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.

results in different optimal allocation mixes for the managers and investors. We then examine a setting where external cyber-insurance is available to mitigate security breach costs. We note that many firms are in fact taking steps to reduce cyber-attacks, protect data and confidential information, and choose insurance policies that cover the loss or liability associated with data breach. For example, according to a 2011 report[8] by British insurance firm Willis Group Holdings, insurance claims for data theft worldwide jumped 56% over that of the previous year. We show that cyber-insurance can help mitigate the difference between the managers' and investors' optimal allocation preferences.

3. Related work

Analysis of information security from an economic perspective has recently attracted much research interest. Gordon and Loeb [18] develop an optimal allocation model among different information assets with different vulnerabilities. Kumar et al. [29] explore firm level security budgeting when decision rights reside with different agents with divergent priorities. Ulvila and Gaffney [46] propose a decision analytic framework for evaluating computer intrusion detection systems. Cavusoglu et al. [11], examine the economic value of individual security technologies such as Intrusion Detection Systems. Cavusoglu et al. [12] study how security patches can reduce vulnerabilities in the system. Cavusoglu et al. [13] study the impact of interaction between different technologies such as firewalls and intrusion detection systems on information security. Yue and Cakanyildirim [48] propose reactive and proactive responses that a firm can undertake in ensuring high levels of information security. Mookerjee et al. [31] develop an analytical model in which a variety of factors are balanced to best manage the detection component within information security management. Mookerjee et al. [32] analyze the optimal amount of effort that a firm should exert to best maintain a detection component within information security management. However, these studies do not explicitly consider the broader firm level resource allocation between revenue generating and security assuring investments.[9]

We develop a general optimal allocation model in which the costs and benefits are not completely specified. We then apply this model to managers and investors based on the costs and benefits that they perceive respectively. The optimal tradeoff from the investors' viewpoint is different from those of the managers because they can diversify the firm-specific risk resulting from security breaches but managers cannot.

Apart from making investments in security assuring operations, a firm could also purchase cyber-insurance from an external provider to mitigate its exposure to financial distress resulting from security breaches. Several researchers examine the feasibility of such external insurance. Kesan et al. [26] justify the purchase of external insurance because it encourages adoption of socially optimal security standards and could prevent a market failure when risks are not transferable. They estimate the potential size (annual premiums) of the cyber-insurance market in the U.S. to be about \$2.5 billion though the actual size of the market was only \$450 million in 2008 [3]. Bandyopadhyay et al. [2] acknowledge the importance of an external insurance for security breaches but attribute the slow growth of the cyber-insurance market partly to demand-side factors and overpricing. Bolot and LeLarge [9] develop an analytical model to examine the role of external insurance in mitigating correlated security risks for individual users on the Internet. At the firm level, Gordon et al. [17] discuss the viability of external insurance as a way to hedge against information security breach costs. Ogut et al. [36] develop a model of information security investment when the firms are assumed to be risk averse and their security risks are interdependent. In this paper, we do not base our analysis on firms' risk aversion or mutual interdependence. Instead, the drivers for external insurance in our paper are financial distress and borrowing costs even when the firms and the insurance providers are risk-neutral.

4. The Security Breach Models

The firm starts with an initial capital endowment K_0. The investment in productive assets produces cash inflows whereas security-enhancing investments reduce the likelihood of security breaches. The security breach costs deplete the residual cash (funds available after investments in productive and security operations) available to the firm. One consequence of this depletion is that a firm will have fewer resources to invest in revenue generating processes and to pay dividends in future time periods.

If the breach costs are higher than available internal funds, the firm will be forced to borrow[10] and incur borrowing costs. If the breach costs are high enough to stretch the firm beyond its borrowing capacity, it could warrant restructuring of the firm including a possible replacement of the current management. We define this condition as financial distress. However, we assume the restructured firm will continue to operate. The aggregate cost of security breaches to the firm includes both the direct and financial distress costs.[11] In addition, the managers incur a personal cost due to the loss of personal human capital and further damage to their reputation which could limit their opportunities at other firms.

The allocation between revenue generating and security assuring activities made in earlier periods affect future investments, breach costs and residual cash available to the firm. The multi-period nature of this decision making suggests the use of a dynamic model to generate the optimal allocation of funds in each period.

In Table 1, we present the notation. Next, we develop the framework that underlies all the models.

4.1. Revenue Generation

The firm generates net cash revenue based on the production function

$$y_{t+1} = F(K_{t+1}) \tag{1}$$

$$K_{t+1} = (1-\beta)K_t + k_t \quad t = 0, 1, ..T \tag{2}$$

In the above expression K_0 is the initial capital, [12] K_t is the productive capital at the beginning of period t and k_t is the new investment in productive assets during the period t. β is a factor that specifies the proportion of the productive capital that is used up or depreciated in any time period; $F(\cdot)$ is assumed to be twice differentiable and satisfies the

[8] (http://www.experian.com/blogs/data-breach/2011/11/16/data-breaches-make-the-hospitality-industry-less-hospitable/).

[9] Budgeting requires the divisions including the IT division to develop a detailed IT budget specifying the methods of security on which the amount will be spent. The top management will consider the aggregated IT budget along with other divisional budgets and makes a lump sum budget allocation to IT. IT division will then prioritize their spending and re-allocate the total budgeted amount to the different methods of security. Budgets of product divisions are revenue-generating budgets. We consider here the aggregate problem of allocation between the IT security and the revenue-generating budgets, *ceteris paribus*.

[10] If the original capital structure includes debt, the firm will be forced to increase its borrowing to meet the cost of security breaches that is not covered by internal funds. For example, Smith [41] points out the loss of a \$700 million contract for American Semiconductors because of intellectual property by its customer Sinovel which resulted in a significant loss of equity, presumably tilting the capital structure of the firm to greater debt.

[11] Financial distress costs include direct legal and administrative costs of liquidation and reorganization and an arguably higher indirect cost because of loss of market share due to decreased customer confidence in post-sales servicing and loss of brand equity, inefficient asset sales at a deep discount, increased reluctance of suppliers to supply products and services on credit, and loss of qualified employees who seek longer term contracts with competitors, among others. For a full description of financial distress costs, refer to Ross et al. [38] and Almeida and Philippon [1].

[12] For the purposes of our analysis, we assume that the firm gives the same expected risk-adjusted returns to investors as they can get by reinvesting dividends. This is in line with the CAPM model.

Table 1
Notations.

Parameter	Description
K_t	Capital stock at the beginning of period t
k_t	New investment in revenue generating operations in period t
y_{t+1}	Net cash revenue in period t + 1
W	Wealth of firm
β	The proportion of the capital stock that is used for replacement and maintenance of capital assets
ξ_t	Information security breach cost, a random variable
s_t	Allocation to Security assuring operations
ϕ	Rate used to discount future cash flows
z_t	Residual cash flow in period t after allocations to revenue generating and security assuring operations
D	Borrowing Limit
ϖ	Aggregate financial distress cost
r	Interest rate on borrowing
$(1-\mu)$	External insurance coverage
$\tau(\mu)$	External insurance premium for coverage $(1-\mu)$
$I(\cdot)$	Binary value function which takes 1 if the argument is true and takes 0 otherwise
V(.)	General notation used to denote the optimum value of an optimization problem

following conditions: $F'(\cdot)>0$, $F''(\cdot)<0$, and $F(0)=0$. Note that the net cash revenue as defined here is net of all cash expenditures including any interest payment on the initial debt and excludes accruals such as credit sales and other non-cash revenues and expenses.

4.2. Security Assurance

The security breach costs are typically asset specific because some components of the IT system and some productive assets are more vulnerable to breaches than others. The funds allocated by managers to security include both specific security-enhancing tools and additional features of productive assets that resist cyber-attacks. For example, they might build firewalls between assets such that the cyber-breaches on one set of assets do not spread to other assets. Both these forms of security investments may force the firm to plan on having a larger IT budget.

We model the aggregate security breach cost as a nonnegative random variable ξ_t which follows a Pareto distribution with the density function $\rho(\xi_t)=\frac{\delta\cdot\xi_m^\delta}{\xi_t^{\delta+1}}$, where $\xi_m>0$ is the location parameter and $\delta>0$ is the shape parameter.[13] Therefore, the probability that the breach cost is greater than $\xi\in[\xi_m,+\infty)$ is given by

$$\Pr(\xi_t>\xi)=\left(\frac{\xi}{\xi_m}\right)^{-\delta}\text{for all }\xi\geq\xi_m \tag{3}$$

Pareto distribution has been found to describe the distribution of the size of insurance claims very well [14,28]. The distribution captures the intuition of Power Law which implies that costs resulting from most breaches are small, whereas a few breaches result in large costs (long tail). This distribution is widely used for insurance modeling [21,40].

The expected cost resulting from information security breach under the Pareto distribution in Eq. (3) is given by

$$E\{\xi\}=\frac{\delta\cdot\xi_m}{\delta-1} \tag{4}$$

The expected information breach cost is a strictly decreasing function of the location parameter (ξ_m). In each period, the firm invests in security assuring processes which mitigate vulnerabilities and reduce the probability of a breach thereby lowering the expected breach costs. We therefore model the location parameter of the Pareto distribution as a strictly decreasing convex function of security allocation s_t such that

$$\Pr(\xi_t>\xi)=\left(\frac{\xi}{\xi_{mt}}\right)^{-\delta}\text{for all }\xi\geq\xi_{mt}\text{ and }\xi_{mt}=h(s_t). \tag{5}$$

The function $h(s_t)$ is characterized by $h'(s_t)<0$, $h''(s_t)>0$, $h(0)=\overline{h}$, $h(+\infty)=\underline{h}$, and $\overline{h}>\underline{h}>0$. This implies that the expected value $E(\xi_t)$ is decreasing convex in s_t. Thus the firm can reduce the expected information breach costs via investing in security assuring processes and the marginal benefits of doing so is decreasing.[14]

4.3. The Firm's Decision Problem

Given an initial productive capital of K_0, the decision-maker's problem is to decide productive capital accumulations $\{K_1, K_2, \ldots, K_{T+1}\}$ [15] and security-enhancing allocations $\{s_0, s_1, \ldots, s_T\}$ to maximize the present value of net cash flows plus the wealth of the firm at the terminal date $T+1$. Larger allocations to security assuring processes reduce the expected breach costs and the probability of financial distress. However, when these allocations go beyond the normal needs of doing business they could potentially compete with the funds available for revenue generating processes and slow down the build-up of productive capital in the long run. In turn, the reduced cash flows decrease the margin of safety available to the firm in withstanding large breach costs and thus make the firm more vulnerable to such breaches in the long run. The optimal tradeoff between productive and security allocations occurs where the marginal short term benefit of reduced breach cost is offset exactly by the sum of the marginal long term reduction in cash flows and the marginal cost of increased vulnerability. For the investor, the marginal benefit of reduced breaches in the short run in any one firm is smaller than for that firm's manager because the investor is diversified among different firms whereas the manager is not. Correspondingly, the effect of lower cash flows over the long run is felt more by the investor than by the manager who personally suffers only a fraction of the reduced cash flows in the short run. This argument implies that the perceived marginal costs and benefits are different for the manager compared to the investors and as a result, the manager is likely to over-invest in security (short-term benefit is higher) and under-invest in productive capital.

