TOWARDS AN ASSESSMENT OF CLOUD E-HEALTH PROJECT RISK: AN EMPIRICAL STUDY

Bouchaib Bahli

School of Information Technology Management, Ted Rogers School of Management, Ryerson University, Toronto, Canada

ABSTRACT

The introduction of information technology and telecommunications (ITC) in the health care sector has brought so many benefits to the health operators, managers, and patients. However, the increasing use and the application of ITC to the management and delivery of health care well known as e-health has been associated with several e-health risks that need to be examined. In this paper we point out several shortcomings of current risk conceptualization and operationalization, particularly they do not address the integration of a variety of risk components, which are crucial for capturing the essence of e-health risks. To fill this gap and drawing on risk analysis perspective we present and discuss a formal framework for e-health cloud computing project risks that captures potential scenarios, their likelihood and, the associated negative consequences. E-health risks were identified in the literature and a cluster analysis was used to classify different risks into several risk domains according to the developed e-health risk framework. Results show several domains including privacy, security, safety, liability, operational, project and business e-health risks. Implications for researchers and managers are also discussed.

KEYWORDS

e-health, e-health risks, risk assessment, health care management

1. INTRODUCTION

This document describes, and is written to conform to, author guidelines for the journals of AIRCC series. It is prepared in Microsoft Word as a .doc document. Although other means of preparation are acceptable, final, camera-ready versions must conform to this layout. Microsoft Word terminology is used where appropriate in this document. Although formatting instructions may often appear daunting, the simplest approach is to use this template and insert headings and text into it as appropriate.

The use of technology to assist in the delivery of quality patient care covers a vast areas from biomechanical devices to robotics to the electronic medical record to email. More particularly, Internet as a source of health information and connectivity between providers and payers has increased interest in e-health as a channel for the delivery of health-related products and services (Trudel et al; 2012). Of the 137 million Americans who surf the Internet, more than 60 percent use the resource for health advice (Harris, 2002). In addition, 90% of adults would like to be able to communicate with their physicians on line and the number of adults who have looked for health information has climbed from 54 million to 110 million (Harris, 2002). In the US alone the

Dhinaharan Nagamalai et al. (Eds) : ITCSE, WiMo, ICAIT, ICDIPV, CRYPIS - 2018
pp. 59–66, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.80706

move to a fully integrated e-Health system has been estimated to improve efficiency and reduce costs, saving some $81bn (Appari & Johnson, 2009). Sometimes, the term e-health has been used very loosely to include any electronic healthcare-related activity (DeLuca and Enmark, 2000). One widely definition of e-health is the one adopted by HIMSS' e-Health SIG (2003). E-health is defined as the application of Internet and other related technologies in the healthcare industry to improve the access, efficiency, effectiveness, and quality of clinical and business processes utilized by healthcare organizations, practitioners, patients, and consumers to improve the health status of patients.

The potential benefits of computerization are considerable. E-health systems can facilitate access to patients medical records, improve the quality of care and the accuracy of treatment decisions, achieve cost savings, and promote clinical research (Baron, 2005) and some health care providers with e-health systems already report better outcomes, fewer complications, lower costs, and fewer malpractice claim payments (Amarasingham et al. 2009). Without discounting any of these potential benefits, e-health systems continue to face challenges and associated risks within the health industry (Tsiknakis and Kouroubali 2009).

This paper focuses on the risks associated with e-health systems and on concerns associated with their use. We argue that despite the promise of this technology, the implementation of e-health systems must proceed with both caution and appropriate oversight. E-health systems give rise to new risks for health care providers and patients alike. Computerized information is vulnerable to large-scale privacy violations associated with hacking, computer theft, malicious electronic distribution, or accidental disclosure, such as sending a file to the wrong e-mail address. Once data security is breached, the most private information can be dispersed on the Internet to a worldwide audience (Hoffman and Podgurski, 2009). Disclosure of psychiatric or sexual histories or other sensitive information can, among other harms, lead to profound embarrassment, ruined careers, or loss of professional and personal opportunities. These, in turn, can generate litigation against those responsible for security breaches (Hoffman and Podgurski, 2009).

