BMC Medical Informatics and Decision Making

RESEARCH ARTICLE

Open Access

Patients' perception of the information security management in health centers: the role of organizational and human factors

Hamid Reza Peikari[1], Ramayah T.[2], Mahmood Hussain Shah[3] and May Chiun Lo[4*]

Abstract

Background: Researchers paid little attention to understanding the association of organizational and human factors with patients' perceived security in the context of health organizations. This study aims to address numerous gaps in this context. Patients' perceptions about employees' training on security issues, monitoring on security issues, ethics, physical & technical protection and trust in hospitals were identified as organizational and human factors.

Methods: After the development of 12 hypotheses, a quantitative, cross-sectional, self-administered survey method was applied to collect data in 9 hospitals in Iran. After the collection of 382 usable questionnaires, the partial least square structural modeling was applied to examine the hypotheses and it was found that 11 hypotheses were empirically supported.

Results: The results suggest that patients' trust in hospitals can significantly predict their perceived security but no significant associations were found between patients' physical protection mechanisms in the hospital and their perceived information security in a hospital. We also found that patients' perceptions about the physical protection mechanism of a hospital can significantly predict their trust in hospitals which is a novel finding by this research.

Conclusions: The findings imply that hospitals should formulate policies to improve patients' perception about such factors, which ultimately lead to their perceived security.

Keywords: Security, Trust, Technical and physical protection, Monitoring, Training, Ethics

Background

Information security breaches result in an average of $7 Billion worth of losses every year in the healthcare industry [1]. This has motivated many researchers to conduct research from different perspectives with an aim to reduce the likelihood of security breaches and the costs associated with it. While the researchers in the field of computer science have explored the phenomenon of information security, most of them have studied the issue from the engineering perspective and focused on the development of technical solutions and neglected to study security from a behavioral approach [2]. Behavioral approach refers to studying the factors which shape individuals' perception and behavior towards the practice of information security in organizations. Therefore, this research intends to answer the following question: what are the anticipating factors of individuals' perceived security?

Investigating the antecedents of information security from the behavioral perspective is important because it plays an important role in evaluating and ensuring the level of information security. Indeed, since most individuals lack technical knowledge of the security technologies implemented, they assess the data protection levels of the organization based on some cues. This phenomenon is called perceived security. Therefore, in order to reduce individuals' concerns about the security of their information, the factors that play a significant role in shaping their perceived security should be enhanced.

* Correspondence: mclo@unimas.my
[4]Research & Innovation Management Centre (UNIMAS INNOVATION), Universiti Malaysia Sarawak (UNIMAS), 94300 Kota Samarahan, Sarawak, Malaysia
Full list of author information is available at the end of the article