4.4. The Base Case: No-Breach Model

In the absence of breach costs, the firm invests only the bare minimum in security assuring processes[16]. Furthermore, we assume that the firm's capital investment can be funded by its internal fund (or that external financing is costless to the firm)[17].

[13] The location parameter is the lower bound of the support of the random variable. The shape parameter measures the heaviness of the right tail of the distribution; the smaller the shape parameter is, the longer right-tail the distribution has. The mean of the distribution $E\{\xi\}$ is given in Eq. (4). Only when $\delta>2$, the distribution has finite variance as can be seen from the expression for the variance: $^2\delta/(\delta-1)^2(\delta-2)$.

[14] Expected information breach cost is the product of the probability of information breach and the loss associated with information breach. While direct investment in security technology is likely to reduce the expected breach cost by reducing the probability of information breach, the investment in robust technology is likely to reduce the amount of loss resulting from information breach.

[15] The decisions are equivalently represented by allocations to productive assets $\{k_0, k_1, \ldots, k_T\}$ in the planning horizon. Apart from budgeting for capital and security-enhancement, the firm's decision problem includes other budget allocations but we abstract away from the other allocations and focus only on these two for modeling.

[16] We consider this case as a base case and it assumes that the firm only invests the bare minimum in security processes and is meant to mainly serve as a benchmark for comparison purposes.

[17] Admittedly, there might be everyday losses in the normal course of business that might require external funding. We assume that the cost associated with all the normal business events other than security breaches are included in the cash flow of the firm so that we can just model only the incremental cost of security breaches. Introducing a full capital resource financing model is beyond the scope of this paper.

The one-period residual cash flow available to the firm in period t is $d(K_t, K_{t+1}) = F(K_t) - k_t$. Substituting for k_t from Eq. (2), we have

$$d(K_t, K_{t+1}) = F(K_t) - K_{t+1} + (1-\beta)K_t$$

Define wealth of the firm at period t as $W(K_t) \equiv F(K_t) + (1-\beta)K_t$ the firm solves the following value-maximization problem.

$$V_0(K_0) = \underset{\{K_{t+1}\}_{t=0}^{T}}{Max} \sum_{t=0}^{T} \phi^t d(K_t, K_{t+1}) + \phi^{T+1} W(K_{T+1}) \tag{6}$$

where $\phi \in (0, 1)$ is the discount factor;[18] $V_0(K_0)$ is the value of the firm at the initial period. The dynamic optimization problem in Eq. (6) can be expressed as the following recursive form

$$\begin{aligned} &V_t(K_t) = \max_{K_{t+1}} d(K_t, K_{t+1}) + \phi V_{t+1}(K_{t+1}) \quad t = 0, 1, ..T \\ &s.t. \; V_{T+1}(K_{T+1}) = W(K_{T+1})(terminal \;\; condition) \end{aligned} \tag{7}$$

In Eq. (7), $V_t(K_t)$ is the value of the firm at the beginning of period $t$given the productive capital K_t; $V_{t+1}(K_{t+1})$ is the value of the firm at the beginning of the next period.[19] The solution of Eq. (7) given in the appendix results in

$$F'(K^*_{t+1}) = \frac{1}{\phi} - (1-\beta), \quad t = 0, 1, 2......T \tag{8}$$

The RHS of Eq. (8) is a constant which implies that the optimal productive capital will also be constant over the entire time horizon and we use K^* to denote the constant optimal productive capital.[20] From the above expression, we get the intuitive result that K^* is larger when the discount rate is closer to 1 and β is larger.

We note that if the manager solves the myopic decision rule Eq. (9) instead of Eq. (7), the capital investments do not change.

$$V_t(K_t) = \max_{K_{t+1}} d(K_t, K_{t+1}) + \phi \cdot W(K_{t+1}) \quad t = 0, 1, ..T \tag{9}$$

4.5. The Model with Information Security Breach Costs and Financial Distress

4.5.1. Model Development

We model information security breach costs as a Pareto distribution given in Eq. (3).[21] s_t denotes the amount allocated to security assuring processes in the budget process. [22]

The available free cash flow *after* investment decisions at the beginning of period t is the net operating cash inflow y_t less the investments in productive and security operations in period t. We denote the free cash flow by $z_t = y_t - k_t - s_t$. From Eq. (2), we have $z_t = F(K_t) - K_{t+1} + (1-\beta)K_t - s_t$. This free cash flow is the amount that is available for covering the costs incurred by information security breaches in period t. The allocation s_t in security assuring processes, results in a distribution of security breach costs with a location parameter $h(s_t)$ as given in Eq. (5).

When the information security breach costs cannot be fully covered by the available internal funds[23], that is $z_t - \xi_t < 0$, the firm resorts to borrowing from the capital market. This results in borrowing costs in addition to the breach costs. When the amount of borrowing exceeds the limit D (imposed by the capital market)[24] the firm faces financial distress. We now formalize the above arguments regarding breach costs and financial distress.

Fig. 1 depicts the three mutually exclusive ranges of security breach costs that are relevant for our analysis. These ranges provide insight about the impact of breach costs vis-à-vis the firms' residual cash flow. In the first range, the breach cost ξ_t is at least $h(s_t)$ but lower than the residual cash flow z_t and therefore it can be fully covered internally. The probability that the realized security breach cost falls in this region is given as $\Pr(h(s_t) \le \xi_t < z_t) = (1 - \rho_t)$ where $\rho_t = \left(\frac{z_t}{h(s_t)}\right)^{-\delta}$. In the second range, the breach cost ξ_t lies between z_t and $(D + z_t)$ in which case the internal residual cash flow alone will not cover the breach costs. Hence, the firm needs to borrow an amount equal to $(\xi_t - z_t)$ at an interest rate of r. The last range is where the breach cost ξ_t exceeds $(D + z_t)$ resulting in financial distress for the firm. The probability of financial distress is $Pr(\xi_t > z_t + D) = \theta_t$ where $\theta_t = \left(\frac{z_t+D}{h(s_t)}\right)^{-\delta}$. In this range, the costs incurred by the firm are comprised of two components. The first component is the cost associated with borrowing an amount D at an interest rate of r. The debt and the interest need to be typically repaid under a restructured agreement over an extended period of time. For simplicity, we assume that the firm is obligated to pay an amount equal to $D(1 + r)$ that covers the debt and the interest within one period. The second component is the incremental cost associated with financial distress which we denote by an amount ϖ. For simplicity we model ϖ as a lump-sum constant amount.

The realized one-period residual cash flow after paying security breach costs at the end of the period t is given as follows:

$$\begin{aligned} &I(z_t \ge \xi_t) \cdot (z_t - \xi_t) - I(z_t < \xi_t \le D + z_t) \cdot (1+r) \\ &\cdot (\xi_t - z_t) - I(z_t + D < \xi_t) \cdot (D(1+r) + \varpi) \end{aligned} \tag{10}$$

$I(\cdot)$ is a binary value function that takes the value of 1 if the argument is true and 0 otherwise. In Eq. (10), these functions represent the breach cost ranges; for example, $I(z_t \ge \xi_t) = 1$ if $z_t \ge \xi_t = 1$ and $I(z_t \ge \xi_t) = 0$ otherwise. Taking expectation with respect to ξ_t, we get the one-period expected residual cash flow as

$$\begin{aligned} &\pi(K_t, K_{t+1}, s_t) \\ &= z_t - \frac{\delta}{\delta-1} h(s_t) - \frac{r}{\delta-1} \rho_t z_t - \theta_t \left[(D(1+r) + \varpi) - (1+r)\left(\frac{\delta}{\delta-1}(z_t + D) - z_t \right) \right] \end{aligned} \tag{11}$$

Eq. (11) describes the partial one-period solution within the context of the overall multi-period optimization problem. Nevertheless it allows us to analyze the changes in the probabilities of borrowing and bankruptcy as well as the expected residual cash flow in response to changes in s_t, given a beginning-period productive capital, K_t. Using numerical analyses, we find that as the firm increases s_t, both the need to borrow and the probability of financial distress decrease. This is reflected in the relationship between the minimum breach cost [location parameter $h(s_t)$] and borrowing and financial distress probabilities (ρ_t and θ_t respectively) as shown in Fig. 2a. These probabilities also decrease with the shape parameter δ as shown in Fig. 2b, i.e., when the probability of

[18] The discounting sequence $(\phi^0, \phi^1, \phi^2, \ldots)$ is the discrete version of the exponential discounting function used to model decision-making under uncertainty in continuous-time setting.

[19] The formulation given here assumes that the residual cash flow after investment in productive capital can be invested in non-operating assets that gives expected risk-adjusted returns at the rate of $\left(\frac{1}{\phi} - 1\right)$ which is the same rate that the investors can earn if it is distributed to them as dividends. Further, we assume that the liquidation proceeds of productive capital at the end of the horizon equal its value at that time.

[20] In the initial periods, it is possible that the first order condition is not satisfied at an interior point. In that case, the entire net cash flow is plowed back to increase the productive capital till the time that the steady state productive capital K^* is reached.

[21] As before, we use the Pareto distribution because of the Power Law – a few breaches are likely to result in very large costs whereas most breaches result in small costs that are not very material.

[22] It is acknowledged that firms in practice have an IT budget which is an integral part of the allocations being made for security assurance processes.

[23] Note that internal funds (free cash flow) come from operations and the initial capital that could include borrowed funds. The borrowing that we refer to here is the additional cash infusion in periods t = 1, 2,.....T to fund investments and to cover realized security breach costs that exceed internal funds available at that time.

[24] We assume that the capital market is not perfect and a borrowing limit exists beyond which the firm incurs incremental financial distress costs.

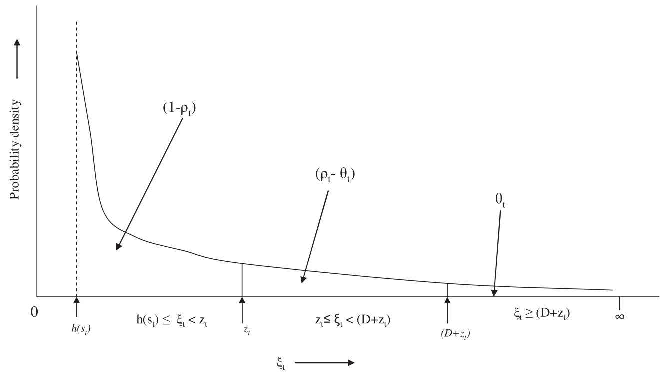

Fig. 1. Probability ranges for information security breach cost ξ_t.

excessive breach cost is low. When the minimum breach cost is high, the residual cash flow is correspondingly lower as shown in Fig. 2c. In other words, the expected breach cost reduction due to higher allocation to security-enhancing investment more than compensates for the decrease in cash flow resulting from a correspondingly lower allocation to the revenue generating operations. As expected, the residual cash flow increases when the probability of excessive security breach cost is low, as shown in Fig. 2d. To summarize, the Fig. 2a–d highlight how varying s_t influences the breach cost distribution thereby moderating the financial distress probability and enhancing the residual cash flow of a firm.

We now present some formal results.

Lemma 1. *The expected one-period residual cash flow function is concave in both the decision variables* (K_{t+1}, s_t) *and in the initial productive capital* K_t.

For proof, see Appendix A.

When the firm chooses allocations to maximize future payoffs, it solves

$$V_0(K_0) = \underset{\{K_{t+1},s_t\}_{t=0}^{T}}{Max} \sum_{t=0}^{T} \phi^t \pi(K_t, K_{t+1}, s_t) + \phi^{T+1} W(K_{T+1}) \tag{12}$$

The above formulation is different from Eq. (6) in that it captures the effects of borrowing, financial distress and allocation to security. In this case, the firm reduces current expected breach costs by diverting

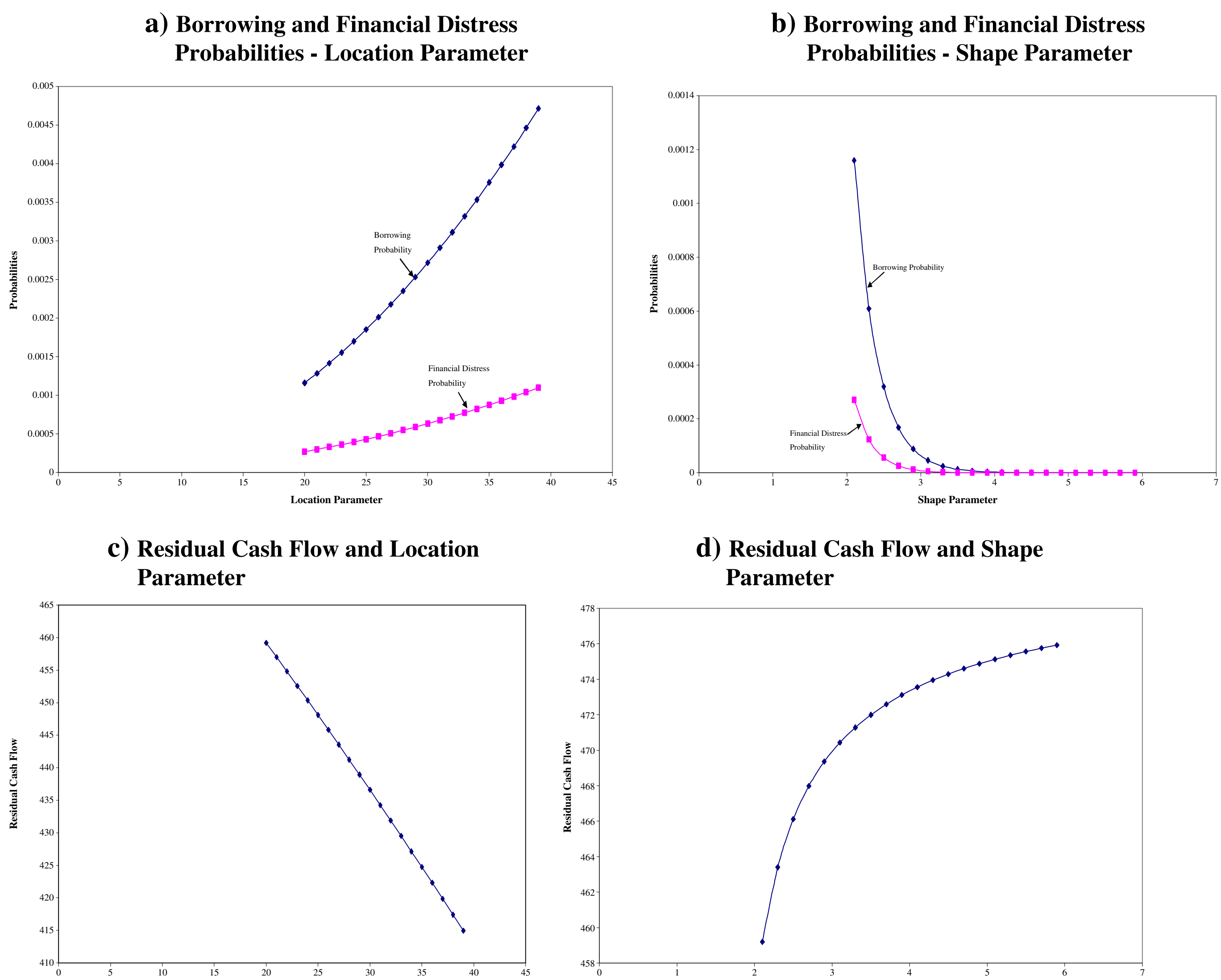

Fig. 2. a: Borrowing and financial distress probabilities — location parameter. b: Borrowing and financial distress probabilities — shape parameter. c: Residual cash flow and location parameter. d: Residual cash flow and shape parameter.

allocations from revenue generating to security assuring operations. As a result, future potential for residual cash flow generation could be compromised.

The dynamic optimization problem in Eq. (12) can be expressed as the following recursive form

$$\begin{aligned} &V_t(K_t) = \max_{\{K_{t+1},s_t\}} \pi(K_{t+1}, s_t; K_t) + \phi V_{t+1}(K_{t+1}) \quad t = 0, 1, ..T \\ &s.t.\ V_{T+1}(K_{T+1}) = W(K_{T+1})(\text{terminal condition}) \end{aligned} \tag{13}$$

We first show that an interior solution to Eq. (13) exists in Lemma 2.

Lemma 2.

(1) *The value function $V_t(K_t)$ for each $t \in [0, T]$ is strictly concave.*
(2) *The value function $V_t(K_t)$ for each $t \in [0, T]$ is differentiable and $V'_t(K_t) = \frac{\partial \pi(K_t, K^*_{t+1}, s^*_t)}{\partial K_t}$ for each $t \in [0, T]$, where K^*_{t+1} and s^*_t denote the optimal allocations in period t.*

Proof. See Appendix A

Using the results of Lemma 2, we now use the first order conditions to characterize the solution for Eq. (13) in Proposition 1.

Proposition 1. *The optimal revenue generating and security assuring allocations are determined uniquely by*

$$F'(K_{t+1}) = \frac{H_t(K_t, K_{t+1}, s_t)}{\phi H_{t+1}(K_{t+1}, K_{t+2}, s_{t+1})} - (1-\beta), \quad t = 0, 1, ...T-1 \tag{14}$$

$$F'(K_{T+1}) = \frac{H_T(K_T, K_{T+1}, s_T)}{\phi} - (1-\beta) \tag{15}$$

$$h'(s_t) = \frac{H_t(K_t, K_{t+1}, s_t)}{\Psi_t(K_t, K_{t+1}, s_t)}, \quad t = 0, 1, ...T \tag{16}$$

Where

$$\begin{aligned} H_t(K_t, K_{t+1}, s_t) &= 1 + r\rho_t \\ &+ \theta_t \left\{ \frac{1+r}{\delta-1} + \frac{\delta}{z_t + D} \left[(D(1+r) + \varpi) - (1+r)\left(\frac{\delta}{\delta-1}(z_t + D) - z_t \right) \right] \right\} \end{aligned} \tag{17}$$

and

$$\begin{aligned} &\Psi_t(K_t, K_{t+1}, s_t) \\ &= -\frac{\delta\theta_t}{h(s_t)} \left[(D(1+r) + \varpi) - (1+r)\left(\frac{\delta}{\delta-1}(z_t + D) - z_t \right) \right] - \frac{\delta}{\delta-1}(1 + r\eta_t) \end{aligned} \tag{18}$$

in which $\eta_t = \left(\frac{z_t}{h(s_t)} \right)^{-\delta+1}$

Proof. See Appendix A.

Eqs. (14)–(16) are nonlinear second-order difference equations characterizing the optimal allocations in the planning horizon. Given the initial productive capital K_0, Eqs. (14)–(16) constitute *2 T* equations to solve uniquely the optimal path of the *2 T* allocations $(K^*_1, K^*_2, \ldots, K^*_{T+1}, s^*_0, s^*_1, \ldots, s^*_T)$. Comparing Eqs. (14) and (15) with Eq. (8), the impact of security breach on the firm's productive investment is captured by the function $H_t(K_t, K_{t+1}, s_t)$, which has intuitive economic interpretations. In the RHS of Eq. (17), the second term represents the expected cost when $z_t < \xi_t \le z_t + D$ and the third term represents expected cost related to financial distress. One could interpret the third term of the right hand side of Eq. (17) in the following way. First, $E(\xi_t | \xi_t > z_t + D) = \frac{\delta}{\delta-1}(z_t + D)$. In the absence of financial distress cost, the firm would still incur the cost $(1+r) \times \left(\frac{\delta}{\delta-1}(z_t + D) - z_t \right)$ when $\xi_t > z_t + D$. When $\xi_t > z_t + D$, the firm would incur a cost of $(D \cdot (1 + r) + \varpi)$. Therefore the difference between $(D \cdot (1 + r) + \varpi)$ and $(1+r)\left(\frac{\delta}{\delta-1}(z_t + D) - z_t\right)$ is the expected net cost attributable to financial distress. Since all the terms of the RHS of Eq. (17) are positive, we have $H_t(K_t, K_{t+1}, s_t) > 1, \forall\, t = 1, \ldots, T$.

From these equations, we characterize dynamic behavior of the optimal allocations over the planning horizon.

Proposition 2.

1. *There exists a unique steady-state optimal allocation. At the steady-state, productive capital is the same as the optimal no-breach and frictionless productive capital K^*.*
2. *On the optimal allocation path, the expected security breach cost decreases over time when productive capital is less than the optimal no-breach productive capital K^* and increases over time when productive capital is greater than the optimal no-breach productive capital K^*.*
3. *On the optimal allocation path, productive capital at the terminal date, K^*_{T+1}, is less than the optimal no-breach productive capital K^*.*

Proof. See Appendix A.

The first part of Proposition 2 shows that when steady state is reached, the firm's cumulative productive investment is the same as the one in the benchmark situation. The intuition behind this result is that a larger productive capital results in larger cash generation capability, provides a greater margin of safety and thereby reduces the chance of future breach costs causing financial distress in the long run. The second part of the proposition shows that if the initial productive capital K_0 is lower than K^* (as it will be because the managers allocate more funds to security and less to productive assets), the firm accumulates productive capital and thereby acquires greater capability to withstand security breaches over time, thus reducing the allocation needed for security. When the productive capital reaches the benchmark no-breach level, the firm will maintain the productive capital at that level since further accumulation is not economically efficient; accumulating productive capital to a level which is higher than K^* causes the firm to face higher expected security breach costs over time. The third part of the proposition shows that towards the end of the horizon, the firm reduces its capital expenditure to increase the residual cash flow. This result is intuitive because the firm needs less self-protection against security breaches as the terminal date approaches.

When a firm's planning horizon is long, its productive capital will approach the steady-state no-breach level. Although security breach costs have no impact on the level of firm's steady-state productive capital, they increase the transition period and slow down the rate at which the firm accumulates its productive capital. Since Eqs. (14)–(16) are nonlinear second-order difference equations, a completely analytical treatment of the comparative dynamics to show how security breach costs affect capital accumulation during the transition period, is not mathematically tractable. Instead, we numerically explore the firm's allocations to revenue generating and security assuring operations over time.

4.5.2. Sensitivity Analysis

In this subsection, we examine the effect of changes in key parameters on the resource allocation decisions.[25]

4.5.2.1. The effect of higher relative financial distress costs. The revenue generating function used in the numerical illustration is Cobb-Douglas where $F(K_t) = 100K_t^{0.3}$ and the security assuring function is characterized by $h(s_t) = 20 + 100 \cdot (1 + s_t)^{-0.1}$. The planning horizon is assumed to be T = 500. The parameters held constant are $\beta = 0.15$,

[25] The parameter values chosen are hypothetical and are only meant to aid analysis of the firm's allocation decisions.

interest rate r = 0.05 and discount rate $\phi = 0.995$. The following parameters are changed: (i) debt limit D = 300, 500, 1000; (ii) aggregate financial distress cost $\varpi = 10000, 20000, 30000$; (iii) shape parameter $\delta = 2.1, 3.0, 5.0$.

Fig. 3a to c depict productive capital accumulations and Fig. 3d to f give security allocations over the first 20 time periods of the planning horizon. Under the chosen values of the parameters, the no-breach steady state productive capital (K^*) is about 1848. Starting from an initial productive capital ($K_0 = 750$), the firm accumulates productive capital asymptotically to K^* over the planning horizon. Initially, when productive capital is low, the firm relies more on higher security allocations to cover current breach costs. As the firm's productive capital approaches the steady-state level, s_t drops. Based on this numerical analysis, we state the following result:

Proposition 3. *On the optimal path, a firm accumulates productive capital faster if the borrowing limit is higher and/or the aggregate financial distress cost and/or the uncertainty is lower. Further, allocation to security assuring operation is higher if the borrowing limit is lower and/or the aggregate financial distress cost and/or the uncertainty is higher.*

Proposition 3 addresses the issue of misalignment of interests between the managers and investors. Managers overweight the financial distress cost because financial distress can destroy their jobs, compensation and reputation compared to investors who diversify away most of the financial distress costs. Therefore, managers making the allocation decisions will follow a path in which the accumulation of productive capital is slower and therefore the cash generation is also lower over a long period compared to what the investors would have chosen if they had the decision-making rights.

It is seen from Fig. 3d to f that the allocation to security is: lower in every period when the debt limit is relaxed (compare D = 1000 with D = 300 or 500 in 3d); higher in every period when the financial distress cost is higher (Compare $\varpi = 30{,}000$ with $\varpi = 10{,}000$ or 20,000 in 3e); and is lower when the shape parameter is higher (Compare $\delta = 5.0$ with $\delta = 2.1$ or 3 in 3f). Managers who ultimately make the allocation decisions are faced with a relatively higher ϖ and therefore make higher security allocation in every period. From Fig. 3b, we find that managers who have higher relative financial distress costs also make lower allocation to productive processes, slowing the accumulation of productive capital.

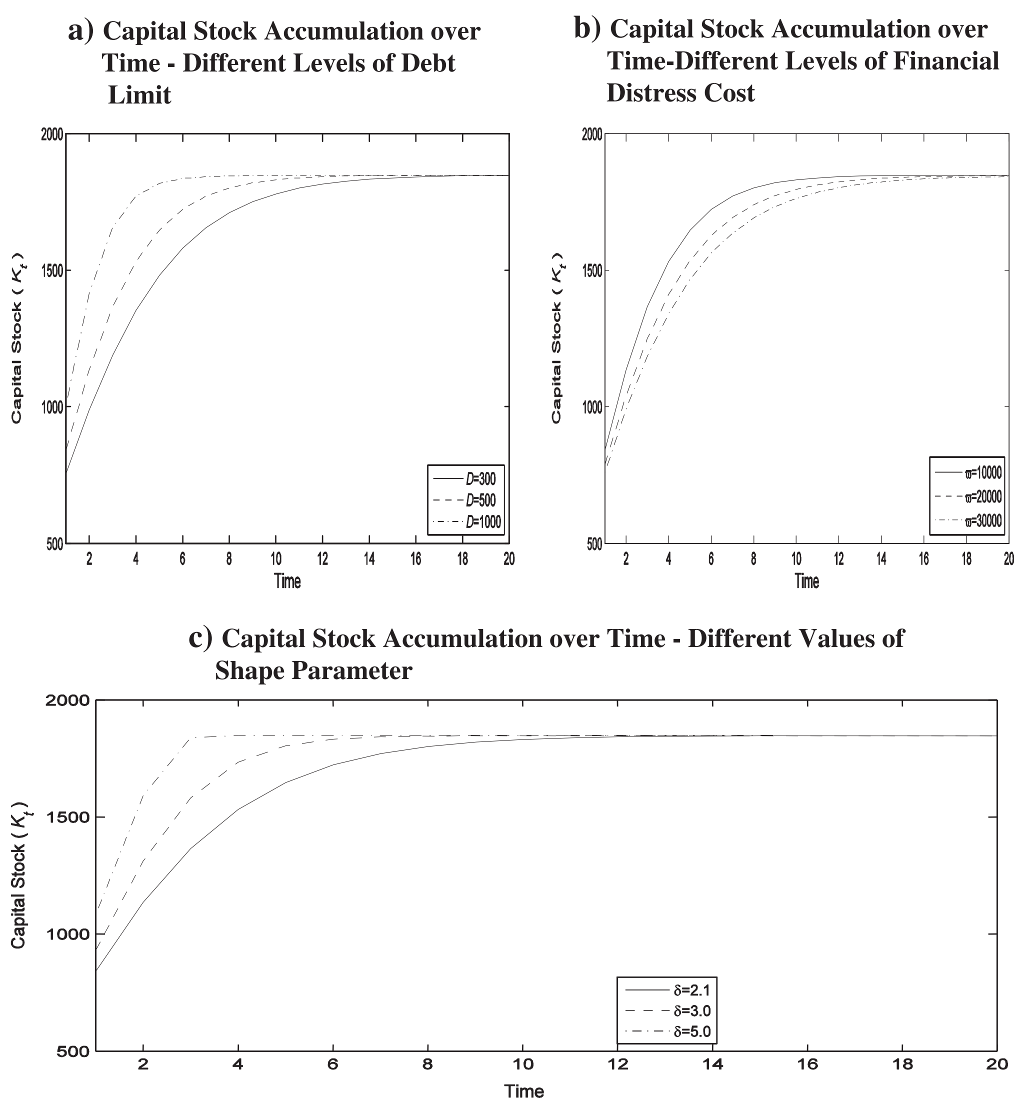

Fig. 3. a: Capital stock accumulation over time — different levels of debt limit. b: Capital stock accumulation over time — different levels of financial distress cost. c: Capital stock accumulation over time — different values of shape parameter. d: Allocations to security over time — different levels of debt limit. e: Allocations to security over time — different levels of financial distress cost. f: Allocations to security over time — different values of shape parameter.

