Understanding Healthcare Data Breaches: Crafting Security Profiles

Completed Research

Alexander McLeod
Texas State University
am@txstate.edu

Diane Dolezel
Texas State University
dd30@txstate.edu

Abstract

Healthcare data breaches are occurring at unprecedented rates, but breach causes are not well delineated. The purpose of this exploratory study was to examine elements associated with data breaches and to create a model of healthcare organizations experiencing data breaches. We considered organizational factors, business process exposure factors, and technological security factors on breach versus no breach occurrences. The aim was to model factors that may be predictive of healthcare data breach weaknesses. Using computer security industry frameworks and healthcare standards, we develop a testable healthcare data breach model.

Keywords

Data breach model, security model, technological security factors, business process exposure factors, organizational factors.

Introduction

Healthcare data breaches have become commonplace with 155 breaches reported during the first five months of 2017 (Department of Health and Human Services 2017). The alarming rise in the theft of personal health information requires greater scrutiny (McLeod and Dolezel 2018; Thomson 2013). Stolen patient information faces potential black-market auction, medical identity pilferage and ransom threats by criminals capitalizing on an organizations’ security weaknesses (Gibbs et al. 2017; Johnson 2009). Protecting against data breaches is hard due to increased business process exposure when larger volumes of data are shared between mobile devices operating on multiple platforms. Other challenges to security include the cost and complexity of securing multifaceted interconnected systems, while facilitating data sharing for professional collaboration, and the driving changes in organizational dynamics (Genes 2016; Stachel and DeLaHaye 2015).

While personal health information loss is concerning, organizations must also consider how breaches impact the entire business (Gatzlaff and McCullough 2010). Following information theft, organizations may face governmental enforcement of fines and penalties, litigation, negative publicity, public anger and disruption of medical services (2009; Davis 2016). These issues have caused healthcare organizations to remain susceptible targets as criminals exploit vulnerabilities with increasing ease, capitalizing on breached data (Floyd et al. 2016; Gibbs et al. 2017). Healthcare organizations need to understand what can be done to lessen the vulnerability of organizations; and why breached organizations are more vulnerable than their counterparts.

Since 2009, there have been 1987 healthcare data breaches reported to the DHHS (Department of Health and Human Services 2017). We attempted to ascertain if breached organizations are more exposed, have less security, or present other factors that might facilitate a breach (Ayyagari 2012; Liu et al. 2015). The purpose of this exploratory study was to examine elements associated with data breaches and to create a model of healthcare organizations experiencing data breaches. We considered factors related to technological security, business process exposure, and the breached organization’s environment on breach
versus no breach occurrences. When these risk characteristics are known, a model of breached organizations may provide insight to hardening healthcare’s security footprint.

**Guiding Standards**

President Barack Obama signed Executive Order 13636: Improving Critical Infrastructure Cybersecurity in 2013, mandating the National Institute of Standards and Technology (NIST) create a Cybersecurity Framework for use by industry in defending against cyber threats (Obama 2013). This initiative advanced when the Department of Homeland Security (DHS) took on the Federal government’s role in securing the nation’s critical infrastructure. For example, Public Health and Healthcare are considered key infrastructure components and are consolidated under the DHHS. To increase awareness and provide recommendations for electronically securing private and public data, the Commission on Enhancing National Cybersecurity was established in 2016 (National Institute for Standards & Technology 2017).

These guidelines and frameworks provide insight into securing against healthcare breaches. As such, they suggest best practices which can be modeled. For example, there are five actionable items recommended in the NIST Cybersecurity Framework – identify, protect, detect, respond and recover. The organizational profile developed using this framework provides an initial view of security within the facility. Organizations can then compare existing security practices with desired states to implement improvements. Using risk management in this fashion introduces a framework analysis process.

Other industry standards such as the Health Insurance Portability and Accountability Act (HIPPA) (1996) and the Health Information Technology for Economic and Clinical Health Act (HITECH) (2009), require healthcare entities to notify DHHS when has been breached. In addition, the HIPPA Security Rule requires healthcare organizations to create a risk management plan protecting all personal health data against security incidents (2009). These types of requirements fit easily into our security profile model.

