Chapter 14
Development of an E-Healthcare Information Security Risk Assessment Method

June Wei
College of Business, University of West Florida, USA

Binshan Lin
College of Business Administration, Louisiana State University in Shreveport, USA

Meiga Loho-Noya
College of Business, University of West Florida, USA

ABSTRACT

This paper developed a method to assess information security risks in e-healthcare. Specifically, it first developed a static E-Healthcare Information Security Risk (EHISR) model to present thirty-three security risk factors by identifying information security threats and their sources in e-healthcare. Second, a dynamic E-Healthcare Information Flow (EHIF) model was developed to logically link these information risk factors in the EHISR model. Pattern analysis showed that information security risks could be classified into two levels, and versatility analysis showed that the overall security risks for eight information flows were close with a range from 55% to 86%. Third, one quantifiable approach based on a relative-weighted assessment model was developed to demonstrate how to assess the information security risks in e-healthcare. This quantitative security risk measurement establishes a reference point for assessing e-healthcare security risks and assists managers in selecting a reliable information flow infrastructure with a lower security risk level.

INTRODUCTION

E-healthcare can be defined as the use of emerging information and communication technology to improve or enable healthcare (HIPAA, 2000, p.2). Information Technology (IT) has presented the healthcare industry with many opportunities such as facilitating the exchange of information and reducing costs while improving services to better the delivery and quality care of patients (Eng,

DOI: 10.4018/978-1-4666-6339-8.ch014

Maxfield, Patrick, Deering, Ratzan, & Gustafson, 1998; Kendall & Levine, 1998; Kerwin, 2002; Nelson, Batalden, Mohr, & Plume, 1998; Newell, 2001; Solovy, 2000; Rao, Teran, & Savard, 2004; Khoumbati, Themistocleous, & Irani, 2006).

E-healthcare was recognized to have important potential benefits. However, researchers and practitioners also recognized potential risks involved in e-healthcare, which sometimes led to undesirable consequences. To fully realize the benefits of e-healthcare, information security had to be carefully considered based on risk assessment (Sweatt, Longnecker, & Sweeney, 2006; Wei & Loho-Noya, 2008; Lin, 2011; Oh, Choi, Ryoo, & Stokes, 2011). Based on the literature review, research on the assessment of information security in e-healthcare was rare. Recent research on e-healthcare security provided conceptual frameworks and descriptive analyses of risk factors (Kelly & Unsal, 2002; Sweatt et al., 2006; Wei & Loho-Noya, 2008; Wen & Tarn, 2001), but failed to provide methods for quantitative assessment. Quantitative methods are important when the level of security risks needs to be assessed, in particular in systems (re) design. In response to the call for both conceptualization and measurement, this paper develops conceptual models and provides a method for quantitative assessment (Sweatt et al., 2006).

The purpose of this paper is to identify information threats involved in e-healthcare and develop a quantitative assessment method to assess information security risks in e-healthcare. It aims at providing a holistic view of risk factors involved in e-healthcare by developing an E-Healthcare Information Security Risks (EHISR) model as a theoretical basis for risk assessment. The risk factors in the EHISR model are further analyzed based on the EHIF model. The relative-weight method is combined with the EHISR and EHIF models to provide a computational assessment model to measure e-healthcare security risks quantitatively. Specifically, the paper

- Provides a holistic view of security risks impacting the success of IT adoption in e-healthcare;
- Creates a model to conceptually analyze these security risk factors and logically link them together based on sources of security attacks;
- Provides pattern analysis and versatility analysis based on the conceptual models; and
- Provides a quantitative method to measure these risk factors in the model, and develops a risk assessment mechanism for high-level e-healthcare decision makers including executives, policy planners, and managers working on decisions regarding e-healthcare security, such as decisions on selecting a reliable information flow infrastructure with a lower level of information security risk.

The remaining of this paper is organized as follows: In the next section, literature review is presented. In the following section, two conceptual models are presented to statically identify information risk factors in e-healthcare based on five security risk problems and three threat sources, with a dynamic information flow model in e-healthcare to illustrate how information security risk factors are being presented in e-healthcare. In the section after, findings are discussed based on pattern analysis and versatility analysis. In the next section, one quantifiable approach based on a relative-weighted assessment model is developed to demonstrate how the security risks in e-healthcare can be measured and assessed. In the last section, discussions, management implications and conclusions are presented.

LITERATURE REVIEW

E-healthcare deeply affect the healthcare industry by providing solutions to the financial distress,