This study's contributions to research and practice are twofold. First, we point out several shortcomings of current risk conceptualization and operationalization and present a more comprehensive approach to risk assessment. Second, we present and discuss e-health risks and map them into the developed risk framework. Our framework provides a step further in systematically assessing e-health risks and provides health operators and managers with a tool that captures a variety of potential scenarios, their likelihood and, the associated negative consequences. Further, we discuss both research and practical implications of this framework, research limitations and further research. The rest of the paper is organized as follows. First, we provide the theoretical foundation for the study. Second, we present the research developed e-health risk framework. Next, we discuss the implications of this framework for research and practice, study's limitations and directions for further research.

2. E-HEALTH RISK: A CONCEPTUALIZATION

For many health care organizations that are providing health services to patients, doctors, nurses, health operators, etc, one real concern is that of the risks associated with conducting transactions through electronic channels (Baker et al., 2005). While the risk construct itself has been conceptualized and measured across disciplines (Bahli and Rivard, 2003), the e-health literature suggests that the conceptualization and measurement of e-health risks is yet to be examined in a formal manner. The first objective of the present research is to refine and validate the conceptualization and measurement of e-health risk in a comprehensive research framework embedding the different types and categories of e-health risks. The term risk is likely to be one of

the most often used words in modern language. Every day, in extremely different circumstances, people use the term risk, be it to talk about the probability of a snowfall or the variability of their investments (Bahli and Rivard, 2003). Risk is defined along a decision theoretic view as the likely variability of future returns from an asset, equity or investment. The behavioural perspective associates risk with the magnitude of a negative consequence of a decision. In this view, a risky choice is one that contains a threat of poor performance. In information systems, the notion of risk exposure – that is, the combination of the probability of occurrence of an undesirable event and the amount of loss related to this event – is often used (Boehm, 1991; Barki et al., 2001).

In their widely cited paper entitled "On the Quantitative Definition of Risk," Kaplan and Garrick (1981) criticized the fact that researchers often took into account the sole probability of occurrence of an undesirable event in defining risk. Furthermore, the traditional expected consequence representation of risk (generally referred to as risk exposure) is deemed inappropriate by Kaplan and Garrick since this representation assumes a risk-neutral decision maker. According to these authors, most people would rather judge a low-probability-high-consequence scenario as more undesirable than a high-probability-low consequence scenario even if the expected consequences of the two events were equal. In other words, this means that concepts like frequency-severity diagrams have the undesirable property that very different situations, among which a rational risk adverse decision maker might have clear preferences, could be mapped into identical diagrams. Rather, Kaplan and Garrick argued that three questions ought to be addressed in order to assess risk. These questions are: what can happen? (i.e., What can go wrong?), how likely is it that will happen?, if it does happen, what are the consequences?. Kaplan and Garrick proposed a general definition of risk as a complete set of triplets involving scenarios (what can happen?), the likelihood of each scenario (how is it likely to happen?), and the consequences or evaluation measure of each scenario, that is, the measure of damage. "To answer these questions we would make a list of outcomes or "scenarios" as suggested in Table 1. The ith line in Table 1 can be thought of as a triplet:

< pi, si, xi>

Where si is the scenario, pi is the probability of that scenario, xi is the consequence

Table 1. Scenario List (Kaplan and Garrick, 1981)

Likelihood	Scenario	Consequence
p1	s1	x1
pn	s2	x2
.	.	.
.	.	.
.	.	.
pn	sn	xn

This conceptualization of risk seems to be more appropriate for the present study in two ways: First, it allows capturing several scenarios that may emerge due to the use and application of e-health systems, the likelihood of these scenarios happen and, the associated negative consequences. Second, managers can visualize a series of triplets and decide which scenarios need to be avoided or attenuated and select appropriate measures to mitigate them. The following section presents an application of Garrick and Kaplan's risk framework to capture e-health risks. A cluster analysis was used on a variety of e-health risks in the literature. The results were then mapped into Garrick and Kaplan's risk framework.

3. DESIGN AND METHOD

The proposed research consists of surveying 10 IT managers in the health sector in Croatia. These managers had no obligation to respond to our questions and they were not evaluated to do so, hence, reducing research bias. The average years of experience in the IT field was 8.65. The managers come from the health sector: Pharmaceutical (6), biotechnology industry (2), hospitals (2). The selected 10 managers were chosen because of accessibility opportunity and it took four seminars to identify them. Our choice was partly opportunistic, in that these managers attended a seminar on IT risks, thus making accessibility less of a problem. More importantly, these managers met our criteria of suitable cases on e-health projects. These managers were involved at different degrees in e-health projects of their organizations.

After explaining the concept of risk and its components as suggested by Kaplan and Garrick (1981), we asked the respondents about their perceptions on the potential e-health project risks. For instance, if one manager perceived a certain type of e-health risks he or she needs to explain what constitutes their judgment. All responses were transcribed, interpreted and analyzed. The following section describes the data analysis process. We limit our study to the mapping of all e-health risks into the RISC framework.

Categorical analysis attempts to make valid inferences from studied texts to their underlying meaning in terms of pre-specified set of categories (Weber 1985). The goal for using categorical analysis was to develop a systematic representation of the different categories of e-health project risks and thereby to reveal their varying foci and rationale. As recommended by Glaser and Straus (Glaser and Straus, 1967), we have produced some explanations of theoretical concepts and patterns (Orlikowski, 1993) of each of the risk categories. Three steps are required: (1) initial analysis of transcripts where the responses were transcribed and analyzed. We highlighted comments about managers' perceived e-health project risks. (2) Interpretation of transcripts to dissect patterns in responses. (3) Analysis of the interpretations. Two people performed this task individually, then, we corroborate both analyses as suggested by Tesch (1990) in order to decontextualize comments. Both individuals agree on the labeling of each level. The coding was conducted by classifying every risk factors, scenario and consequences using RISC components. Before actual coding, we agreed on a number of coding rules. Each risk component was assigned to one RISC coding scheme. The coding was based on component content description. Sometimes this lead to a further reading of the component description in the main body of the text to further clarify its meaning. In our situation, this analysis technique helps clarify the e-health risk categories. In particular, categorical analysis reveals several groups or risk domains. Then, within each domain, we identified scenarios, risk factors and the associated consequences. Several risk domains were identified: privacy risks, security risks, litigation and liability risks, safety risks, project risks and, operational risks.

Privacy Risks include the unauthorized collection, use and disclosure of personal health information and, any threat to the ability of the patient to exercise any right under privacy legislation (Karsh et al. 2006). Computerized information is vulnerable to large-scale privacy violations associated with hacking, computer theft, malicious electronic distribution, or accidental disclosure. Once data security is breached, the most private information can be dispersed on the Internet to a worldwide audience (Hoffman et Podgurski , 2009).

Security Risks are breaches of confidentiality, integrity and availability of personal health information and/or critical health information systems (Kolkowska, Hedstrom, & Karlsson, 2009). Security risks include the loss, corruption or unauthorized modification of personal health information and; loss of critical ICT services (Baker et al., 2005). Security of data in medical applications is particular complex because patient data is typically fragmented controlled by

whoever provided health services. Moreover, the security mechanism must be arranged so that users can quickly share information in the event of an emergency (Lorence and Churchil, 2005). On the other hand many healthcare professional are reluctant to use information and communication tools due to the security risks entailed.

Safety risks include physical or mental harm to patients and health care providers (including death). Safety Risks. Patient injury or death, health provider injury or death and Population injury or death (Karsh et al., 2006). Security issues are the most likely sources of e-health safety problems. Integrity and availability issues could certainly impact patient and health provider safety (Lohr et al. 2009), particularly as we become more dependent on e-health programs. Consider what could happen to a patient if a security breach brought down an e-health portal that provided access to critical health information systems or a software bug that causes a lab system to deliver inaccurate test results (Balka et al. 2006). Human factors issues – where the human/information system interface fails. This could include user interfaces that are confusing, overly complex procedures that promote error or failure to catch common user errors (e.g. input procedures that make it easy to enter the wrong data or displays that make it easy to misinterpret data).

Patients who learn that their medical information has been inappropriately disclosed to third parties may be inclined to sue their physicians. In fact, patients might initiate litigation not only when the physician has carelessly or intentionally disclosed private information, but also when the disclosure occurred because of hacking or a system defect (Hoffman and Podgursk, 2009). Use of e-health systems could generate negligence claims against providers for a variety of reasons. EHR system operation can be time-consuming and burdensome, and increased work demands could cause rushed physicians to make medical mistakes. Greater access to existing diagnostic data and economic pressures to avoid duplicating tests could lead to errors from inappropriate reliance on outdated or inadequate prior testing. Mistakes may also result from data entry errors (Hoffman and Podgursk, 2009).

Project risks include cost overruns, scope creep, unacceptable delays, failure to deliver required functionality or project failure (Balka et al., 2006). Heeks (2006) estimated that 20-25 percent of IT projects in healthcare are total failures and 33-60 percent are partially successful. This is attributed to poor IT investment decision making and to the increasing complexity of IT implementations in recent years (Trudel, Paré & Laflamme, 2012). Prior research shows that the management of IS projects is often marked by inadequate planning, a poor grasp of the overall development process, and no clear management framework, even as the focus shifts from a technology perspective to a more process-centric view (Agarwal and Rathod, 2006). .

Operational risks include incompatible technology, obsolescence, inability to meet service levels, lack of skilled human resources (Barki et al. 2001). While an e-health project will end, the e-health program will extend through time until the program is eventually replaced or retired. The operations phase is the phase in which identified benefits will materialize. During this phase threats to the continuing success of the program may materialize (Schabetsberger et al. 2006). There is a close relationship between operational risks and security risks. Adapting the security threat and risk assessment methodology to address broader operational risks would address many of the issues arising in the operational environment (Garg et al, 2005).

Table 2. E-health Risk Framework

Risk Type	Risk Factors	Scenarios	Consequences
Privacy Risks	Weak patient consent procedures	Unauthorized collection Unauthorized use Unauthorized disclosure Denial patient rights	Loss damage of the patient privacy
Security Risks	Malicious use or attack Natural IT service failure	Loss of personal health information Unauthorized modification of health information Loss of critical IT services	Loss damage of the patient security
Saftey Risks	Critical failure of IT services Failure to communicate critical safety procedures	Patient injury or death Health provider injury or death Population injury or death	Loss damage of the patient safety
Liability Risks	Litigation Political constraints User resistance Loss of critical resources	Legal liability Financial loss Business interruption External interefernces Rejection by users	Loss damage of the business
Project Risks	Unrealistic expectations Resources not available Scope creep Poor budgeting	Scope compromise Time delay Cost overrun	Loss damage of the project failure
Operational Risks	Poor maintenance Systems obsolescence Lack of skilled resources	Loss of service	Loss damage of the operational business

4. PRACTICAL IMPLICATIONS AND EXPECTED CONTRIBUTIONS

The proposed research paper contributes to a better understanding of how e-Health risk is defined and measured. It also provides a formal tool for the assessment of e-Health risks. The identification of the components of e-Health risk is based on Seaton (2007) categorization of risks. We mapped this categorization into the risk framework developed by Garrick and Kaplan (1981). The proposed research will contribute to both research and practice. For research, the main contribution is to further our understanding of how e-health risk components are modeled. In addition, this research could contribute to the field of e-health by providing a better understanding of risk in general and e-health risks in particular. For practice, understanding the polymorphism of risk could help healthcare organizations more adequately and fully exploit the benefits of e-health systems. From this research it can be seen that while e-health systems are bringing many benefits to the work flow and practices of these health care practitioners, there is a need for further development of the technology in order for it to fulfil its potential and truly achieve a categorisation of success as indicated by user satisfaction with e-health systems.

REFERENCES

[1] Agarwal, N. and Rathod, U. 2006. Defining "success" for software projects: An exploratory revelation. International Journal of Project Management, 24, pp. 358-370.

[2] Appari, A. and Johnson, E. 2010. Information security and privacy in healthcare: current state of research". Int. J. of Internet and Enterprise Management, 6, 4, pp. 279-314.

[3] Amarasingham, R et al. 2009. Clinical Information Technologies and Inpatient Outcomes: A Multiple Hospital Study. Archives of Internal Medicine, 169, 2, pp. 108-114

[4] Baron, J. et al. 2005. Electronic Health Records: Just around the Corner? Or over the Cliff?. Annals of Internal Medicine, 143, 3, pp. 222-226.

[5] Bahli, B. and Rivard, S. 2003. The information technology outsourcing risk: a transaction cost and agency theory-based perspective. Journal of Information Technology, 18, pp. 211-221

[6] Baker et al. 2005. The Canadian adverse events study: the incidence of adverse events among hospital patients in Canada, CMAJ, 170, 11, pp. 1684-1689.