**Conceptual Framework**

Factors influencing health care data breaches exist in all organizations. Categorizing an entity’s information system technologies, business processes and other organizational factors is easily done using standards and cyber security frameworks (NIST Computer Security Division 2006).

![Figure 1 - NIST Strategic/Tactical Security Risk Triangle (Technology 2014)](image)

Theorizing that breaches occur due to a series of associated events; various researchers have suggested tactical and strategical risks (Kraemer et al. 2009; Liginlal et al. 2009; Nicho 2012). Figure 1 shows how this chain of events links the tactical and strategic events. The Strategic/Tactical Security Risk Triangle provides the conceptual framework for this research. To summarize, all information systems technology, healthcare business processes and organizational factors represent potential data breach sources.
Organizational Factors

Prior work examining the cause of data breaches provides insight into the organizational effects on security. Kamoun and Nicho (2016) determined six classes or groups of security related factors considered desirable for risk prevention including security culture, governance practices, policies and procedures for handling, ongoing employee security training, vendor selection and strong risk management processes.

The best way to motivate employee behavior is via a strong security culture. All employees must be kept up to date about the technology, business processes and organizational factors influencing the personal health information (Almubark et al. 2016). Encouraging employees to report breaches through a security incident management system is part of building a strong security culture. Organizational actions supporting a security culture could be measured by security and awareness training activities, security planning activities, and risk management activities.

In modern organizations, top management support for IT governance practices includes internal compliance audits, implementation of data classification frameworks, providing a data governance team, and retaining a Chief Security Officer (Zafar et al. 2016). Funding governance practices ensures adequate activities and processes, reducing factors associated with data breaches.

Policies and procedures flow from the top of an organization, where top management works to ensure they align with the organization’s mission statement. Strong user policies governing access control, acceptable use, password requirements, email use and file sharing, help employees know what the organization expects (Kamoun and Nicho 2014; Kobus 2012).

The NIST (Wilson and Hash 2003), HIPAA (Department of Health and Human Services 2006), and other standards require employee security training. Moreover, it is well established that employee training and education are important in preventing security incidents by increasing awareness, explaining best practices and highlighting social engineering attempts (Wilson and Hash 2003). Providing such training is not a one-time event, but rather a repetitive roll out of teaching on current risks and responses (Kamoun and Nicho 2014). Partners, vendors and other business associates must also be diligent in securing their interconnected systems (Khalfan 2004). Therefore, a review of contracted organization’s (e.g. business associates) security habits needs to be included in the software and hardware selection processes. Additionally, a security assessment of business associate’s vulnerability and planning improves an organizations security footprint.

Well considered risk management processes inform organizations about security risks and facilitate reduction of data breach vulnerabilities (Kamoun and Nicho 2014). These actions allow a facility to proactively manage risk. Weak risk management programs, such as those lacking oversight of mandatory security policies, may result in preventable system vulnerabilities (Straub and Welke 1998). Variables measuring these organizational factors might include risk assessment, risk management planning, and training for facility managers.

Standards, frameworks and research have provided a variety of organizational measures to assess factors that may affect data breaches. Variables considered by Zafar (2011) could be suitable in cause determination of data breaches. Measures such as age of the facility and the organization’s size could serve as proxies for complexity and should be considered in a profile. Use of security standards at the corporate level might also be included in a security research model.

The role of other organizational factors was assessed by Kraemer et al. (2009). They developed nine classes that included external influences, human error, management, organization, performance and resource management, policy issues, technology, and training. Other researchers explored how organizational factors might curb cybercrime (Maasberg and Liu 2015). Cybercrime mitigation efforts include security management best practices such as the presence of management support, having security policies and security plans, using application whitelisting, and employing a chief information security office. They include restricting or monitoring access with firewalls, secured remote access, use of strong passwords, managing privileged accounts and restricting internet access, and the use of antivirus software. Recovering from security breaches or incidents must also be addressed, there should be incident response policies and procedures, business continuity and disaster recovery plans.
Obviously, there is a solid research foundation for consideration of organizational variables when examining the association with technological security and business process exposure factors.

