2011

Predicting Threats on Electric Health Record Systems

Jason E. Nelms
Florida State University, jen10@fsu.edu

PREDICTING THREATS ON ELECTRONIC HEALTH RECORD SYSTEMS

Jason E. Nelms
Florida State University
jen10@fsu.edu

ABSTRACT

Security is a key concern in the development of electronic health record (EHR) systems. This paper considers Neutralization Theory and the Fear Appeals Model in proposing a conceptual model for use in predicting breach behaviors within EHR systems. The goal of the model is to determine which factors influence security breach intent on the part of the offender. Specifically, perceived penalty, perceived evasiveness, awareness of opportunity, enforcement, and user participation are proposed to act as antecedents to security breach intent, a surrogate for actual breach behavior.

Keywords

Electronic health records, security, neutralization, fear appeals

INTRODUCTION

The quantity of health data stored in electronic form continues to grow at an exponential rate, and recent healthcare legislation calls for nationwide electronic health records (EHRs) by 2014 (Thielst, 2007). The tremendous growth mandated by this legislation, coupled with technological advances such as telemedicine (Dwivedi et al., 2007), creates a need for tools which facilitate the use and management of the records.

As with other technologies, rapid growth in EHR tools presents a number of issues that must be addressed. One of the primary issues currently facing EHR management is that of security (Hewitt, 2010), with threats on EHR systems originating both within and outside of the systems. This paper focuses on internal threats, specifically those enacted by users of an EHR system. Reflecting upon two information security theories – neutralization theory and the fear appeals model (FAM), I create a conceptual model for predicting security breaches within an EHR system. The proposed model examines security breach intent from the perspective of offender (i.e. actor) contemplating a system breach.

LITERATURE REVIEW

Prior to the development of the conceptual model discussed in this paper, a thorough review of relevant literature is first provided. This review takes place within two primary streams: healthcare information technology (placing a specific focus on EHRs and EHR systems) and information systems security (ISS). This section outlines the relevant literature present within each stream with the aim of justifying constructs within the hybrid model.

EHR Literature

In considering legislation enacted during the previous two presidential terms, one is not surprised to see that most of the EHR literature examines the current state of EHR usage. Although EHRs have existed in some format since the 1960s (Lincoln et al., 1993), focus on the importance of EHR systems has only recently become urgent. However, only one in five members of the Medical Group Management Association claimed to be using EHRs as late as 2008 (Swartz, 2008). Also, the aforementioned call for EHRs and the popularity of such records among United States (U.S.) citizens have not prompted much action on the part of the U.S. government. The government has failed to make adequate strides to enforce healthcare initiatives that would likely quicken the conversion process from paper-based records to EHRs (Swartz, 2007).

Current research on EHRs has begun to explore issues related to implementation and technology concerns. Hewitt (2010) explores the many obstacles faced as organizations implement EHR systems, including staff resistance, increased costs, and a plethora of security issues. Boaden and Joyce (2006) posit that the process of change from a paper-based to an integrated EHR system must be viewed within the context of governance and patient safety in order to yield an effective system. While Sherer (2010) examines the role of mimetic forces on EHR adoption, Hennington et al. (2009) investigate mandated EHR systems, a concept of increasing relevance due to mandates within recent healthcare legislation.

Dwivedi et al. (2007) discuss the future of telemedicine, a technology that will use electronic exchange to allow patients to carry out routine medical testing through streaming or delayed data transfers. The technology, which is likely to emerge as an alternative medium for healthcare over the next 10-15 years, has the potential to reduce office visits, an outcome that, if

realized, would reduce the cost of routine consultations with physicians. Thielst (2007) furthers the discussion of electronic exchange as he proposes more efficient EHR delivery method, namely virtual health records (VHRs), a type of record which enables practitioners to access a patient's entire health history from within a web portal. VHRs have the potential to interact with telemedicine technologies to have a major impact on the development of EHRs on a worldwide basis.

IS Security Literature

Siponen and Vance (2010) bring Neutralization Theory, one of the primary focuses in this paper's contribution, into the context of IS. They propose that neutralization theory, a theory prominent in Criminology, can provide compelling explanations of the motivational factors behind IS security breaches and should be considered in the development and implementation of IS security policies. More on this study will be included in the model formation of this paper.

