Int. J. Production Economics 141 (2013) 255–268

Contents lists available at SciVerse ScienceDirect

Int. J. Production Economics

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

# Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints

C. Derrick Huang *, Ravi S. Behara

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

ARTICLE INFO

*Article history:*
Received 28 October 2011
Accepted 19 June 2012
Available online 3 August 2012

*Keywords:*
Cost benefit analysis
Information security
Investment analysis
Budget allocation
Scale-free network

ABSTRACT

In this study we develop an analytic model for information security investment allocation of a fixed budget. Our model considers concurrent heterogeneous attacks with distinct characteristics and derives the breach probability functions based on the theory of scale-free networks. The relationships among the major variables, such as network exposure, potential loss due to a security breach, investment effectiveness, and security investment levels, are investigated via analytical and numerical analyses subject to various boundary conditions. In particular, our model shows how a firm should allocate its limited information security budget to defend against two classes of security attacks (targeted and opportunistic) concurrently. Among the results of these analyses, we find that a firm with a limited security budget is better off allocating most or all of the investment to measures against one of the classes of attack. Further, we find that managers should focus the security investment on preventing targeted attacks when the information systems are highly connected and relatively open and when the potential loss is large relative to the security budget.



## 1. Introduction

In the era of commoditization of information technology (IT) and globalization of the world economy, it is argued that the most challenging aspect of managing today's networked organizations is not so much about using IT to create competitive advantages in the marketplace but about managing the potential risks created by IT (Alter and Sherer, 2004; Carr, 2003; Goel and Chen, 2008). Among the risks, security breaches of the corporate information systems are perhaps the most prominent and visible, as evidenced by the headlines of mass media in recent years. It is estimated that the total cost to a company of recovering from a single data breach could exceed $6 million (Ponemon Institute, 2009), and that these breaches have resulted in billions of dollars of financial losses in the U.S. alone and possibly trillions worldwide (Mercuri, 2003). The common (and seemingly rational) reaction to this growing risk has been to increase spending on information security technologies. However, it is also recognized that complete information security at the corporate level is virtually impossible without hindering the normal business activities in today's economy, where connectivity to external business partners and customers is essential (Bellovin, 2001, Kumar et al., 2000). As a result, some recent studies have focused on the determination of return on security investments (Arora et al., 2004, Cavusoglu et al., 2004) and the economics of security investment under different attack scenarios (Gordon and Loeb, 2002; Huang et al., 2008a) to provide guidance to firms on optimizing security investment given the unattainable state of complete security.

Prior studies on information security investments give insight into optimizing investments based on system parameters, attack conditions, and investment return, with two key assumptions: (1) Firms defend against separate and individual attacks one at a time and (2) Firms invest in security solely based on optimization without budget limitation. In reality, firms often face various types of security challenges concurrently, each with different attack characteristics and requiring different defense mechanisms. Additionally, a firm's ability to invest in information security, or everything else for that matter, is limited by its finances. In particular, information security has to compete with other projects for funding, and its share of the total IT budget has trended downwards recently (Karr, 2006). Given the multitude of concurrent heterogeneous attacks and budget limitations, the greater challenge to managing information security investment is not so much the total investment level needed, but the allocation of the finite resources to defend against different classes of attacks.

In order to produce relevant results, this study aims to close the research gaps described above by adopting a more practical set of assumptions. To do so, we examine the allocation of security

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

0925-5273/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijpe.2012.06.022

investment to defend against concurrent heterogeneous attacks on a firm's information system. We also take a firm's ability to invest into consideration in the form of budget constraints. Further, we derive breach probabilities for different classes of attacks based on the concept of scale-free networks, a theoretically robust and empirically validated framework (Albert et al., 1999, 2000; Barabási and Albert, 1999). Our analysis produces the following interesting findings: (1) when a firm has limited security budget (relative to the potential loss), it should concentrate its security investment on defending against one class of attacks, even if the threats from other classes of attacks exist; (2) when its information systems have high connectivity to the outside world, a firm is better off allocating more of its security budget towards targeted attacks than opportunistic attacks; and (3) when investments have cross-over effects on other classes of security attacks, security measures with higher impact on other attacks should receive higher allocation, regardless of systems characteristics and attack conditions. Detailed derivations and discussions of these findings can be found in later sections.

The rest of the paper is arranged as follows. We first review the literature on economics of information security that addresses optimal resource allocation problems and the theoretical frameworks for modeling complex networks. Based on this review, we proceed to set up the basic analytic framework for this study and derive the fundamental conditions for optimal resources allocation under generic attack and budgetary scenarios. This is followed by in-depth analyses of optimal allocation under a number of specific attack and budgetary conditions. Simulation results are provided to validate some of the conditions and findings. Finally, we discuss the theoretical and practical implications of our analytical findings and explore future research possibilities and directions.