**Business Process Exposure Factors**

Vulnerabilities represent flaws in technology that can be exploited by criminal hackers introducing technical threats to computers, software, networks or data AHIMA (Group 2014). Using weak passwords, leaving data unencrypted, not patching software in a timely fashion and failing to monitor data transmissions, leaves business process susceptible and increases the threat of exposure to data breaches.

Hardware and software require multiple levels of threat protection. For example, computer workstations must be physically secured and restricted from unauthorized access. Hardware must be inventoried and enabled for data encryption and set to provide automatic logoffs and to produce trace logs. All software should be required to be current with devices protected via anti-virus software and password protection. Remote storage needs to be segregated by firewalls that examine data packets and create logs. When employees work from home, personal health information exposure increases because data is transmitted over the Internet as employees access electronic health records (EHRs), health portals, and health information exchanges (HIEs) (Levine 2015; Win 2005).

We believe that increasing connectivity increases the possibility of a data breach. Examples of increase connectivity include participating in a HIE (Akhlaq et al. 2016; Kuperman and McGowan 2013; Vest and Gamm 2010), increasing the number of workstations or the number of mobile devices, implementing EHRs (Ancker et al. 2014a; Bowman 2013; Sandefer et al. 2015), mandating the use of CPOEs (Spaulding and Raghu 2013) and adopting patient health portals (Ancker et al. 2014b; Cronin et al. 2015; Highfield et al. 2014; Ossebaard et al. 2012; Zettel-Watson and Tsukerman 2016).

**Technological Security Factors**

Security factors have been shown to be directly related to access control, maintenance, validation and technology planning (Wiant 2005). Technological assessments of hardware, software and the probability of these devices introducing vulnerabilities must be considered (Jain et al. 2006). Historically, technology has lead the way in reducing security risk (Merete Hagen et al. 2008). For technology to improve computer security, it must protect against accidental or malicious data disclosure, data modification, and data destruction utilizing tools such as authentication, backups, data encryption, and other existing protections (Hash et al. 2005; OCR 2010). Security plans should include employee id badges, biometric authentication, RFID tags, barcoding, two factor authentication and surveillance cameras (Wu et al. 2013). Evidence of these tools existing in an organization reflects greater computing security.

**Research Model**

After reviewing the literature, we developed a research model to guide analysis of data breaches. Using existing standards and framework requirements, the organizational factors, business process exposure factors and technological security factors provided potential constructs for analysis. Measurable data variables derived from the literature were applied to each construct in the model. To develop the model the existing requirements for managing risks to healthcare data were examined, and concepts related to the facilities’ organizational, technological security and business process exposure factors were explored.

Similar to Mejias (2012), we developed an assessment model for evaluating factors related to a healthcare data breaches. In their work, they employed Confirmatory Factor Analysis to examine the associations of three constructs: technical knowledge (e.g. system attacks and system vulnerabilities), organizational impact (e.g. IT Asset Evaluation and Organizational profitability) and attacker assessment (e.g. attacker motivation, deterrence factors and attacker profiles)(Mejias and Balthazard 2014).

Venkatesh (2015) looked at cyber-attacks associated with risk management and used the Common Vulnerability Scoring System (CVSS) as a tool to determine vulnerability. The final score represented the outcome variable with the predictors represented by the quantity of vulnerabilities and the volume of network traffic. They considered authentication, authorization, availability, software coding, configuration,
environmental, password protocol as independent variables for logistic regression. Results indicated higher CVSS levels were associated with increased vulnerabilities and network traffic (Venkatesh 2015).

