Computers & Industrial Engineering 110 (2017) 1–12

Contents lists available at ScienceDirect

Computers & Industrial Engineering

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

Decisions making in information security outsourcing: Impact of complementary and substitutable firms

Yong Wu [a,b], Richard Y.K. Fung [b,*], Gengzhong Feng [a], Nengmin Wang [a]

[a] School of Management, Xi'an Jiaotong University, Xi'an, China
[b] Department of Systems Engineering and Engineering Management, City University of Hong Kong, Hong Kong, China

ARTICLE INFO

Article history:
Received 19 December 2015
Received in revised form 19 February 2017
Accepted 17 May 2017
Available online 22 May 2017

Keywords:
Managed security service providers
Information security investment
Information security outsourcing
Complementary
Substitutable

ABSTRACT

This paper constructs a contract-theory model to investigate how an MSSP's (Managed Security Service Provider) operating characteristics of cost efficiency, multiple clients, security externality and firms' information nature affect the MSSP's strategic decisions, including the contract structure and the optimum investment level for firms. The analysis shows that firms' information nature, either complementary or substitutable, plays a crucial role in influencing an MSSP's decisions. First, the MSSP tends to provider a contract with a lower refund and exert a lower security investment level when the degree of complementation is higher while tending to provider a contract with a higher refund and exert a higher security investment level when the degree of substitution is higher. Second, there is a lot of differences that how the security externality affects the decisions of the MSSP who serves complementary firms and that who serves substitutable firms. Third, the MSSP's optimum refund (service fee) to complementary firms is greater than firms' expected loss (expected cost), while the MSSP's optimum refund (service fee) to substitutable firms is smaller than firms' expected loss (expected cost). Fourth, serving a smaller number of substitutable firms is more economic for an MSSP while serving complementary firms the more the better. In addition, the optimum contract structures between an MSSP and complementary (and substitutable) firms are discussed in this paper. These findings give some insights that can guide an MSSP to determine an optimum contract structure and investment level for firms. Future research directions are discussed based on the limitations and possible extensions of this study.

1. Introduction

Information security is facing many challenges nowadays, such as the rising cost of security breaches, increasing scale, scope, and sophistication of security attacks, complexity of information technology (IT) environments, and compliance as well as regulatory obligations (Cezar, Cavusoglu, & Raghunathan, 2014). These challenges have motivated firms to outsource their information security functions to a Managed Security Service Provider (MSSP). Typical security services that are outsourced vary from perimeter protection including managing services for firewalls, IDSs (Intrusion detection Systems), VPNs (Virtual Private Networks) to security event monitoring, incident management (e.g., emergency response and forensic analysis). The MSSP industry is relatively new, but growing quickly. According to a CSI (Computer Security Institute) survey, 36 percent of respondents outsource their security functions to MSSPs in 2010 (Richardson, 2011), and the managed security service market in North America is expected to reach $3.9 billion in 2016 (Schwartz, 2010).

In practice, an MSSP is often more cost-efficient in managing security than firms who manage information in-house because of the better technology, more experienced staff, and higher operational efficiency (Zhao, Xue, & Whinston, 2013). To capitalize on cost efficiency, an MSSP usually serves multiple firms, as it is prevalent in information security outsourcing industry. Owing to multiple clients, the MSSP industry exhibits significant security externalities of investment, where an MSSP's investment in one firm affects other firms' security. For instance, investment in one firm may lead to broader improvement of security technologies and implementation that benefit other firms in the same group (Anderson & Moore, 2006), which is referred to as positive security externality. On the other hand, investment in one firm to reduce its security risk potentially diverts strategic hackers to other firms and thus increases other firms' risks, and in this case an MSSP's investment generates negative security externality (Cremonini & Nizovtsev, 2009).

* Corresponding author.
E-mail addresses: wuyong1202@sina.com (Y. Wu), richard.fung@cityu.edu.hk (R.Y.K. Fung), gzfeng@mail.xjtu.edu.cn (G. Feng), wangnm@mail.xjtu.edu.cn (N. Wang).

http://dx.doi.org/10.1016/j.cie.2017.05.018
0360-8352/

Information security relationship between firms includes not only the security externality but also the nature of firms' information. Nowadays, firms achieve product innovation or value creation via the network economy. As a result, many firms' information is complementary or substitutable with each other in varying degrees. In the information security context, when firms' information is complementary, the combined information from various firms is very valuable, while that of a single firm may of little value to hackers. For example, a commercial airplane outsources the design of a major component of a new airplane to a vendor firm. A hacker who is interested in getting business intelligence regarding the entire design of the new airplane would have to obtain design information from both the airplane company and the vendor firm (Liu, Ji, & Mookerjee, 2011). Firms' information is substitutable means the information held by firms is very equivalent to hackers, and hackers can achieve benefit by breaching any of them. It is well known that Walmart and Proctor & Gamble (P&G) share retail sales information on P&G products at Walmart stores (Grean & Shaw, 2002). If a hacker is interested in obtaining such sales information, then successfully penetrating either Walmart's or P&G's systems would achieve this goal (Liu et al., 2011). In conclusion, the operations of an MSSP are related to four characteristics: cost efficiency, multiple clients, (positive or negative) security externality, and firms' information nature (complementary and substitutable), as explained above.

