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

Contents lists available at SciVerse ScienceDirect

Int. J. Production Economics

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

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

C. Derrick Huang *, Ravi S. Behara

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

ARTICLE INFO

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

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

ABSTRACT

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

1. Introduction

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

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

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

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

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

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

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

2. Research background

2.1. Classification of security attacks

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

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

2.2. Economics of information security investments

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

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

Table 1
Summary of prior studies on information security investment.

Study	Base Theory	Assumption				Finding
		Attack[a]	Budget	Interconnection	Risk Profile	
Gordon and Loeb (2002)	Economic benefit maximization	Hypothesized attacks[1] and functions[2]; one-at-a-time[3]	Unlimited	Not specified	Risk neutral	• Optimal investment does not always increase with system vulnerability • Optimal security investment should be less than 36.8% of potential loss
Arora et al. (2004)	Risk-based return	Not specified	Unlimited	Not specified	Risk neutral	• Return on security investment can be measured with the residual risks, based on the product of attack bypass rate of individual security system
Cavusoglu et al. (2005)	Game theory	Targeted (implied)[1]	N/A	Not specified	Risk neutral	• IDS creates positive value for the deploying firms if and only if the detection rate is greater than a critical value • Firms realize strictly non-negative value in optimally configured IDS
Ogut et al. (2005)	Expected utility theory	Not specified	Unlimited	Random	Risk averse	• Interdependence of security risk reduces firms' incentive to invest • Interconnected firms with liability tend to over-invest in security
Cremonini and Nizovtsev (2006)	Economic benefit maximization	Targeted (implied)[1]	Unlimited	Not specified	Risk neutral	• Attackers tend to choose weak targets among heterogeneous systems when their security measures are known • Systems with better level of protection have stronger incentive to reveal their security characteristics
Hauske (2006)	Economic benefit maximization	Hypothesized attacks[1] and functions[2]; one-at-a-time[3]	Unlimited	Not specified	Risk neutral	• Upper limit of optimal security investment [] is not applicable when the boundary conditions of breach functions are relaxed
Huang et al. (2008a)	Expected utility theory	Hypothesized attacks[1] and functions[2]; one-at-a-time attack[3]	Unlimited	Not specified	Risk averse	• There exists a minimal potential loss for non-zero security investment • Decision makers that are more averse to risks do not always invest more in security

[a] Nature of attack: (1) Attack type—opportunistic or targeted; (2) formulation of breach function—hypothesized or derived; (3) attack sequence—one-at-a-time or concurrent heterogeneous.

Our review of the literature shows that prior studies have focused on optimizing the *total* investment in information security and assumed that attacks happen individually and one at a time. In reality, firms face heterogeneous attacks concurrently and have to defend against them within budget constraints. Also, the breach probabilities used in these studies are either hypothesized or not specified. We intend to address these research gaps by developing a model to consider the optimal allocation of security budget when a firm faces concurrent heterogeneous attacks based on an established network theory.

2.3. Network characteristics for information security

We regard a firm's information system, our unit of analysis, as the whole corporate network, which physically interconnects with other systems via external network connections. Because a firm's information system receives attacks via these external connections, an understanding of the network properties is essential to study the information security characteristics. The information system can connect to external networks via single – a proxy server, for instance – or multiple connections, and such connections can be simple (such as a connection to an Internet Service Provider) or open and deep (such as a joint design network that links member companies' product development databases to each other). The network exposure c represents the connectedness of the firm's information systems: The more connections an information system has and the more open the connections are, the higher the network exposure. It is intrinsic to an information system's accessibility and connectivity but is independent of its security setup. All security measures, such as password protection or choice and configuration of programs, is part of the firm's security investment S (to be defined in Section 3) on top of the given network exposure. So, for instance, the firm in question may choose to allow its vendors to access certain areas of its information systems, a decision which may facilitate its business operations but would increase the network exposure. As this example shows, network exposure is determined by not only the technology choices but also the firm's business requirements.

Network topology is another key characteristic in the study of information security. In 1999, physicist Barabási and colleagues discover that, although the majority of the nodes have only limited number of links, a few of the nodes (called "hubs") in the Worldwide Web have large number of connections. Such a topology, which they termed "scale-free network," follows a power law in the distribution of nodal connectedness: The probability that a node connects with k other nodes is roughly proportional to $k^{-\gamma}$, where γ is between 2 and 3 for most networks (Albert et al., 1999; Barabási and Albert, 1999). This is in contrast to the commonly believed random network topology, where the connectivity of any node in the network follows a random pattern or even distribution, and where new nodes are added to the existing network randomly. Since then, researchers have found that, in addition to the large scale interconnection of computer networks, many diverse types of networks, from Hollywood actors to sexual relationships to cellular metabolism, exhibit the characteristics of scale-free network. For instance, Wal-Mart's RetailLink system directly links its own system with

thousands of its suppliers', which, in turn, connect to other retailers or supply chain vendors, forming a large web of information systems consisting of mostly limited-connected nodes (the suppliers' systems) with a few hubs (that belong to Wal-Mart and other large retailers). Recent critics have argued that the physical structure of the Internet, with its router-based architecture, may not follow the power law of connectedness (Alderson et al., 2005; Wallinger et al., 2000). However, it has been theoretically and empirically shown that the interconnection of corporate information systems, logically resembling the topology of Worldwide Web or P2P networks regardless of the physical connections, can be best explained with scale-free network (Anderson and Moore, 2006; Faloutsos et al., 1999; Kumar et al., 2000; Nagaraja and Anderson, 2005; Watts and Strogatz, 1998). Therefore, we adopt the scale-free network theory in this study as a foundation for building our analytical models.

3. Model formulation

We consider a two-stage, single-period, multi-event model for information system security of a firm. (In the context of this study, a "period" is equivalent to a budget cycle of the firm in question.) Fig. 1 shows a conceptual description of the model. Security adversaries generate attacks on the firm's information systems with an attack probability ξ, defined as the likelihood of the information systems receive certain type of attacks within a given period of time. The security property of the information systems, in turn, is determined by their exposure to the network and security investment to keep them safe. The network exposure c, defined in Section 2.3, is intrinsic to the connectedness of the firm's information systems. To be successful, an attack has to successfully penetrate the connections and breach the computers or servers internal to the corporate network where the targeted information resides. To protect against such attacks on the information systems *with a given network exposure*, the firm invests S in various security measures. This investment can take many forms, from technologies such as firewalls and anti-virus software, to procedures such as auto log-off and password aging, to policies such as user training and security audits. Table 2 summarizes the parameters and variables used in our model.

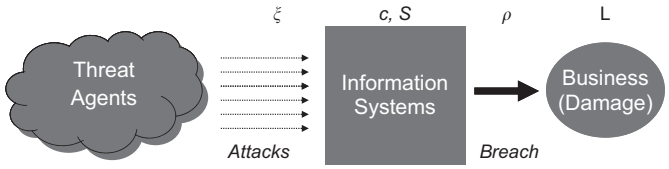

Fig. 1. Information security model.

The breach probability ρ – probability of a security breach to occur – can be considered as a function of the behavior of the security adversaries, as described by the attack probability, and the security property of the information systems, which, in our model, is determined by the network exposure and investments in security measures. In other words, this can be written as $\rho=\rho(\xi,c,S)$. We observe that ρ exhibits certain properties and is subject to boundary conditions. First, for any given system, the higher the likelihood of attacks and the more exposed to attacks, the higher the breach probability; that is, both $\partial\rho/\partial\xi \geq 0$ and $\partial\rho/\partial c \geq 0$. Further, the effect of the security investment is to reduce the breach probability, i.e., $\partial\rho/\partial S \leq 0$, governed by the law of diminishing return, or $\partial^2\rho/\partial S^2 \geq 0$. (In making this assumption, we preclude the case where security measures actually add vulnerability to the system, a possible but rare and undesirable case.) We also require the boundary condition that when the firm does not make any security investment, the breach probability is solely determined by and can be described as a product of the attack probability and the network exposure of the systems:

$$\rho^0 = \rho(\xi,c,0) = \xi c. \quad (1)$$

Table 2
Summary of Variables and Functions.

Notation	Name	Definition	Key assumptions
c	Network exposure	Connectedness of an information system; normalized to [0,1]	• Intrinsic to information system's connectedness, determined by firm's business requirements and technology implementation • Independent of any security properties
ξ_i	Attack probability of class i	Likelihood that an information system receives class i attack; $\xi_i \in [0,1]$	• Exogenous to firm's defensive activities
S_i	Security investment of class i	Firm's investment made to protect against class i attack; $S_i \in [0, L_i)$	• Security investment will never exceed potential loss • Initial security investment has to produce positive benefit
ρ_i	Breach probability of class i	Probability that a security breach can occur due to class i attack; $\rho_i(\xi_i,c,S_i) \in [0,1]$	• $\rho^0 = \rho(\xi,c,0) = \xi c$
L_i	Potential loss of class i	Potential economic loss caused by a security breach from attack class i; $L_i \in [0, \infty)$	• Potential loss is fixed for each class of attack
z_i	Security risk of class i	Security risk a form faces due to attack class i; $z_i = \rho_i L_i$	
κ_i	Normalization parameter for S_i	Measuring the (relative) effectiveness of class i security investment; $\kappa_i \in [0,1]$	
Z	Total security risks	$Z = \sum_{i=1}^{n} z_i$	
S	Total security investments	$S = \sum_{i=1}^{n} S_i$	
Φ	Total benefit function	$\Phi = \sum_{i=1}^{n} (\Delta z_i - S_i)$	
μ_{ij}	Cross-over coefficient	Effect of security investment in the Class j attack on Class i attack; $\mu_{ij} \in [0,1]$	• $\mu_{ii} = 1, \forall i$

Without loss of generality, we can normalize c to $0 \le c \le 1$.

