Cyber-analytics: Modeling factors associated with healthcare data breaches

Alexander McLeod *, Diane Dolezel

Health Information Management Department, College of Health Professions, 601 University Drive, Texas State University, San Marcos, TX 78163, USA

ARTICLE INFO

Article history:
Received 14 August 2017
Received in revised form 17 February 2018
Accepted 17 February 2018
Available online xxxx

Keywords:
Security
Cyber security
Cyber risk
Data breach
Risk management
Exposure
Vulnerability assessment
Level of exposure
Level of security
Security modeling
Cyber-analytics

ABSTRACT

The purpose of this study was to develop a model of factors associated with healthcare data breaches. Variables were operationalized as the healthcare facilities’ level of exposure, level of security, and organizational factors. The outcome variable was the binary value for data breach/no data breach. Because healthcare data breaches carry the risk of personal health information exposure, corruption or destruction, this study is important to the healthcare field. Data were obtained from the Department of Health and Human Services database of healthcare facilities reporting data breaches and from a large national database of technical and organizational infrastructure information. Binary logistic regression was utilized to examine a representative data breach model. Results indicate several exposure, security and organizational factors significantly associated with healthcare data breaches.

© 2018 Elsevier B.V. All rights reserved.

1. Introduction

Preventing healthcare data breaches is hard. Connected healthcare systems necessitate information exchange across multiple devices and platforms, increasing the level of exposure and security risk, exposing the organization to potential data breaches. Patient data may be corrupted, stolen or modified by intrusive cyber agents, causing patients harm when data is used to obtain medical treatment or when the patient's stolen data is used for identity theft [1].

The organization may suffer disruption of services, incur significant costs, and face the possibility of litigation [2]. Moreover, Federal laws mandate heavy penalties for facilities whose negligence contributes to data breaches. For example, New York Presbyterian (NYP) Hospital was fined 3.3 million dollars for the Internet disclosure of 6800 patients’ data due to their improperly configured web servers and lax policies for granting database access [3]. In a related lawsuit, Columbia University paid a 1.5 million dollar fine for failing to conduct appropriate risks analyses on IT equipment used to connect to the NYP database servers.

Breach detection is another concern. Although Federal laws dictate that patients be notified of breaches within 60 days, discovery of data breaches may not occur for some time causing a significant lag time in event reporting [4]. Reporting lag time was evident when a cancer center data breach remained undetected for several months, and patients affected by the breach were not notified until five months after it was detected allowing malicious agents to scrutinize the data of 22,000 patients [5].

At the time of this writing in 2017, a record number of breaches had occurred including an employee responding to a phishing email with login credentials [6], successful hacking efforts by the Dark Overlord [7] and a multitude of various WannaCry ransomware encryptions [8]. While only 18 data breaches were reported in the last quarter of 2009, there were 351 data breaches reported during the first half of 2017 – almost two breaches per day! Fig. 1 reports the number of healthcare data breaches by category for the years 2009–2017 as presented in the Department of Health Human Services (DHHS) data breach report for breaches affecting over 500 people [9].

Encrypting data is necessary but not sufficient to prevent data theft. Most data breaches are reported as lost or stolen devices, indicating a lack of physical security for devices. Device loss may also reflect weak security plans (e.g. not physically securing laptops) or inadequate security training of employees. The bottom line is that healthcare institutions remain vulnerable targets for a wide range of cyber threats including technical, physical and human issues [11–13].

Cyber perpetrators continue to exploit these vulnerabilities with increasing sophistication, capitalizing on stolen healthcare records [14,15].

There are many negative effects caused by data breaches impacting uninvolved populations, organizational assets and the healthcare

* Declarations of interest: none.

+ Corresponding author.

E-mail address: amm@txstate.edu (A. McLeod).
environment in general. Because of the vulnerability of healthcare organizations and the many negative consequences for those experiencing a data breach [16], this work examined factors associated with data breach occurrences. The topic is important because healthcare data breaches expose personal data to theft, modification or misuse [17]. By exploring data breach factors, this paper helps healthcare organizations develop cyber profile models to test associations of data breach occurrence.

2. Background

Securing personal health information has been the focus of many important healthcare laws, security frameworks and national computing initiatives. In 2013, then President Barack Obama signed Executive Order 13636: Improving Critical Infrastructure Cybersecurity requiring the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework to help manage cyber risk [18]. To provide guidance on best practices for public and private cybersecurity programs, NIST was mandated to create a Cybersecurity Framework [19]. Subsequently, the Department of Homeland Security (DHS) assumed the Federal government’s lead in securing the nation’s critical infrastructure, which includes monitoring Healthcare and Public Health components of the Cyber Security infrastructure. In 2016, the Commission on Enhancing National Cybersecurity was established to provide recommendations for raising security awareness for electronically stored public and private data [20]. These federal organizations set requirements for healthcare facilities, mandating data breach reporting and enforcing best practices.

2.1. Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) [21] mandates that covered entities notify the DHHS when personal health information has been breached. Breach notification is also required for vendors and third-party service providers under the Health Information Technology for Economic and Clinical Health Act (HITECH) [22]. “A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information [23].” Following a breach, covered entities must notify individuals affected by the breach, the Secretary of the DHHS and sometimes the media. If a breach involves 500 or more individuals, entities discovering the data breach must notify the Secretary via the DHHS website. This requirement enables administrative review of previously unknown occurrences and provides some sense of the scale and frequency of healthcare data breaches.

Per the HIPAA Security Rule, healthcare facilities must implement a risk management plan that protects the confidentiality, integrity and security of all data that they create, maintain, receive or transmit. They must provide protection against security incidents for personal health information used for provisioning patient care [24]. In this context, a security incident is defined as the “attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system” [25]. The HIPAA Security Rule does not specify what methods or processes when analyzing risk. Healthcare organizations must create their own plan. Many organizations assign a risk level to each anticipated risk, based on the probability of the loss occurring, allowing them to prioritize risks. This is important because realistically all risks cannot be addressed. The disadvantage of this facility-specific approach is that there is no standard way to ensure compliance with HIPAA requirements. Some guidance can be found in the HIPAA implementation plan from NIST [26] and the Office for Civil Rights (OCR) annual guidance on the security rule [27].

2.2. Risk management

At a minimum, a facility must have procedures to detect and report all breaches within 60 days of discovery, as required by the OCR. Failing to do so will subject the facility to financial penalties. Penalties to date have been substantial. The first HIPAA enforcement for lack of timely breach notification was a $475,000 penalty paid by Presence Healthcare [28]. Explicitly, a breach of paper operating room schedules with the personal health information of 836 individuals occurred on October 22, 2013. It was not reported to OCR until January 31, 2014, which is well over the mandatory 60 day reporting period [28].

An associated issue is that the number of data breaches may be under reported. It has been postulated that facilities are considering encryptions as security incidents, which do not involve accessing personal health information, instead of the more serious data breach of personal health information [29]. In reality, facilities should refer to OCR guidelines on encryptions [30] and assume a data breach has occurred unless they have proof that personal health information was not compromised. E.g. ransomware encryptions were reported by over 50% of all hospitals between April 2015 and April 2016, and an additional 25% admitted they had no way to tell if they had been compromised [31]. Although, this translates into 4000 encryption attacks in 2016, a 300% increase over 2015, only nine such intrusions were reported to OCR [32].
دریافت فوری

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات