Decision Support Systems 75 (2015) 49–62

Contents lists available at ScienceDirect

Decision Support Systems

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

Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors

Bin Srinidhi [a,*], Jia Yan [b,1], Giri Kumar Tayi [c,2]

[a] Department of Accounting, College of Business, University of Texas at Arlington, Arlington, TX 76010, United States
[b] Department of Economics, Washington State University, Pullman, WA, United States
[c] School of Business, State University of New York at Albany, Albany, NY, United States

ARTICLE INFO

Article history:
Received 27 August 2013
Received in revised form 11 February 2015
Accepted 24 April 2015
Available online 5 May 2015

Keywords:
Decision-making security breach costs
Financial distress
Insurance
Resource allocation

ABSTRACT

Cyber-security is increasingly seen as an important determinant of firm-specific financial risk. Agency theory suggests that managers and investors have different preferences over such risk because investors can diversity their capital over different firms to reduce firm-specific risk but managers cannot diversify their investment of human capital in their firm. Therefore managers face greater personal cost of financial distress during their limited tenure. We develop an analytical model for optimally allocating investments to general productive assets and specific cyber-security assets incorporating costs of security breaches, borrowing and financial distress. We note that investment in productive assets can generate cash flows that allow the firm to better withstand security threats in the long run but investment in specific security-enhancing assets reduce security breaches in short run while leaving the firm's finances vulnerable over a longer period. Using our model, we show that managers over-invest in specific security-enhancing assets to reduce security breaches during their tenure. We then incorporate cyber-insurance in our model and show that it has the effect of reducing managers' over-investment in specific security-enhancing assets.

1. Introduction

The importance of protecting intellectual and other property rights from cyber-attacks has grown exponentially over the last few years [45]. Innovative young firms could be eviscerated by the loss of their intellectual capital to cyber-attacks [34]. Cybercrime could inflict devastating losses even on large firms. Smith [41] points out that Nortel Networks filed for bankruptcy in 2009 after a decade of hacking into executive computers to access business plans, reports, emails and other documents. A recent McKinsey study estimates that the economic losses due to cyber-attacks may well reach $20 Trillion by 2020 [15].

Recognizing this problem, the Corporate Finance Division of the U.S. Securities and Exchanges Commission (SEC) has issued guidelines for listed US firms in 2011 for disclosing the costs and risks of cybercrime. In this paper, we develop a decision support model for the allocation of resources to combating cyber-attacks. We use an agency-theoretic view of the firm to identify the misalignment of interests between managers and investors in such allocation. Further, we document the usefulness of cyber-insurance.

In the agency-theoretic view of the firm, managers and investors have differing preferences over the allocation of investment between income-generating (productive) assets and security-enhancing assets and activities. Productive assets increase cash flows that reduce the vulnerability of the firm to financial distress from security problems in the long run, whereas security-enhancing assets and activities reduce security breaches in the short run at the expense of cash flow over the long run. Managers prefer security investments that can protect the assets of the firm and in turn, protect their jobs and pay during their tenure whereas investors prefer productive assets that increase long run productivity because they can mitigate the short term financial risk through diversification. Managers, not investors, choose the mix of productive and security investments in the firm, making the decision subject to the agency problem [20].[3]

The agency-theoretic view we utilize in this paper has direct and strong linkage to the IT governance perspective as enunciated by Weill

* Corresponding author: Tel.: +1 817 272 1310; fax: +1 817 272 5793.
E-mail addresses: srinidhi@uta.edu (B. Srinidhi), jiay@wsu.edu (J. Yan), g.tayi@albany.edu (G.K. Tayi).
[1] Tel.: +1 509 335 7809; fax: +1 509 335 1173.
[2] Tel.: +1 518 956 8328; fax: +1 518 442 2568.

[3] In identifying the need for corporate governance, Hart [20] argues that managers might get decision rights by default because of many different reasons. For example, the shareholders in a diffusely owned firm are too small and numerous to exercise control on a day-to-day basis and have little incentive to monitor management resulting in a free rider problem. The decision right will therefore be effectively be exercised by managers in the pursuit of their own goals at the expense of those shareholders.

http://dx.doi.org/10.1016/j.dss.2015.04.011
0167-9236/

and Ross [47]. IT governance specifies accountabilities for IT-related business outcomes and helps a firm to align its IT investments (for example in security enhancements) with the firm's strategic objectives. According to Weill and Ross [47] one of the key decisions that underpins effective IT governance is Prioritization and investment — decisions about how much and where to invest in IT. Specifically one factor that is relevant to this decision is the relative importance of enterprise-wide versus business unit investments and how far actual practice reflects their relative importance. This factor highlights a potential tension that may exist, in practice, between a business unit managers' goals, preferences and time horizon on one hand and the relative importance enterprise-wide managers' (could be Business Monarchy archetype) associate with corporate and investor goals. This paper primarily addresses this tension and helps to highlight how firms can make IT governance transparent.

Our motivation to study the problem arises from the following trends: (i) the importance of cyber-security is rapidly increasing; (ii) the vulnerability of the firms to cyber-attacks is increasing; and (iii) security-enhancing tools that improve the visibility into networks, web applications and end points have become more effective in preventing security breaches and are available to managers to invest in. By allocating funds to security–enhancing tools, managers can effectively reduce the probability and the potential loss from cyber-attacks but at the same time, the diversion of funds away from productive assets reduces cash flow and increases vulnerability of the firm to financial distress from cyber-attacks in the long run.