Following the common definition of risk as the combination of the likelihood and the consequence of a specified hazard being realized (Behara and Bhattacharya, 2007; Khamooshi and Cioffi, 2009), the security risk z a firm faces can be written as $z=\rho L$, where L is potential economic (i.e., monetary) loss caused by a security breach (Schechter, 2005). This loss can be the direct – for instance, stolen product information – or indirect – for instance, customer losing trust of a company that could not safeguard credit card data – result of security breach of a particular type of attack. For our model, $L>0$ is a fixed amount, as estimated by the firm based on the type of attack. We further assume that L can be very large but always remains finite; that is, our model does not cover the case of potential losses at a catastrophic level. In the case of n classes of heterogeneous attacks concurrently

$$z_i = \rho_i L_i \quad \forall i \in [1,n] \cap I, \tag{2}$$

where $\rho_i=\rho_i(\xi_i,c,S_i)$, and L_i represents the potential loss the firm faces when the ith type of attack penetrates the systems. We assume that the network exposure c is the same for all classes, because it is intrinsic to the systems being attacked and is independent of the security measures. We further assume that $S_i<L_i$ for all i classes, because it makes no sense for a firm to spend as much on security as the potential loss. So in the case of a firm facing n types of attacks, the total information security risk can be expressed as

$$Z = \sum_{i=1}^{n} z_i = \sum_{i=1}^{n} \rho_i(\xi_i,c,S_i)L_i. \tag{3}$$

To protect against the ith type of attack, the firm makes investment S_i to reduce the breach probability ρ_i, reducing the information security risks that the firm faces by

$$\Delta z_i = (\rho_i^0-\rho_i)L_i = (\xi_i c-\rho_i)L_i. \tag{4}$$

(By assigning a security investment to each type of attack, we assume that the firm invests in security measures with distinctive attacks in mind. This assumption, however, does not preclude effects that one type of investment has on another type of attack. We discuss both independent and interacting security investments in Sections 4 and 5, respectively.) If the firm repeats the same process for all n classes of attacks, then the net benefit Φ of all the security investments of S_i, $i=1,\ldots,n$, can be expressed as

$$\Phi(S_1,\ldots,S_n) = \sum_{i=1}^{n}(\Delta z_i - S_i) = \sum_{i=1}^{n}(\xi_i c-\rho_i)L_i - \sum_{i=1}^{n} S_i. \tag{5}$$

In practice, a firm must see a need or a positive return for it to make any initial security investment. In other words, the first dollar of security investment has to generate benefits for the firm; otherwise, it would not invest in security at all (Gordon and Loeb, 2002). This leads to the boundary (initial) condition the marginal net benefit of any security investment S_i at $S_i=0$ is non-negative, which can be written as

$$\frac{\partial \Phi}{\partial S_i}(S_1,\ldots,S_i=0,..,S_n) \ge 0 \quad \forall i = 1,\ldots,n. \tag{6}$$

The task of optimizing the security investments is to maximize their benefits Φ, which is performed by setting the first-order partial differentiation of $\Phi(S_1,\ldots,S_n)$ in (6) with respect to each S_i; that is, $\partial\Phi/\partial S_i=0$. We note that this operation indeed yields maximum, not minimum, of Φ, because $\partial^2\Phi/\partial S_i^2 = (-\partial^2\rho/\ \partial S_i^2)$ $L_i \le 0$, where $\partial^2\rho/\partial {S_i}^2 \ge 0$, $\forall i$.

In the case of $n=2$, or two concurrent heterogeneous attacks, (5) becomes

$$\Phi(S_1,S_2) = (\xi_1 c-\rho_1)L_1 + (\xi_2 c-\rho_2)L_2 - (S_1+S_2). \tag{7}$$

Following the discussion in Section 2.1, we consider the two common classes of attacks, namely targeted (class 1) and opportunistic (class 2), for this study. S_1 and S_2 are investments against targeted and opportunistic attacks, respectively. To find ρ_1 (for targeted attacks) and ρ_2 (for opportunistic attacks) as representative of reality as possible, we adopt the approach of mathematical derivations based on practically validated a priory principles. As discussed in Section 2.3, scale-free network has been theoretically and empirically validated as the framework that represents the topology of the Internet connections regardless of physical devices (Anderson and Moore, 2006; Faloutsos et al., 1999; Kumar et al., 2000; Nagaraja and Anderson, 2005; Watts and Strogatz, 1998) and is thus adopted as the guiding theory for this study. We posit that, in such a network, targeted attacks share the similar characteristics of a one-to-one attack against a particular node, and that the propagation of opportunistic attacks is analogous to the epidemic spreading among nodes.

We first examine the epidemic dynamics of a scale-free network, a subject that has been extensively studied in various disciplines from biology to computer science for cases such as a virus on the Internet, a sexually transmitted disease among people, or even ill-intentioned rumors within a professional community (Griffin and Brooks, 2006; Gross et al., 2006; Lai et al., 2003; Telo da Gama and Nunes, 2006; Watts, 1999; Zhou et al., 2006). It has been shown that, in the steady state, when an epidemic spreads in the scale-free network, the infection probability of an average node is a function of the infection rate, exposure to the broad network, and attack rate. Assume that the effect of security investment S in protecting the information systems against the potential breach can be represented as the reduction of the infection rate, the breach probability of opportunistic attack can then be expressed as (see Technical Appendix A.1 for detailed derivation)

$$\rho_2 = \xi_2 c^{\kappa_2 S_2 + 1}, \tag{8}$$

where ξ_2 is the attack probability for opportunistic attacks, and κ_2, a normalized parameter ($0 \le \kappa_2 \le 1$), measures the impact of investment S_2.

In the case of a one-to-one, targeted attack on a particular node, from the attacker's perspective, the scale-free network effectively collapses into a regular randomly connected network, because the actual attack has to come through from a connected node regardless of the topology of the overall network. In such a random network, the network exposure c – the level of exposure of the firm's system to other nodes in the network – can be interpreted as the probability that an attacker would successfully identify a connecting node among all available nodes in the network to initiate such an attack, and the infection rate represents probability of such an attack (or "infection") being successful. Therefore, the breach probability in this case becomes product of the attack probability – the tendency for the attackers to attack, network exposure – probability of randomly selecting a connected node, and the infection rate (defined in (T6) of Technical Appendix A.1)

$$\rho_1 = \frac{\xi_1 c}{\kappa_1 S_1 + 1}, \tag{9}$$

where ξ_1 is the attack probability for targeted attacks, and κ_1 is a normalized parameter for S_1 (as defined above).

A quick comparison between ρ_1 and ρ_2 reveals their different characteristics. ρ_2 is much more convex with respect to S than ρ_1; in practice, it means that an initial (or a small amount of) investment in security is likely to have a more significant impact against opportunistic attacks than against targeted attacks. This seems to fit well with practice, because it is often more difficult and costly to block targeted attacks than to block random ones.

The associated potential losses of the two classes are L_1 and L_2. Substituting (8) and (9) into (7) and rearranging the terms, we have the total net benefit Φ:

$$\Phi(S_1,S_2)=\frac{\xi_1 c\kappa_1 S_1 L_1}{\kappa_1 S_1+1}+\xi_2 c(1-c^{\kappa_2 S_2})L_2-(S_1+S_2). \tag{10}$$

Maximizing Eq. (10) then yields the optimal security investment allocation to defend against both classes of attacks.

4. Optimal allocation of information security investment

When a firm has set the total information security budget to a fixed amount S, this budget is to be allocated to defending against targeted (Class 1) and opportunistic (Class 2) attacks, that is, $S_1+S_2=S$. Because $S_2=S-S_1$, we can rewrite ρ_2 in (8) as a function of S_1:

$$\rho_2(S_1)=\xi_2 c^{\kappa_2(S-S_1)+1}=\xi_2 c^{\kappa_2 S+1}c^{-\kappa_2 S_1}. \tag{11}$$

Substituting $S_1+S_2=S$, (8), and (11) into (7), we get

$$\Phi(S_1)=\frac{\xi_1 c\kappa_1 S_1 L_1}{\kappa_1 S_1+1}+\xi_2 c(1-c^{\kappa_2 S-\kappa_2 S_1})L_2-S. \tag{12}$$

Differentiating $\Phi(S_1)$ with respect to S_1, we get

$$\left.\frac{\partial\Phi}{\partial S_1}\right|_{S,L_1,L_2,c,\xi_1,\xi_2}=-\frac{\partial\rho_1}{\partial S_1}L_1-\frac{\partial\rho_2}{\partial S_1}L_2=\frac{\xi_1\kappa_1 cL_1}{(\kappa_1 S_1+1)^2}+\xi_2\kappa_2\ln c L_2 c^{\kappa_2 S+1}c^{-\kappa_2 S_1}. \tag{13}$$

The boundary condition (6) requires that (13) is equal to or greater than zero when $S_1=0$. After rearranging terms, we get

$$-\frac{L_2}{L_1}\frac{\kappa_2}{\kappa_1}\frac{\xi_2}{\xi_1}(\ln c)c^{\kappa_2 S}\le 1. \tag{14}$$

This leads to the following (see Technical Appendix A.2 for proof):

Lemma 1. *In the case of independent investments to counter the attacks as described by the two breach probability functions (8) and (9), the total budget constraint has a lower bound* $S_0=(1/\kappa_2\ln c)\ln(-(L_1/L_2)(\kappa_1/\kappa_2)(\xi_1/\xi_2)(1/\ln c))$ *when* $c<c'=e^{-(L_1/L_2)(\kappa_1/\kappa_2)(\xi_1/\xi_2)}$.

Lemma 1 states that when the network exposure c of the firm's information system is sufficiently small ($c<c'$), for the security investment to make a difference in reducing the security risks, the total information security budget S has to be higher than a minimum S_0. However, when the network exposure is large ($c>c'$), there is no minimum level of investment S_0. This is likely because when the network is widely exposed, any amount of investment will help reduce the security risks.