In related literature, Bulgurcu et al. (2010) find that an employee's intention to comply with an information security policy is influenced by attitude, outcome beliefs, and self-efficacy to comply. Outcome beliefs significantly affect beliefs about consequences, which, in turn, affect employee attitude. As a precursor, information security awareness (ISA) positively affect both attitude and outcome beliefs. Conversely, fear-inducing arguments, known as fear appeals, do not impact user behavior intentions (Johnston and Warkentin, 2010). For this reason, this paper functions on the assumption that the individual targeting a system has a strong ISA, being fully aware of the existence and implementation of security measures within and surrounding the targeted EHR system. Also, like Ransbotham and Mitra (2009), this study also considers the roles of countermeasures as a factor within the offender's consideration of the perceived penalty involved in a security breach.

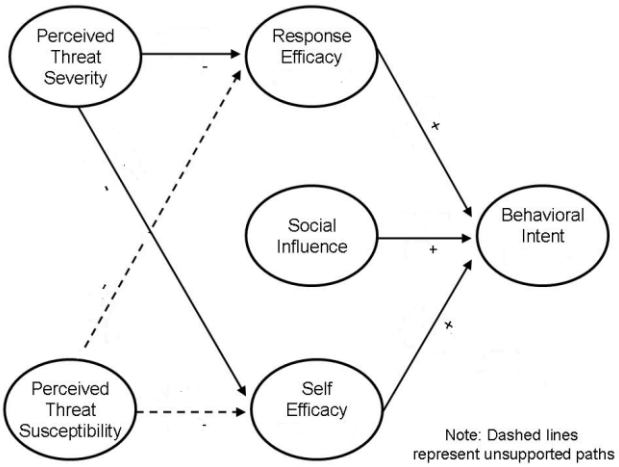
Smith et al. (2010) study the effect of mandatory compliance to information security standards, an aspect of new healthcare legislation that has been enacted, but not recently enforced by government agencies in the U.S. (Swartz, 2006). Due to this lack of activity, it is difficult to determine the number of breaches that occur on a regular basis although recent literature has shown that this number remains high, with an alarming 50% of U.S. hospitals affected by breaches in 2009 (Information Management Journal, 2009a). With the help of legislation such as The HITECH Act, a part of the American Recovery and Reinvestment Act of 2009, these numbers should decrease, however, as stiffer penalties can now be applied to those found in violation of health information standards, namely HIPAA. This type of mandatory compliance is a key issue in the model detailed in the next section.

CREATING A HYBRID MODEL FOR BREACH PREDICTION

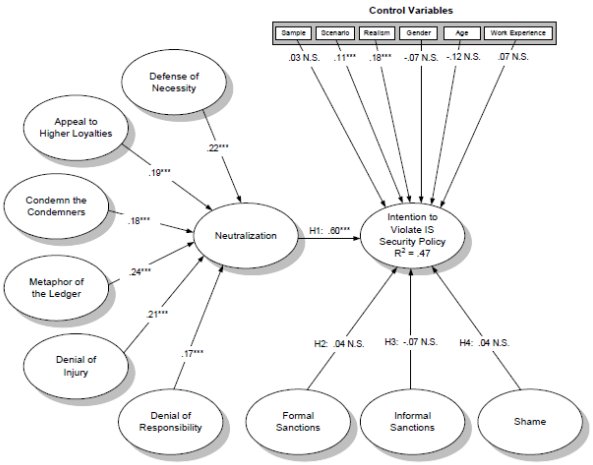
As previously stated, the goal of this paper is to create a conceptual model that incorporates the original FAM framework, taking into consideration neutralization variables. The original FAM model developed by Johnston and Warkentin (2010) explained user intentions to engage in individual computer security actions recommended through fear-inducing persuasive communication. Neutralization Theory (Siponen and Vance, 2010) describes several justification techniques undertaken by offenders to displace the blame or responsibility they face when planning or enacting a breach. The model represented in Figure 2 modifies the Johnston and Warkentin's (2010) FAM while inserting into each modified construct justification techniques utilized by Siponen and Vance (2010). Each theory is detailed below to provide a context for the development of the Breach Predictor Model (BPM) for ISS breach activities.

Fear Appeals Model (FAM)

In the original FAM model proposed by Johnston and Warkentin (2010), the authors asserted that response- and self-efficacy mediated the influence of threat severity and threat susceptibility on behavioral intent. They ultimately concluded that fear appeals did not have an effect on a user's activity as it pertained to the adoption of proposed security measures. Johnston and Warkentin concluded that Perceived Threat Susceptibility (a user's basic awareness of a threat) had no significant influences on other constructs. As such, this study tests the same concept from the point of view of one committing a breach, aptly applying to it the label of Perceived Evasiveness.



