Decision Support Systems 61 (2014) 1–11

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Optimal information security investment in a Healthcare Information Exchange: An economic analysis

C. Derrick Huang *, Ravi S. Behara, Jahyun Goo

Department of Information Technology & Operations Management, College of Business, Florida Atlantic University, Boca Raton, FL 33431, United States

ARTICLE INFO

Article history:
Received 6 March 2013
Received in revised form 11 September 2013
Accepted 25 October 2013
Available online 8 November 2013

Keywords:
Healthcare Information Exchange
Healthcare information technology
Information security
Optimal investment
Scale free network

ABSTRACT

The complexity of the problem, the increasing security breaches, and the regulatory and financial consequences of breached patient data highlight the fact that security of electronic patient information in Healthcare Information Exchanges (HIEs) is an organizational imperative and a research priority. This study applies classical economic decision analysis techniques and models the HIE based on its network characteristics to offer key insights into the issue of determining the optimal level of information security investment. We find that for an organization in a HIE, only security events with the potential loss reaching some critical value are worth protecting, and organizations would only spend a fraction of the intrinsic security risk on protection measures. Even when business benefit from security investment exists, organizations in a HIE tend to invest based on risk reduction alone. The implications of such decisions made at the node level and the resulting built-in moral hazard at the HIE level is discussed.

1. Introduction

The Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009, unleashed a major IT overhaul of the entire healthcare sector in the United States. Along with the promised benefits, however, came the challenge of safeguarding patient information in the digital world [42]: In 2010 and 2011, based on the Department of Health and Human Services (HHS) mandated public notification of breaches involving 500 or more patient records, more than 16 million individuals have been affected by healthcare data breach [80]. In a benchmark study on patient privacy and data security [59], 28% of the respondents have no staff dedicated to managing data protection, while 35% have fewer than two such dedicated staff. It was estimated that data breaches of patient information cost healthcare organizations nearly $6 billion annually, and that many breaches go undetected [59].

Healthcare organizations are just beginning to appreciate the scale and impact of the information security problem. Decision makers are faced with the multitude of technical and economic issues involved in securing their data and systems. This is further compounded by the fact that there are many health care providers and organizations, including some small, unsophisticated players, involved that handle, share, and coordinate care [42] via a Health Information Exchange (HIE), the electronic network for sharing health-related information among organizations according to nationally or regionally recognized standards. The complexity of the problem, the increasing security breaches, and the regulatory and financial consequences of breached patient data, taken together, highlight the fact that security of electronic patient information in HIEs is an organizational imperative and a research priority [9]. Although recent research has shed light on the understanding of security risks in such a healthcare environment, it is limited when it comes to informing the responses by member organizations in a HIE to these risks. This paper represents an effort to address this research gap by examining a key aspect of the management of information security by an organization in a HIE, namely the decision on how much to invest to defend itself against such adversarial events, given the security risks that it faces.

Given that no organization can be completely secure without unlimited budget, it is important for an organization to know what the "right amount" of investment is, before it attempts to engage in defensive mechanisms. In this study, we address the question of optimal level of information security investment by an organization in a HIE, given the security threat it faces and the network environment it is in. We apply classical economic analysis to examine the interaction between the organizational investment decisions and the security risks, modeling the HIE based on its network characteristics with a priori network principles. Further, in addition to the common approach of treating security measures as risk-reduction mechanism, we also consider the business benefits that security investment would bring to an organization and how they would affect the investment decision. As such, our study offers insight into how an organization in a HIE could manage its investment in information security based on a variety of threat environments and systems configurations as well as the impact of individual investment decision on the HIE as a whole.

* Corresponding author. Tel.: +1 561 297 2776.
E-mail addresses: dhuang@fau.edu (C.D. Huang), rbehara@fau.edu (R.S. Behara), jgoo@fau.edu (J. Goo).

0167-9236/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.dss.2013.10.011

The remainder of this paper is organized as follows. The next Section 2 provides research background on HIE and its information security characteristics from existing literature. Next, a model is constructed to study information system security for an organization in a HIE network. We then use the model to derive the optimal investment based on risk reduction as well as business benefits brought on by information security measures. Finally, we offer managerial insights and implications for future research based on our findings.

2. Research background

2.1. Health Information Exchange

The term Health Information Exchange, or HIE, has emerged as the common description for systems that facilitate sharing of an individual's personal health records among healthcare service providers. Such a timely sharing of information is considered to be an important contributor to the improved quality and safety of care, while reducing delivery costs. It is estimated that a fully standardized HIE at the national level could yield a net benefit of over $70 billion a year [70].