To find the optimal investment S_1^* (and S_2^* is therefore determined), we set (13) to zero. After rearranging terms, we get the following equation:

$$\frac{c^{\kappa_2 S_1^*}}{(\kappa_1 S_1^*+1)^2}=-\frac{L_2}{L_1}\frac{\kappa_2}{\kappa_1}\frac{\xi_2}{\xi_1}(\ln c)c^{\kappa_2 S}. \tag{15}$$

We first observe that (15) indeed yields the maximum of $\Phi(S_1)$, because $\partial^2\Phi/\partial S^2{}_1=-(\partial^2\rho_1/\partial S_1{}^2)L_1-(\partial^2\rho_2/\partial S_1{}^2)L_2\le 0$, where $(\partial^2\rho_1/\partial S_1{}^2)\ge 0$ and $(\partial^2\rho_2/\partial S_1{}^2)\ge 0$. We also note that the boundary condition (14) holds for (15), because the left-hand side of (15) is always smaller than or equal to 1: $c^{\kappa_2 S_1{}^*}\le 1$ (since $c\in[0,1]$) and $(\kappa_1 S_1^*+1)^2\ge 1$, for all $S_1^*>0$.

Using this optimization condition, we examine the optimal investment level S_1^* and how the firm should *allocate* security investments given a budgetary constraint, as represented by S_1^*/S with respect to four sets of parameters of interest, namely the total security budget S, the network exposure c, ratio of investment effectiveness κ_1 and κ_2, and the ratio of potential loss L_1 and L_2 (The ratio of ξ_1 and ξ_2 would have the same effect on S_1^*/S as that of the ratio of L_1 and L_2, as evidenced by (15)). Because no closed-form solution from (15) is possible, we adopt the implicit function analysis; specifically, when $y=y(x)$ and $F(x,y)=0$, we have

$$\frac{dy}{dx}=-\frac{\partial F/\partial x}{\partial F/\partial y}. \tag{16}$$

In our case, we let, from (15)

$$F=\frac{c^{\kappa_2 S_1{}^*}}{(\kappa_1 S_1^*+1)^2}+\frac{L_2}{L_1}\frac{\kappa_2}{\kappa_1}\frac{\xi_2}{\xi_1}(\ln c)c^{\kappa_2 S}=0. \tag{17}$$

By setting $y=S_1^*$ and x as each of the four sets of parameters alternately in (16), we can examine the behavior of the optimal investment S_1^* and the optimal investment allocation to Class 1 attack S_1^*/S (and allocation to Class 2 attack, S_2^*/S, is thus determined). We use numerical analysis to compute and graph the effects of these parameters on the optimal allocation under different scenarios.

4.1. Network exposure and security investment

We first examine how S_1^*/S varies with c, the system's network exposure. By setting $y=S_1^*$ and $x=c$ in (16), we arrive at the following proposition (see Technical Appendix A.3 for proof):

Proposition 1. *There exists* $\underline{c}\in[0,\ e^{-(1/\kappa_2)})$, *where both* $\partial S_1^*/\partial c\ge 0$ *and* $\partial(S_1^*/S)/\partial c\ge 0$ *, for all* $c\ge\underline{c}$.

Proposition 1 states that when the network exposure c is larger than a minimum $\underline{c}$, both the optimal investment S_1^* and the optimal allocation to Class 1 attack S_1^*/S increases with c (with the latter also implying that S_2^*/S decreases with c). Since $\kappa_2\in[0,1]$, $\underline{c}$ is always smaller than $e^{-1}=0.368$ and approaches 0 when κ_2 is small. Thus, this proposition states that for the bulk of the network exposure value ($\underline{c}\le c\le 1$), allocation to Class 1 attacks increases with c, while allocation to Class 2 attacks decreases, given a total budget S.

To show Proposition 1 numerically, we fix ξ_1, ξ_2, κ_1, κ_2, L_1, L_2, and S, and run a series of c values to obtain the ratio S_1^*/S. Fig. 2 shows the results of S_1^*/S vs. c at different ratio of L_1 and L_2, while fixing $L_1=\$2$ M, $\kappa_1=\kappa_2=0.000005$, $\xi_2=10\xi_1$, and $S=\$100{,}000$ (as 5% of L_1). (The results are similar when we vary the values of S, ξ_1, and ξ_2) We can see that, for each combination of L_1 and L_2, S_1^*/S increases with c between a minimum c where S_1^* remains zero and a maximum c where S_1^*/S approaches 100%. Further, the relative size of L_1 vs. L_2 shifts the curves to the left.

Proposition 1 and the computational result in Fig. 2 suggest that opportunistic attacks should receive higher amount of investment when the network exposure is small. This result can understood as

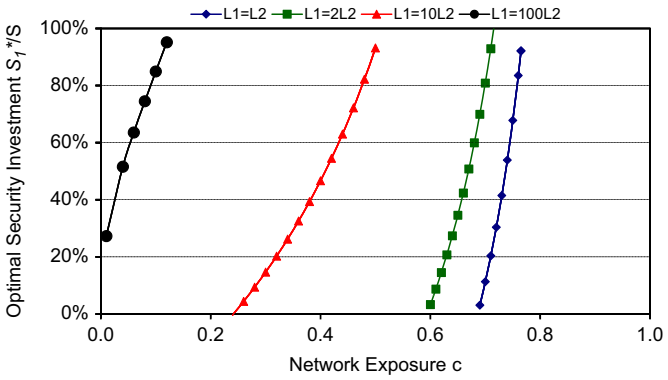

Fig. 2. Optimal information security investment allocated to S_1 vs. c, independent investments with budget constraint.

follows: In a scale-free network, when a firm reduces its network exposure, opportunistic attacks stay relatively constant, because they depend more on the network behavior – in particular, the connectivity of the hubs – than individual firm's connectivity, while targeted attacks are likely to be reduced with the decreased interconnections. Therefore, when c is small, it is more important for a firm to defend against opportunistic attacks than targeted attacks. When the total investment is fixed, the optimal allocation would shift gradually from opportunistic to targeted attacks with increasing network exposure. This result is consistent with the notion that when a firm's system is more connected and exposed, there are more ways for adversaries to initiate targeted attacks, and higher amount of investment is required to combat such attacks. Additionally, when targeted attack takes on more importance (as represented by the relative size of L_1 vs. L_2), this shift from opportunistic to targeted attacks happens at a lower c (thus covering a broader range of network exposure). In practice, this result implies that a firm should allocate large amount of its investment to combat opportunistic attacks when the network exposure is low, and increase the allocation to targeted attacks when the network exposure increases. Further, with larger potential loss due to targeted vs. opportunistic attacks, the range of network exposure where the optimal investment allocated to the former is wider (i.e., starts at smaller network exposure).

4.2. Relative losses and security investment

In this section, we examine how S_1^*/S varies with L_1/L_2. Using (16) and setting $y=S_1^*$ and $x=L_1/L_2$, we have the following proposition (See Technical Appendix A.4 for proof):

Proposition 2. *Both the optimal investment S_1^* and the optimal allocation S_1^*/S increase with the relative potential loss L_1/L_2.*

Proposition 2 states that a firm should allocate more against those attacks that cause higher potential losses. This is intuitive, because such an action would likely result in higher level of risk reduction. Fig. 3 shows the results of the computational analysis of Proposition 2, where we set $\kappa_1=\kappa_2=0.000005$, $c=0.4$, $L_1=\$2$ M, and $\xi_2=10\xi_1$, while recording the relationship S_1^*/S vs. L_1/L_2 by varying L_2 for multiple values of S as 1%, 5%, 25%, and 80% of L_1. (The results are similar when we vary the values of c, ξ_1, and ξ_2.) For the curve with small S, S_1^* starts to become non-zero and quickly takes the entire budget S with increasing L_1, while the curves of larger S are smoother and over a larger range of L_1/L_2. In other words, the allocation shift from investing against one class of attack to the other occurs at a higher relative loss and increases faster when the total budget is smaller.

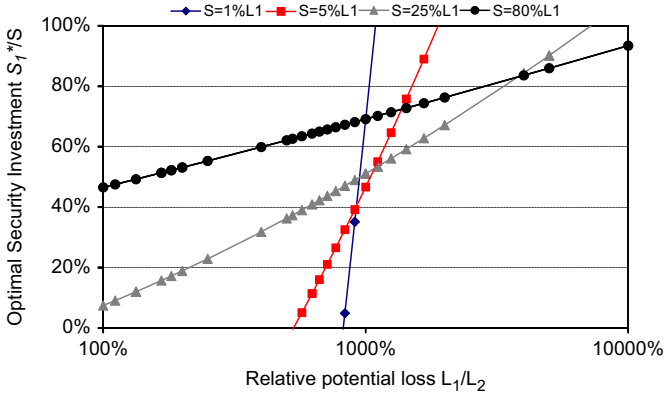

Fig. 3. Optimal information security investment allocated to S_1 vs. relative potential loss L_1/L_2, independent investments with budget constraint.

4.3. Investment effectiveness and security investment

Next, we examine how the relative effectiveness of security technology, represented by κ_1/κ_2, affects the allocation of investment. Because implicit function analysis with (16) and (17) is impossible in this case – the occurrences of κ_1 and κ_2 cannot be isolated as κ_1/κ_2 completely – we use numerical analysis to study the relationship of S_1^*/S and κ_1/κ_2. This is done by leaving all other parameters (S, L_1/L_2, ξ_1/ξ_2, and c) constant while varying κ_1/κ_2. Fig. 4 shows the result of one set of the calculation for $L_1=\$2$ M, $L_2=\$200{,}000$, $c=0.4$, $\xi_2=10\xi_1$, and varying levels of S (as 1%, 5%, 25%, and 80% of L_1). Initially, when κ_1/κ_2 is very small, investing in measures against Class 1 attack is simply too ineffective, resulting in a zero allocation to it. S_1^* starts to become positive after certain level of κ_1/κ_2; with increasing κ_1/κ_2, the optimal allocation to S_1^* increases to capture the increasing relative effectiveness of investment in Class 1. Here, similar to the case of S_1^*/S vs. L_1/L_2 for the reason of investment efficiency, the minimum level of κ_1/κ_2 for S_1^* to become non-zero and the rate of increase thereafter are higher for small S. As κ_1/κ_2 crosses certain level, S_1^* starts to decrease with increasing κ_1/κ_2, signaling that the gain in increasing effectiveness has peaked. When this happens, the optimal allocation starts to shift more towards Class 2.