From Johnston and Warkentin, 2010



From Siponen and Vance (2010)

Figure 1. Fear Appeals Model (FAM) and Neutralization

As illustrated in Figure 1, Perceived Penalty and Perceived evasiveness, constructs chosen to act as opposites of the FAM constructs of Perceived Threat Severity and Perceived Threat Susceptibility are hypothesized to directly affect security breach intent, assuming that an information security policy has been put into place.

Neutralization Theory

Siponen and Vance (2010) found all of the antecedents to neutralization to be significant. They also found the construct of neutralization to be significant in influencing one's intention to violate IS policy (see Figure 1). In other words, the denial factors (justification techniques) surrounding neutralization increase an actor's intentions to violate an ISS policy. Thus each of the antecedents should be considered in the development of a conceptual model. These elements are common activities undertaken by individuals involved in rule-breaking in order to relieve themselves of fault. The six significant actions found in the Neutralization Theory results are as follows: defense of necessity, appeal to higher loyalties, condemning the condemners, invoking the metaphor of the ledger, denial of injury and denial of responsibility.

Siponen and Vance (2010) reference prior literature to define the six significant denial factors. Defense of necessity involves justification on the premise that rule-breaking is necessary. Appealing to higher loyalties is typically manifested in an appeal to organizational values or hierarchies as a justification for committing a breach. Condemning the condemners means placing the blame for an action on its target. When invoking the metaphor of the ledger, an offender attempts to justify deviant act (e.g., an ISS breach) by claiming that offsets a series of previous positive actions. Denial of injury is simply the denial that harm has occurred. Finally, denial of responsibility happens when a person claims to lack control over his or her actions.

A Proposed Conceptual Model

The model represented in Figure 2 extends Johnston and Warkentin's (2010) model and inserts into each adapted construct the significant justification techniques utilized by Siponen and Vance (2010). The following subsections detail each of the constructs contained within the BPM. Each subsection discusses relationships between BPM constructs and those contained within the neutralization mode. Additionally, each subsection provides the hypothesized relationships between the construct and others within the model. The descriptions proceed from the left of the model (User Participation) to Security Breach Intent, the model's dependent variable and proposed surrogate for breach behavior.

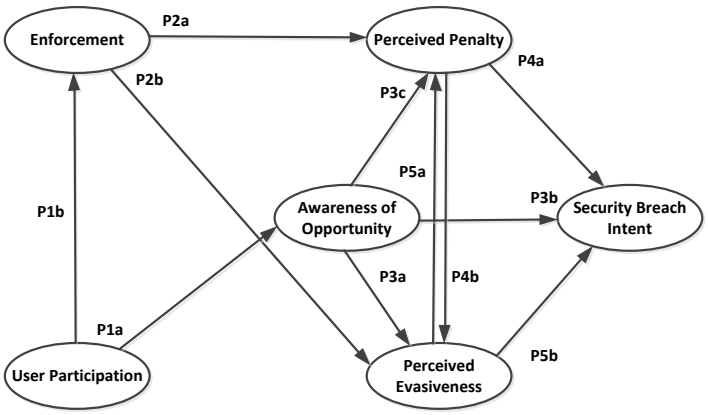


Figure 2. Proposed Breach Predictor Model (BPM)

User Participation

Wiant (2005) states that despite stringent security measures, an information security policy reaches its full effective potential only when breaches are reported along with their degree of seriousness. As part of this process, adequate participation on the part of users is an important factor in mitigating risks within the system (Spears and Barki, 2010).

Spears and Barki (2010) concluded that user participation is a key element in the successful development and implementation of information security policies. For the purposes of this model, user participation, typically stems from training in a system's use. Thus, the construct serves as a possible antecedent to user system efficacy, reporting tendencies, and enforcement, all of which will be described below. Within an EHR system, user participation can be used to prepare a potential offender to utilize one of the six neutralization actions in breach behavior, specifically appeal to higher loyalties and metaphor of the ledger, as the user's participation in system development could possibly encourage a sense of responsibility or entitlement on the part of a potential actor. In relation to user participation, the following propositions emerge:

P1a: User Participation positively affects awareness of opportunity
P1b: User Participation positively affects enforcement

Enforcement

The only effective information security policy is one that is consistently and fully enforced (Swartz, 2007). It is important to clarify the difference between government mandate and enforcement as they apply to the BPM. The mandated changes detailed within the review of EHR and ISS literature are the basis for government mandate. The systems described within this paper are only required by law. Enforcement outside of the mandate is seen as a continual follow-up measure. As stated above, recent literature has shown a lack of enforcement on the part of government agencies as they pertain to mandated healthcare legislation enforcement (Swartz, 2006b). As a result, many breaches have gone unreported and unenforced, thus skewing the number of actual breaches versus breaches reported over a number of time periods. Lack of adequate enforcement of ISS policies and government legislation are predicted to lessen the actor's perception of the impact of a breach activity on himself/herself or others. Additionally, lacking enforcement prompts the actor to perceive an increase chance of committing the crime without being caught or punished. Thus, the proposed propositions regarding the effect of enforcement on perceived penalty and perceived evasiveness are as follows:

P2a: Enforcement positively affects perceived penalty
P2b: Enforcement negatively affects perceived evasiveness

A test of these propositions will clarify the effect of community and government enforcement on a potential attacker's perception of potential impact and penalty, as well as his or her ability to commit a breach undetected.

Awareness of Opportunity, Perceived Penalty, and Perceived Evasiveness

As this paper operates under the assumption that only intentional breaches can have pre-meditation antecedents, the potential actor's awareness of a breach opportunity must be taken into consideration. Based on Johnston & Warkentin's (2010) model, it is proposed that an actor, once aware of a possible breach opportunity, establishes a set of beliefs pertaining to his or her ability to successfully carry out a security breach and escape undetected. This idea, termed perceived evasiveness in this study, is closely related to the neutralization activities of invoking the metaphor of the ledger, denial of injury, and denial of responsibility, as each activity is aimed at relieving the offender from blame (Siponen & Vance, 2010).

As indicated in Figure 2, the following propositions provide a basis for the testing of the construct as an antecedent to other constructs within the BPM, and as a distal precursor to security breach intent.

P3a: Awareness of opportunity positively affects perceived evasiveness
P3b: Awareness of opportunity positively affects security breach intent
P3c: Awareness of opportunity positively affects perceived penalty

As this paper operates under the assumption that only intentional breaches can have pre-meditation antecedents, the potential actor's awareness of a breach opportunity must be taken into consideration. Johnston & Warkentin's (2010) FAM posits that an individual, once aware of a threat, establishes beliefs as to the seriousness of the threat and probability of personally experiencing the threat. The perceived evasiveness and perceived penalty constructs within this model approach these beliefs from a different angle. Essentially, it is proposed that an actor, once aware of a possible breach opportunity, establishes a set of beliefs pertaining to his or her ability to successfully carry out an undetected security breach. This idea, termed perceived evasiveness in this study, is closely related to the neutralization activities of invoking the metaphor of the ledger, denial of injury, and denial of responsibility, as each activity is aimed at relieving the offender from blame (Siponen & Vance, 2010).

As previously discussed, an actor typically considers possible penalties and impacts prior to conducting a breach within a system. In a healthcare setting, these penalties may come in the form of impacts in the care received by patients. Simultaneously, the actor's perceived penalty can also be viewed as the severity of punishment that the actor expects to confront when caught. The construct of Perceived Penalty is used in this study as part of an assumption that those attempting to make a breach have considered the possible impacts of a system breach on themselves and others.

The construct of Perceived Evasiveness refers to the actor's perception of his or her ability to refrain from being caught by the proper authorities. In other words, the stronger the perceived evasiveness felt by the potential actor, the more he or she feels that the breach can be committed. In their original FAM model, Threat is a construct defined as an external stimulus that exists whether or not it is perceived by an individual (Johnston & Warkentin, 2010). The BPM model uses Perceived Evasiveness as the actor's perception of his or her ability to be an invisible threat.

It is proposed that Perceived Penalty be tested as a variable directly influencing security breach intent as well as a moderator between Perceived evasiveness and Security breach intent. Therefore, the following propositions become apparent:

P4a: Perceived penalty negatively affects security breach intent
P4b: Perceived penalty negatively affects perceived evasiveness
P5a: Perceived evasiveness negatively affects perceived penalty
P5b: Perceived evasiveness positively affects security breach intent

As seen in P4a, it is proposed that perceived penalty negatively affects security breach intent. In other words, the higher the severity of penalty perceived by the actor, the less likely he or she is to possess the lower his or her security breach intent. Additionally, it is proposed that as the actor's perception of perceived evasiveness increases, his or her perception of perceived penalty will decrease. Finally, it is proposed that an increase in the actor's perceived evasiveness will increase his or her security breach intent.

Security Breach Intent

Security breach intent is the potential actor's intent to commit a security breach within an EHR system. As used in the theory of planned behavior (Ajzen, 1991) and theory of reasoned action (Ajzen and Fishbein, 1980), behavior intent acts as a surrogate to actual behavior. Following this pattern, security breach intent performs similarly, acting as a surrogate to the act of committing a breach. The construct also mirrors Siponen and Vance's (2010) intention to violate ISS policy. As seen in the BPM, all of the constructs within the model are proposed antecedents to security breach intent.

