Chapter 4
A New Perspective on the Swiss Cheese Model Applied to Understanding the Anatomy of Healthcare Data Breaches

Faouzi Kamoun
ESPRIT School of Engineering, Tunisia

Mathew Nicho
Zayed University, UAE

ABSTRACT

The healthcare industry has been lagging behind other industries in protecting its vital data. Over the past few years, researchers and practitioners have been trying to gain a better understanding of the anatomy of healthcare data breaches. In this chapter, the authors show how Reason's swiss cheese model (SCM) provides a powerful analytic model to explain the human, technical, and organizational factors of healthcare data breaches. They also show how the SCM brings forwards the latent conditions of healthcare data breach incidents that have often been overlooked in previous studies. Based on an extensive literature review and an analysis of reported breaches from credible sources, the authors provide an explanation of the cheese layers and the associated holes. Since the SCM endorses the "defenses in depth" approach, it can assist healthcare organizations and business associates in developing a comprehensive and systematic approach to prevent and mitigate data breach incidents.

INTRODUCTION

Personal health records (PHR) and electronic medical records play an important role in managing health information and enhancing the quality of patients' healthcare through enhanced collection, compilation, storage, tracking and dissemination of health records and medical history among healthcare providers (Kierkegaard, 2012). Health information is considered among the most confidential of all types of personal information (Fernández-Alemán et al, 2013).The health sector is characterized by a wealth of

DOI: 10.4018/978-1-5225-5460-8.ch004

ever growing information that is dispersed throughout the healthcare organization and its downstream chain of business associates (BA) which includes any person or entity that creates, receives, maintains, or transmits protected health information (PHI) in fulfilling certain functions or activities for the health organization (HHS, 2013a). At the same time, as the healthcare sector is shifting from paper-based to electronic records, electronic data archives are accumulating in healthcare facilities and administrative agencies (O'Keefe & Connolly, 2011). In this respect, modern technologies have amplified the number of potential medical records that can be exposed to theft, damage or loss (Agaku et al, 2014). The exchange of electronic protected health information (ePHI) and electronic health records (EHR) further accentuated the need to secure patients' health information against unauthorized access, while guaranteeing easy access and a smooth flow of this information among the authorized entities. Kotz et al (2015) argue that the acclaimed benefits of modern healthcare information systems will be diluted if the associated security concerns were not properly addressed.

According to Johnson (2009) healthcare data hemorrhages come from many different sources like ambulatory healthcare providers, acute-care hospitals, physician groups, medical laboratories, insurance carriers, back-offices of health maintenance organizations, and outsourced service providers such as billing, collection, and transcription firms. The effects of data breaches on these parties are manifold. The improper disclosure or misuse of health information can cause serious reputational harm such as discrimination, stigmatization, loss of insurance and/or employment (Kulynych & Korn, 2002). The financial costs of data breaches, which include both direct costs, such as "clean-up" costs, and indirect costs, such as loss of revenues from reputational harm, are perhaps the most damaging factors from an organizational perspective. Data breaches can also lead to privacy violations, medical identity fraud, financial identity theft (such as forged taxation, fake health insurance and drug prescription claims) and identity theft (Johnson, 2009). Thus healthcare information security and privacy is a major ethical and legal issue (Appari & Johnson, 2010). In particular, the ethical principle of personal autonomy suggests that individuals have the right to control all matters related to their own body, including their personal health information (Neame, 2012). This right translates into public expectations and legal requirements that healthcare providers shall secure the privacy and confidentiality of patients' health records.

Despite the ethical and legal obligations of healthcare providers to protect the confidentiality of patients' health records, the past few years have witnessed an increase in the number and scope of reported healthcare data breach incidents. This is due to many factors, including (1) the fact that breach reporting became mandatory in September 2009, (2) the ease at which the healthcare sector can be penetrated, (3) the wide adoption of IT for the storage, processing and transmission of electronic health records (Ben-Assuli, 2015), (4) the wealth of sensitive personal and financial information available and accessible to criminals in a patient's health record (Kruse et al, 2017) and (5) the lack of adoption of security technologies and solutions (Kwon & Johnson, 2014). For example, a PHR may reveal personal information (such as name, dates of birth, social security number, address, employer and phone numbers), financial and insurance information (such as bank account, credit card numbers, and insurance numbers) and health information (such as diagnosis results, medications, allergies, addiction problems and treatment types). Healthcare data breaches have evolved into four main themes, namely data loss, monetary theft, and attacks on medical devices and on infrastructures (Perakslis, 2014).

Despite all forms of legislation, data encryption, and security technologies made available during the past years, one fundamental question remains that is still not fully addressed: "why do data breaches[1] still occur in the healthcare sector?" While a thorough answer is not evident, this research aims to shed light on the anatomy of healthcare data breaches so that proper countermeasures can be put in place.