Information Security and Insider Threats in Small Medical Practices

Research-in-Progress

Nancy L. Martin
Southern Illinois University
nlmartin@siu.edu

Thomas R. Imboden
Southern Illinois University
timboden@siu.edu

Abstract

This research in progress investigates insider threats and the use of security policies in small medical practices. Results from an exploratory survey of 18 small medical practices are discussed. Key findings warranting further study include the response from one third of the practices that no security policy currently exists. The primary reason given was a lack of expertise available to create a policy. Of those with a policy, when the policy was ignored, it was primarily due to the impact on productivity. These discoveries led to a broader research question related to the noncompliance of medical practices with HIPAA Security Rule guidelines. The exploratory survey is described and then the rationale and plan for an extended study are discussed.

Keywords

Insider threat; Information security; HIPAA compliance, Healthcare information systems.

Introduction

Insider threats account for an alarming number of security breaches each year. Although external threats are increasing (Ernst & Young 2013), some argue that insiders are the greatest threat to system security (Warkentin and Willison 2009). Many times those threats are simply due to the carelessness or negligence of individuals in the organization. For example, the 2013 State of Cybercrime Survey (PwC 2013a) reports that 34 percent of identified incidents were the result of unintentional actions which exposed sensitive data. Survey respondents also reported that sensitive data loss was twice as likely to be caused by unintentional actions rather than malicious actions. Even though unintentional, these threats can lead to a range of difficulties not only for the organization, but also for the individuals’ whose information was exposed.

Threats to information security in the healthcare environment carry additional risk. The exposure of sensitive information can cause financial hardship, mental anguish, and especially in healthcare, lead to social stigma and impacts on medical decisions and treatment (Appari and Johnson 2010). Also unique to the healthcare industry is the federal, and sometimes state, regulation of the protection of personal health information (PHI). While there is a broad range of research devoted to the behavior aspect of information security in various organizations, relatively little research has been dedicated specifically to the healthcare setting.

Information security research in small businesses is another area in need of more extensive academic research. Despite reports of growing threats to information security in small businesses, few research studies have helped to broaden understanding of the unique information security issues in these organizations.

When considering that in the US, more than 60 percent of physicians practice in what can be considered a small business, the need for more attention to information security in healthcare becomes clear. Not only is this population at risk as a small enterprise, they may also be subject to civil and criminal penalties in the event of a PHI breach. This paper reports on an exploratory survey designed to gather preliminary
information for a broader study of insider threats and information security practices in small medical practices. The results, though limited, certainly provide incentive to further develop research in this area.

The next several sections of this paper briefly discuss literature related to insider threats, the information security landscape of healthcare and small business, and the limited literature about small medical practices. Then the exploratory survey and results are discussed, followed by the next steps planned for this research.

**Information Security in the Workplace**

Considerable research has focused on information security-related behavior in the workplace. Generally, workplace threats are divided into those external to the organization and those internal to the organization. Because these two types of threats often stem from different motivations, research studies usually treat them separately. Insider threats have also been further defined to include human versus nonhuman and accidental versus intentional (Loch et al. 1992).

User errors and negligence are some of the most common accidental errors and are considered one of the worst threats to information security (Whitman and Mattord 2004). Although reasons for user errors are numerous, simple lack of awareness of the importance of information security is an obvious factor. Another consideration is that users find the requirements (such as complex passwords or installing updates) to be burdensome. Moreover, the potential for accidental or unintentional threats is increased since many employees use social networking sites, even while at work, and may be unclear what information can be shared on those sites. The growing use of mobile devices also creates new concerns when the negligence of end users can lead to theft of devices and the potentially sensitive data that reside on them. Employees connecting to networks with their personal devices create yet another weakness in security. A 2012 survey of more than 700 information technology professionals worldwide reported that 71 percent believed mobile devices have led to an increased number of security incidents. The survey results also showed that a lack of employee awareness has the greatest impact on mobile data security and 72 percent of respondents said that “careless employees are a greater security threat than hackers” (Check Point Software Technologies Ltd. 2012, p. 1).

An important precursor to conscientious security behavior is awareness. Information security awareness is a complex construct and has been studied in terms of two components: information security policy awareness and general information security awareness (Bulgurcu et al. 2010). Robust security policies are recommended as one prevention for insider threats and for organizations with security policies, compliance or noncompliance of individuals is a primary concern. In that vein, many researchers have addressed the factors that contribute to compliance/noncompliance behaviors (e.g. D’Arcy et al. 2009; Guo et al. 2011; Herath and Rao 2009; Ifinedo 2012; Silvius and Dols 2012; Siponen and Vance 2010). This has led to the further refinement of human threats to include security policy noncompliance behaviors which have been defined as 1) passive, non-volitional, 2) volitional, non-malicious, and 3) intentional, malicious (Willison and Warkentin 2013). Guo (2013) conducted a review and synthesis to more clearly inform the conceptualization of security-related behaviors and identified eight categories, some of which include *omissive security behavior* (Workman et al. 2008), *violation of policy* (Siponen and Vance 2010), and *non-malicious security violation* (Guo et al. 2011).

Even with the urgent and apparent need for security education, training, and awareness (SETA) programs, 29 percent of organizations in a recent survey report their SETA communication was either nonexistent or not yet developed (Ernst & Young 2013). “Only 23% of respondents rated security awareness and training...as their number one or two priority; 32% ranked it last (Ernst & Young 2013, p.8).

**Information Security in Healthcare**

All industries and organizations that use networks are vulnerable to information security threats. However, the healthcare environment presents a particularly risky setting due to the personal information necessary to operate a healthcare organization. Not only are patients’ identities and financial information at risk, but health data must also be protected and this is not a new concern (e.g. Rindfleisch 1997).
The security landscape of healthcare has been altered in recent decades due to the advancement of information technology. While privacy and security of patient information has long been a priority of medical practitioners and consumers, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 enacted broad federal protections specifically for PHI (1996). HIPAA was not the first law to address personal information protection. For example, the Freedom of Information Act of 1967 (1967), the Privacy Act of 1974 (1974), and federal drug and alcohol laws all either protect certain types of information or protect information collected by specific entities. However, HIPAA was the first comprehensive legislation to address PHI. HIPAA applies to covered entities (CE). A CE, according to HIPAA, is a health care provider, health plan, or healthcare clearinghouse, and their respective business associates. HIPAA also only applies to providers that conduct certain electronic transactions. In reality, if a provider bills any insurance payer, which most do, HIPAA applies.

The HIPAA statute consists of five sections, one of which addresses information privacy and security. That HIPAA section was implemented as two administrative rules: HIPAA Privacy Rule (2003), implemented in 2003, and HIPAA Security Rule, implemented in 2005 (2005). The Privacy Rule focuses on policies and procedures that give individuals greater rights and privacy protections of health information and applies to all formats of PHI: electronic, paper, and oral. The HIPAA Security Rule protects electronic health information only and applies to entities that create, maintain, or transmit PHI. The Security Rule requires that entities ensure the confidentiality, integrity, and availability of electronic PHI, protect PHI against reasonably anticipated threats and inappropriate use of disclosure, and ensure employee compliance.

The HIPAA Security Rule consists of standards in five categories: physical, technical, and administrative safeguards, organizational requirements, and policies/procedures/documentation requirements. The standards are further delineated through numerous implementation standards which may either be required or addressable, meaning that if not implemented, documentation must exist to justify the reasons.

Of particular interest to our study are the three categories of safeguards. Physical safeguards apply to systems, buildings, and equipment and are designed to prevent environmental hazards and unauthorized intrusion. Technical safeguard standards address access and audit controls, data integrity, user authentication, and data transmission security. Administrative safeguards comprise over half of HIPAA security requirements and serve as the basis of a broad security program for organizations. These standards require that potential risks must be analyzed and appropriate response measures be implemented to reduce vulnerabilities. Additionally, organizations must designate a security official, control PHI access, train workforce, sanction policy violations, and periodically evaluate security procedures.