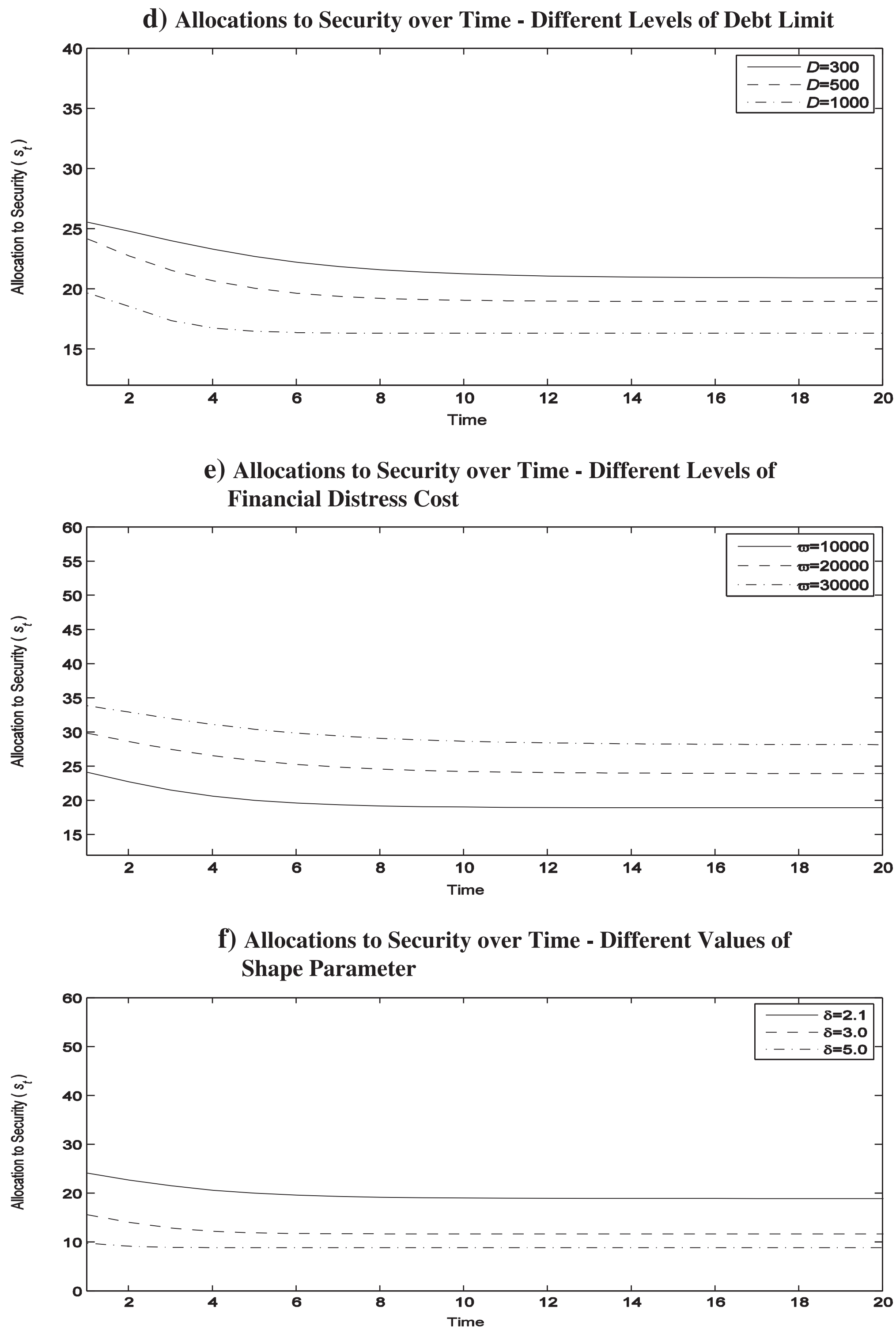

Fig. 3 (*continued*).

4.5.2.2. The effect of short planning horizon. The analysis in the previous section shows that when a firm's planning horizon is long, (i.e., as T approaches ∞), the firm will either accumulate the productive capital to the no-breach level or maintain that level forever. In reality, managers have limited tenures in their firms and therefore have shorter horizons for their investment decisions compared to investors [4,10,37,42,43]. In particular, Stein [43] shows that in a non-cooperative game between managers and long-term investors, myopic behavior by managers can be Nash equilibrium when their interests are not aligned.

As in Eq. (9), we consider a myopic decision maker who maximizes only current earnings and wealth. In contrast to a no-breach environment, the myopic decision rule impacts the capital investment of the firm when it faces security breaches and financial distress costs.

Under the myopic decision rule, the firm solves

$$\underset{K_{t+1},s_t}{Max} \quad \pi(K_t, K_{t+1}, s_t) + \phi \cdot [F(K_{t+1}) + (1-\beta)K_{t+1}] \tag{19}$$

in each period such that given an initial productive capital, the path of capital accumulation and security assurance allocations are uniquely determined by the first-order conditions (by the concavity of both $\pi(K_t, K_{t+1}, s_t)$ and $F(K_{t+1})$):

$$F'(K_{t+1}) = \frac{H_t(K_t, K_{t+1}, s_t)}{\phi} - (1-\beta) \quad t = 0, 1, ..T \tag{20}$$

$$h'(s_t) = \frac{H_t(K_t, K_{t+1}, s_t)}{\Psi_t(K_t, K_{t+1}, s_t)} \quad t = 0, 1, ..T \tag{21}$$

where $H_t(K_t, K_{t+1}, s_t)$ and $\Psi_t(K_t, K_{t+1}, s_t)$ are the same as in Eqs. (17) and (18). By comparing Eqs. (20) and (21) with Eqs. (14)–(16), we can have the following results.

Proposition 4.

1. *Let K^m_{t+1} be the optimal productive capital under myopic decision rule given a K_t. Then we have $K^m_{t+1} < K^*$ for any K_t.*
2. *Let $\Delta \equiv K^* - K^m_{t+1}$ denote the deviation of K^m_{t+1} from K^*. For any given K_t, The deviation increases with the increase in external finance cost (r) and the deviation decreases with the increase in borrowing limit (D).*
3. *Under myopic decision rule, a firm spends more on security assuring operations than it does at the steady-state under long planning horizon.*

Proof. See Appendix A.

Proposition 4 shows that in contrast to the base case where the length of planning horizon does not impact the firm's capital investment decision, managers with short planning horizon will not accumulate the firm's productive capital to the optimal level. Myopic managers' capital investments are smaller when the firm's cost of external finance is larger and the firm is more credit constrained.

Intuitively, compared to investors with long planning horizon, managers with short planning horizon have more incentive to boost current earnings and less incentive to accumulate productive capital. As a result, myopic managers accumulate less productive capital than desired by investors with long horizon. Because they operate with less capital, the demand for protecting against current security risks forces them to allocate more funds (compared with identical firms with long planning horizon) to security assurance. An implication for corporate management from Proposition 4 is that it is more important for firms facing higher security breach risks to discourage myopic behavior.

5. Model with Cyber-Insurance

The study of cyber-insurance as a way to mitigate cyber-security risks has received considerable attention over the last decade. Several studies consider cyber-insurance contracts in an interconnected system with different stakeholders when there are correlated security breach damages due to organizational interdependencies (links between suppliers and producers in a supply chain) (Ogut and Menon 2005; [35]; Yurcik 2002; Shetty et al. 2009). A second stream of literature focuses on cyber-insurance as a means to mitigate under-investment in security ([6,8]; Shetty et al. 2009; [24,25]). Another stream of research develops analytical models to determine the cyber-risk insurer's premium [7,22,33]. They use copula based models to price insurance products that incorporate risk profiles and the wealth of the insured firm. We model a case where the firm can purchase cyber-insurance for information security breach costs and both the firm and the insurer are risk neutral. Risk aversion is not necessary for our results.[26]

The previous sections described models that did not include cyber-insurance. In order to be consistent with the earlier models, we do not include the insurance premium paid by the firm in the breach costs. We use $\sigma_t \equiv \mu \xi_t$ (where $\mu \in (0,1)$) to denote the firm's net realized information breach costs after claiming the insurance. Thus $(1 - \mu)$ represents the external insurance coverage obtained by the firm. We denote the insurance premium paid by the firm for the coverage $1 - \mu$ as τ. Since ξ_t follows the Pareto distribution, we get the density function of σ_t as

$$f(\sigma_t) = \frac{1}{\mu} \frac{\delta \cdot h(s_t)^\delta}{\left(\frac{1}{\mu}\sigma_t\right)^{\delta+1}} = \frac{\delta \cdot (\mu \cdot h(s_t))^\delta}{\sigma_t^{\delta+1}} \tag{22}$$

Eq. (22) shows that σ_t also follows a Pareto distribution with shape parameter δ and location parameter $\mu \cdot h(s_t)$. The optimal allocations with this insurance coverage can be determined uniquely by Eqs. (14)–(16) after replacing ρ_t with $\tilde{\rho}_t \equiv \left(\frac{z_t}{\mu h(s_t)}\right)^{-\delta}$, θ_t with $\tilde{\theta}_t \equiv \left(\frac{z_t + D}{\mu h(s_t)}\right)^{-\delta}$, and η_t with $\tilde{\eta}_t \equiv \left(\frac{z_t}{\mu h(s_t)}\right)^{-\delta+1}$.

Further, external insurance coverage is helpful in partially correcting the under-investment (overinvestment) in productive capital (security) caused by managers' actions.

Proposition 5.

1. *The steady-state productive capital increases with the increase in the external insurance coverage.*
2. *The steady-state security assuring allocation under myopic decision rule decreases with the increase in the external insurance coverage.*

Proof. See Appendix A.

By analyzing resource allocations of a firm under external insurance coverage, we conclude that there exists a feasible premium τ for the coverage $1 - \mu$ since that a firm, even the managers are risk neutral, can always benefit from an external insurance coverage. In particular, we have

Proposition 6. *In any period t, insurance with a premium τ for the coverage $1 - \mu$ is feasible if the following condition holds:*

$$\frac{(1-\mu)}{(1-\mu^\delta)} < \frac{\theta_t}{h(s_t)} \left[\frac{\delta}{(\delta-1)} \varpi + z_t + D\right] \tag{23}$$

Proof. See Appendix A

We illustrate Proposition 6 by a numerical example where $\varpi = 200000$, $D = 1000$, $z_t = 500$ and $h(s_t) = 40$. Fig. 4a shows the effect of variation in the shape parameter δ on the range (RHS–LHS) of the inequality (23). When this range is positive, purchasing insurance can be beneficial to both the firm and the insurance provider. This is true for smaller values of δ. For larger values of δ, the probability of financial distress and the resulting cost is smaller. This could render the purchase of insurance unnecessary. Fig. 4b shows the effect of the variation in μ on the range over which it benefits both the entities. Consistent with our intuition, the plot shows that there is a threshold level beyond which the coverage becomes excessive (i.e., the range becomes negative). Fig. 4c and d show the effect of insurance coverage on productive capital and security allocation respectively. It is seen that insurance coverage increases the rate of productive capital accumulation and reduces the allocation to security.

From this analysis, we can also draw several implications for the design of efficient cyber insurance policy. First, an excessive insurance coverage may result in the *moral hazard* problem which has been widely documented in other insurance contexts. Our analysis indicates that managers in client firms will reduce allocation to security assuring operations under external insurance coverage. This behavior cannot be

[26] We assume that the firm still invests in security protection without which the insurer is unlikely to provide the insurance.

