Economic Modelling 36 (2014) 398–404

Contents lists available at ScienceDirect

Economic Modelling

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

Network externality and incentive to invest in network security

Chun-Hsiung Liao [a,b], Chun-Wei Chen [b,*]

[a] Institute of Telecommunications Management, National Cheng Kung University, Tainan, Taiwan, R.O.C
[b] Department of Transportation and Communication Management Science, National Cheng Kung University, Tainan, Taiwan, R.O.C

ARTICLE INFO

Article history:
Accepted 1 October 2013

JEL classification:
O25
O32
P51

Keywords:
Network externality
Online service firm
Network security investment
Self-protect rate
Survival probability

ABSTRACT

Breaches of network security can result in substantial losses for businesses. A game theory-based model is developed to investigate in the short run how network externality influences the optimal strategy of competing online firms producing homogenous services to invest in NS. A firm's self-protect rate and survival probability against NS security incidents differ depending on its related investment decisions. The incentive of a firm to invest in NS is derived, and the impact of the survival probability and the effect of the number of firms investing in NS on a firm's incentive to invest in NS are also analyzed. Policy implications drawn from the study are provided at the end the work.

1. Introduction

Electronic commerce (e-commerce) plays an increasingly important role in both daily life and in the business world due to rapid advances in information technology (IT). According to the U.S. Census Bureau (2010), the percentage of e-commerce sales to total U.S. retail sales increased from 3.4% (137 billion) in 2007 to 3.6% (142 billion) in 2008, as more and more consumers now shop and carry out financial transactions online, without the need to leave their homes. However, this has been accompanied by rise in the number of network security (NS) breaches, with new patterns of online fraud behavior being discovered each year. The Computer Security Institute and Federal Bureau of Investigation surveyed 522 Internet-related firms about their financial losses due to computer crime and security, and the results showed that the average loss per respondent in 2008 was $288,618.00, a sharp increase of 72.1% from $167,713.00 in 2006 (Richardson, 2008).

The use of network systems in e-commerce businesses is driven by the lower costs and increased customer satisfaction that they offer, as well as by the trend to greater globalization. The development of e-commerce has had profound impacts on many individual sectors of the economy, as well as on macroeconomic performance and national economic policies (Coppel, 2000). The use of e-commerce in the U.S. software industry provides a good example of the cost advantages of this form of delivery, as it is estimated that seller transaction costs are $15 for face-to-face transactions, $5 for telephone transactions, and only between 20 and 50 cents for those occurring online (Bollier, 1996). Similar results have been found in the Australian market, in which seller transaction costs are $300 for a sales representative visit and less than 25 cents for an Internet transaction (Callaghan, 1999).

Reliable network security is necessary to protect online business operations because harmful consequences can arise if unauthorized users can gain access to the information and services in a network. In particular, the security risks associated with malicious hackers and viruses can lead to financial losses and the loss of customer confidence and even force companies to leave their online markets (Kumar et al., 2008). Warrington et al. (2000) concluded that initiating consumer trust and developing stable relationships with online shoppers are the keys to exploiting the full potential of e-commerce and to improving its profitability. Strategic decision-making in an online context must thus take into account issues of information security. Various NS technologies (e.g., firewalls, anti-virus software and intrusion detection systems) are thus used in order to maintain and protect firms' online business operations and information assets from malicious security incidents.

Investments in NS have two effects; one is a decrease in the potential losses resulting from security incidents, and the other is an increase in operating costs. A firm thus has to make a choice from among various security investment options depending on the level of threats that it faces and its budget constraints (van Kessel, 2009). Therefore, the issue of selecting the optimal NS strategy against computer-related

* Corresponding author. Tel.: +886 937 311324; fax: +886 6 275 3882.
E-mail address: r5896103@mail.ncku.edu.tw (C.-W. Chen).

0264-9993/$ – see front matter.
http://dx.doi.org/10.1016/j.econmod.2013.10.006

risks has attracted considerable academic attention, with the literature assessing the influence of network vulnerability and evaluating both threat probability and the value of the assets to be protected (Gordon and Loeb, 2002; Hoo, 2000; Schechter and Smith, 2003). Various financial metrics and forms of cost-benefit analysis have been adopted to compare potential losses and the costs of NS investments based on quantitative decision analysis.

A qualitative risk analysis prioritizes the identified project risks using a pre-defined rating scale. Risks will be scored based on their probability or likelihood of occurrence and the impact on project objectives should they occur. Probability/likelihood is commonly ranked on a zero to one scale, and the impact scale is organizationally defined. A qualitative risk analysis will also include the appropriate categorization of the risks, either source-based or effect-based. A quantitative risk analysis is a further analysis of the highest priority risks in which a numerical or quantitative rating is assigned in order to develop a probabilistic analysis of the project. In order to conduct a quantitative risk analysis, high-quality data, a well-developed project model, and a prioritized lists of project risks would be needed. While qualitative risk analysis should generally be performed on all risks, for all projects, quantitative risk analysis has a more limited use, based on the type of project, the project risks, and the availability of data to use to conduct the quantitative analysis (Passionate Project Management, 2013).