Above analysis suggests that when a firm invests a fixed amount of budget against two concurrent attacks, investment allocation to protecting against one class of attack increases with the effectiveness of such an investment vs. that of the investment in the other class. When the relative effectiveness reaches a certain level, however, the allocation of investment starts to shift towards the less effective class, because the investment in the former is so effective that less allocation is needed to achieve some required level of security against attacks of that class (in agreement with the law of diminishing returns). It is also interesting to note that for smaller total budgets, the peak allocation for protecting against one class of attacks occurs at a higher relative effectiveness and a greater share of total budget. In the case where the total budget S is very small (such as the curve of $S=1\%$ L in Fig. 4), the allocation becomes extreme: The class with higher level of effectiveness tends to get most or all of the investment. This may seem counterintuitive, because the law of diminishing returns implies that putting high amount of investment in one would produce less than investing at least some in

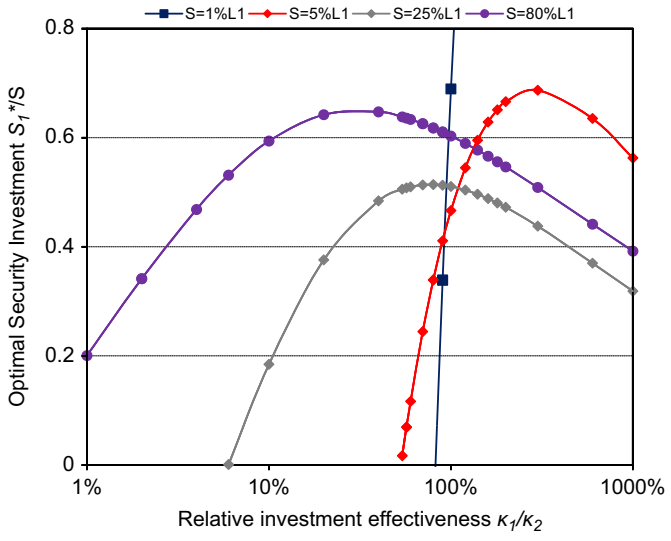

Fig. 4. Optimal information security investment allocated to S_1 vs. relative effectiveness factor κ_1/κ_2, independent investments with budget constraint.

each class. A reasonable explanation of this result is that for any security measure for protecting against an attack class to be effective, a minimum threshold (or some critical mass of investment) needs to be reached. (For instance, buying licenses for and installing anti-virus programs on only a few computers among the many systems a firm has will not protect the firm against viruses.) Therefore, it is optimal to allocate most or all of the budget to the class with higher relative effectiveness – which in turn means lower investment threshold – when the budget is small.

4.4. Budgetary constraint and security investment

Our last analysis is focused on the optimal allocation among S_1^* and S_2^* at different levels of budgetary constraint S. Performing the implicit function analysis by setting $y=S_1^*$ and $x=S$ yields the results summarized in the following proposition (see Technical Appendix A.5 for proof):

Proposition 3. *The optimal investment S_1^* increases with S, and the optimal allocation S_1^*/S increases with S when S is sufficiently large. However, S_1^*/S decreases with S when $c > c' = e^{-(L_1/L_2)(\kappa_1/\kappa_2)(\xi_1/\xi_2)}$ and S is small.*

Proposition 3 states that, in most cases, the optimal allocation to Class 1, targeted attacks increases with total budget S. This is consistent with practice and intuition, because security measures against targeted attacks, being more difficult to defend against, can draw higher amount from a larger budget while still keeping enough investment to combat opportunistic attacks. But in the case where the network exposure is high and the total budget is small, Class 2, opportunistic attacks should get more allocation with increasing S.

This proposition can be further illustrated with numerical examples. Two sets of the computational results are presented in Fig. 5, where S_1^*/S, the optimal allocation to Class 1 attack, is plotted against S/L_1, the "normalized" budget constraint, in a family of "iso-exposure" curves. In Fig. 5(a), where $\kappa_1=0.000003$, $\kappa_2=0.000005$, $L_1=\$2$ M, $L_2=\$3$ M, and $\xi_1=\xi_2$, those curves are all concave and increasing, implying that the percentage allocated to S_1^* increases, albeit at a decreasing rate, with S. Also, both the value and the slope of S_1^*/S are higher for larger c, implying that the allocation to S_1^* increases with c for any given S. These results are consistent with both the above observation of (15) and earlier result with respect to c. However, Fig. 5(b), where we set $\kappa_1=\kappa_2=0.000005$, $L_1=\$2$ M, $L_2=\$200{,}000$, and $\xi_2=10\xi_1$, shows a distinctively different behavior of S_1^*/S vs. S/L_1. At small c, the iso-exposure curves are concave and increasing, similarly to those in Fig. 5(a). When c becomes sufficiently large, however, the iso-exposure curves become U-shape. That is, for c greater than some "inflection point" c', S_1^*/S is convex and non-increasing in S/L_1: at small S, S_1^*'s share *decreases* with increasing total investment, and approaches 100% when $S\to 0$; for large S, optimal allocation S_1^* *increases* with the total investment, and approaches 100% when S becomes large. Throughout all levels of total investment, S_1^*'s share never approaches 0.

The distinctive behavior of the curves can be interpreted with Proposition 3 and Lemma 1. In Fig. 5(b), where $c' = e^{-(L_1/L_2)(\kappa_1/\kappa_2)(\xi_1/\xi_2)} = e^{-1} \cong 0.3678$ (since $(L_2/L_1)(\kappa_2/\kappa_1)(\xi_2/\xi_1)=1$), all the iso-exposure curves with $c > c'$ exhibit U-shape, because $\partial(S_1^*/S)/\partial S < 0$ when S is small and $\partial(S_1^*/S)/\partial S > 0$ when S is large. When $c < c'$, S has a lower bound (which is $S_0 = 1/\kappa_2 \ln c \ln(-(L_1/L_2)(\kappa_1/\kappa_2)(\xi_2/\xi_1)(1/\ln c))$ given by Lemma 1), hence the behavior of the lower curves. However, when $(L_2/L_1)(\kappa_2/\kappa_1)(\xi_2/\xi_1)$ becomes large enough such that $c' = e^{-(L_1/L_2)(\kappa_1/\kappa_2)(\xi_1/\xi_2)} > 1$, which is the case for Fig. 5(a), $c < c'$ for all $c \in [0,1]$, and all the iso-exposure curves behave like those in Fig. 5(a).

In summary, our analytic and computational results show that under most circumstances (e.g., Fig. 5(a) and part of Fig. 5(b)), the optimal allocation to Class 1 increases with total security budget. However, when the relative size L_1 to L_2 is large enough for a given ratio of ξ_1 and ξ_2, and when the network exposure is sufficiently large, optimal allocation to protecting against Class 1 attack approaches 100% when the total investment constraint is very small, decreases briefly and then increases with increasing S, and approaches 100% with large budgetary constraint.

Proposition 3 and the ensuing numerical analysis offer key practical implications. When a firm with relatively low network exposure and limited budget faces both opportunistic and targeted attacks, it is more effective to allocate the bulk of it to opportunistic attacks. (See Section 4.1 for detailed discussions on investment allocation and network exposure.) The percentage allocated to protecting against the targeted attacks goes up with increasing security budget. This can be understood from the fact that opportunistic attacks are, in general, less sophisticated and stopped more effectively with relatively low level of security investments. On the other hand, when the information systems are highly connected and open, the firm with even a limited budget should cast most of its security investments against targeted attacks. The network exposure threshold, at which the investment focus shifts from opportunistic attacks to targeted attacks at limited budget, depends largely on the relative size of the potential losses from the two classes of attacks (Lemma 1): the higher the potential loss from targeted attack relative to that from opportunistic attack, the lower the exposure threshold.

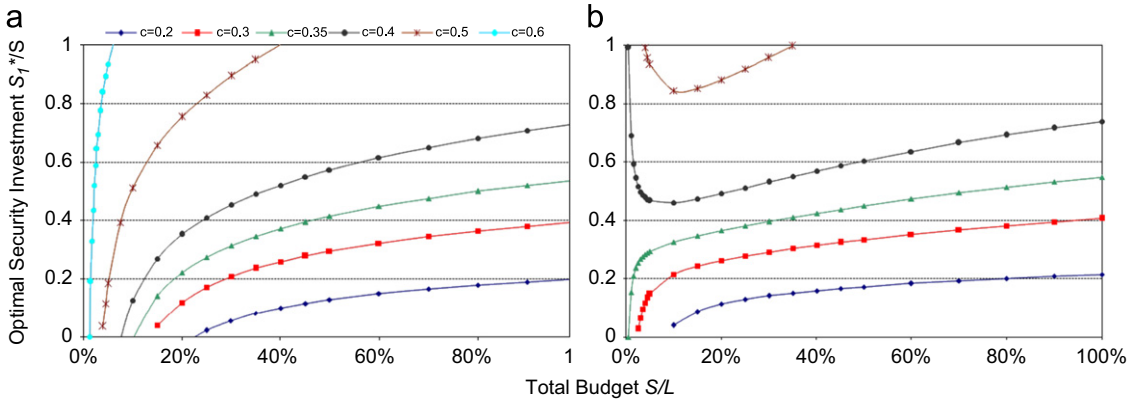

Fig. 5. Optimal investments vs. total budget, independent investments with budget constraint.

To summarize, a manager with a limited security budget should focus on protecting against targeted attacks when their potential loss is high and the information systems widely connected and open. But in a business environment where information systems have lower network exposure, it is better for the firm to spend its limited security investment to defend against opportunistic attacks.

5. Interacting investments with budget constraint

So far, our model has assumed that the security investments to counteract the two classes of attacks are independent of each other; that is, we assume that a firm can invest specifically to reduce the security breach probability of a particular type of attack. In reality, however, security measure taken to prevent one class of attack might help prevent another class of attack. For instance, anti-virus software, generally deployed to prevent opportunistic attacks, can also block some targeted attacks. In this section, we relax the assumption of independent security investments to account for the interacting or cross-over effect in the presence of budgetary constrain.