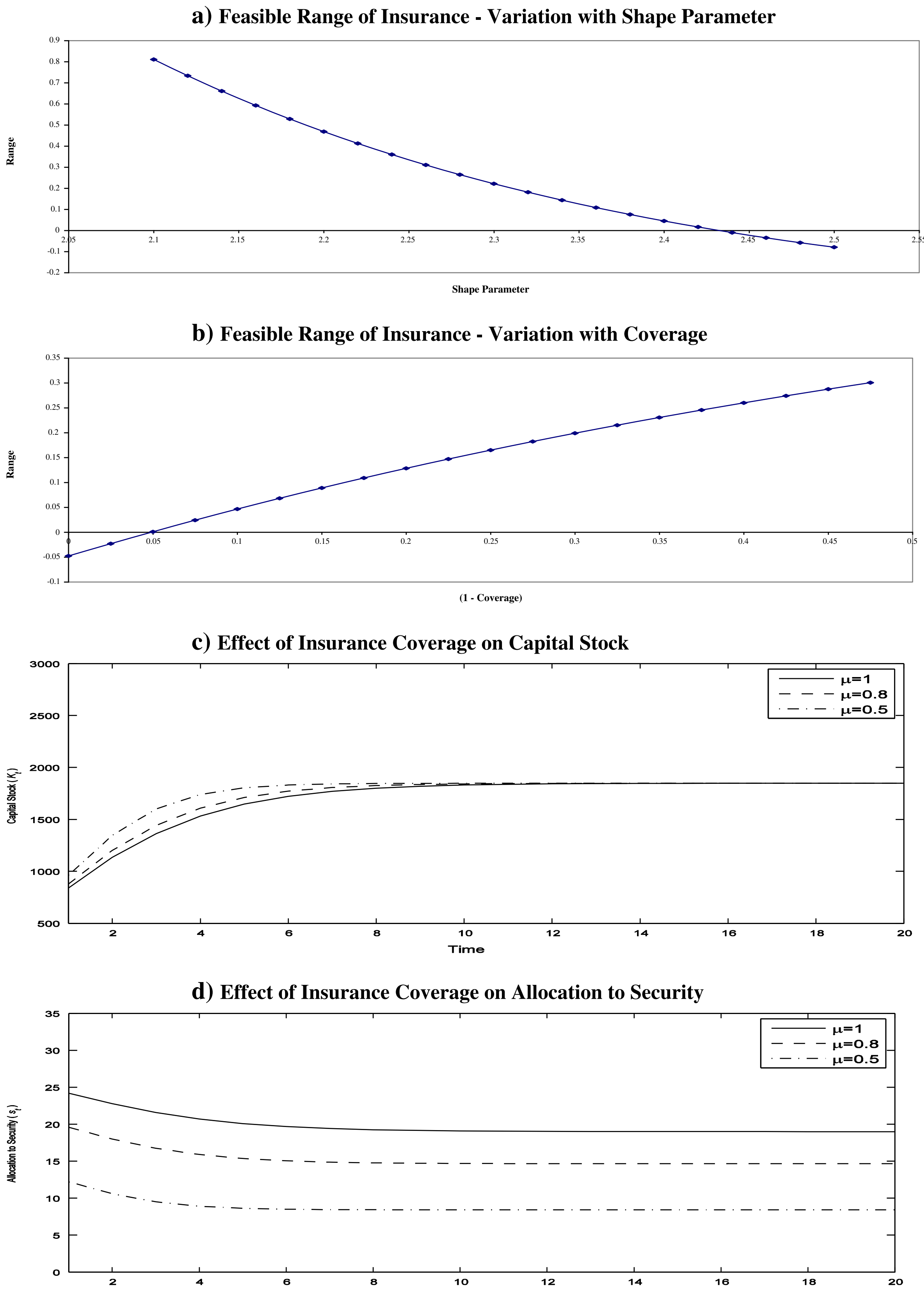

Fig. 4. a: Feasible range of insurance — variation with shape parameter. b: Feasible range of insurance — variation with coverage. c: Effect of insurance coverage on capital stock. d: Effect of insurance coverage on allocation to security.

monitored by insurance providers. Therefore, excessive insurance coverage can cause significant underinvestment in security assurance. This observation is in line with Ogut et al. [36] where it was concluded that the interdependency of cyber-risk leads firms to invest less than the socially optimal levels in IT security technologies and instead buy insurance coverage. Insurers are also not keen in absorbing large risks since the firm allocates reduced resources to security assuring operations. As a result, the number of security breaches could rise significantly. When firms' behavior cannot be monitored, it is important for a cyber-insurance provider to design the insurance coverage and premium policy to induce firms to make adequate resource allocation to security assurance. Mukhopadhyay et al. [33] show that firms' investment in cyber-insurance varies according to their risk profiles. Our analysis adds to this stream of findings and highlights that insurance coverage also varies according to the size of the firm. When a firm's size is small, a large insurance coverage can help the firm speed up its capital accumulation. However, when a firm's size is already large and its productive capital is close to the steady-state level, insurance coverage has little effect on the firm's productive investment and mainly crowds out its allocation to security assurance.

6. Summary and concluding remarks

In this paper, we examine the allocation of resources to productive assets and security operations in the presence of costly security breaches that could result in financial distress. In addition, we also investigate the role of external insurance in mitigating the effects of breach costs. We build a decision support model to aid the decision makers in the allocation of resources to productive and security operations in the presence of cyber-security breach costs and financial distress costs. Using that model, we show that the rate at which the productive capital stock accumulates is affected by the costs of debt and financial distress. Using the same optimization model, managers will over-invest in security and under-invest in productive assets because of two reasons. They have invested their non-diversifiable human capital in the firm which makes their personal costs of the firm's financial distress higher than for the investors who can diversify across firms. Second, they have limited tenures and therefore shorter time horizons than investors. In this paper, we examine the effect of these differences in incentives of investors and managers.

Our investigation of the role of external insurance indicates that insurance could be beneficial to both the firm and the provider. Furthermore, our analysis shows that insurance helps firms whose managers have short planning horizons to speedily accumulate productive capital and thus offset the adverse effects of the misalignment of managerial and investor interests. As cyber-security draws more attention and investments at private firms and government agencies, the results and insights obtained in this paper could be of value to both academicians and practitioners. Specifically the results could provide a basis for structuring incentives such that the goals of both managers and investors are properly aligned.

While this analysis has focused on information security breaches, it can be broadened to address resource allocation in the presence of other security and internal control breaches including terrorist attacks, governance failures and internal control failures. One limitation of the current analysis is that it does not account for potential learning about the effectiveness of the resources allocated to security in the previous period. A future study could incorporate learning effect in fine-tuning the allocations over the planning horizon.

Appendix A

Derivation of Eq. (8): Let K_t^* denote the optimal investment decision made at the beginning of time period t. We show that if $K_t^*{}_{+1}$ is a constant (not a function of K_t^*), so is K_t^* and K_t^* is determined by $F'(K_t) = \frac{1}{\phi} - (1-\beta)$.

The value function at time t is

$$V_t(K_t) = F(K_t) - K_{t+1}^* + (1-\beta)K_t + \phi V_{t+1}\left(K_{t+1}^*\right)$$

Differentiating, we have $V_t'(K_t) = F'(K_t) + (1-\beta)$ if K_{t+1}^* is a constant.

The solution is then determined by the first order condition. $\phi V_t'(K_t) = 1 \Rightarrow F'(K_t) = \frac{1}{\phi} - (1-\beta)$, and K_t^* is a constant.

We can then finish the proof by showing that K_{T+1}^* is a constant and is determined by $F'(K_{T+1}) = \frac{1}{\phi} - (1-\beta)$. At $t = T$, the firm solves

$$\underset{K_{T+1}}{Max}\ F(K_T) - K_{T+1} + (1-\beta)K_T + \phi F(K_{T+1}) + \phi(1-\beta)K_{T+1}$$

So K_{T+1}^* is a constant and it is determined by the first order condition $F'(K_{T+1}) = \frac{1}{\phi} - (1-\beta)$. ■

Proof of Lemma 1. Define $M_1(K_t, K_{t+1}, s_t) = z_t - \frac{\delta}{\delta-1}h(s_t) - \frac{r}{\delta-1}\rho_t z_t$ and $M_2(K_t, K_{t+1}, s_t) = \theta_t\left[(1+r)\left(\frac{\delta}{\delta-1}(z_t+D) - z_t\right) - (D(1+r)+\varpi)\right] = \theta_t \cdot E_t$, the one-period residual cash flow is

$$\pi(K_t, K_{t+1}, s_t) = M_1(K_t, K_{t+1}, s_t) + M_2(K_t, K_{t+1}, s_t)$$

We can show that both $M_1(K_t, K_{t+1}, s_t)$ and $M_2(K_t, K_{t+1}, s_t)$ are concave in decision variables and state parameter. First for $M_1(K_t, K_{t+1}, s_t)$, by differentiating the function with respect to K_t,

$$\frac{\partial M_1(K_t, K_{t+1}, s_t)}{\partial K_t} = \left[F'(K_t) + (1-\beta)\right] \cdot (1 + r \cdot \rho_t) > 0$$
$$\frac{\partial^2 M_1(K_t, K_{t+1}, s_t)}{\partial K_t^2} = F''(K_t)[1 + r \cdot \rho_t] - r\left[F'(K_t) + (1-\beta)\right]\frac{\partial \rho_t}{\partial K_t} < 0$$

Then, by differentiating $M_1(K_t, K_{t+1}, s_t)$ respect to the decision variables,

$$G_K(K_{t+1}, s_t) \equiv \frac{\partial M_1(K_t, K_{t+1}, s_t)}{\partial K_{t+1}} = -1 - r \cdot \rho_t$$

$$G_s(K_{t+1}, s) \equiv \frac{\partial M_1(K_t, K_{t+1}, s_t)}{\partial s_t} = -\frac{\delta}{\delta-1}h'(s_t) \cdot \left(1 + r \cdot \left(\frac{z_t}{h(s_t)}\right)^{1-\delta}\right) - 1 - r\rho_t$$

The Hessian matrix is then

$$H1 = \begin{bmatrix} G_{KK} & G_{Ks} \\ G_{sK} & G_{ss} \end{bmatrix}$$

where

$$G_{KK} \equiv \frac{\partial G_K(\cdot)}{\partial K_{t+1}} = -\delta \cdot r \cdot \rho_t \cdot \frac{1}{z_t}$$
$$G_{Ks} \equiv \frac{\partial G_K(\cdot)}{\partial s_t} = G_{sK} \equiv \frac{\partial G_s(\cdot)}{\partial K_{t+1}} = -\delta \cdot r \cdot \rho_t \cdot \left(\frac{h'(s_t)}{h(s_t)} + \frac{1}{z_t}\right)$$
$$G_{ss} \equiv \frac{\partial G_s(\cdot)}{\partial s_t} = \frac{\delta}{1-\delta} \cdot h''(s_t) \cdot \left(1 + r \cdot \left(\frac{z_t}{h(s_t)}\right)^{1-\delta}\right) - 2 \cdot \delta \cdot r \cdot \rho_t \cdot \frac{h'(s_t)}{h(s_t)}$$
$$-\delta \cdot r \cdot \rho_t \cdot \left(\frac{h'(s_t)}{h(s_t)}\right)^2 z_t$$
$$-\delta \cdot r \cdot \rho_t \cdot z_t^{-1}$$

The determinant of H1 is $det(H1) = \frac{\delta}{\delta-1}h''(s_t) \cdot \left[1 + \left(\frac{z_t}{h(s_t)}\right)^{1-\delta}\right] \cdot \delta \cdot r \cdot \rho_t \cdot \frac{1}{z_t} > 0$. Combining this with $G_{KK} < 0$, we get that $M_1(K_{t+1}, s_t; K_t)$ is strictly concave in the decision variables.

