A differential game approach to security investment and information sharing in a competitive environment

Xing Gao and Weijun Zhong

School of Economics and Management, Southeast University, Nanjing, People's Republic of China

ABSTRACT
Information security economics, an emerging and thriving research topic, attempts to address the problems of distorted incentives for stakeholders in an Internet environment, including firms, hackers, the public sector, and other participants, using economic approaches. To alleviate consumer anxiety about the loss of sensitive information, and to further increase consumer demand, firms usually integrate their information security investment strategies to capture market share from competitors and their security information sharing strategies to increase consumer demand across all member firms in industry-based information sharing centers. Using differential game theory, this article investigates dynamic strategies for security investment and information sharing for two competing firms under targeted attacks, in which both firms can influence the value of their information assets through the endogenous determination of pricing rates. We analytically and numerically examine how both security investment rates and information sharing rates are affected by several key parameters in a non-cooperative scenario, including the efficiency of security investment rates, sensitivity parameters for pricing rates, coefficients of consumer demand losses, and the density of targeted attacks. Our results reveal that, confronted with a higher coefficient of consumer demand loss and a higher density of targeted attacks, both firms are reluctant to aggressively defend against hackers and would rather decrease the negative effect of hacker attacks by lowering their pricing rates. Also, we derive feedback equilibrium solutions for the situation where both firms cooperate in security investment, information sharing, or both. It is revealed that although a higher hacker attack density always decreases a firm's integral profits, both firms are not always willing to cooperate in security investment and information sharing. Specifically, the superior firm benefits most when both firms fully cooperate and benefits the least when they behave fully non-cooperatively. However, the inferior firm enjoys the highest integral profit when both firms only cooperate in information sharing and the lowest integral profit in the completely cooperative situation.

1. Introduction

Competition between firms has become increasingly fierce due to the rapid development of science and technology, the intensive evolution of economic globalization, and in-depth changes in market environments. To address these challenges, an increasing number of firms are tending to adopt information technology to construct and rebuild their business structures. However, unimaginable losses may occur as a result of information security incidents. Traditional approaches to technology security programs have gradually become inadequate to effectively reduce frequent information security incidents. These information security technologies primarily focus on better access control policies, complex cryptographic protocols, advanced firewalls and intrusion detection systems (IDS) (Cavusoglu and Raghunathan, 2004; Cavusoglu et al., 2009; Gao et al., 2013c), better system evaluation tools, perfect code design, and so on. Although these security technologies perform outstandingly, more and more firms and organizations have suffered serious cyber-attacks from hackers and thus incurred heavy losses in business, customer trust, reputation, and competitiveness. For example, JPMorgan Chase Bank, one of the largest financial service organizations in America, with sophisticated security network systems, was attacked by hackers in 2014 and incurred a data loss that included user names, home addresses, telephone numbers, and email addresses of 76 million families and 7 million small enterprises. SafeNet Corporation reported that during the first quarter of 2014, nearly two hundred million record stealing incidents occurred, representing an increase of 233% over the same period in 2013.

An underlying shortcoming of traditional security technologies is that they only concern technology solutions and thus neglect the economic motivations of stakeholders in the context of Internet security. Information security economics has recently emerged as a fast-moving inter-disciplinary research branch that links information systems and economics. This research is aimed at improving the security level of information systems by fully highlighting the behavior of all agents in a network environment, such as competitor firms (Gal-Or and Ghose, 2005; Kolfal et al., 2013), hackers (Cavusoglu et al., 2008; Galbreth and Shor, 2010), security software vendors (Kim et al., 2009, 2011; August et al., 2014a, 2014b), security software insurers (Bandyopadhyay et al., 2009; Mukhopadhyay et al., 2013), security software outsourcers (Lee et al., 2013; Cezar et al., 2014), and public sectors (Kannan and Telang, 2005). Generally
Speaking, information security economics takes various economic and social elements into account, applies the concepts and ideology of economics and management, addresses the problems of conflict and divergence of interest of all stakeholders, and finally formulates reasonable information security management strategies. It is important to understand information security economics because, as argued by Anderson and Moore (2006), information security failures result from the distorted economic incentives of participants at least as often as from poor technological design.

