model (here Class 1 because there are only two classes),

%C#2%

[
i(int2)
s(Slope2)
BrchY_05$1(Thres)
BrchY_06$1(Thres)
BrchY_07$1(Thres)
BrchY_08$1(Thres)
BrchY_09$1(Thres)
BrchY_10$1(Thres)
BrchY_11$1(Thres)
BrchY_12$1(Thres)
BrchY_13$1(Thres)
];

Part 3: Model Options

ANALYSIS: TYPE=MIXTURE;
STARTS =1000 250; ! = (#Random Starts; #Optimizations)
Estimator=ML;

Part 4: Abbreviated Model Output

Tests of Categorical Latent Variable Multinomial Logistic Regressions Using the Three-Step Procedure

			Two-Tailed	
	Estimate	S.E.	Est./S.E.	P-Value
C#1 ON				
M_SAIDT	0.068	0.030	2.228	0.026
M-SYSSZ	0.017	0.008	2.207	0.027
LN_STBED	0.475	0.167	2.835	0.005
LN_HOSAG	-0.535	0.13	-3.840	0.000
FAITHBSD	-0.677	0.353	-1.920	0.055
P_PROF	-4.415	1.309	-3.374	0.001
P_ACAD	1.878	0.382	4.921	0.000
Intercepts				
C#2	5.035	0.933	-5.399	0.000

Parameterization Using Reference Class 1 *(the results under this heading correspond with Table 4 in the paper)*

C#1 ON				
M_SAIDT	-0.068	0.030	-2.228	0.026
M-SYSSZ	-0.017	0.008	-2.207	0.027
LN_STBED	-0.047	0.167	-2.835	0.005
LN_HOSAG	0.535	0.139	3.840	0.000
FAITHBSD	0.677	0.353	1.920	0.055
P_PROF	4.415	1.309	3.374	0.001
P_ACAD	-1.878	0.382	-4.921	0.000
Intercepts				
C#2	5.035	0.933	-5.399	0.000

Model Results *(these are for the model in which ITSec is held constant across classes; results displayed in Panel 1 of Table 5 in the paper)*

			Two-Tailed	
	Estimate	S.E.	Est./S.E.	P-Value
Latent Class 1				
1 ON				
M_ITS	**0.344**	**0.047**	**7.351**	**0.000**
S ON				
M_ITS	**0.017**	**0.010**	**1.633**	**0.102**
Intercepts				
I	0.000	0.000	999.000	999.000
S	0.371	0.061	6.099	0.000
Thresholds				
BRCHY_05$1	4.914	0.318	15.444	0.000
BRCHY_06$1	4.914	0.318	15.444	0.000
BRCHY_07$1	4.914	0.318	15.444	0.000
BRCHY_08$1	4.914	0.318	15.444	0.000
BRCHY_09$1	4.914	0.318	15.444	0.000
BRCHY_10$1	4.914	0.318	15.444	0.000
BRCHY_11$1	4.914	0.318	15.444	0.000
BRCHY_12$1	4.914	0.318	15.444	0.000
BRCHY_13$1	4.914	0.318	15.444	0.000
Latent Class 2				
1 ON				
M_ITS	**0.344**	**0.047**	**7.351**	**0.000**
S ON				
M_ITS	**0.017**	**0.010**	**1.633**	**0.102**
Intercepts				
I	-0.173	0.310	-0.558	0.577
S	-0.145	0.049	-2.936	0.003
Thresholds				
BRCHY_05$1	4.914	0.318	15.444	0.000
BRCHY_06$1	4.914	0.318	15.444	0.000
BRCHY_07$1	4.914	0.318	15.444	0.000
BRCHY_08$1	4.914	0.318	15.444	0.000
BRCHY_09$1	4.914	0.318	15.444	0.000
BRCHY_10$1	4.914	0.318	15.444	0.000
BRCHY_11$1	4.914	0.318	15.444	0.000
BRCHY_12$1	4.914	0.318	15.444	0.000
BRCHY_13$1	4.914	0.318	15.444	0.000

Model Results *(these are for the model in which ITSec is allowed to vary across classes; results displayed in Panels 2 and 3 of Table 5 in the paper)*