For $M_2(K_t, K_{t+1}, s_t)$, by direct differentiation with respect to K_t, we get

$$\frac{\partial M_2(K_t,K_{t+1},s_t)}{\partial K_t} = -\frac{\delta}{z_t+D}\theta_t \cdot E_t \cdot [F'(K_t)+(1-\beta)] + \theta_t\frac{1+r}{\delta-1}[F'(K_t)+(1-\beta)]$$

$$\frac{\partial^2 M_2(K_t,K_{t+1},s_t)}{\partial K_t^2} = \left(\frac{\delta\theta_t}{z_t+D}[F'(K_t)+(1-\beta)]\right)^2\cdot E_t + \frac{\delta\theta_t}{(z_t+D)^2}[F'(K_t)+(1-\beta)]\cdot E_t$$
$$-\frac{\delta\theta_t}{z_t+D}F''(K_t)\cdot E_t - 2\frac{\delta\theta_t}{z_t+D}\frac{1+r}{\delta-1}[F'(K_t)+(1-\beta)] + \theta_t\frac{1+r}{\delta-1}F''(K_t)<0$$

Above term is strictly negative because $E_t < 0$ and $F(K_t)$ is increasing and concave. By direct differentiation with respect to decision variables,

$$\frac{\partial M_2(K_t,K_{t+1},s_t)}{\partial K_{t+1}} = \frac{\delta}{z_t+D}\theta_t E_t - \theta_t\frac{1+r}{\delta-1}$$
$$\frac{\partial M_2(K_t,K_{t+1},s_t)}{\partial s_t} = \delta\cdot\theta_t\cdot\left[\frac{1}{z_t+D}+\frac{h'(s_t)}{h(s_t)}\right]\cdot E_t - \theta_t\frac{1+r}{\delta-1}$$

The Hessian matrix is $H2 = \begin{bmatrix} G_{KK} & G_{Ks} \\ G_{Ks} & G_{ss}\end{bmatrix}$ where

$$G_{KK}\equiv\frac{\partial^2 M_2(K_t,K_{t+1},s_t)}{\partial K_{t+1}^2} = \frac{\delta(1+\delta)\theta_t}{(z_t+D)^2}E_t - 2\frac{\delta\theta_t(1+r)}{(z_t+D)(\delta-1)}<0$$
$$G_{Ks}\equiv\frac{\partial^2 M_2(K_t,K_{t+1},s_t)}{\partial K_{t+1}\partial s_t} = \frac{\delta(1+\delta)\theta_t}{(z_t+D)^2}E_t - 2\frac{\delta\theta_t(1+r)}{(z_t+D)(\delta-1)} + \delta\theta_t(1+r)\frac{h'(s_t)}{h(s_t)} = G_{KK} + \delta\theta_t(1+r)\frac{h'(s_t)}{h(s_t)}$$
$$G_{ss}\equiv\frac{\partial^2 M_2(K_t,K_{t+1},s_t)}{\partial s_t^2} = G_{KK} + \delta\theta_t(1+r)\frac{h'(s_t)}{h(s_t)}\frac{D}{z_t+D} + \delta\theta_t\frac{h''(s_t)}{h(s_t)}E_t<0$$

Thus

$$\det(H2) = \delta\theta_t(1+r)\frac{h'(s_t)}{h(s_t)}\cdot\left[2G_{KK} + G_{KK}\frac{D}{z_t+D} + \delta\theta_t(1+r)\frac{h'(s_t)}{h(s_t)}\right] + \delta\theta_t(1+r)\frac{h''(s_t)}{h(s_t)}E_tG_{KK}>0$$

and $M_2(K_t, K_{t+1}, s_t)$ is concave in decision variables. ■

Proof of Lemma 2. The proof of Lemma 2: (1) is carried out by backward induction. We first show that $V_T(K_T)$ is strictly concave.

Let $G(K_T, K_{T+1}, s_T) = \pi(K_T, K_{T+1}, s_T) + \varphi W(K_{T+1})$, and $G(K_T, K_{T+1}, s_T)$ is concave in both decision variables $\Gamma_T \equiv (K_{T+1}, s_T)$ and the state variable K_T from Lemma 1 and the concavity assumption of the revenue generating function $F(K_{T+1})$. Considering two capital stocks K_T' and K_T'', let $\Gamma_T' \equiv \Gamma(K_T')$ and $\Gamma_T'' \equiv \Gamma(K_T'')$ denote the optimal solutions corresponding to the two capital stocks; also, let $K^\lambda = (1-\lambda)K_T' + \lambda K_T''$ and $\Gamma^\lambda = (1-\lambda)\Gamma_T' + \lambda\Gamma_T''$ for $\lambda \in (0, 1)$, we have

$$V_T\left(K^\lambda\right) = G\left(\theta\left(K^\lambda\right),K^\lambda\right)\geq G\left(\theta^\lambda,K^\lambda\right)>(1-\lambda)G(\Gamma_T',K_T') + \lambda G\left(\Gamma_T'',K_T''\right)$$
$$=(1-\lambda)V_T(K_T') + \lambda V_T\left(K_T''\right)$$

that is, $V_T(K_T)$ is strictly concave.

Defining $G(K_{t-1}, K_t, s_{t-1}) = \pi(K_{t-1}, K_t, s_{t-1}) + \varphi V_t(K_t)$, by the same way we can show that if $V_t(K_t)$ is strictly concave, $V_{t-1}(K_{t-1})$ is also strictly concave and this completes proof of Eq. (1).

For Lemma 2: (2), consider a capital stock K_t'. Let K_{t+1}^* and s_t^* denote the optimal solutions corresponding to this capital stock. Define

$$L(K_t) = \pi\left(K_t,K_{t+1}^*,s_t^*\right) + \phi V_{t+1}\left(K_{t+1}^*\right)$$

$L(K_t)$ is concave and differentiable; also $L(K_t) \leq V_t(K_t)$ with equality only at $K_t = K_t'$. We then have $V_t(K_t)$ differentiable at K_t', and $V_t'(K_t') = L'(K_t')$ (From Theorem 4.10 in [44]). ■

Proof of Proposition 1. The first order conditions of the optimization problem in (13) are:

$$\frac{\partial\pi(K_t,K_{t+1},s_t)}{\partial K_{t+1}} + \phi V'(K_{t+1}) = 0 \quad t=0,1,\,..T$$
$$\frac{\partial\pi(K_t,K_{t+1},s_t)}{\partial K_{t+1}} + \phi W'(K_{t+1}) = 0, t=T$$
$$\frac{\partial\pi(K_t,K_{t+1},s_t)}{\partial s_t} = 0$$

Based on Lemma 2, $V_t'(K_{t+1})$ can be replaced by $\frac{\partial\pi\left(K_t,K_{t+1}^*,s_t^*\right)}{\partial K_t}$. Furthermore, the optimal investment plans are determined uniquely by the first-order conditions because of the strict concavity of the value function and the one-period expected profit function. This completes the proof of Proposition 2. ■

Proof of Proposition 2. For Eq. (1), let $K_t = \overline{K}$ for each $t \leq T$, from Eq. (16) security allocation is determined by

$$h'(s_t) = \frac{H_t(\overline{K},s_t)}{\Psi_t(\overline{K},s_t)}$$

Since capital stock is fixed, the solution for security allocation will be the same for all periods, that is, $s_t = \bar{s}$ for each t. Now, $H_t(K_t, K_{t+1}, s_t) = H_{t+1}(K_{t+1}, K_{t+2}, s_{t+1})$ from Eq. (14). The capital stock in each period t is determined by $F'(K_{t+1}) = \frac{1}{\phi} - (1-\beta)$, which is the same as benchmark steady-state condition.

For Eq. (2), because of the strict concavity of $F(K_{t+1})$, $K_{t+1} < K^* \Leftrightarrow H_t(K_t, K_{t+1}, s_t) > H_{t+1}(K_{t+1}, K_{t+2}, s_{t+1})$ and $K_{t+1} > K^* \Leftrightarrow H_t(K_t, K_{t+1}, s_t) < H_{t+1}(K_{t+1}, K_{t+2}, s_{t+1})$.

For Eq. (3), it is trivial because in Eq. (16) $H_T(K_T, K_{T+1}, s_T) > 1$ and $F(K_{t+1})$ is strictly concave. ■

Proof of Proposition 4. For point 1, because $H_t(K_t, K_{t+1}, s_t) > 1$ for each t given $r > 0$ or $\theta_t > 0$, from the strict concavity of $F(K_{t+1})$ we know that the solution determined by Eq. (20) is less than K^* which is determined by Eq. (8) for any a given K_t. Point 2 can be obtained by showing that $H_t(K_t, K_{t+1}, s_t)$ is strictly increasing in borrowing cost r and strictly decreasing in borrowing limit D. By taking the first order differentiation of $H_t(K_t, K_{t+1}, s_t)$ on r and D, we can have the conclusion. In the extreme case when $r = 0$ and $D \to +\infty$, K^m approaches K^* because $H_t(K_t, K_{t+1}, s_t) \to 1$. For point 3, by taking the first-order differentiation of $h'(s) = \frac{H_t\left(K_t,K_{t+1}^m,s\right)}{\Psi_t\left(K_t,K_{t+1}^m,s\right)}$ with respect to K_{t+1}^m and we have $\frac{ds}{dK_{t+1}^m} < 0$. We can have the conclusion in point 3 because from point 1 we also know that $K_{t+1}^m < K^*$ for any a given K_t.