Constructing a differential game framework, this article discusses dynamic strategies for security investment and information sharing for two competitor firms, both of which are confronted with targeted attacks by hackers and are able to affect the values of information assets related to information systems by endogenous pricing choices. We focus on security-related industries involving electronic commerce, electronic payment, electronic banking, credit cards, etc., in which consumers are likely to be concerned about information security. Both security investment and information sharing are the main components of the security strategies that firms usually employ to defend against hackers and to influence their market share. Faced with two different firms, consumers make choices based on the security investment undertaken by each firm. When a firm increases its security investment to prevent security breaches of its information systems, consumer anxiety about a transaction with that firm will be assuaged and their confidence and willingness to pay for a product will be enhanced, thus attracting the competitor’s consumers. However, if the competitor increases its security investment, the first firm incurs a loss of consumers, as the competitor will be considered to be a more reliable and secure firm. In other words, a firm can acquire market share from its competitor through a greater investment in security.

Gal-Or and Ghose (2005), Cezar et al. (2010), and Kolfal et al. (2013) explicitly assume that a firm’s consumer demand function is dependent on its security investment and that of its competitor in a competitive environment. Again, some evidence here shows that consumers can indeed perceive information security investments when making purchasing decisions, at least in the security-related industries under consideration. There are many facets of security mechanisms and measures that firms invest in and employ in different business environments. Although some security tools, such as firewalls, IDSs, and encrypted transmissions, are highly technical and therefore not always visible to consumers, they are still able to form strong perceptions of a firm’s information security levels (Miyazaki and Fernandez, 2000; Suh and Han, 2003; Cheung and Lee, 2006; Román, 2007; Kim et al., 2010; Ray et al., 2011; Hartono et al., 2014). In particular, Kim et al. (2010) categorize the factors that influence consumers’ perceptions of information security in the use of e-payment systems into technical protection, security statements, and transaction procedures. Precisely speaking, technical protection involves specific and technical mechanisms to ensure privacy, integrity, confidentiality, and stability in online transactions, which can be achieved by using certain specific policies such as explicit standardization. Security statements refers to the information provided to consumers in the operation of e-payment systems and related security solutions. Security statements that are posted on websites usually involve security feature statements, data protection and privacy statements, security-policy statements, and other descriptive content concerning security precautions. Transaction procedures indicate the processes of authentication, modification, and confirmation, which can be informed to consumers. Obviously, authentication is a visible procedure by which the identity of consumers is verified through their identity and password. In one type of e-payment system, online banks in China have adopted different types of identity authentication mechanisms to guarantee information security, such as the first-generation USB key, the second-generation USB key, and the dynamic password. The first-generation USB key guarantees identity authentication security through a physical USB key; however, it can be hijacked by a Trojan virus launched by hackers. The second-generation USB key ensures identity authentication security not only by the physical USB key but also by a manual confirmation by the consumer on an additional LCD display, which reduces the risk of being hijacked by a Trojan virus. The dynamic password approach ensures the best identity authentication security by using changeable passwords for every transaction. Moreover, Kolfal et al. (2013) assume that consumers can perceive information security investments because they must be notified of security breaches in a timely manner by laws such as California’s SB 1386, HIPAA, and DPA in the UK. As evidenced by Marte (2014), consumer purchasing decisions are indeed affected by security breaches. Although the number of security breaches that one firm suffers does not necessarily exactly correlate with the security investment of that firm, higher information security investment on the part of a given firm is usually accompanied by fewer security breaches. Cremonini and Nizovtsev (2009) find that firms have the ability to signal security characteristics in their information systems as a deterrence tool.

In our model, information sharing serves as another key factor to improve the level of information security. The U.S. federal government has even encouraged the establishment of industry-based Information Sharing and Analysis Centers (ISACs), including the Aviation ISAC (A-ISAC), Defense Industrial Base ISAC (DIB-ISAC), Electric Sector ISAC (ES-ISAC), Financial Services ISAC (FS-ISAC), Information Technology ISAC (IT-ISAC), Supply Chain ISAC, Real Estate ISAC, Public Transit ISAC, and so on. Meanwhile, there are other information sharing organizations such as the Computer Emergency Response Team, Information Sharing and Analysis Centers, Electron Crimes Task Forces and Chief Security Officers Round Tables. When firms share security information through such organizations, the information can be analyzed and classified to quickly disseminate physical and cyber threat alerts and security solutions can be recommended to member firms to protect their information systems as soon as possible. By reporting security breaches and sharing related security information in these information sharing organizations, all member firms can send a strong message to their customers that they are committed to developing rigorous information security procedures and are taking all necessary steps to mitigate damage from future breaches (Schenk and Schenk, 2002). Recognizing an increase in information security levels, consumers will become more willing to transact with all member firms. Hence, unlike security investments, information sharing allows all member firms to
experience a positive demand shock and enlarge their market share.