The Health Information Technology for Economic and Clinical Health (HITECH) Act was passed as part of the American Reinvestment and Recovery Act of 2009 (2009) and made significant changes to HIPAA. The final HITECH rule, implemented in 2013, expanded the definition of covered entities which must adhere to HIPAA requirements and increased penalties for noncompliance (2013). Among other changes, HITECH also expanded patients’ rights related to access and use of PHI and breach notification.

Regarding breach notification, HITECH removed the discretionary feature of breach reporting in HIPAA and added specific requirements. With HITECH, both CEs and business associates must notify those potentially affected in the event of a breach. Subcontractors must report breaches to business associates as well. These notifications put providers and organizations in the media spotlight and also on the regulating agencies’ radar.

While the details of breach notifications are outside the scope of this paper, it should be noted that HITECH requires that the Secretary of Health and Human Services annually submit to Congress information about reported breaches. Additionally, information related to breaches affecting 500 or more people is publicly available from the HHS.gov website. The report includes the breach type but does not specify internal versus external source.

Redspin’s 2013 Breach Report analyzed reported incidents, and since 2009, 804 large breaches (more than 500 impacted) have affected more than 29.2 million patients (Redspin 2014). While the largest breaches involved storage systems, theft and human error were the leading causes in 2013. Forty-five percent of reported incidents in 2013 involved stolen devices resulting from careless or negligent actions.
Insider Threats: IT Abuse, Misuse and Crime

such as leaving a laptop in a car or a flash drive out in the open. In another study including a variety of industries, North American healthcare organizations reported that 32 percent of security incidents were from current employees and another 22 percent from former employees (Check Point Software Technologies Ltd. 2012).

Specific to healthcare, academic studies have looked at a variety of information security related topics. For example, studying a totally integrated hospital information system, Samy et al. (2010) identified 22 types of threats with the single most critical threat being a power failure or loss. Other critical threat categories included acts of human error, technological obsolescence, and hardware/software failures or errors. Landry et al. (2011) produced a further refinement based on HIPAA privacy and security implications. Their health information threat tree categorizes threats between inside or outside threats to data disclosure. Although helpful, it does not consider threats other than disclosure. Van Deursen et al. (2013) identified the six most common threat scenarios based on actual incidents and expert opinion, and note that all were human behavior-related. Their categories included missing asset/record, password/token sharing, email disclosure to wrong recipient, theft on premises, procedures not followed, and wrong system privileges set.

It is clear that in the healthcare setting, information security is of paramount importance. Not only is PHI security legislated, but threats to PHI can cause financial hardship, mental anguish, and social repercussions, and could even impact medical decisions and treatment (Appari and Johnson 2010). While academic research on issues surrounding information security in healthcare is growing, it is still a young stream and in need of further attention. (Appari and Johnson 2010).

Information Security in Small Organizations

Academic literature focusing specifically on information security in small organizations also seems to be relatively rare. Some report that small businesses have limited understanding of information security, technologies, and controls, and fail to perform risk assessment or create security policies (e.g. Dimopoulos et al. 2004; Gupta and Hammond 2005). Others found that small organizations were less likely to implement preventive measures when compared to larger organizations (Kankanhalli et al. 2003). Many agree that the primary reasons for lax security in small organizations are the basic lack of financial resources, time, and/or the specialized knowledge needed implement effective information security policies and procedures (e.g. Dimopoulos et al. 2004; Gupta and Hammond 2005; Imboden et al. 2013).

The lack of research in this area is concerning since other sources frequently report issues with information security in small organizations. For example, a 2013 study reported some alarming results among over 1000 businesses with less than 100 employees: 1) 69 percent did not know or believe that lost or stolen data would have financial impact or harm the organization’s credibility, 2) 40 percent had no data security protocols in place, 3) 48 percent had no one directly responsible for data security, and 4) more than one third never offered staff any information security training (Shred-it 2013). A study conducted in the UK reports that in organizations of less than 50 employees, 87 percent had a security breach in the past year (PwC 2013b).

Information Security in Small Medical Practices

The American Medical Association reports that nearly 60 percent of physicians work in practices with fewer than 10 physicians and another 16 percent work in practices of 10-24 physicians (Kane and Emmons 2013). As far as structure, 60 percent reported that their practices were wholly owned by practice physicians as opposed to practices that were partially or wholly owned by hospitals. Solo practices comprised about 18 percent according to report estimates. The landscape of medical practices therefore strongly resembles that of small, owner-run businesses. Similar to other industries, it is likely that small healthcare organizations, and specifically small medical practices, struggle with information security as well.

Information systems research attention has been more motivated toward healthcare in recent years due to the increasing use of various healthcare information systems and technologies. For small practices, the most common focus is on the adoption of electronic health records (e.g. DesRoches et al. 2012; Rao et al. 2011; Zhang 2013). Barriers to adoption of electronic health records appear similar to barriers other small organizations report in the adoption of information security protocols. For example, Horowitz and Zhang...
(2012) cite lack of funding, lack of standardized implementation, and lack of skilled workforce as barriers to adoption of electronic health records. While this focus on newer healthcare systems and technologies is important, practices also use network technology for other routine office processes such as email, payment processing, and electronic billing. All of these systems and the data they contain are only as secure as the weakest security link in the practice.

**Methodology and Results**

During the course of the literature review, it became evident that information security in small medical practices was an area in need of attention. We believed that our best approach was to gather some preliminary exploratory data from small practice providers in an effort to prepare a more comprehensive study. We anticipated building a model of compliance behavior unique to the small medical practice to tease out peculiarities since it has been recommended that focused research is needed to identify and characterize threats based on “organizational contexts” (Appari and Johnson 2010, p. 298). We also believed that due to the legislative requirements of HIPAA and HITECH, it would be less fruitful to focus on security policy development and information security training and awareness programs. However, as discussed in the following sections, our exploratory results painted quite a different picture.

To gather exploratory data to confirm the need to study a larger population, we first identified small medical practices in the southern part of a Midwestern state. Practices were identified through local healthcare directories; and postcards with an invitation and link to an electronic survey were mailed to 93 offices. Additionally, an invitation to participate in the survey was posted on a user forum for an electronic health records system commonly used by small practices. A total of 18 usable responses were collected between March 20 and April 20, 2013.

Since the survey was anonymous, it is not clear how many responses came from which source, but eight were from Illinois, two from Florida, two from Texas and one each from Michigan, Montana, New York, Ohio, and Pennsylvania. Practice demographics included number of employees and the type, or structure, of the practice. Twelve practices employed less than 10 individuals, two employed between 10 and 19, and four employed between 20 and 49. Sixteen were independently structured, one was loosely affiliated with a larger organization, and one was administered by a larger organization. None were owned by another organization. All organizations used some type of information system or electronic process that would be subject to HIPAA/HITECH rules.

Individual demographics included respondents’ role, education level, age, gender, and their perceived level of information security within the organization. Eleven respondents, or 61 percent, were female. The other demographics are shown in Tables 1 through 4. Only four of the 18 respondents reported that if someone at their organization was responsible for information security, that person had some educational background related to information technology.

<table>
<thead>
<tr>
<th>Role</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sole Provider</td>
<td>7</td>
<td>38.9</td>
</tr>
<tr>
<td>One of Multiple Providers</td>
<td>1</td>
<td>5.6</td>
</tr>
<tr>
<td>Office/Practice Manager</td>
<td>7</td>
<td>38.9</td>
</tr>
<tr>
<td>Admin/Support Staff</td>
<td>1</td>
<td>5.6</td>
</tr>
<tr>
<td>Multiple Roles</td>
<td>2</td>
<td>11.1</td>
</tr>
<tr>
<td>Total</td>
<td>18</td>
<td>100.0</td>
</tr>
</tbody>
</table>

**Table 1. Respondents’ Role**

<table>
<thead>
<tr>
<th>Education Level</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical Doctor</td>
<td>6</td>
<td>33.3</td>
</tr>
<tr>
<td>Master’s Degree</td>
<td>4</td>
<td>22.2</td>
</tr>
<tr>
<td>Bachelor’s Degree</td>
<td>3</td>
<td>16.7</td>
</tr>
<tr>
<td>Associate Degree</td>
<td>5</td>
<td>27.8</td>
</tr>
<tr>
<td>Total</td>
<td>18</td>
<td>100.0</td>
</tr>
</tbody>
</table>

**Table 2. Education Level**

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 to 34</td>
<td>3</td>
<td>16.7</td>
</tr>
</tbody>
</table>
Respondents were also asked to report types of information security incidents that have occurred in their organization. Table 5 displays those results categorized by the perceived level of information security in the organization for which the incidents were reported. The categories of data theft and hardware theft were also offered but both received zero responses. Except for the three organizations that reported “Unsure”, all other organizations reported at least one type of incident.