[7] Balka et al. 2006. Technology, governance and patient safety: Systems issues in technology and patient safety, International Journal of Medical Informatics, 76, pp. 35-37.

[8] Boehm, B.W. 1991. Software risk management: principles and practices. IEEE Software, 12, pp. 32-41.

[9] Currie, W and Finnegan, D. 2011. The Policy- Practice Nexus of Electronic Health Records Adoption in the UK NHS: An Institutional Analysis. Journal of Enterprise Information Management, 24, 2, pp. 146-170.

[10] Currie, W and Guah, W.M. 2007. A national program for IT in the organisational field of healthcare: A Example of Conflicting Institutional Logics. Journal of Information Technology, 22, 3, pp. 235-248.

[11] DeLuca, J & Enmark, R. 2000. "E-Health: The Changing Model of Healthcare," Frontiers of Health Services Management, Vol. 17, No. 1, pp. 3-15.

[12] Garg et al. 2005. Effects of computerized clinical DSS on practitioner performance and patient outcomes: A systematic review, JAMA, 293, 10, pp. 1223-1232.

[13] Hair, J., Black, W., Babin, B., Anderson, R., and Tatham, R. 2006. Multivariate Data Analysis, 6th ed. Pearson Prentice Hall, Upper Saddle River, New Jersey.

[14] Harris Interactive, 2002; Boston Consulting Group, US.

[15] Heeks, R. 2006. Health information systems: Failure, success and improvisation. International Journal of Medical Informatics, 75, pp. 125-137.

[16] HIMSS, 2003. "Section II: National Preparedness & Response (NPR)" and "Section IV:National Health Information Infrastructure (NHII)," HIMSS Advocacy Dispatch, www.himss.org.

[17] Hoffman S, Podgurski A. 2009. E-Health Hazards: Provider Liability and Electronic Health Record Systems. Berkeley Technology Law Journal. 24, 4, pp. 1523-1581.

[18] Kolkowska, E., Hedstrom, K., & Karlsson, F. 2009. Information Security Goals in a Swedish Hospital. In G. Dhillon (Ed.), Proceedings of the 8th Annual Security Conference Discourses in Security Assurance and Pri-vacy, pp. 16,111.

[19] Kaplan, S and Garrick, B.J. 1981. On the Quantitative Definition of Risk, Risk Analysis, 1, 1, pp. 11-27.

[20] Karsh et al. 2006. A human factors engineering paradigm for patient safety: designing to support the performance of the healthcare professional, Qual Saf Health Care. 1 pp. i59–i65.

[21] Lohr, H; Sadeghi, A; Vishik, C; Winandy, M. 2009. Trusted privacy domains { challenges for trusted computing in privacy-protecting information sharing. In Information Security Practice and Experience, 5th International Conference, (ISPEC'09), vol 5451 of Lecture Notes in Computer Science, pp. 396-407.

[22] Lorence, D. and Churchill, R. 2005. Incremental adoption of information security in health-care organizations: implications for document management. Information Technology in Biomedicine, IEEE Transactions on, 9, 2, pp.169–173.

[23] Schabetsberger, T; Ammenwerth, E; Andreatta, S; Gratl, G; Haux, R; Lechleitner, G; Schindelwig, K; Stark, C; Vogl, R; Wilhelmy, I; Wozak, F. 2006. From a paper-based transmission of discharge summaries to electronic communication in health care regions. International Journal of Medical Informatics, 75, pp. 209-215.

[24] Seaton B. 2007. Managing e-health Risks and Opportunities. In Proceedings of Annual OACCAC Conference (Ontario Association of Community Care Access Centres), Toronto, Ontario.

[25] Smaltz, D. H., Carpenter, R., & Saltz, J. 2007. Effective IT governance in healthcare organisations: a tale of two organisations. International Journal of Healthcare Technology Management, 8, 2, pp. 2-17.

[26] Trudel, M.; Paré, G. & Laflamme, J. 2012. Health information technology success and the art of being mindful: Preliminary insights from a comparative case study analysis. Health Care Management Review, Vol 37, Issue 1, pp 31–42.

[27] Tsiknakis, M., and Kouroubali, A. 2009. "Organizational Factors Affecting Successful Adoption of Innovative E-health Services: A Case Study Employing the Fitt Framework," International Journal of Medical Informatics, 78, 1, pp. 14.