Based on hacker behavior, cyber-attacks can be classified as either a targeted attack or a mass attack. Targeted attacks, such as pharming, industrial espionage, denial of service, and intrusions, are aimed at high-return firms, whereas mass attacks such as worms, viruses, spam, spyware, and bots are intended for all firms (Cavusoglu et al., 2008). That is, in targeted attacks, hackers execute cyber-attacks discriminately based on the related returns they can obtain, but mass attacks are implemented as pharming, industrial espionage, denial of service, and intrusions (Cavusoglu et al., 2008; Mookerjee et al., 2011; Dey et al., 2012, 2014). In addition to behavior characteristics, the hacker community can be divided into those whose motivations are profit-driven, fame-driven, excitement-driven, and politics-driven (Leeson and Coyne, 2006; Kim et al., 2012). However, their motivations have mainly moved from fame and excitement to financial and political gains. This article focuses on profit-driven hackers launching targeted attacks, which constitute an increasingly large proportion of hackers in this networked world of electronic commerce.

In the current study, in addition to security investment and information sharing, we assume that firms can endogenously determine the prices of their products and services over time, which has a further impact on consumer demand and even on the value of information assets in information systems. Information assets are mainly related to customer names, credit card data, user names, passwords, social security numbers, addresses, phone numbers, and other sensitive data. Firms that possess and control information assets can gain economic benefits by utilizing them in their business activities. As information assets contribute to a firm's profits, their value can be reflected in that firm's profits when all other factors such as the conversion efficiency of information assets remain unchanged. The value of information assets for firms, which is realized in legal business processes, is not necessarily equal to the value to a hacker, which is realized by unauthorized and unlawful use in black markets. For instance, credit card firms realize the value of information assets by facilitating the customer payment process during purchasing transactions, whereas hackers illegally achieve the value by fraudulent purchase and identity theft (Bandyopadhyay et al., 2014). Even so, a hacker's evaluation of information assets should be positively related to the value of information assets for a firm (Hausken, 2007, 2008; Png and Wang, 2009; Kannan et al., 2016). Given that a firm's value of information assets can be measured by its profits, a hacker's evaluation of information assets would also be influenced by the profits of that firm. As for the example of credit card firms, their prices for information assets can be approximately evaluated by the status and the payment capacity of the credit cards. As a firm's profit increases, its price for information assets becomes higher for a given market share or, alternatively, their market share becomes larger for a given price of information assets. Hackers can obtain greater gains by breaching firms with higher profits, due to more valuable data or larger volumes of information. The degree of positive correlation between a hacker's returns and a firm's profits commonly depends on whether the hacker can easily sell their stolen information assets on the black market. In targeted attacks that are aimed at stealing a firm's information assets from information systems discriminatively, the value of information assets can be influenced by the endogenous determination of pricing. Therefore, a firm's pricing strategy becomes sophisticated and needs a comprehensive consideration of the effects of the behavior of both competitors and hackers.

The current research attempts to answer the following questions.

1. What should a firm's dynamic security investment, dynamic information sharing, dynamic pricing, and even integral profit be in a competitive environment?
2. How do market characteristics and cyber-attack characteristics influence such dynamic strategies and integral profit?
3. How do such dynamic strategies and integral profit change when firms cooperate in security investment, information sharing or both?

To the best of our knowledge, this article is the first to address the value of information assets by endogenous pricing decisions under targeted attacks. These questions are important but remain unaddressed in information security economics. This study can help a firm to formulate dynamic strategies for security investment, information sharing, and pricing over time and to analyze the effects of market characteristics, cyber-attack characteristics, and cooperation forms on these strategies and the resulting integral profit. To obtain the main findings, we build a differential game model that reflects the dynamic effects of security investment, information sharing, and pricing under targeted attacks and in addition facilitates the mathematical tractability of the feedback equilibrium solution.

Unlike static game approaches, differential game approaches can characterize the inherently dynamic features of related problems and are apparently more appropriate for formulating information security issues. From the perspective of modern firms, when their business structures alter, the information systems supporting these structures dynamically change, and the security programs for information systems must be correspondingly adjusted. More important, from the perspective of hackers, attacking modes (Mookerjee et al., 2011), knowledge dissemination (Mookerjee et al., 2011), and virus propagation (Chen and Carley, 2004; Griffin and Brooks, 2006; Yuan et al., 2009; Ransbotham et al., 2012) have to be characterized in a dynamic setting. Many studies on configuration and investment in information security have been conducted based on optimal controls (Yue and Cakanyildirim, 2007; Mookerjee et al., 2011) and differential games (Bandyopadhyay et al., 2014; Garcia et al., 2014). In addition to security investment and information sharing, which are aimed at defending against hackers, a firm's pricing decisions are assumed to be dynamic in this article. Pricing decisions, including skimming and penetration pricing, are long-run strategies and are usually characterized dynamically (Feichtinger and Dockner, 1985; Krishnamoorthy et al., 2010). We construct our model using differential games, in which pricing, security investment, and information sharing interact with each other in their dynamic effects.