Let $\tilde{S}_i$ represent the *effective* security investment for defending against the ith attack. When investments are independent, $\tilde{S}_i = S_i$. However, in the existence of cross-over effect of security investment $\tilde{S}_i$ is expressed as follows:

$$\tilde{S}_i = \sum_{j=1}^{n} \mu_{ij} S_j, \tag{18}$$

where μ_{ij} represent the effect of security investment against the Class j attack on Class i attack. In other words, when an investment S_j is made to counter Class j attack, $\mu_{ij}S_j$ can also be considered as part of the investment made to counteract Class i attack. Taken all n classes of attack together, we have

$$\begin{bmatrix} \tilde{S}_1 \\ \vdots \\ \tilde{S}_n \end{bmatrix} = \begin{bmatrix} \mu_{11} & \cdots & \mu_{1n} \\ \vdots & \ddots & \vdots \\ \mu_{n1} & \cdots & \mu_{nn} \end{bmatrix} \begin{bmatrix} S_1 \\ \vdots \\ S_n \end{bmatrix}. \tag{19}$$

By definition, $\mu_{ii}=1$, $\forall i$. We further assume that investment in defending against one attack does not negatively impact another; that is, $\mu_{ij} \geq 0$. Therefore, we have $0 \leq \mu_{ij} \leq 1$, $\forall i, j$. Incorporating the cross-over effects of security investment using the effective security investment$\tilde{S}_i$, we rewrite (3) and (5) as

$$Z = \sum_{i=1}^{n} z_i = \sum_{i=1}^{n} \tilde{\rho}_i L_i \tag{20}$$

and

$$\Phi(S_1,\ldots,S_n) = \sum_{i=1}^{n} (\Delta z_i - S_i) = \sum_{i=1}^{n} (\xi_i c - \tilde{\rho}_i) L_i - \sum_{i=1}^{n} S_i, \tag{21}$$

where $\tilde{\rho}_i = \tilde{\rho}_i(\xi_i, v, \tilde{S}_i)$ is the breach probability function with cross-over investment effect, for which the following holds true:

$$\begin{bmatrix} \tilde{\rho}_1 \\ \vdots \\ \tilde{\rho}_n \end{bmatrix} = \begin{bmatrix} \rho_1 \\ \vdots \\ \rho_n \end{bmatrix} \text{ when } \begin{bmatrix} \tilde{S}_1 \\ \vdots \\ \tilde{S}_n \end{bmatrix} = \begin{bmatrix} S_1 \\ \vdots \\ S_n \end{bmatrix} \text{ or } \begin{bmatrix} \mu_{11} & \cdots & \mu_{1n} \\ \vdots & \ddots & \vdots \\ \mu_{n1} & \cdots & \mu_{nn} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{22}$$

Again, we consider the case of $n=2$. With this cross-over effect of security investments taken into consideration, the two breach probability functions (8) and (9) become

$$\tilde{\rho}_1 = \frac{\xi_1 c}{\kappa_1 \tilde{S}_1 + 1} = \frac{\xi_1 c}{\kappa_1 (S_1 + \mu_{12} S_2) + 1} = \frac{\xi c}{\kappa_1 (1-\mu_{12}) S_1 + \kappa_1 \mu_{12} S + 1}, \tag{23}$$

$$\tilde{\rho}_2 = \xi_2 c^{\kappa_2 \tilde{S}_2 + 1} = \xi_2 c^{\kappa_2 (S_2 + \mu_{21} S_1) + 1} = \xi_2 c^{\kappa_2 S + 1} c^{-\kappa_2 (1-\mu_{21}) S_1}, \tag{24}$$

where $\tilde{S}_1 = S_1 + \mu_{12} S_2$, and $\tilde{S}_2 = S_2 + \mu_{21} S_1$. Note that the budgetary constraint $S_1 + S_2 = S$ is used to rewrite both breach probabilities as functions of S_1. The net benefit (7) in this case can be written as

$$\Phi(S_1) = (\xi_1 c L_1 + \xi_2 c L_2 - S) - \frac{\xi_1 c L_1}{\kappa_1 (1-\mu_{12}) S_1 + \kappa_1 \mu_{12} S + 1} - \xi_2 L_2 c^{\kappa_2 S + 1} c^{-\kappa_2 (1-\mu_{21}) S_1}. \tag{25}$$

To find the optimal level of S_1, we differentiate Φ in (25) with respect to S_1 to get

$$\left.\frac{\partial \Phi}{\partial S_1}\right|_{S, L_1, L_2 v, \xi_1, \xi_2} = \frac{\xi_1 c \kappa_1 L_1 (1-\mu_{12})}{[\kappa_1 (1-\mu_{12}) S_1 + \kappa_1 \mu_{12} S + 1]^2} + \xi_2 c \kappa_2 L_2 \ln c (1-\mu_{21}) c^{\kappa_2 S} c^{-\kappa_2 (1-\mu_{21}) S_1}. \tag{26}$$

To find optimal level of investment S_1^*, we set (26) to zero. After rearranging terms, we have

$$\frac{c^{\kappa_2 (1-\mu_{21}) S_1^*}}{\left(\kappa_1 (1-\mu_{12}) S_1^* + \kappa_1 \mu_{12} S + 1\right)^2} = -\frac{L_2 \kappa_2 \xi_2 (1-\mu_{21})}{L_1 \kappa_1 \xi_1 (1-\mu_{12})} (\ln c) c^{\kappa_2 S}, \tag{27}$$

subject to the following boundary condition ($\partial \Phi / \partial S_1 \geq 0$ at $S_1 = 0$),

$$\frac{\xi_1 \kappa_1 L_1 (1-\mu_{12})}{(\kappa_1 \mu_{12} S + 1)^2} + \xi_2 \kappa_2 L_2 \ln c (1-\mu_{21}) c^{\kappa_2 S} \geq 0. \tag{28}$$

It is important to note that, when $\mu_{12} = \mu_{21} = 0$, (27) and (28) revert back to (15) and (14), the independent case. That is, the independent investment model in the previous section can be considered as a special case of this general investment model when the cross-over effect is nil. Further, the left-hand side of (27) is always smaller than or equal to one, since the numerator ≤ 1 for all $c \in [0, 1]$ and the denominator ≥ 1. Because $\ln c \leq 0$, we have

$$0 \leq -\frac{L_2 \kappa_2 \xi_2 (1-\mu_{21})}{L_1 \kappa_1 \xi_1 (1-\mu_{12})} (\ln c) c^{\kappa_2 S} \leq 1. \tag{29}$$

Compared with the independent case (15), we first note the appearance of the additional term of S in the denominator on the left-hand side the cross-over effect of security investment in (27), besides the addition of the parameters μ_{12} and μ_{21}. As S increases, both sides of (27) decrease. This is important, because the relationship that the absolute value of S_1^* increases with S in the independent investment case no longer holds for this general model. In other words, in the cross-over case, increasing the total budget does not guarantee a higher optimal investment to defend against individual classes of attacks. However, that S_1^* increases with L_1/L_2 is still true, because the left-hand side of (27) is a decreasing function of S_1^*, given S, c, κ_1, κ_2, ξ_1, ξ_2, μ_{12}, and μ_{21}.

6. Computational result

Because a closed-form solution of S_1^* is impossible from (27), and the implicit function analysis does not yield interpretable results, we resort to numerical techniques to examine the properties of S_1^* and S_1^*/S. Fig. 6 shows how the allocation S_1^*/S changes with (normalized) budget constraint S/L_1, with the same set of parameters ($\kappa_1 = \kappa_2 = 0.000005$, $L_1 = \$2$ M, $L_2 = \$200{,}000$, and $\xi_2 = 10\xi_1$) but at different levels of network exposure c, to compare with Fig. 5(b) in the independent investment case. We can see that, although the shape of iso-exposure curves looks similarly to those in Fig. 5(b), there are some important

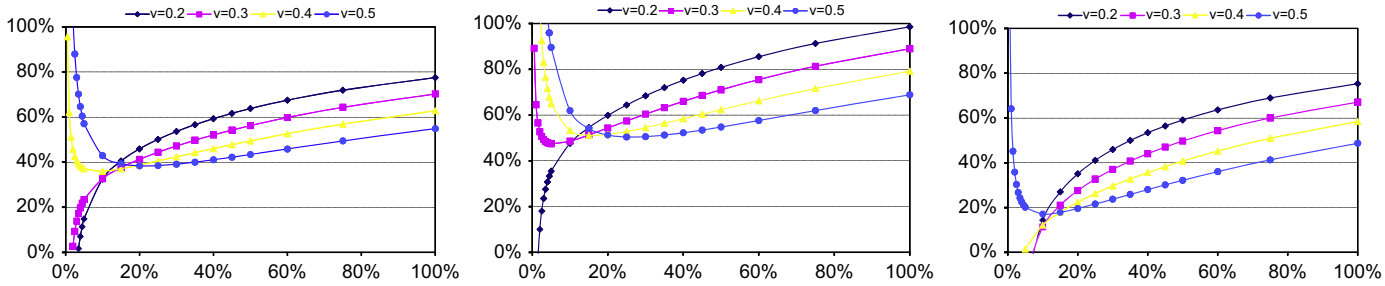

Fig. 6. Optimal information security investment allocated to S_1 vs. S/L, cross-over investments with budget constraint.

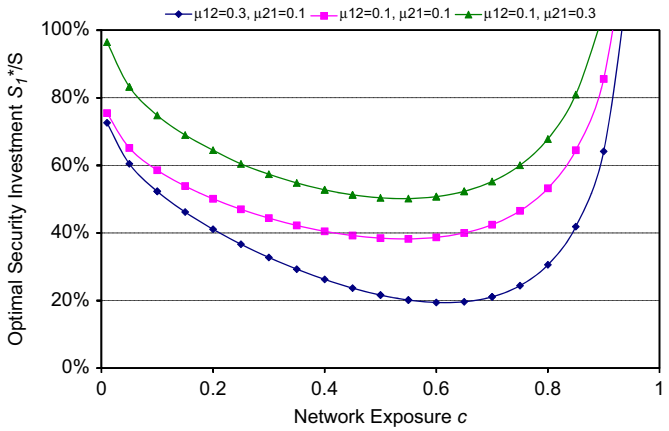

Fig. 7. Optimal information security investment allocated to S_1 vs. c, cross-over investments with budget constraint.