<table>
<thead>
<tr>
<th></th>
<th>Excellent</th>
<th>Above Average</th>
<th>Average</th>
<th>Adequate</th>
<th>Poor</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Failure</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>Virus/Spyware/Malware</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>Software Failure/Corruption</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Unsure</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>28</td>
</tr>
</tbody>
</table>

The response that most intrigued the researchers was that seven of the 18 organizations reported that no security policy currently exists. The reasons given for a lack of policy are presented in Table 6. Respondents were allowed to check as many reasons as applied resulting in more than seven responses.

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of expertise</td>
<td>5</td>
<td>38.9</td>
</tr>
<tr>
<td>Cost prohibitive</td>
<td>1</td>
<td>5.6</td>
</tr>
<tr>
<td>No perceived need</td>
<td>1</td>
<td>38.9</td>
</tr>
<tr>
<td>Other (only 2 provided explanations)</td>
<td>4</td>
<td>5.6</td>
</tr>
<tr>
<td>- Task is daunting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Still working on it</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>11</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Discussion

A few of the exploratory survey results are interesting. First, even though all 18 organizations are subject to HIPAA/HITECH rules, two respondents perceived their organizations security level as poor. Second, as reflected in Table 5, even practices that believed their security level was above average or excellent...
experienced some type of incident. Third, the most startling result was that seven of the 18 practices did not have a security policy in place. Although only a portion of the small exploratory survey results are reported here, they clearly identify a need for more extensive study.

Before we delve into the study of compliance behavior in small medical practices, it is imperative to first understand why, in the face of legislative rule and known risks, some small practices do not even have a security policy. One consideration is that while HIPAA and HITECH regulations are clear in the responsibility to protect PHI, they do little to guide providers in how to best implement protections for PHI.

Numerous and varied information security policy tools and templates are available to providers through the HealthIT.gov website and other sources such as professional organizations. Yet a large number of our limited sample of providers were not using them. Of those that had policies, only four reported using such a template. It is possible that time and expertise factors prevent small practice staff from finding what is really needed or understanding how to use the tools and templates when they are located. For example, the "Information Security Policy Template" available on the HealthIT.gov website is a 94 page document and is highlighted to signify where to fill in practice-specific information. However, to an individual unfamiliar with the language and specific requirements of the Security Rule, the template and its contents may very well be meaningless. If using the template, even altered to reflect a specific practice environment, what is the likelihood that each and every area is tended to and reassessed as recommended given the time and expertise constraints on small practices?

Other guides, such as “Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices”, also available from HealthIT.gov, are helpful only when staff have enough time away from other duties or when a practice at least has partially dedicated staff to address security policy. And even this guide states “If you consider your experience with security policies to be less than what may be assumed by this document, you may want to contact a local or national association that can identify educational materials for you or consult a qualified professional” (ONC n.d., p. 3).

Conclusion

As far as we have been able to ascertain, no known studies have looked at insider threats in the form of policy compliance or HIPAA Security Rule compliance in small medical practices. The first step will be to address the organizational compliance issue related to HIPAA Security Rule. While HIPAA/HITECH compliance in hospitals has been studied through the lens of institutional theory, the privacy and security rules were treated as one component rather than two (Appari et al. 2009) and the study did not address issues uncovered in our preliminary data. Therefore, our research effort will include building a theoretical model of compliance and developing a valid set of measures in an effort to better understand why, in the face of security threats and even civil and criminal penalties, information security policies are not followed, and worse, not even developed in small medical practices. The next phase will then focus on the compliance behaviors of organizational insiders in small medical practices that do have security policies.

REFERENCES