			Two-Tailed	
	Estimate	S.E.	Est./S.E.	P-Value
Latent Class 1				
1 ON				
M_ITS	**-0.118**	**0.185**	**-0.637**	**0.524**
S ON				
M_ITS	**0.061**	**0.031**	**1.944**	**0.052**
Intercepts				
I	0.000	0.000	999.000	999.000
S	0.195	0.102	1.915	0.056
Thresholds				
BRCHY_05$1	3.288	0.641	5.129	0.000
BRCHY_06$1	3.288	0.641	5.129	0.000
BRCHY_07$1	3.288	0.641	5.129	0.000
BRCHY_08$1	3.288	0.641	5.129	0.000
BRCHY_09$1	3.288	0.641	5.129	0.000
BRCHY_10$1	3.288	0.641	5.129	0.000
BRCHY_11$1	3.288	0.641	5.129	0.000
BRCHY_12$1	3.288	0.641	5.129	0.000
BRCHY_13$1	3.288	0.641	5.129	0.000
Latent Class 2				
1 ON				
M_ITS	**0.379**	**0.052**	**7.244**	**0.000**
S ON				
M_ITS	**0.020**	**0.013**	**1.453**	**0.146**
Intercepts				
I	-1.923	0.731	-2.632	0.008
S	-0.173	0.071	-2.436	0.015
Thresholds				
BRCHY_05$1	3.288	0.641	5.129	0.000
BRCHY_06$1	3.288	0.641	5.129	0.000
BRCHY_07$1	3.288	0.641	5.129	0.000
BRCHY_08$1	3.288	0.641	5.129	0.000
BRCHY_09$1	3.288	0.641	5.129	0.000
BRCHY_10$1	3.288	0.641	5.129	0.000
BRCHY_11$1	3.288	0.641	5.129	0.000
BRCHY_12$1	3.288	0.641	5.129	0.000
BRCHY_13$1	3.288	0.641	5.129	0.000

Appendix E

Model Comparisons, Two-Factor Versus One- and Three-Factor Solutions

Recent research has offered insight into the determination of the number of classes to use in a latent class analysis (Diallo et al. 2017; Nylund et al. 2007). While the central argument still holds that theory should guide the choice (Diallo et al. 2017; Tofighi and Enders 2008), these new approaches offer an empirical test and guidance for comparing models with different numbers of classes. Importantly, Diallo et al. (2017) evaluate the effect of including covariates in this type of model comparison and find that models should be compared in the absence of covariates. Following their guidance, we use the GMM for binary outcomes in the absence of covariates and compare one- and three-class models to our baseline two-class model. We find that our theoretically derived two-class solution performs better than the other two models. Specifically, the three-class model does not converge due to singularity (i.e., the matrix that is being optimized has a determinant of zero), meaning that it is ill-conditioned, likely as a result of being over-fitted. Thus, we cannot compare it to the two-class model. The fit criteria for the other classes are shown below.

Fit Criteria[1]	One-Class Model	Two-Class Model (i.e., baseline model)
Akaike (AIC)	8867.8	8857.7
Bayesian (BIC)	8901.2	8891.1
Sample-size adjusted BIC	8885.3	8875.2

[1]Lower numbers represent a better fitting model

References

Diallo, T. M. O., Morin, A. J. S., and Lu, H. 2017. "The Impact of Total and Partial Inclusion or Exclusion of Active and Inactive Time Covariants on the Class Enumeration Process of Growth Mixture Models," *Psychological Methods* (22), pp. 166-190.

Jung, T., and Wickrama, K. A. S. 2008. "An Introduction to Latent Class Growth Analysis and Growth Mixture Modeling," *Social and Personality Psychology Compass* (2:1), pp. 302-317.

Nylund, K. L., Asparouhov, T., and Muthén, B. 2007. "Deciding on the Number of Classes in Latent Class Analysis and Growth Mixture Modeling: A Monte Carlo Simulation Analysis," *Structural Equation Modeling* (14:4), pp. 535-569.

Tofighi, D., and Enders, C. K. 2008. "Identifying the Correct Number of Classes in Growth Mixture Models," in *Advances in Latent Variable Mixture Models*, G. R. Hancock and K. M. Samuelson (eds.), Charlotte, NC: Information Age Publishing, pp. 317-341.