The remainder of this article is organized as follows. Section 2 reviews the related literature on information security economics. Section 3 presents the model in a non-cooperative
situation, and Section 4 discusses a firm’s feedback equilibrium solution and resulting integral profit. Section 5 analyzes feedback equilibrium solutions and integral profits when two firms cooperate partially and completely, respectively. Section 6 concludes this article. All omitted proofs are relegated to the online Appendices.

2. Related literature

In their pioneering research, Gordon and Loeb (2002) show that a firm should not necessarily heavily invest in security for an information system with high levels of vulnerability, because it may incur the most frequent cyber-attacks from hackers. This finding can to some degree illustrate that an underlying reason for information security failures rests with misaligned incentives for stakeholders, as confirmed by Anderson and Moore (2006). Since then, information security economics has developed rapidly; this branch of study involves economics and management models and considers all related agents in a network environment. Introducing a strategic hacker, Cavusoglu et al. (2008) construct a game between a hacker and a firm to analyze the effect of their move-timing on the information security investment of the firm. Cremonini and Nizovtsev (2009) find that well-protected firms can use the signal of their superior protection level as a deterrence tool when hackers can change cyberattacks between firms. Hausken (2006) examines how hackers’ income and ability affect a firm’s information security investment. Hausken (2008) and Cárceles-Poveda and Tauman (2011) consider a two-stage security investment game and a security allocation game, respectively. It should be noted that real options techniques (Herath and Harath 2009), the value-at-risk method (Wang et al., 2008), the analytic hierarchy process (Bodin et al., 2005), and the empirical approach (Kannan et al., 2007) are all employed to examine information security investment.

With the establishment of the origins of information sharing, information sharing as a powerful approach to enhancing information system security has been extensively examined. Gordon et al. (2003) show that exogenously given information sharing may reduce the information security expenditure and increase information security levels and total social welfare. Gal-Or and Ghose (2005) show that a firm benefits more from information sharing in more competitive industries. Hausken (2007) discusses the effect of interdependence on information sharing between two firms. Liu et al. (2011) find that whether firms are willing to share security information depends on the relationship between their information assets. Gao et al. (2014, 2015) examine information sharing for firms with different relationships between information assets. Böhme (2010) discusses the relation between security investment models and security metrics. Böhme and Moore (2009) consider a security investment model that reflects the dynamic interaction between a defender facing uncertainty and an attacker repeatedly targeting the weakest link. Khouzani et al. (2014) analyzes security information sharing regarding vulnerabilities in competitive environments.

Another interesting area in the field of information security economics is the analysis of hackers’ modes of cyber-attacks on information security investments, targeted attacks and mass attacks. Png and Wang (2009) find that more effort should be exerted in precautions against mass attacks rather than targeted attacks. Ransbotham and Mitra (2009) empirically analyze paths and strategies under mass and targeted attacks. Mookerjee et al. (2011) examine the effect of mass and targeted attacks on the discrimination ability of a security system. Huang and Behara (2013) investigate how a firm should allocate its limited information security budget between mass and targeted attacks. Dey et al. (2012) examine the effect of two types of cyber-attacks on the security software market. Kim and Kim (2014) study the effect of mass and targeted attacks on malware resolution processes. August and Tunca (2006, 2011) analyze user incentives for security investment and liability policies for security incidents under mass attacks in a network environment.

The current article investigates dynamic competition in security investment and information sharing, whereas the previous relevant literature only considers static counterparts or fails to fully characterize the targeted attacks of hackers. Although Gal-Or and Ghose (2005) build their model under static price competition, unlike our article, they still neglect to incorporate the hackers’ economic incentives and partial cooperation between firms. Bandyopadhyay et al. (2014) and Gao et al. (2013a, 2013c) use a differential game approach to investigate dynamic security investment; neither of them, however, takes pricing or targeted attacks into account. This article examines the dynamic interaction between security investment and information sharing in a competitive environment when targeted attacks are taken into account, which helps to understand the effects of competitors and hackers in information security economics.

3. The model

We now characterize the effects of security investment rates, information sharing rates, and pricing rates on changes in consumer demand rates. As emphasized by Gal-Or and Ghose (2005, p. 192):

When a given firm increases its investment in security technology to prevent security breaches or enhance the effectiveness of security products, and consumers become informed of this increase, their level of anxiety about transacting with the firm declines, thus enhancing their expected utility and willingness to pay for the product.