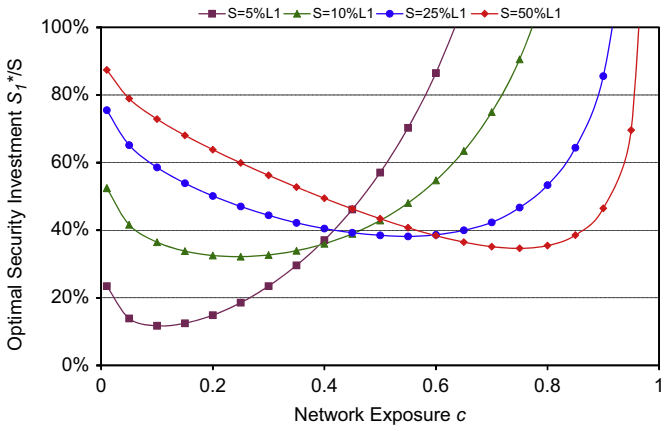

Fig. 8. Optimal information security investment allocated to S_1 vs. c, cross-over investments with budget constraint.

differences. First, the inflection exposure c' changes with different settings of μ_{12} and μ_{21}. This can be understood by examining the cross-over model equivalent of Lemma 1. When we solve for the boundary condition for S in (28), we can see that for $c > c' = e^{-(L_1\kappa_1\xi_1(1-\mu_{12})/L_2\kappa_2\xi_2(1-\mu_{21}))}$, S has a lower limit S_0 (although here it cannot be expressed in a closed form as in Lemma 1, because of the addition of the quadratic term in S in (27)). Thus, c' decreases with higher μ_{21}, and the inflection happens at a lower level of network exposure (as in Fig. 6(b) where $c' \cong 0.2765$). Conversely, c' increases with higher μ_{12} (as in Fig. 6(c) where $c' \cong 0.4594$). To summarize, in the case of cross-over investment effect with fixed security budget, the inflection exposure, above which the optimal allocation to Class 1 attack no longer strictly increases with budget, goes down when the impact of such investment on Class 2 increases (and vice versa)..

Another key difference in the cross-over case is the relationship of S_1^*/S with c. Proposition 1 and Fig. 5 show that, in that, when in the independent investment case, the allocation S_1^*/S always increases with c. However, as shown in Fig. 6, when S is larger than S_0 (the value of which cannot be shown in a closed form, as previously), this relationship is reversed. Moreover, such a reversed relationship is more pronounced with larger cross-over effect (as represented by μ_{12} and μ_{21}), and the relationship reverts back to the independent investment case when $\mu_{12}=\mu_{21}=0$. In other words, contrary to the independent investment case, when security investments show cross-over effect, optimal allocation to Class 1 (as represented S_1^*/S) decreases with network exposure c when the total budget S is large.

Lastly and more importantly, we examine the relationship between the optimal allocation and the extent of cross-over effect. To do so, we run a series of numerical analysis of S_1^*/S vs. c at different levels of μ_{12} and μ_{21} (Fig. 7) and at different levels of S/L_1 (Fig. 8), while keeping other parameters constant ($\kappa_1=\kappa_2=0.000005$, $L_1=\$2$ M, $L_2=\$200{,}000$, and $\xi_2=10\xi_1$). We note that, for any c, S_1^*/S increases with; in other words, S_1^*/S is larger when μ_{21} (i.e., the impact of Class 1 investment on Class 2 attacks) relative to μ_{12} is larger. We also note that $S_1^*/S>0$ for all c, even when c is very small. Furthermore, the concavity of the curves, which increases with the magnitudes of μ_{21} and μ_{12}, shows that, S_1^*/S first decreases then increases with increasing c. These observations are in contrast with the independent investment case, where S_1^*/S is a strictly increasing function of c while remaining 0 until $c>\underline{c}$. (The concavity disappears, and the curves revert back to those the independent investment case, when $\mu_{12}=\mu_{21}=0$.) To summarize, the cross-over effect of investments changes the behavior of optimal allocation to Class 1 from strictly increasing to positive and concave. Additionally, at any given level of network exposure, the more impact the investment on defending against Class 1 attacks has on the defense against Class 2 attacks, the higher the optimal allocation to Class 1 attack is.

Our analysis shows that, in general, the investment with the higher impact on other attacks should receive higher allocation. This is to be expected, because one would need to spend less on, say, targeted attacks when the investment in opportunistic attacks can also protect against targeted attacks to a certain degree. While the characteristics associated with individual attack dominate the optimal allocation in the case of independent investment with budgetary constraint, the cross-over scenario, as expected, introduces a mixed response. This is evident when one compares Fig. 2, where optimal investment displays an "all or nothing" allocation for very large and very small network exposure, to Fig. 7, where a smooth and moderate allocation among the two classes of attacks over a large range of network exposure results from the cross-over effects. Our model suggests that the firm in question should spread the investment allocation to both classes of attacks over a large range of network exposure, particularly when the budget is large relative to the potential

loss. However, when security budget is limited, a firm with high network exposure should quickly focus on one of the attacks, similar to the independent investment case. It is important to note that analyses in the cross-over scenario revert back to the independent case when both μ_{21} and μ_{12} are zero.

7. Discussion and conclusion

In this study, we develop a model for optimizing information security investment allocation against multiple attacks. This study advances the theoretical development in the growing field of economics of information security by closing several gaps in the extant literature and, in doing so, offers important management implications. First, our analytic model takes into account the organizational reality that all firms face budgetary constraints when making investment decisions. Second, our model incorporates the concurrent heterogeneous attacks, a more realistic assumption than the individual, one-at-a-time attacks assumed by prior studies. We identify opportunistic and targeted as two classes of attacks that firms face and derive the breach probability functions for these attacks using first principles. Third, we adopt the concept of scale-free networks, a theoretically robust and empirically supported framework for examining the topology and epidemics in networks of corporate information systems, as the basis for investigating the security characteristics of firms in a network. Lastly, we develop a framework to consider security investments with cross-over effects on other classes of attacks.

Our results offer insights into how managers should allocate security investment budget at various levels of network exposure, relative potential loss, investment effectiveness, and total budget. In particular, we show that, when security budget is small, firms are better off concentrating their investments on only one class of attack. There are occasions, particularly when the total investment is very small relative to the expected loss, where allocating 100% of the security budget to one class of attack is the optimal decision, suggesting an important principle of security investment: When the total investment budget is limited, it is better off concentrating on defending against one class of attack only, even when threats from other classes of attacks exist. This runs counter to the common attempt to cover all attacks all the time. Such a practice, though intuitive (as in "do not put all eggs in one basket"), would not produce enough protection against any of the attacks when the budget is limited, resulting in a sub-optimal allocation. In other words, when a firm plans to spend only a small amount on security, it is better off for the firm to spend on one measure for adequate protection against one class of attack than to split the small budget to both classes, resulting in inadequate protection against both. For instance, when a firm only has the budget to install anti-virus programs on every computer, it is better off to do so than buying only a few anti-virus software licenses to save money for the installation of IDS on one of the several production servers, resulting in ineffective protection against both types of attacks. It is worth emphasizing that such a result is the artifact of a very small budget. Without budget limitation (or if the budget is large relative to security investments), our model shows that firms should invest in protection against both classes of attacks, which is consistent with prior research such as Kumar et al. (2008).

Among the many numerical results, those with $L_1 \gg L_2$ and $\xi_1 \ll \xi_2$ (such as in Fig. 5(b)) simulate the two classes of attacks the best. This is because targeted attacks (Class 1) often result in higher losses than opportunistic attacks (Class 2), although the latter happens much more often than the former. Our first observation is, in the case of independent investments (Section 4), that optimal allocation to targeted attacks increases with network exposure. This result is consistent with the general property of scale-free networks: They tend to be robust against random, opportunistic attacks but are vulnerable against targeted attacks (Anderson and Moore, 2006). Such vulnerability comes from the fact that attacks targeted at those highly connected nodes can endanger the whole network (Albert et al., 2000). When a firm's information systems are highly connected and open (i.e., with high network exposure, as implied by (10)), it is highly vulnerable to targeted attacks; it, therefore, demands more of its security budget to defend them. With higher network exposure, protecting against targeted attacks that have lower attack probability but higher potential loss should be given a higher priority.

As with all analytics, a number of assumptions for making the model manageable may limit its applicability and generality. For instance, mathematical assumptions (continuous, twice differentiable, and bounded) for all the variables and functions in the models are customary in most economic analyses but still represent an ideal case for manipulation. The classification of attacks into two classes – opportunistic and targeted – can be imperfect: Although, as noted in many studies (Casey, 2003; Poff, 2009) that the majority attacks can be classified as such, there are exceptions that should be considered as an extension to the current model. Spear phishing, for example, can be considered as a hybrid of opportunistic and targeted attacks (Vijaya, 2011). The two-stage model (Fig. 1), which assumes that security breaches result in losses to the firm, is a simplified version of reality. In practice, measures such as intrusion detection systems and entrapment servers can help companies avoid losses even when the first layer of security defense is compromised. Also, our assumption that $S_1+S_2=S$ means that the budget is spent in whole. Although in reality employees often tend to use up the budget allocated to a specific project or program, theoretically firms do not have to spend all of their security budget, in which case the constraint would be $S_1+S_2 \le S$. Our assumption is made mainly to simplify the model development and to make the mathematical manipulation manageable; we expect future studies to consider the more general case $S_1+S_2 \le S$. Finally, even in the current model, there are other possible relationships among variables that could be further explored and modeled. Such relationships include potential loss with respect to network exposure (to model the benefits of particular system configurations to business) and attack probability (ξ) with respect to security investment. Although these considerations can add to the existing model, we limit the functional relationships to those presented in this paper based on our belief that they yield the most significant insights without overly taxing the analyses and computations.