In the U.S., HIE depends on local and regional organizations that bring together stakeholders with healthcare data and set up joint infrastructure. Specifically, the following network terms have been defined by the National Alliance of Health Information Technology for the U.S. Federal Government [54]:

- Health Information Exchange (HIE): The electronic movement of health-related information among organizations according to nationally recognized standards.
- Health Information Organization (HIO): An organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards.
- Regional Health Information Organization (RHIO): A health information organization that brings together health care stakeholders within a defined geographic area and governs health information exchange among them for the purpose of improving health and care in that community.

Although HIE started early, the progress has been slow. A 2009 survey, for instance, found that most RHIOs focused only on exchanging test results as opposed to a comprehensive clinical data and suffered a fairly high failure rate of about 25% over the course of 18 months [2]. Along with costs, leadership, and interoperability, security and privacy concern is cited as a major barrier to the growth of HIE [15,26]. HIE participants have expressed discomfort with issues related to privacy, security, data ownership, data control, and liability [1]. Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules that have been in force to protect individually identifiable health information have been adapted to individual electronic health records (EHR) at the provider's level, but HIEs poses new issues and involves organizations that were not contemplated at the time the rules were developed. HITECH Act requires HIEs to be subject to the breach notification rule as a business associate. This, along with other legal and contractual obligations, provides incentives to the organizations in a HIE to prevent and manage breach of their data and information systems [3]. However, with the ownership and the responsibility of HIE security unclear, further analysis and study of the security investment by organizations in a HIE are necessary.

2.2. Information security investment

For any organization, questions regarding information security investment can be summarized in three key issues: 1) the optimal amount of information security investment, 2) in what measures to invest, and 3) how to make the investment effective. Several research streams attempt to address these three issues independently.

The first question of optimal level of information security investment is often addressed via the traditional decision analysis to compare the risk and return of investments. This approach, though widely adopted for evaluating IT investments, is complicated by the fact that the "return" of security investment does not usually come from increased revenues or decreased costs like other IT investments do, but from managing and reducing the security risks that an organization is facing [7,76]. Such risk analysis can be based on the measurement of security risk = (likelihood of loss event) * (cost of loss event) [63] or more complex variations such as the value-at-risk approach [50,73]. Based on this formulation of risk, Gordon and Loeb [28] in their seminal paper analyze the economics of security investment for a risk-neutral organization by comparing the cost of the investment and the potential loss caused by possible security breaches. They find that the optimal security investment would be far less than (with a theoretical maximum of less than 40% of) the potential loss if a security breach does happen, and that the optimal security investment does not necessarily increase with system vulnerability. In extending the Gordon and Loeb model, Huang et al. [38] adopt the expected utility theory to study the behavior of a risk-averse decision maker and find that there exists a minimum potential loss for non-zero optimal information security investment; above that minimum, optimal investment increases with potential loss. In addition, contrary to the risk-neutral case, a risk-averse decision maker may continue to invest in information security until the spending is close to (but never exceeds) the potential loss.

After the amount of investment is determined (by optimization, budget, or other constraints), an organization needs to decide what security measures to invest in. Often, selection of the right investments is aided by traditional management tools such as cost-benefit analysis [30] and financial analyses based on such measures as return on investment (ROI), net present value (NPV), and internal rate of return (IRR) [14,29,35,60,67]. Studies have proposed other decision analysis methodologies for selecting the right security investments. For instance, analytic hierarchical process (AHP) employs pair-wise comparisons among different security technologies to determine the priority of implementation [13]. Arora et al. [10] propose to value security investments by associating bypass rate with each of the security technologies adopted at an organization. And Kumar et al. [46] propose a model to use NPV generated by each countermeasure to evaluate an information security portfolio. Alternatively, the issue of selecting and prioritizing security technologies can be treated as optimizing the allocation of the limited security investment. Taking such an approach, Viduto et al. [69] propose a risk assessment and optimization model for the selection of security countermeasures to minimize financial costs and risks. Sawik [62] formulates the problem of selection of countermeasures based on their effectiveness, costs, and attack probabilities using a bi-objective trade-off model in a scenario-based analysis. He finds that the selected portfolio of security measures depends explicitly on preferred confidence level and cost-risk preference of the decision maker. Huang and Behara [37] propose an analytic model for security investment allocation that considers simultaneous attacks from multiple threat agents with distinct characteristics. Their analysis shows that an organization is better off allocating most or all of the investment to defending against one type of attack when its security budget is small. Further, an organization should focus on technologies against targeted attacks when its information systems are highly connected.

The third aspect of security investment is its performance. In addition to the common operational and procedural issues of technology deployment, an important issue for an effective security investment is its ability to configure and adapt to the adversarial conditions that an organization faces, and game theory can be a useful tool for such consideration. From a methodological perspective, game theoretic approach is best suited for modeling the performance of a specific security technology with limited rounds (often two or three) of actions and reactions by a limited number of players (often the organization and the attacker). Using this approach to evaluate intrusion detection systems (IDS),