There are very similar arguments presented in both Cezar et al. (2010) and Kolfal et al. (2013). That is, when a given firm increases its security investment rate, the security level of its information system becomes higher, resulting in a lower chance of security breaches or a smaller loss from security breaches. Therefore, some consumers of a rival firm will switch to this firm due to its advantage in information system security. In contrast, when the rival firm increases its security investment rate, some consumers of the first firm will lose their sense of security and switch to the rival that is comparatively more secure. The change in the consumer demand rate of firm $i$ due to security investment rates can be described by

$$
\dot{x}_{i,t} = a_i z_i(t) \sqrt{x_{3,i}(t) - a_{i-1} z_{i-1}(t) \sqrt{x_{3,i-1}(t)}},
$$

where $z_i(t)$ denotes the security investment rate of firm $i$ at time $t \in [0, \infty)$ and $a_i$ is the related efficiency ($i = 1, 2$). The form of Equation (1) has been widely used (He et al., 2009; He et al., 2012) and characterizes the effects of both firms’ security
investment rates and also guarantees an analytical solution to our problem.

Note that each firm’s information sharing rate can contribute to the information security level of the entire related industry through industry-based information sharing organizations such as A-ISAC, DIB-ISAC, ES-ISAC, FS-ISAC, IT-ISAC, and others. Firm $i$ will experience the following positive demand shock:

$$
\dot{x}_{i,t}(t) = c_1 s_1(t) + c_2 s_2(t),
$$

where $s_i(t)$ represents the rate of information sharing provided by firm $i$ to these organizations and $c_i$ is the related efficiency. Note that security information rate that firm $i$ offers and shares with its rival has a positive effect on firm $i$. That is, the effect of information sharing rates on each firm should be weighed by the collective measure, $c_1 s_1(t) + c_2 s_2(t)$. The reason for this observation is that in practice, the security information about a particular security attack received by a firm through information sharing centers may be fragmented and thus it will carry very little substantive information until it is combined with related security information of its own (Liu et al., 2014). As reported above, when firm $i$ offers and shares its security information through information sharing centers, the member firms in such centers are able to obtain timely and better information for decision-making on security that will allow improvement in their security control mechanisms, leading to a higher security level for their information systems. As a result, there is a lower chance of security breaches for member firms and, thus, potential consumers may pick these firms for transactions.

The change in the consumer demand rate of firm $i$ due to pricing rates is characterized by

$$
\dot{x}_{i,p}(t) = -b_i p_i(t) x_i(t) + b_3 \ldots p_3 \ldots (t) x_{3 \ldots}(t),
$$

where $p_i(t)$ is firm $i$’s pricing rate and $b_i$ is the sensitivity parameter. Equation (3) is a somewhat revised form of the change in market share rates defined by Feichtinger and Dockner (1985), who assume that in a dynamic oligopoly the proportion of customers driven away from firm $i$, $b_i p_i(t) x_i(t)$ is allocated to its competitors.

The total change in the consumer demand rate of firm $i$ is

$$
\dot{x}_i(t) = \dot{x}_{i,c}(t) + \dot{x}_{i,s}(t) + \dot{x}_{i,p}(t).
$$

Summing Equations (1), (2), and (3), the total effect of security investment rates, information sharing rates, and pricing rates is given by

$$
\dot{x}_i(t) = a_i z_i(t) \sqrt{x_{3 \ldots}(t)} - a_{3 \ldots} z_{3 \ldots}(t) \sqrt{x_i(t)} + c_1 s_1(t) + c_2 s_2(t) - b_i p_i(t) x_i(t) + b_3 \ldots p_3 \ldots (t) x_{3 \ldots}(t).
$$

We are now in a position to discuss the effect of targeted hacker attacks on consumer demand. Targeted attacks imply that hackers launch more frequent cyber-attacks on firms with higher profits. Breaching the information system of a firm with higher profits can bring greater gains for hackers. In an environment of rigorous laws against information security incidents, hackers can convert information assets stolen from firms for low gains on the black market. On the contrary, hackers can benefit more when the related laws are loose. In either case, hackers can earn higher profits when a firm’s value of its information assets (measured by its profits) is higher. Note that Hausken (2007) assumes that the value attached to information assets remains unchanged between firms and hackers. The positive relation of the value of information assets between firms and hackers can also be found in Png and Wang (2009) and Dey et al. (2012). Assuming that the marginal product costs of both firms are zero, the instantaneous profit of firm $i$ in the current model is $p_i(t) x_i(t)$. The effect of targeted attacks by hackers on the consumer demand rate of firm $i$ is thus $\dot{x}_i(t) = l_i d p_i(t) x_i(t)$, where $d$ is the density of the hackers’ targeted attacks and $l_i$ is a coefficient of consumer demand loss caused by security breaches. Parameter $d$ reflects hackers’ efforts for the unit profit of firm $i$ and, therefore, hackers who are more profit-motivated have a higher $d$. Also, parameter $d$ can indicate the rigorousness degree of security laws, and a higher $d$ implies loose security laws. Parameter $l_i$ characterizes the loss in the consumer demand rate to measure the negative effect of targeted attacks. When there are more (less) security-sensitive consumers for firm $i$, the value of $l_i$ will be higher (lower).