Proof of Proposition 5. The steady state (K^m, s^m) is determined by

$$F'(K^m) = \frac{\tilde{H}(K^m,s^m)}{\phi} - (1-\beta)$$
$$h'(s^m) = \frac{\tilde{H}(K^m,s^m)}{\tilde{\Psi}(K^m,s^m)}$$

Differentiate the above two equations with respect to μ and solve for $\frac{ds^m}{d\mu}$ and $\frac{dK^m}{d\mu}$, we can have $\frac{ds^m}{d\mu} > 0$ and $\frac{dK^m}{d\mu} < 0$. ■

Proof of Proposition 6. Using Eq. (22) and the definitions of $\tilde{\rho}_t$ and $\tilde{\theta}_t$, the decrease in the expected cost of financial distress to the firm when it purchases insurance can be shown to be

$$\Delta EFD = \left(1-\mu^\delta\right)\frac{h(s_t)^\delta}{(D+z_t)^{(\delta-1)}}\left[\frac{1}{(D+z_t)} + \frac{\delta}{(\delta-1)}\right]$$

The firm will find it advantageous to purchase insurance in period t if $\Delta EFD > \tau$. The expected payout by the insurance provider is $(1-\mu)\frac{\delta h(s_t)}{(\delta-1)}$. The insurance provider will offer the insurance if its expected payout is less than the premium τ. Following the above reasoning, we get Eq. (23).

References

[1] H. Almeida, T. Philippon, The risk adjusted cost of financial distress, Journal of Finance LXII (6) (2007) 2557–2586.
[2] T. Bandyopadhyay, V.S. Mookerjee, R.C. Rao, Why IT managers don't go for cyber-insurance products, Communication of the ACM 52 (11) (2009) 68–73.
[3] Betterley Report, Cyberrisk Market Syrvey, http://www.betterley.com2008.
[4] S. Bhojraj, R. Libby, Capital market pressure, disclosure frequency-induced earnings/cash flow conflict, and managerial myopia, The Accounting Review 80 (1) (2005) 1.
[6] R. Bohme, G. Schwartz, Modeling cyber-insurance: towards a unifying frame-work, Workshop on the Economics of Information Security (WEIS), Harvard, June 2010.
[7] R. Bohme, Security metrics and security investment models, in: I. Echizen, N. Kunihiro, R. Sasaki (Eds.), Advances in Information and Computer Security (IWSEC 2010), LNCS 6434, Springer-Verlag, Berlin Heidelberg 2010, pp. 10–24.
[8] R. Böhme, Cyber-insurance revisited, Workshop on the Economics of Information Security (WEIS), Harvard, 2005.
[9] J. Bolot, M. LeLarge, Cyber insurance as an incentive for internet security, Paper Read At Workshop In Economics Of Information Security (WEIS) At Hanover, NH, 2008.
[10] B.J. Bushee, The influence of institutional investors on myopic R&D investment behavior, The Accounting Review 73 (3) (1998) 305.
[11] H. Cavusoglu, B. Mishra, S. Raghunathan, The value of intrusion detection systems in information technology security architecture, Information Systems Research 16 (1) (2005) 28.
[12] H. Cavusoglu, H. Cavusoglu, J. Zhang, Security Patch Management: Share the Burden or Share the Damage? Management Science 54 (4) (2008) 657–670.
[13] H. Cavusoglu, S. Raghunathan, H. Cavusoglu, Configuration of and interaction between information security technologies: the case of firewalls and intrusion detection systems, Information Systems Research 20 (2) (2009) 198–217.
[14] M. Cerullo, V. Cerullo, Threat assessment and security measures justification for advanced IT networks, Information Systems Control Journal 1 (2005) 1–9.
[15] D. Chinn, J. Kaplan, A. Weinberg, Risk And Responsibility In A Hyper-Connected World: Implications For Enterprises Insights And Publications, McKinsey & Company, 2014.
[17] L.A. Gordon, M.P. Loeb, T. Sohail, A framework for using insurance for cyber-risk management, Association For Computing Machinery. Communications Of The ACM 46 (3) (2003) 81.
[18] L. Gordon, M.P. Loeb, The economics of information security investment, ACM Transactions of Information Systems Security 5 (4) (2002) 438–457.
[20] O. Hart, Corporate governance: some theory and implications, The Economic Journal 105 (430) (1995) 678–689.
[21] K. Hausken, Returns to information security investment: the effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability, Information Systems Frontiers 8 (5) (2006) 338.
[22] H. Herath, T. Herath, Copula based actuarial model for pricing cyber, Insurance Policies Insurance Markets and Companies: Analyses and Actuarial Computations 2 (2011).
[24] J.P. Kesan, P.M. Ruperto, J.Y. Willam, The economic case for cyberinsurance, Working Paper Series No. Paper No. LE04–004, Illinois Law and Economics, 2004.
[25] J.P. Kesan, R. Majuca, Cyberinsurance as a market-based solution to the problem of cybersecurity: a case study, Fourth Workshop on the Economics of Information Security (WEIS), Harvard, 2005.
[26] J.P. Kesan, R.P. Majuca, W.J. Yurcik, The Economic Case for Cyberinsurance, in: A. Chander, et al., (Eds.), Securing Privacy in the Internet Age, Stanford University Press, 2005.
[28] Christian Kleiber, Samuel Kotz, Statistical Size Distributions in Economics and Actuarial Sciences, Wiley, 2003.
[29] V. Kumar, R. Telang, T. Mukhopadhyay, Optimally securing interconnected information systems and assets, Paper read At Workshop In Economics Of Information Security (WEIS), At Pittsburgh, PA, 2007.
[30] S.J. Lubben, The direct costs of corporate reorganization: an empirical examination of professional fees in large chapter 11 cases, American Bankruptcy Law Journal 509 (2000) 508–552.
[31] R. Mookerjee, V. Mookerjee, Wei T. Yue, A. Bensoussan, Managing information security under continuous drift and sudden shocks, Proceedings of CIST 2011, November 12–13 2011.
[32] V. Mookerjee, R. Mookerjee, A. Bensoussan, W.T. Yue, When hackers talk: managing information security under variable attack rates and knowledge dissemination, Information Systems Research 22 (3) (September 2011) 606–623.
[33] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, S.K. Sadhukhan, Cyber-risk decision models: to insure IT or not? Decision Support Systems 56 (December 2013) 11–26.
[34] C. Newman, D. Stein, Cyberattacks a huge threat to start-ups, and their investors, New York Times (April 19 2013).
[35] H. Ögüt, S. Raghunathan, N. Menon, Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection, Risk Analysis 31 (3) (2010) 497–512.
[36] H. Ogut, S. Raghunathan, N. Menon, Cyber Insurance and IT security investment: impact of interdependent risk, Paper read At Workshop In Economics of Information Security (WEIS), Harvard University, Boston, MA, 2005.
[37] J. Ronen, J. Tzur, V.L. Yaari, The effect of directors' equity incentives on earnings management, Journal of Accounting and Public Policy 25 (4) (2006) 359.
[38] S. Ross, R. Westerfield, J. Jaffe, B.D. Jordan, Modern Financial Management, Eight edition Mc-Graw Hill, 2008.
[39] R. Rue, S.L. Pfleeger, D. Ortiz, A framework for classifying and comparing models of cyber security investment to support policy and decision making, Paper read at Workshop in Economics of Information Security (WEIS), at Pittsburgh, PA, 2007.
[40] J. Rust, C. Phelan, How social security and medicare affect retirement behavior in a world of incomplete markets, Econometrica 65 (4) (1997) 781.
[41] G. Smith, Hackers Cost U.S. Economy up to 500,000 Jobs Each Year, Study FindsHuffington Post.com Posted: 07/25/2013 4:45 pm EDT Updated: 07/25/2013 9:04 pm EDT http://www.huffingtonpost.com/2013/07/25/hackers-jobs_n_3652893.html2013.
[42] J.C. Stein, Takeover threats and managerial myopia, The Journal of Political Economy 96 (1) (1988) 61.
[43] J.C. Stein, Efficient capital markets, inefficient firms: a model of myopic corporate behavior, Quarterly Journal of Economics 104 (4) (1989) 655–669.
[44] N.L. Stokey, R.E. Lucas, E.C. Prescott, Recursive Methods In Economic Dynamics, Harvard University Press, Boston, 1989.
[45] P. Taylor, Data breaches: heart of world business faces hidden and wily enemy, Financial Times (June 07 2013) p. 2.
[46] J.W. Ulvila, J.E. Gaffney Jr., A decision analysis method for evaluating computer intrusion detection systems, Decision Analysis 1 (1) (2004) 35–50.
[47] P. Weill, J. Ross, IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, HBS Press, Boston, MA, 2004.
[48] W. Yue, M. Cakanyildirim, Intrusion prevention in information systems: reactive and proactive response, Journal of Management Information Systems 24 (1) (2007) 329–353.

Bin Srinidhi is the Carlock Endowed Distinguished Professor of Accounting at University of Texas at Arlington. Dr. Srinidhi's research covers the areas of information economics, corporate governance, auditing, internal control systems and capital market research. His papers have been published in *The Journal of Accounting and Economics, The Accounting Review, Contemporary Accounting Research, Review of Accounting Studies, Management Science, Journal of Accounting and Public Policy and Journal of Accounting, Auditing and Finance*, among others. He serves as the Co-editor of *Journal of Contemporary Accounting and Economics* and Associate Editor of *Asia Pacific Journal of Accounting and Economics*. Prior to joining University of Texas at Arlington, Dr. Srinidhi was Chair Professor of Accountancy at City University of Hong Kong.

Jia Yan is now an assistant professor of economics at Washington State University. Dr. Yan's research covers wide topics in applied microeconomics and applied econometrics. Recent research topics include insurance and evaluating public policies aimed at reducing highway congestion and improving airport/port efficiency. His research papers have appeared in such journals as *Econometrica, Journal of Public Economics, Journal of Urban Economics, Brookings-Wharton Papers on Urban Affairs, Insurance: Mathematics and Economics, and Transportation Research Part B: Methodological.*
Dr. Yan received the best dissertation award from the transportation and public utility group of the American Economic Association in 2002. He also received the best paper award from the Transportation Research Forum in 2008 and from the International Transportation Economics Association in 2011. Since 2007, he has served on the editorial board of *Transportmetrica* and will serve as the Associated Editor of *Journal of Air Transport Management* starting 2013.

Giri Kumar Tayi is a Professor of Management Science and Information Systems at the State University of New York at Albany. He obtained his Ph.D. from Carnegie Mellon University and his research and teaching interests are interdisciplinary and span the fields of Information Systems, Operations Management and Operations Research. His papers appeared in top-tier academic journals such as *Operations Research, Management Science, MIS Quarterly, IEEE Transactions, Networks, Naval Research Logistics, EJOR, Journal of Combinatorial Optimization, INFORMS Journal of Computing, Journal of Computer Security, Government Information Quarterly, Communications of the ACM.*
He serves or has served on the *Editorial Board* of several academic journals such as *Information Systems Research, IEEE Intelligent Systems, Decision Sciences, ACM Journal of Data and Information Quality, Information Technology Management, Information Systems Frontiers, Information and Management, International Journal of Shipping and Transport Logistics.*