An MSSP should design an appropriate contract structure to make sure that firms could receive a higher or at least the same expected payoff compared to doing it in-house, while making a reasonable profit simultaneously. In practice, bilateral refund contracts are widely adopted in security practice in the form of service level agreements (SLAs), which determine a fixed payment from a firm to an MSSP, and a refund paid by the MSSP to the firm in the event of security breach to the firm (Cezar et al., 2014; Lee, Geng, & Raghunathan, 2013). For example, IBM Internet Security Systems, as one of the largest MSSPs, pays $5000 refund each time to firms who suffer a breach. Once firms decide to accept the contract structure provided by an MSSP, the MSSP should decide an appropriate security investment level to firms, which has become one of the critical decisions faced by the CEO (Chief Security Offers) (Berinato, 2002). Although firms normally understand the contract structure well, they would not be able to effectively evaluate or monitor the MSSP's investment levels, and thus suffer from moral hazard problems (Cezar et al., 2014). Consequently, MSSPs may invest inefficiently. When deciding the security investment level, the MSSP faces two risks: the risk of loss from security breach (security risk) and the risk of over-spending in security (investment risk). An MSSP's security risk is high when the refund level is high and the investment risk is high when the investment level is high. In conclusion, an MSSP has two important strategic decisions, including the contract structure and the optimum investment for firms.

Thus, the following research questions are important to an MSSP's decision marker. First, is it necessary to distinguish firms' information nature, and if necessary, how does the degree of complementation (or substitution) between firms affects the MSSP's decisions? Second, how does cost efficiency affects the MSSP's optimum investment level? Third, for complementary firms and substitutable firms, what is the optimum contract structure and security investment that the MSSP should exert? Fourth, is there any differences that the security externality affects the decisions of the MSSP who serves complementary firms and that who serves substitutable firms? Fifth, when serving clients with different information nature, how does the number of the MSSP's clients changes? To answer the above research questions, this paper constructs a contract-theory model to investigate how an MSSP's operating characteristics of cost efficiency, multiple clients, security externality and firms' information nature affect the MSSP's strategic decisions, including the contract structure and the optimum investment level for firms.

The rest of the paper is organized as follows. The next section reviews the related literature. In Section 3, the preliminaries of a model for an MSSP severing complementary or substitutable firms are introduced. Effects of all operating characteristics on an MSSP's decisions are analysed in two subsequent sections. Section 4 studies the contract between an MSSP and complementary firms in detail while the case of substitutable firms is discussed briefly in Section 5. The basic model is extended to the case of three or more firms in Section 6. Managerial and policy implications of implementing the proposal models are concluded, and potential future work is discussed in Section 7.

2. Literature review

Since the present paper discusses information security outsourcing contracts, it is related to the vast literature on IT outsourcing. Rather than attempting to identify the difference between the present paper and the voluminous IT outsourcing/-contracting literature, here confines the discussion to those references that related to information security outsourcing contracts. In one of the earlier paper on information security outsourcing, Ding, Yurcik, and Yin (2005) examine the characteristics of an MSSP's optimum contracts by considering Moral hazard problem and reputation effects. Hui, Hui, and Yue (2012) examine how system interdependency risks would interact with a mandatory security requirement to affect the equilibrium behaviours of an MSSP and its clients. More recently, Lee et al. (2013) propose a multilateral contract to solve the double moral hazard problem in security outsourcing with the existence of security externality and the multi-client nature of MSSP services. Zhao et al. (2013) examine three alternative risk management approaches and show that an MSSP serving multiple firms can internalize the externality of security investments and mitigate the inefficiency in security investment. Cezar et al. (2014) group the nature of security function into two categories (prevention and detection) and propose a new contract to enhance the advantages offered by complementarity between prevention and detection functions. The extant information security contracting literature assumes that firms' information that an MSSP serves is independent with each other, and firms' information nature has no impact on the MSSP's decisions. This paper considers an MSSP serves two firms with complementary (or substitutable) information and analyse the question of whether it is necessary to distinguish firms' information nature, and if necessary, how does the degree of complementation (or substitution) between firms affects the MSSP's decision?

The present paper is related to the topic of parallel and series systems, which has been extensively researched in the reliability literature. In their seminal paper, Bier, Nagaraj, and Abhichandani (2005) apply game theory on security to systems with series or parallel structures. They show that the optimum allocation of defensive investments depends on the structure of the systems, the cost-effectiveness of infrastructure protection investments, and the adversary's goals and constraints. Following that paper, several papers look at various problems related to security and safety in parallel and series systems. For example, Hausken (2008) considers a system of independent components defended by a strategic defender and attacked by a strategic attacker, where the system could be parallel or series. The nature of firms' information (complementary and substitutable) is essentially the same to the structure of systems (parallel and series). With limited literature available on information security with complementary and substitutable information, Liu et al. (2011) discuss security