In particular, most studies of the losses related to an NS breach event only consider its immediate effects rather than those that are indirect. However, the indirect effects can have serious impacts on firms, as they can harm their reputations, lead to the loss of trust felt by customers and supplier partners, and damage relationships with partner companies (Dynes et al., 2007; Jean Camp and Wolfram, 2004; Rowe and Gallaher, 2006). Since a firm's optimal investment amount is based on the results of a cost-benefit analysis, ignoring the indirect effects of NS breaches related to network externalities will lead to suboptimal decisions being made.

The externality of a good of service being consumed refers to when one entity is affected by another's use of that good or service. NS in a communication network depends not only on the security-related investments made by individual users, but also on the reciprocal relations among the users. If the related network externalities are not considered, then the optimal level of NS investment may be underestimated (Jiang et al., 2008b; Yue et al., 2007).

This study analyzes, by considering a game theory-based threat versus an investment model, the optimal strategy in the short run for investing in NS for competing online firms producing homogenous services. The paper is structured as follows: Section 2 reviews the related studies on optimal strategies for NS investment. Section 3 sets up the framework of a firm's NS investment incentive within a competing online market and investigates the influence of survival probability and network externality on this incentive. Finally, the conclusions of this work and its managerial implications are presented in the final section, with the aim of promoting a better NS environment.

2. Literature review

The losses associated with breaches of NS in e-commerce businesses are attracting increasing attention from academics. The three main aims in the literature on optimal NS investment are preventing and/or reducing the potential losses caused by security breaches, reducing the problem of “free riders” among stakeholders who do not contribute their fair share to the related investments, and the imbalanced monetary and technical resources input by firms and attackers with regard to this issue (Huang et al., 2008). Various approaches to optimal NS investment decisions have been adopted in different types of firms and in different environments, and studies since Anderson (2001) have adopted an economic perspective of the assessment of the necessary level of investment in security technology that can be divided into two streams according to the methodologies used, those based on decision theory and those based on game theory.

In the literature that takes a decision theory-based approach, NS strategy is assessed by calculating the costs and benefits of NS investments by identifying the key variables (e.g., asset value, security risk, degree of threats and cost of breaches). This quantifying approach adopts financial metric indexes by using multiple economic indexes of annual loss expected (ALE), return on investment (ROI) (Bojanc and Jerman-Blažič, 2008a; Hausken, 2006; Iheagwara et al., 2004; Purser, 2004; Tsiakis and Stephanides, 2005), net present value (NPV) (Bojanc and Jerman-Blažič, 2008b), and internal rate of return (IRR) (Bojanc and Jerman-Blažič, 2008a). For example, Bojanc and Jerman-Blažič (2008b) introduced methods for identifying the assets, threats, and vulnerabilities of Information and Communications Technology systems, and proposed a procedure to recommend the optimal investment choice for the necessary security technology based on the quantification of various values of the protected systems (e.g., an economic index combination of ROI, NVP and IRR). The efficiency of different NS options was evaluated, and the optimal NS investment was then selected under various scenarios. However, no single index can be used to assess the optimal investment required for the prevention of security threats, and thus the application of these simple rules has not been fully validated, as they fail to take into account the wide range of factors and constraints that may influence the NS investment process, such as network externalities and market size. The probability, frequency and size of true network security losses and benefits therefore remain difficult to identify and estimate using the approaches in these works.

Another stream of literature uses game theory to model and analyze the optimal NS investment (Cavusoglu et al., 2004b; Garcia and Horowitz, 2007; Jiang et al., 2008a; Liu et al., 2005; Wang et al., 2012). A game is a description of strategic interaction that places constraints on the actions that players can take and their interests, but does not specify the actions that the players do take. A solution or equilibrium is a systematic description of the outcomes that may emerge in a family of games. Garcia and Horowitz (2007) presented a game theory-based model to analyze the economic motivations for investment in additional NS and explored possible market failures due to underinvestment in NS. They found that if Internet service providers (ISP) cannot completely appropriate the social surplus created by investments in security (i.e., the social value derived from successful operation of the Internet exceeds the revenue received by ISPs), there is potential for underinvestment, and some form of regulation may become necessary to address this. Wang et al. (2012) proposed using stochastic game nets to analyze the competitive behaviors in a dynamic enterprise network by incorporating the actions of enterprise administrators and attackers, the probability of successful security incidents, and the mean time required by administrators to repair any damage to the system. A series of experiments demonstrated that the mean time for a successful attack is longer, while the mean time to repair is shorter, with a high transition firing rate after a certain time point.

In a connected network, one firm's NS-investment usually depends on those of other firms, which can be referred to as “neighborhood effects” or “network externalities”. In terms of network security, a positive “externality” is when one firm's investment protects not only its own system, but also those of other firms'. However, this can lead to a classic free-rider problem, in which every firm would prefer other firms to invest in NS rather than make their own investments (Varian, 2004), thus leading individual firms to choose less security than the socially optimal level (Kunreuther and Heal, 2003; Ogut and Menon, 2005; Powell, 2005; Tsiakis et al., 2012). Tsiakis et al. (2012) proposed an impact pathway approach that distinguishes the economic tradeoffs for security investments along with security measures and investments in private and public goods. Externalities are social costs that are not carried by the private costs and prices of market goods/services. Their