## 2. Research background

### 2.1. Classification of security attacks

Companies face many different types of information security attacks on a daily basis. CSI 2008 report, for instance, lists no few than 20 (Richardson, 2009). These attacks can be categorized in many ways based on factors such as system vulnerability, point of initiation, attack technique, and resulting loss. In this study, we adopt the classification of attacks based on attackers' intention and concentration to classify them into two classes (Casey, 2003; Dhanjani, 2009; Collins et al., 2006; Mirkovic and Reiher, 2004; Poff, 2009): opportunistic and targeted. Opportunistic attacks are not directed at any particular information systems; instead, they are created and released by attackers to look for and infect, opportunistically, any reachable and accessible information systems via a network. Virus, worm, spyware, phishing, and spam e-mail are common examples of opportunistic attacks. By nature, they are massive and frequent, and firms encounter them on a daily basis. Further, the probability of such attacks overwhelms other types of security incidents, although their consequences (or potential losses) are often limited (CERT, 2007; Verizon, 2011). The other class is targeted attacks, which are directed at specific information systems to steal data, inflict damages, or both. Denial of service, website defacement, or a purposeful penetration into a bank's systems to transfer large amount of money by hackers are examples of targeted attacks. Such attacks may be less frequent than opportunistic attacks, but they tend to cause much larger damages to the targeted firms—per-respondent loss from "theft of proprietary information" is three times that from virus, according to the 2008 CSI survey (Richardson, 2009).

Both classes of attacks often threaten an information system concurrently: A firm, while under constant virus and ping-of-death attacks, can at the same time be a target of hackers to steal confidential data. Further, the techniques to defend against different attacks can be different. For instance, anti-virus, anti-spyware, vulnerability patch management, web/URL filtering are typical techniques against opportunistic attacks, while application-level firewall, data loss prevention and monitoring, forensic tools, intrusion detection systems, and so on are directed at targeted attacks. (Some security measures, such as firewall and encryption, are useful to defend against both classes.) Therefore, to protect its information system, a firm needs to invest in and operate, concurrently, information security measures to fend off heterogeneous attacks. Without budget limitations, a firm would invest whatever is needed to defend itself against the different classes of attacks. In the real world, such a scenario is not realistic, given the fact that no companies have unlimited financial resources. A more common approach, therefore, is budgetary: A firm assigns a certain information security budget, the amount of which may be dependent on such factors as the industry type, the attack environment, firm's own financial situation, and so on. The decision then becomes the optimal allocation of the budget to most effectively protect the firm's information resources. In this paper, we examine the optimal allocation of a fixed security budget to defending against these two different classes of attacks.

### 2.2. Economics of information security investments

Recent research in the area of the economics of information security investment generally falls into two streams, and both are in their early stage of development. Table 1 summarizes the assumptions and results of prior research. One stream focuses on investment decision based on the actions and reactions made between a firm trying to protect its information assets and attackers intending to access or damage the proprietary information, with the help of game theory (Cavusoglu and Raghunathan, 2004; Cavusoglu et al., 2004, 2005). From the methodological perspective, game theory approach is best suited for modeling the outcome of a specific security technology with limited rounds (often two or three) of actions and reactions between a limited number of players (often the firm and the attacker). However, to be useful, such an application requires estimating the attacker's utility parameters, which is a much more difficult task than estimating those of the targeted firm. This difficulty in determining attacker's utility parameters may partially explain why game theory has not been extensive adopted by researchers in this field.

The other research stream analyzes the economics of information security with traditional decision analysis and expected utility theory. This approach, widely adopted for evaluating IT investments, examines the risk and return of information security investment in a specific period of decision making and outcomes. Unlike most other IT projects, the "return" of security investment does not come from increased revenues or decreased costs like other IT investments do, but from reduced security risks that a firm is facing (Alter and Sherer, 2004). To account for this risk economics, Schechter (2005) proposes an econometric model, in which risk is evaluated as security risk=(likelihood of loss event)*(cost of loss event). In their seminal article, Gordon and Loeb (2002) adopt the decision analysis approach and risk economics to analyze the optimal level of investment in information security by a firm. Ensuing studies (Cremonini and Nizovtsev, 2006; Hauske, 2006; Huang et al., 2008a; Ogut et al., 2005) relax restrictive assumptions made by Gordon and Loeb to both extend and modify their findings. When there is more than one technology, bypass rates – defined as the probability that an attack would breach a particular security technology – can be combined and compared for the purpose of evaluating the effect of risk reduction of each security investment (Arora et al., 2004). These studies are outlined in Table 1.