Future studies that relax these and other assumptions, as well as empirical verifications of the analytical results, can help advance this stream of research. For instance, an extension to the model in Fig. 1 to take into account multiple stages of information security can offer additional insights into how a firm should choose among different types of security investments. Another interesting research direction could be to complement the "equilibrium" conditions implicit in all economic analyses with considerations of the dynamic and interactive nature of various aspects of information security with techniques such as real options analysis (Li, 2009; Kaufman and Li, 2005). In addition, although we recognize that the scale-free network theory is suitable for our model of corporate networks, other network theories, such as heuristically optimal topology (HOT) (Wallinger et al., 2000), have been proposed for analyzing information security characteristics in a more physically oriented network environment and can be adopted to extend the current research. Also, although the breach functions in this study are mathematically derived based on a priori principles that are theoretically and practically validated, it would be interesting to compare their functional forms to empirical data in a future study. Lastly, although we only focus on security

investment on individual information systems, scale free network theory has policy implications of information security beyond firm's level, such as the robustness of the network (Albert et al., 2000) and security of an information supply chain (Huang et al., 2008b). It is both academically challenging and practically important to extend the nodal analysis presented here to the network level to understand those important policy issues.

A. Technical appendix

A.1. Derivation of opportunistic attack breach probability

Because the theory and results are well developed in the prior literature, we summarize the key assumptions and findings below without reproducing the detailed derivations. Consider the case that an epidemic event starts spreading in a scale-free network. The rate of epidemic spreading, λ, is determined by ν, the infection rate of a previously uninfected node if it is connected to an infected one, and δ, the remediation rate of an infected node:

$$\lambda = \frac{\nu}{\delta}. \tag{T1}$$

Let $P_k(t)$ denote the relative density of infected nodes with k connections – that is the probability that a node with k connections is infected – at time t. The mean field rate equation gives (Pastor-Satorras and Vespignani, 2001)

$$\frac{\partial P_k(t)}{\partial t} = -P_k(t) + \lambda k[1-P_k(t)]\Theta(\lambda), \tag{T2}$$

where $\Theta(\lambda)$ is the probability that any given connection points to an infected node, which can be given in the lowest order of λ (Chang and Young, 2005)

$$\Theta(\lambda) = \frac{e^{-\lambda m}}{\lambda m}, \tag{T3}$$

where m is the minimum number of nodes available for connection in such a network. Solving for P_k in a steady state (i.e., $\partial P_k(t)/\partial t = 0$), we get

$$P_k = \frac{k\lambda\Theta(\lambda)}{1+k\lambda\Theta(\lambda)}. \tag{T4}$$

Substituting (T3) into (T4) and averaging P_k over k, we get the average infection probability of any node in the network (Pastor-Satorras and Vespignani, 2001)

$$P_{epidemic} = \beta e^{-(1/\lambda m)}, \tag{T5}$$

where β is a normalization constant.

To extend the (T5) to our model for security investment of the firm's information systems, we make the following observations. First, we assume that the effect of security investments S in protecting the information systems against the potential breach can be represented as the reduction in the infection rate λ in (T5), and, for simplicity and without loss of generality, we assume a linear inverse relationship between security investment and infection rate. We further require that λ and S satisfy the following boundary conditions: First, the attack spreads freely to the node when there is no security investment made; that is, $\lambda=1$ when $S=0$; second, no finite security investments can fully block all attacks; that is $\lambda\to 0$ only when $S\to\infty$. Such a relationship with the above boundary conditions can be expressed in the following manner:

$$\lambda \equiv \frac{1}{\kappa S+1}, \tag{T6}$$

where $\kappa\in[0,1]$ is a scaling factor for S. As such, κ also measures the level of impact, or the effectiveness, of the security investments—for any given security investment S, the higher the κ, the greater reduction of the infection rate.

Next, we note that the network exposure c of an average node in such a network is strictly increasing in m. And $c=0$ when $m=0$. Further, the systems are highly exposed to attacks when they are completely open; that is, $c\to 1$ when $m\to\infty$. Without loss of generality, we assign the following relationship between c and m that satisfies all the above conditions:

$$c \equiv e^{-(1/m)}. \tag{T7}$$

Lastly, we note that the level of threat from attacks is not explicitly considered in (T5), which can be accounted for by multiplying (T5) with the attack probability ξ. With this modification, (T6) and (T7), and adjusting the normalization constant β to reflect the boundary condition (1), we find that the breach probability for an opportunistic attack can be written as

$$\xi\cdot P_{epidemic} = \xi\cdot\left(e^{-(1/m)}\right)^{1/\lambda} = \xi c^{\kappa S+1}, \tag{T8}$$

which gives the expression for ρ_2.

A.2. Proof of Lemma 1

Rewriting the boundary condition (14), we have

$$c^{\kappa_2 S} \le -\frac{\xi_1\kappa_1 L_1}{\xi_2\kappa_2 L_2}\frac{1}{\ln c}. \tag{T9}$$

Because $\ln c<0$. Taking natural logarithm on both sides, we get

$$\kappa_2(\ln\nu)S \le \ln\left(-\frac{\xi_1\kappa_1 L_1}{\xi_2\kappa_2 L_2}\frac{1}{\ln c}\right). \tag{T10}$$

Solving for S, we get

$$S \ge \frac{1}{\kappa_2 \ln c}\ln\left(-\frac{\xi_1\kappa_1 L_1}{\xi_2\kappa_2 L_2}\frac{1}{\ln c}\right). \tag{T11}$$

Since $\ln c<0$, the right hand side is greater than 0 when the term $\ln\left(-(\xi_1\kappa_1 L_1/\xi_2\kappa_2 L_2)(1/\ln c)\right)<0$, or

$$-\frac{\xi_1\kappa_1 L_1}{\xi_2\kappa_2 L_2}\frac{1}{\ln c} < 0. \tag{T12}$$

Solving for c, we get

$$c < e^{-(L_1/L_2)(\kappa_1/\kappa_2)(\xi_1/\xi_2)}. \tag{T13}$$

Therefore, from (T13) and (T11), we know that when $c<c'=e^{-(L_1/L_2)(\kappa_1/\kappa_2)(\xi_1/\xi_2)}$, S has a lower bound

$$S_0 = \frac{1}{\kappa_2 \ln c}\ln\left(-\frac{L_1}{L_2}\frac{\kappa_1}{\kappa_2}\frac{\xi_2}{\xi_1}\frac{1}{\ln c}\right),$$

and that proves Lemma 1.

A.3. Proof of Proposition 1

Starting with (17), we find the relationship of S_1^* and S_1^*/S with c by setting $y=S_1^*$ and $x=c$ in (16):

$$\frac{\partial S_1^*}{\partial c} = -\frac{\partial F/\partial c}{\partial F/\partial S_1^*}. \tag{T14}$$

Note that $\partial S_1^*/\partial c = dS_1^*/dc$ in (16), because c is independent of all other parameters S, L_1, L_2, κ_1, κ_2, ξ_1, and ξ_2. We first examine the denominator of the right-hand side of (T14) using (17):

$$\begin{aligned}\frac{\partial F}{\partial S_1^*} &= \frac{\kappa_2(\ln c)c^{\kappa_2 S}}{(\kappa_1 S_1^*+1)^2} - \frac{2\kappa_1 c^{\kappa_2 S}}{(\kappa_1 S_1^*+1)^3} \\ &= \frac{\kappa_2(\ln c)c^{\kappa_2 S}}{(\kappa_1 S_1^*+1)^2}\left[\kappa_2(\kappa_1 S_1^*+1)\ln c - 2\kappa_1\right].\end{aligned} \tag{T15}$$

But we know $[\kappa_2(\kappa_1 S_1^*+1)\ln c-2\kappa_1]\le 0$, because its first term is negative ($\ln c\le 0$) and its second term positive. In other words,

$$\frac{\partial F}{\partial S_1^*}\le 0. \tag{T16}$$

And since we can rewrite (T14) as

$$\frac{\partial S_1^*}{\partial c}=\frac{\partial F/\partial c}{-(\partial F/\partial S_1^*)}, \tag{T17}$$

we know that the sign of $\partial S_1^*/\partial c$ is determined by the numerator, $\partial F/\partial c$, alone. Using (17) and rearranging the terms, we have

$$\frac{\partial F}{\partial c}=\frac{\kappa_2 S_1^* c^{\kappa_2 S_1^*-1}}{(\kappa_1 S_1^*+1)^2}+bc^{\kappa_2 S-1}[1+\kappa_2(\ln c)], \tag{T18}$$

where, for simplicity of manipulation

$$b=\frac{L_1}{L_2}\frac{\kappa_1}{\kappa_2}\frac{\xi_2}{\xi_1}. \tag{T19}$$

$[1+\kappa_2(\ln c)]$ determines the sign of (T15), because all other terms on the right-hand side are positive. Therefore, as a sufficient (but not necessary) condition, when $[1+\kappa_2(\ln c)]\ge 0$, or

$$c\ge \underline{c}=e^{-(1/\kappa_2)}, \tag{T20}$$

we have (T18) ≥ 0, and subsequently, as argued earlier, $\partial S_1^*/\partial c\ge 0$. Also note that, because S is independent of c, $\partial(S_1^*/S)/\partial c=(\partial S_1^*/\partial c)/S\ge 0$ follows. Therefore, for all $c\ge\underline{c}$, where $\underline{c}\in[0, e^{-(1/\kappa_2)}]$, both $\partial S_1^*/\partial c\ge 0$ and $\partial(S_1^*/S)/\partial c\ge 0$.

A.4. Proof of Proposition 2

The proof of Proposition 2 is omitted, because it is straightforward from (16) and (17) and setting $y=S_1^*$ and $x=L_1/L_2$.