Kamoun and Nicho (2014) considered preventative measures using their Swiss Cheese Model. Their work explored the data breach causation chain, depicting systems as slices of cheese where a hole represents a failure and shifting weaknesses due to organizational failures. If the cheese holes align, a chain of events forms and the probability of a data breach increases. Weaknesses influencing data breaches included: inadequate security defenses, organizational influence, precursors of unsafe data handling and unsafe act of data handling. Organizational influences might be reflected in a lack of data security policies and procedures or failing to enforce existing data security policies and procedures or weak termination policies. Other factors noted include failing to use data encryption, lax physical security, mishandling mail and poor data security (Kamoun and Nicho 2014). These authors recommend adding additional slices to the healthcare system to plug holes by enhancing security measures. For example, educating staff about handling, increasing and improving information governance and risk management programs, mandating data encryption, strong password requirements and physical security of personal health information are all potential deterrents to hackers (Kamoun and Nicho 2014).

Drawing on concepts from these studies and the literature review, this study examined the data breach factors related to business process exposure, technological security and organizational variables. The conceptual model is shown in Figure 2.

![Conceptual Model of Data Breach Factors](image.png)

**Figure 2 - Conceptual Model of Data Breach Factors**

**Research Questions**

Because of the importance of identifying the factors potentially impacting a healthcare data breach, we sought to understand the following research questions:

- **RQ1** What is the relationship between specific organizational factors and the likelihood of the occurrence of a data breach?
- **RQ2** What is the relationship between the business process exposure factors and the likelihood of the occurrence of a data breach?
- **RQ3** What is the relationship between technological security factors and the likelihood of the occurrence of a data breach?
- **RQ4** What is the relationships between technological security, business process exposure, and organizational factors and the likelihood of the occurrence of a data breach?
Measurement Model

Drawing on prior literature, we crafted a measurement model to evaluate healthcare security profiles. In this model, the dependent variable is data breach occurrence. Figure 3 shows how items relate to constructs forming the measurement model and potential variables for inclusion in analysis.

![Figure 3 - Measurement Model of Data Breach Factors](image)

Table 1 lists the potential variables for organizational factors, business process exposure and technological security factors selected from the computer security frameworks and standards literature for exploration.

<table>
<thead>
<tr>
<th>Organizational Factors</th>
<th>Business Process Exposure Factors</th>
<th>Technological Security Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Systems (IS) Budget</td>
<td>Clinical Decision Support System (CDSS)</td>
<td>Auto Identification</td>
</tr>
<tr>
<td>Net Operating Revenue</td>
<td>Connectivity</td>
<td>Barcoding</td>
</tr>
<tr>
<td>Payroll Expense</td>
<td>Computerized physician order entry (CPOE)</td>
<td>Biometric Technologies</td>
</tr>
<tr>
<td>Security Culture</td>
<td>EHR</td>
<td>Data Backup</td>
</tr>
<tr>
<td>Total Operating Expense</td>
<td>HIE</td>
<td>Information Systems (IS) Plan</td>
</tr>
<tr>
<td>Vendor Selection Process</td>
<td>Number of Computers</td>
<td>Radio-frequency identification (RFID)</td>
</tr>
<tr>
<td>Workforce Policies</td>
<td>Number of Employees</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td>Employee Training and Education</td>
<td>Patient Portal</td>
<td>Storage Initiatives</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Telecommunications Plan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Threat Detection</td>
</tr>
</tbody>
</table>

Table 1 – Potential Variables by Associated Factor

Conclusion

The number of healthcare data breaches continues to increase despite industry and government’s greater awareness of factors predisposing an organization to a data breach. Researchers offer guidance when
industry problems generate serious societal impacts such as identity theft, ransomware and hacking. Thus far, little research has been done to uncover common traits of breached healthcare providers. Determining healthcare organizations weaknesses can lead to greater understanding of what protections are needed and how to respond to protect personal health information. Measuring factors associated with data breaches and creating security profiles of breached organizations might provide greater information to the healthcare sector. This work developed a research model suitable for use by healthcare security researchers evaluating factors associated with data breaches.

REFERENCES


Bowman, S. 2013. "Impact of Electronic Health Record Systems on Information Integrity: Quality and Safety Implications," Perspectives in Health Information Management (10:Fall), 2013/10/01/.