LIMITATIONS AND FUTURE RESEARCH

This paper provides a conceptual model to predict security breach intent within the context of HER systems based on FAM (Johnston and Warkentin, 2010) and Nuetralization Theory. Therefore, it only assesses variables related to the intent to commit a breach, although the six neutralization activities are potential variables of justification. Nevertheless, the model does not take into account those variables present during the mitigation stages of a breach.

Another limitation is that this research studies intentional breaches, specifically those behavioral antecedents that lead to security breach intent, the construct used in this paper as a surrogate for the action of a breach. Further research should explore the combination of intentional and unintentional breaches and proper measures to minimize each. Such a study would, however require that the assumption that all breaches are planned be discarded.

Lastly, this paper focuses on EHR systems that have been mandated by governing powers. These types of systems have been chosen for this study due to the current state of their implementation. Such a transformation is a huge undertaking that is likely to warrant much attention from researchers and practitioners for years to come. As EHR systems become more prevalent, the relevance of this research should also continue to increase.

References

1. Anonymous. (2009). Breaches Affected 50% of Hospitals in 2009. *Information Management Journal*, 44 (2), p. 14.
2. Ajzen, I. (1991). A Theory of Planned Behavior. *Organization Behavior and Human Decision Processes*, 50 (1), p. 179.
3. Ajzen, I. and Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior. Englewood Cliffs*, NI: Prentice-Hall.
4. Boaden, R., and Joyce, P. (2006). Developing the Electronic Health Record: What About Patient Safety? *Health Services Management Research*, 19 (2), p. 94.
5. 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), p. 523
6. Dwivedi, A., Bali, R., and Raouf, N. (2007). Telemedicine: The Next Healthcare Delivery Medium: Fad or Future?. *International Journal of Healthcare Technology & Management*, 8 (3/4), p. 226.
7. Hennington, A., Janz, B., Amis, J., and Nichols, E. (2009). Understanding the Multidimensionality of Information Systems Use: A Study of Nurses' Use of a Mandated Electronic Medical Record System. *Communications of the Association for Information Systems*, 25 (1), p. 79.
8. Hewitt, B. (2010). Exploring How Security Features Affect the Use of Electronic Health Records. *International Journal of Healthcare Technology & Management*, 11 (1), p. 31.
9. Johnston, A., and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 34 (3), p. 549.
10. Lincoln, T., Essin, D., Ware, D., and Willis, H. (1993). The Electronic Medical Record: A Challenge for Computer Science to Develop Clinically and Socially Relevant Computer Systems to Coordinate Information for Patient Care and Analysis. *Information Society*, 9 (2), p. 157.
11. Ransbotham, S., and Mitra, S. (2009). Choice and Chance: A Conceptual Model of Paths to Information Security Compromise. *Information Systems Research*, 20 (1), p 121.
12. Sherer, S. (2010). Information Systems and Healthcare XXXIII: An Institutional Theory Perspective on Physician Adoption of Electronic Health Records. *Communications of the Association for Information Systems*, 26 (1), p. 25.
13. Siponen, M., and Vance, A. (2010). Neutralization: New Insights Into the Problem of Employee Information Policy Violations. *MIS Quarterly*, 34 (3), p. 487.
14. Smith, S., Winchester, D., Bunker, D., and Jamieson, R. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security de Jure Standard in a Government Organization. *MIS Quarterly*, 34 (3), p. 463.
15. Spears, J., and Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly*, 34 (3), p. 503.
16. Straub, D. (1989). Validating Instruments in MIS Research. *MIS Quarterly*, 13 (2), p. 147.
17. Swartz, N. (2006a). EHR Adoption Moving Slowly but Surely. *Information Management Journal*, 40 (4), p. 19.
18. Swartz, N. (2006b). Government Not Enforcing HIPAA. *Information Management Journal*, 40 (5), p. 20.
19. Swartz, N. (2007). Americans Prefer Electronic Health Records. *Information Management Journal*, 41 (4), p. 8.
20. Swartz, N. (2008). Report: Few Doctors Using EHRs. *Information Management Journal*, 42 (5), p. 22.
21. Thielst, C. (2007). The Future of Healthcare Technology. *Journal of Healthcare Management*, 52 (1), p. 7.
22. Wiant, T. (2005). Information Security Policy's Impact on Reporting Security Incidents. *Computers & Security*, 24 (6), p. 448.