A.5. Proof of Proposition 3

To find the relationship of S_1^* and S_1^*/S with S, we set $y=S_1^*$ and $x=$S in (16):

$$\frac{\partial S_1^*}{\partial S}=-\frac{\partial F/\partial S}{\partial F/\partial S_1^*}. \tag{T21}$$

(We use partial derivatives on the left-hand side, because S is independent of all other parameters.) Substituting (17) into the numerator, we have

$$\frac{\partial F}{\partial S}=\frac{L_1}{L_2}\left(\frac{\kappa_2}{\kappa_1}\right)^2\frac{\xi_2}{\xi_1}(\ln c)^2 c^{\kappa_2 S}\ge 0. \tag{T22}$$

With (T16) and (T22), we know

$$\frac{\partial S_1^*}{\partial S}\ge 0. \tag{T23}$$

Next, we examine how S_1^*/S varies with S. We start by writing out the following:

$$\frac{\partial S_1^*/\partial S}{\partial S}=\frac{\partial S_1^*/\partial S}{S}-\frac{S_1^*}{S^2}=\frac{1}{S^2}\left(-S\frac{\partial F/\partial S}{\partial F/\partial S_1^*}-S_1^*\right). \tag{T24}$$

Substituting (T15) and (T22) into (T24) and rearranging terms, we get

$$\begin{aligned}\frac{\partial S_1^*/\partial S}{\partial S}&=\frac{-\kappa_2 b(\ln c)^2 c^{\kappa_2 S}S/(c^{\kappa_2 S_1^*}/(\kappa_1 S_1^*+1)^2)[\kappa_2(\kappa_1 S_1^*+1)\ln c-2\kappa_1]-S_1^*}{S^2}\\&=\frac{\kappa_2 b(\ln c)^2 c^{\kappa_2(S-S_1^*)}S(\kappa_1 S_1^*+1)^2+S_1^*[\kappa_2(\kappa_1 S_1^*+1)\ln c-2\kappa_1]}{-S^2[\kappa_2(\kappa_1 S_1^*+1)\ln c-2\kappa_1]},\end{aligned} \tag{T25}$$

where b is defined in (T19). Because the denominator is positive, the sign of (T25) is determined by the numerator, which can be written as the following, after rearranging the terms,

$$\text{Numerator of (T25)}=\kappa_2(\kappa_1 S_1^*+1)\times\ln c\left[b(\ln c)c^{\kappa_2(S-S_1^*)}S(\kappa_1 S_1^*+1)+S_1^*\right]-2\kappa_1 S_1^*. \tag{T26}$$

It is not possible to determine, in general, the sign of (T26), but we can examine the boundary cases where S is very small and very large. When $S\to\infty$, the first term in the bracket dominates and is positive (since we have $(\ln c)^2$ and all other parameters are positive), (T26) is positive. Therefore, when S is sufficiently large, $(\partial S_1^*/\partial S)/\partial S\ge 0$.

When $S\to 0$, $S_1^*\to 0$ also (since $S_1^*\le S$ always), and (T26) approaches $\kappa_2\ln cS_1^*-2\kappa_1 S_1^*$, which is negative, because $\ln c\le 0$. This condition is only possible when $c>c'=e^{-(L_1/L_2)(\kappa_1/\kappa_2)(\xi_1/\xi_2)}$ according to Lemma 1. Therefore, when $c>c'=e^{-(L_1/L_2)(\kappa_1/\kappa_2)(\xi_1/\xi_2)}$ and S is small, $(\partial S_1^*/\partial S)/\partial S\le 0$. This concludes our proof of Proposition 3.

References

Albert, R., Jeong, H., Barabási, A.L., 1999. Diameter of the world-wide web. Nature 401, 130–131.

Albert, R., Jeong, H., Barabási, A.L., 2000. Error and attack tolerance of complex networks. Nature 406, 378–382.

Alderson, D., Li, L., Wallinger, W., Doyle, J.C., 2005. Understanding Internet topology: principles, models, and validation. IEEE/ACM Transactions on Networking 13 (6), 1205–1218.

Alter, S., Sherer, S., 2004. A general, but readily adaptable model of information system risk. Communications of the AIS 14 (1), 1–28.

Anderson, R., Moore, T., 2006. The economics of information security. Science 314, 610–613.

Arora, A., Hall, D., Pinto, C.A., Ramsey, D., Telang, R., 2004. Measuring the risk-based value of IT security solutions. IEEE IT Professional 6 (6), 35–42.

Barabási, A.L., Albert, R., 1999. Emergence of scaling in random networks. Science 286, 509–512.

Behara, R.S., Bhattacharya, S., 2007. Process-Centric Risk Management Framework for Information Security. In: Chen, H., Raghu, T.S., Ramesh, R., Vinze, A., Zeng, D. (Eds.), National Security, 349–366. Elsevier, The Netherlands.

Bellovin, S., 2001. Computer security: an end state? Communications of ACM 44 (3), 131–132.

Carr, N.G., 2003. It doesn't matter. Harvard Business Review 81 (5), 41–49.

Casey, E., 2003. Determining Intent—Opportunistic vs. Targeted Attacks. Computer Fraud & Security 4, 8–11.

Cavusoglu, H., Raghunathan, S., 2004. Configuration of intrusion detection systems: a comparison of decision and game theoretic approaches. INFORMS Journal of Decision Analysis 1 (3), 131–148.

Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. A model for evaluating IT security investments. Communications of ACM 47 (7), 87–92.

Cavusoglu, H., Mishra, B., Raghunathan, S., 2005. The value of intrusion detection systems in information technology security architecture. Information Systems Research 16 (1), 28–46.

Chang, D.B., Young, C.S., 2005. Infection dynamics on the internet. Computer Security 24, 280–286.

Collins, M., Gates, C., Kataria, G., 2006. A model for opportunistic network exploits: the case of P2P worms. In: Fifth Workshop on Economics of Information Security, Cambridge, England.

Cremonini, D., Nizovtsev, M., 2006. Understanding and influencing attackers' decisions: implications for security investment strategies. In: Fifth Workshop on Economics of Information Security, Cambridge, England.

CERT, 2007. Overconfidence is Pervasive Amongst Security Professionals, E-Crime Watch Survey by CSO Magazine, CERT, and U.S. Secret Service.

Dhanjani, N., 2009. Hacking: The Next Generation. O'Reiley Media.

Faloutsos, M., Faloutsos, P., Faloutsos, C., 1999. On power–law relationships of the internet topology. ACM SIGCOMM Computer and Communications Review 29 (4), 251–262.

Goel, S., Chen, V., 2008. Can business process reengineering lead to security vulnerability: analyzing the reengineered process. International Journal of Production Economics 115 (1), 104–112.

Gordon, L.A., Loeb, M.P., 2002. The economics of information security investment. ACM Transactions on Information Systems Security 5 (4), 438–457.

Griffin, C., Brooks, R., 2006. A note on the spread of worms in scale-free networks. IEEE Transactions on Systems, Man, Cybernetics B 36 (1), 198–202.

Gross, T., D'Lima, C.J.D., Blasius, B., 2006. Epidemic dynamics on an adaptive network. Physical Review Letters 96 (20), 2087011.

Hauske, K., 2006. Returns to information security investment: the effect of alternative information security breach functions on optima investment and sensitivity to vulnerability. Information Systems Frontier 8, 338–349.

Li, X., 2009. Preemptive learning, competency traps, and information technology adoption: a real options analysis. IEEE Transactions on Engineering Management 56 (4), 650–662.

Huang, C.D., Behara, R.S., Hu, Q., 2008a. An economic analysis of the optimal information security investment in the case of a risk-averse firm. International Journal of Production Economics 114 (2), 793–804.

Huang, C.D., Behara, R.S., Hu, Q., 2008b. Managing risk propagation in extended enterprise networks. IEEE IT Professional 10 (4), 14–19.
Karr, K., 2006. The State of information security spending. Forrester Research 4.
Kaufman, R., Li, X., 2005. Technology competition and optimal investment timing: a real options perspective. IEEE Transaction on Engineering Management 52 (1), 15–29.
Khamooshi, H., Cioffi, D.F., 2009. Program risk contingency budget planning. IEEE Transactions on Engineering Management 56 (1), 171–179.
Kumar, R., Raghavan, P., Rajagopalan, S., Sivakumar, D., Tomkins, A., Upfal, E., 2000. The web as a graph. In: Proceedings of 19th ACM Symposium of Principles of Database Systems, Dallas, Texas, 1–10.
Kumar, R.L., Park, S., Subramaniam, C., 2008. Understanding the value of countermeasure portfolios in information systems security. Journal of Management Information Systems 25 (2), 241–279.
Lai, Y.C., Liu, Z., Ye, N., 2003. Infection dynamics on growing networks. International Journal of Modern Physics B 17 (22/23/24), 4045–4061.
Mercuri, R.T., 2003. Analyzing security costs. Communications of ACM 46 (6), 15–18.
Mirkovic, J., Reiher, P., 2004. A taxonomy of DDoS attack and DDoS defense mechanism. ACM SIGCOMM Computer and Communications Review 34 (2), 39–53.
Nagaraja, S., Anderson, R., 2005. The Topology of Covert Conflict, Computer Laboratory Technical Report UCAM-CL-TR-637. University of Cambridge.
Ogut, H., Menon, N., Raghunathan, S., 2005. Cyber insurance and IT security investment: impact of interdependent risk. In: Fourth Workshop on Economics of Information Security, Cambridge, MA.
Pastor-Satorras, R., Vespignani, A., 2001. Epidemic spreading in scale-free networks. Physical Review Letters 86 (14), 3200–3203.
Poff, J., 2009. What's really happening in IT security? InterBusiness Issues.
Ponemon Institute, 2009. 2008 Annual Study: Cost of Data Breach. PGP Corporation.
Richardson, R., 2009. 2008 CSI Computer Crime & Security Survey. Computer Security Institute.
Schechter, S.E., 2005. Towards econometric models of the security risk from remote attacks. IEEE Security & Privacy 3 (1), 40–44.
Telo da Gama, M.M., Nunes, A., 2006. Epidemics in small world networks. European Physics Journal B 50, 205–208.
Verizon, 2011. Data Breach Investigations Report.
Vijaya, Jaikumar, 2011. Epsilon a Victim of Spear-Phishing Attack, Says Report. Computer World, April 7.
Wallinger, W., Govindan, R., Jamin, S., Paxson, V., Shenker, S., 2000. Scaling phenomena in the internet: critically examining criticality. Proceedings of National Academy of Science 99 (1), 2573–2580.
Watts, D.J., 1999. Small worlds: the dynamics of networks between order and randomness. Princeton University Press, Princeton, New Jersey.
Watts, D.J., Strogatz, S.H., 1998. Collective dynamics of ''small-world''. Networks, Nature 393, 440–442.
Zhou, T., Liu, J.G., Bai, W.J., Chen, G., Wang, B.H., 2006. Behavior of susceptible-infected epidemics on scale-free networks with identical infectivity. Physical Reviews E 74 (5), 0561091.