Int. J. Production Economics 114 (2008) 793–804

Contents lists available at ScienceDirect

Int. J. Production Economics

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

An economic analysis of the optimal information security investment in the case of a risk-averse firm

C. Derrick Huang *, Qing Hu, Ravi S. Behara

Department of Information Technology and Operations Management, College of Business, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, USA

ARTICLE INFO

Article history:
Received 7 March 2007
Received in revised form
21 February 2008
Accepted 7 April 2008
Available online 16 April 2008

Keywords:
Information security
Optimal investment
Expected utility theory

ABSTRACT

This paper presents an analysis of information security investment from the perspective of a risk-averse decision maker following common economic principles. Using the expected utility theory, we find that for a risk-averse decision maker, the maximum security investment increases with, but never exceeds, the potential loss from a security breach, and there exists a minimum potential loss below which the optimal investment is zero. Our model also shows that the investment in information security does not necessarily increase with increasing level of risk aversion of the decision maker. Relationships between vulnerability and investment effectiveness and two broad classes of security breach probability functions are examined, leading to interesting insights that can be used as guidelines for managers to determine the optimal level of security investment for certain types of security threats faced by risk-averse firms. Future research directions are discussed based on the limitations and possible extensions of this study.

1. Introduction

If the theme of IT management in the 1990s can be characterized as investing for competitive advantage and strategic necessity, then that of the 2000s might be described as ensuring information and systems security. Computer worms and viruses, spyware, cyber attacks, and computer system security breaches are common occurrences and have resulted in financial losses amounting to billions of dollars worldwide (Denning, 2000). High profile attacks on firms, such as Microsoft, eBay, Yahoo, and Amazon.com, and government agencies, such as Department of Defense and Federal Bureau of Investigation, made regular headlines (Kesan et al., 2004). In a CSI/FBI survey, over 75% of the respondents report some kind of security breaches in 2005 (Gordon et al., 2005). As a result, firms, large and small, are investing heavily in information and network security technologies to reduce the likelihood of major damages caused by security problems. It is estimated that US companies spent on average $196 per employee per year on security (Geer et al., 2003); a survey of more than 1000 US corporation shows that companies spent on average 20 percent of their total technology budget in 2006 on security measures, up from 12 percent in 2004, and nearly one-half of those surveyed planned to continue to increase IT security spending (CompTIA, 2007).

In the race to secure data and systems, research conducted by practitioners and academics has primarily focused on the technical and behavioral aspects of information security; rigorous analyses based on economic principles are rare. This is understandable, because information security investments usually do not generate direct monetary benefits such as higher revenues or lower costs; their main contribution is to prevent potential economic loss from happening. However, given the high cost of information security and the fact that a "completely secure organization" is an insurmountable, if not impossible, goal in today's networked economy, one critical question in determining the investment in security is, "What is the right amount of investment?" In other words, a firm needs to determine the most effective level

* Corresponding author. Tel.: +1 561 297 2776.
E-mail address: dhuang@fau.edu (C. Derrick Huang).

0925-5273/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.ijpe.2008.04.002

of information security investment, based on the nature of the information sets it intends to protect, the vulnerability of its information systems, the potential loss associated with a security breach if it does occur, and the security environment that it faces. Recent academic research in the economics of information security, albeit limited, intends to address this issue. Some scholars argue that there exists an optimal level of security investment for a given security vulnerability and threat environment of each organization. Investing less than that optimal level will result in unacceptable security risks; on the other hand, investments exceeding the optimal level do not bring justifiable returns for the investment (Gordon and Loeb, 2002; Soo Hoo, 2000).

In this study, we apply classical economic theories to offer new insights into the issue of determining the optimal level of information security investment. We model the decision maker of a firm as risk-averse, and adopt the expected utility theory to determine the security investment level that maximizes the utility of the investment. This theoretical approach yields results that shed lights on how a firm could manage its investment in information security based on different characteristics of threat environments and system configurations.

The rest of the paper is organized as follows. In Section 2, we review the literature on the economics of information security investment and introduce the background of our research. We then establish the foundation of the security investment model based on the utility function approach and the risk-aversion assumption. In Section 3, the model is applied to derive the boundary condition of maximum level of security investment. In Section 4, the optimal security investment levels are determined using the two classes of security breach probability functions proposed by Gordon and Loeb (2002), and we discuss both the mathematical results and the practical implications of our findings. Finally, this paper concludes by pointing out the limitations of this study and future research directions and potential ways of extending and improving our model (Section 5).

2. Research background

Amid the proliferation of the use of information technology in businesses and organizations, the management and planning of information security had been identified as an important issue in MIS research more than a decade ago (Niederman et al., 1991). A stream of literature on this subject has since been established (Loch et al., 1992; Straub, 1990; Straube and Welke, 1998). Unlike most IT investments, information security measures, be they technical or procedural, exhibit some unique economic characteristics. First, the benefits of such investment do not come from "making something happen" by enabling a strategy or enhancing an operation, but from the prevention and/or reduction of potential losses caused by security breaches. The "free rider" problem, in which many stakeholders (departments in a firm, for example) would usually not contribute to such efforts while expecting to enjoy others' contributions, is prominent in information security (Varian, 2000). Further, this information warfare, as Anderson (2001) puts it, is imbalanced: even very modest resources of the attackers can create huge threats to firms trying to fend off potential attacks, despite the latter's extensive monetary and technical resources.

To address these issues, a number of analytical frameworks for evaluating information security investment have been proposed. Dutta and Mccrohan (2002) follow a traditional, sequential cost–benefit analysis, starting with identifying the assets and financial consequences and risks of a security breach, followed by estimating the cost of implementing proper mechanisms to enhance the security of the assets in questions, and finally comparing the benefits of such mechanisms with the risks and estimated cost. In determining the appropriate level of investments, Cavusoglu et al. (2004) propose a game tree approach, spanning the three components of the IT architecture for security—prevention (such as firewall), detection (such as intrusion detection system), and response (such as manual monitoring)—that takes into account the interaction between a firm and potential hackers. Bodin et al. (2005) adopt the rating method of the analytic hierarchy process to determine the optimal allocation of information security investment budget. Purser (2004) examines the security investment and management from a business return on investment perspective. Schechter (2004) uses the threat-scenario approach to find the market price for vulnerability in software and to forecast risks posed by new threats. Soo Hoo (2000) provides a decision analysis framework for the evaluation of various IT security policies, which are baskets of security control measures.

In addition to these decision-theory-based evaluation methods, rigorous analyses that examine and interpret information security investments based on economic theories and principles start to emerge. Being a relatively new area of research, however, the literature in this stream is sparse. There are basically two approaches (Cavusoglu, 2004). The first is to use game theory—commonly used to examine the attacker's behavior, e.g., Lu et al. (2005)—to model the strategic interaction between a firm that protects its information sets and attackers attempting to access or damage the information illegally. Using this approach to evaluate intrusion detection systems, Cavusoglu et al. (2005) find that investing in such a technology provides a positive return to a firm only when the detection rate is higher than a critical value determined by the cost and benefit parameters of the hackers. In general, configuration of intrusion detection systems using game theory results in lower cost than configuration using decision theory, if firms can effectively estimate attackers' utility parameters (Cavusoglu and Raghunathan, 2004). From the methodological perspective, game-theory approach is best suited for modeling the outcome of a specific security technology with limited rounds of actions and reactions by a limited number of players (often the firm and the attacker).

The other approach is to use the traditional risk-return analysis that is common in management and economics