Firm $i$’s integral profit is thus

$$
\Pi_i = \int_0^\infty e^{-rt} \left[ p_i(t) \left( x_i(t) - l_i d p_i(t) x_i(t) \right) - 0.5 \alpha z_i^2(t) - 0.5 \beta s_i^2(t) \right] dt,
$$

where $r$ is the discount rate of both firms, $\alpha$ is the cost coefficient of security investment rates, and $\beta$ is the cost coefficient of information sharing rates. Parameter $\beta$ refers to the leakage cost of the security information that is incurred due to the information sharing rates. There exists a leakage cost for information sharing that involves disclosing security breaches information, including the moral hazard of participating firms, loss of consumer loyalty and satisfaction (Gal-Or and Ghose, 2005; Lee and Lee, 2012; Liu et al., 2014), a membership fee, and a possible reduction in welfare (Kannan and Telang, 2005). The cost structures of security investment rates and information sharing rates in Equation (5) ensure that they exhibit diminishing marginal returns. Such types of cost structures have been commonly used in other economic activities, such as advertising investment (He et al., 2009; He et al., 2012) and R&D investment (Cellini and Lambertini, 2009; Lambertini and Mantovani, 2009, 2010). The decision variables for each firm are therefore the pricing rate, the security investment rate, and the information sharing rate, so the discounted profit-maximization problem can be described by the following differential game:

$$
V_1(x_1, x_2) = \max_{p_1(t), z_1(t), s_1(t)} \int_0^\infty e^{-rt} \left[ p_1(t) \left( x_1(t) - l_1 d p_1(t) x_1(t) \right) - 0.5 \alpha z_1^2(t) - 0.5 \beta s_1^2(t) \right] dt,
$$

$$
V_2(x_1, x_2) = \max_{p_2(t), z_2(t), s_2(t)} \int_0^\infty e^{-rt} \left[ p_2(t) \left( x_2(t) - l_2 d p_2(t) x_2(t) \right) - 0.5 \alpha z_2^2(t) - 0.5 \beta s_2^2(t) \right] dt,
$$

subject to

$$
\dot{x}_1(t) = a_1 z_1(t) \sqrt{x_1(t)} - a_2 z_1 \sqrt{x_1(t)} + c_1 s_1(t) + c_2 s_2(t) - b_1 p_1(t) x_1(t) + b_3 \ldots p_3 \ldots (t) x_{3 \ldots}(t),
$$

$$
\dot{x}_2(t) = a_1 z_2(t) \sqrt{x_2(t)} - a_2 z_2 \sqrt{x_2(t)} + c_1 s_1(t) + c_2 s_2(t) - b_2 p_2(t) x_2(t) + b_3 \ldots p_3 \ldots (t) x_{3 \ldots}(t),
$$

$$
x_1(0) = x_{10}, x_2(0) = x_{20}.
$$
in which \( V_i(x_1, x_2) \) is the value function of firm \( i \). From Equations (6) and (7), one can discover that the rates of security investment and information sharing of each firm exert a positive effect on its consumer demand rate, whereas targeted attacks against this firm have a negative effect on the consumer demand rate.

4. Equilibrium analysis

In this section, we first attempt to derive the analytical solution of the differential game in which both firms choose their rates for pricing, security investment, and information sharing in a non-cooperative manner. Then, the comparative statistics of these decision variables are discussed as a function of some key parameters including \( a_i, l_i, b_i, \) and \( d \).

4.1 Equilibrium solution

We now attempt to find the feedback equilibrium solution of the differential game given by Equations (6) and (7). The feedback equilibrium solution, which is also the Markov perfect equilibrium or closed-loop equilibrium, appears to be more meaningful than the open-loop equilibrium in that the former takes into account strategic interaction between firms through the evolution of consumer demand rates over time and the associated adjustment in controls. Appendix A provides the feedback equilibrium solution in Proposition 1.

Proposition 1.