We address this problem by developing a multi-period model of the firm's allocation of its internal and available external funds between productive assets and security activities when faced with costs related to security breach, borrowing and financial distress. The investment in security takes two forms: direct investments in security-enhancing assets and the choice of productive assets that are less vulnerable to security threats. Productive assets that have the added feature of resisting security threats are likely to be costlier than similar assets without those features. Either form of investment in security reduces the availability of funds that can be invested in increasing cash inflows. We allow the investments in productive capital to accumulate over time. We show that although the ultimate steady state productive capital accumulation is not affected by security breach and financial distress costs, the initial investment in productive capital is lower and the rate of accumulation is slower because of them. Security breach and financial distress costs slow down capital accumulation while accelerating the allocation to security in the short run. Managers who bear higher personal financial distress costs invest more in security and less in productive capital compared to the optimal allocation from the investors' viewpoint. Further, managers have limited tenure in the firms unlike owner-investors and therefore are more incentivized to protect the firm's assets in the short run during their tenure rather than focus on the long run. Further, we show that external cyber-insurance can benefit both the firm and the insurer over a feasibility range determined by cost parameters. A noteworthy effect of external insurance is that it reduces the difference between the manager-optimal and investor-optimal allocations.

Our paper contributes to the literature in three ways. First, we develop a decision-support model that helps in making resource allocation decisions between productive and security operations in the presence of costly security breaches and financial distress costs. Second, we show that managers have incentives to invest more in security than is optimal for investors. Third, we show that cyber-insurance can be mutually beneficial to both the insured and the insuring firms by reducing the managers' over-allocation of resources to security.

We give the background and description of our approach in the next section, and discuss prior related research in Section 3. Section 4 gives the models, results and numerical illustrations for settings with security breach, borrowing and financial distress costs. We examine the role of external insurance in Section 5 and provide summary and concluding remarks in Section 6.

2. Background and description of our approach

2.1. Evidence on the threats and costs of security failures and their mitigation

Increasingly, there are attempts both by parties with malicious intent and by seemingly unrelated third parties (such as hackers) to breach corporate information and financial systems. U.S. GAO report (GAO-10-536 T March 24, 2010) warns about the vulnerability of the federal computer systems to such intrusions, prompting the U.S. Congress to require federal agencies to pursue both technological and organizational measures to enhance cyber security. There is also evidence that the frequency of security breaches is increasing rapidly.[4] According to the latest report available from the Computer Security Institute (CSI), the 2010/2011 Annual Computer Crime and Security Survey indicates that 45.6% of the respondent firms reported they had been subject of at least one targeted attack, mostly due to malware infection.

The GAO report suggests that the attacks can be controlled by allocating resources to security-enhancing technological and organizational measures. The information technology managers in the CSI survey ranked the tools that improve visibility into networks, web applications, and endpoints as being the most efficient in improving information security. However, investment in these security-enhancing processes and assets divert funds away from productive assets that generate cash flow and allow accumulation of productive capital. We note higher cash flows also reduce the vulnerability of the firm to financial distress from cyber-attacks in the long run.

2.2. Allocation of resources to revenue generation and security improvement activities

We model the optimal allocation of investment between security operations and productive assets.[5] The difficulty in effectively allocating resources under circumstances characterized by the uncertain nature and severity of breach costs has been pointed out by Rue et al. [39]. In contrast to prior literature, we examine this allocation by explicitly considering the possibility that a firm could face financial distress and bear the costs related to reorganization and recovery.[6] When the security breach costs exceed the combined internal and external funds available to a firm[7], the firm faces financial distress. Financial distress is known to result in deadweight costs to the firm and its investors. In the U.S., severely financially distressed firms operate under Chapter 11 provisions that increase direct costs by an average of 1.8% but up to 5% of the firm's total assets [30]. Both these and the less severely distressed firms incur indirect costs resulting from an impairment of their ability to conduct normal business (for example, suppliers might be reluctant to supply materials on credit). Our model captures these costs. Managers in financially distressed firms face additional personal costs because they are likely to lose both their jobs and reputation — a human capital risk that cannot be diversified by holding other investments. The difference in the perceived financial distress costs faced by investors and managers

[4] The Ponemon Institute's Annual Cost of Cyber Crime Study (October 2012) reports that cyber-attacks have become common occurrences and firms surveyed in the study experienced 102 successful attacks per week and about 1.8 successful attacks per company per week. This according to the study represents an increase of 42% from last year. Similarly the study also reports that the average annualized cost of cyber-crime is $8.9 million per year, with a range of $1.4 million to $46 million. The most costly cyber-crimes being denial of service, malicious insiders and web-based attacks.

[5] Although other activities such as research and development are important, our focus in this paper is on security and revenue-generating activities. Revenue generating activities include production and marketing activities.

[6] However, we do not assume that financial distress necessarily leads to the liquidation of the firm.

[7] We use the terms "firm" and "organization" interchangeably. However, our model and findings are not dependent on the organizational form and can be applied to non-business organizations.