(a) The feedback equilibrium solution for firm \( i \) is

\[
p_i^*(t) = \frac{1}{2l_i d} \left[ 1 - b_i (\beta_i - \gamma_i) \right],
\]

\[
z_i^*(t) = \frac{a_i}{\alpha} (\beta_i - \gamma_i) \sqrt{x_{3-i}(t)} \quad \text{and} \quad s_i^*(t) = \frac{c_i}{\beta} (\beta_i + \gamma_i),
\]

provided that \( 2a_i^2/\alpha - b_i^2/(l_i d) > 0 \), and parameters \( \beta_i \) and \( \gamma_i \) satisfy the following equations:

\[
r\beta_i = \frac{1}{4d_i l_i} \left[ 1 - b_i (\beta_i - \gamma_i) \right]^2
\]

\[
- \frac{a_i^2}{\alpha} (\beta_i - \gamma_i) (\beta_{3-i} - \gamma_{3-i})
\]

\[
r\gamma_i = \frac{a_i^2}{2\alpha} (\beta_i - \gamma_i)^2 + \frac{b_i}{2l_i d_i} (\beta_i - \gamma_i) \left[ 1 - b_{3-i} (\beta_{3-i} - \gamma_{3-i}) \right].
\]

(b) The integral profit for firm \( i \) is

\[
\Pi_i = \frac{1}{4d_i l_i} \left[ 1 - b_i (\beta_i - \gamma_i)^2 \right] \left( \frac{F_i}{O_1 + O_2 + r} + \frac{G_i}{r^2} + \frac{H_i}{r} \right)
\]

\[
- \frac{a_i^2}{2\alpha} (\beta_i - \gamma_i)^2 \left( \frac{F_{3-i}}{O_1 + O_2 + r} + \frac{G_{3-i}}{r^2} + \frac{H_{3-i}}{r} \right)
\]

\[
- \frac{c_i^2}{2\beta r} (\beta_i + \gamma_i)^2
\]

with \( O_i, F_i, G_i, \) and \( H_i \) being given in Appendix A.

Note that the restriction condition \( 2a_i^2/\alpha - b_i^2/(l_i d) > 0 \) guarantees a positive feedback equilibrium solution. When this condition fails to be satisfied, the feedback equilibrium solution may still be positive, implying that the feedback equilibrium solution may be available for a wider range of parameter setting. It follows from Proposition 1(a) that each firm’s security investment rate is increasing with its competitor’s consumer demand rate, while each firm’s information sharing rate and pricing rate are stationary. Unlike the value function in an instantaneous setting, the integral equilibrium profit given by Proposition 1(b) is derived in an infinite-horizon setting and is of more importance for firms that focus on their long-term profits.

The feedback equilibrium solution for symmetric firms is obtained explicitly in Corollary 1, in which \( a_i = a, b_i = b, c_i = c, \)

\( l_i = l, x_{10} = x_{20} = x_0 \).

Corollary 1. The feedback equilibrium solution for each firm in the symmetric situation is

\[
p_C^* = \frac{1}{2ld} (1 - \Theta), \quad s_C^* = \frac{c}{\beta} \left[ \frac{1}{4rld} - \left( \frac{b^2}{4rld} + \frac{a^2}{2r^2} \right) \Theta^2 \right],
\]

\[
z_C^*(t) = \frac{\Theta a}{\alpha} \sqrt{2cs_C^* t + x_0}
\]

and the integral profit is

\[
\Pi_C = \left( p_C^* (1 - ld p_C^*) - 0.5 \Theta^2 a^2/\alpha \right) \left( 2cs_C^*/r + x_0/r \right) - 0.5b (s_C^*)^2/r,
\]

where

\[
\Theta = \frac{b \sqrt{4a^2(b + ldr)^2 + 3a (2a^2ld - ab^2) - 2ab(b + ldr)}}{3(2a^2ld - ab^2)}.
\]

Letting \( a = 1, b = 1, c = 1, l = 1, x_0 = 0, r = 0.05, \alpha = 1, \beta = 1 \), we can obtain the feedback equilibrium solution and the integral profit with \( t = 50 \) over the density of targeted attacks \( d \) shown in Fig. 1. From Fig. 1(a), one can observe that the rates of security investment, information sharing, and pricing decrease with the density of targeted attacks. When the density of targeted attacks increases, hackers become more profit-motivated and launch more frequent targeted attacks, even though the profit rates of firms may not be higher. Considering the costs of the security investment rate and the information sharing rate, a rational firm that is confronted with more frequent targeted attacks would have to decrease both of them. Meanwhile, to decrease the consumer demand loss caused by targeted attacks, a firm needs to decrease its pricing rate. It is consistent with common sense that the higher density of targeted attacks seems to always harm a firm’s integral profit, as shown in Fig. 1(b).

Given the optimal decisions for security investment rates, information sharing rates, and pricing rates, one can obtain the long-run equilibrium market share rates of the two firms, which is given in Proposition 2.
Proposition 2. When both firms non-cooperatively choose their rates of security investment and information sharing, their long-run market share rates are

\[
\hat{x}_1 = \frac{(a_1^2/\alpha) (\beta_1 - \gamma_1) + [b_2/(2l_2d)] [1 - b_1 (\beta_2 - \gamma_2)]}{(a_1^2/\alpha) (\beta_1 - \gamma_1) + (a_2^2/\alpha) (\beta_2 - \gamma_2) + [b_1/(2l_1d)] [1 - b_1 (\beta_1 - \gamma_1)] + [b_2/(2l_2d)] [1 - b_2 (\beta_2 - \gamma_2)]}
\]

\[
\hat{x}_2 = \frac{(a_2^2/\alpha) (\beta_2 - \gamma_2) + [b_1/(2l_1d)] [1 - b_1 (\beta_1 - \gamma_1)]}{(a_1^2/\alpha) (\beta_1 - \gamma_1) + (a_2^2/\alpha) (\beta_2 - \gamma_2) + [b_1/(2l_1d)] [1 - b_1 (\beta_1 - \gamma_1)] + [b_2/(2l_2d)] [1 - b_2 (\beta_2 - \gamma_2)]}
\]

Figure 1. The effect of \(d\): (a) decision variables as a function of \(d\) and (b) integral profit as a function of \(d\).

One can observe that the long-run market share rates are unaffected by the cost coefficient and efficiency of information sharing rates. A possible reason for this behavior is that information sharing rates increase the consumer demand rate of the total industry, not the relative proportion of consumer demand rates of the two firms. The effects of other key model parameters on the long-run market share rates are difficult to analytically examine and are thus discussed numerically in the next section.

4.2 Comparative statics

Although we are able to obtain the analytical form of the feedback equilibrium solution, we unfortunately fail to analytically derive all results of comparative statics for such a solution. Hence, numerical methods must be used. Due to symmetry properties, this section only discusses the effects of \(a_1, l_1, b_1, l_2, b_2\), and \(d\) on the feedback equilibrium solutions and the resulting profits for both firms. Throughout this article, we assume that \(r = 0.05\), \(\alpha = \beta = 1\), \(c_1 = c_2 = 1\), and \(x_{10} = x_{30} = 0\).

Letting \(a_2 = 1\), \(b_1 = b_2 = 0.1\), \(l_1 = l_2 = 1\), \(d = 0.1\), one can obtain the change in feedback equilibrium solutions and the resulting integral profits for both firms over the efficiency of the security investment rate of firm 1, \(a_1\), as shown in Table 1. When \(a_1\) increases, firm 1 can protect its information system more effectively by using a higher security investment rate, whereas firm 2 finds it difficult to capture firm 1’s consumers and rationally lowers its security investment rate; see Fig. 2. In this situation, firm 1 becomes more aggressive in that it would be more willing to share its security information. In contrast, firm 2 takes the free-ride strategy and shares less security information. The free-ride effect seems so strong that firm 2 will increase its pricing rate without any major concern about consumer loss due to hacker attacks. One can observe that \(a_1\) does not always increase firm 1’s pricing rate. Intuitively, when \(a_1\) is increased from an existing low value, firm 1’s rates of security investment and information sharing are lower, although both are increasing. In this case, firm 1 would not increase its pricing rate out of consideration for consumer loss. When \(a_1\) is increased from an existing high value, firm 1 takes enough security measures and increases the pricing rate without worrying about security breaches. One can find that, consistent with common sense, the integral profit of firm 1 increases with \(a_1\), whereas that of firm 2 decreases.

Assuming that \(a_1 = a_2 = 1\), \(l_1 = l_2 = 1\), \(b_2 = 0.1\), \(d = 0.1\), one can find the change in feedback equilibrium solutions and

| \(a_1\) | 0.25 | 0.5 | 0.75 | 1 | 1.25 | 1.5 |
|-------|------|-----|------|---|------|-----|
| \(\beta_1\) | 10.5572 | 12.7107 | 16.0952 | 20.1858 | 24.2935 | 27.9450 |
| \(\gamma_1\) | 9.5235 | 11.6744 | 15.0650 | 19.1794 | 23.3296 | 27.0355 |
| \(\beta_2\) | 34.8930 | 30.7612 | 25.3977 | 20.1858 | 15.9607 | 12.8258 |
| \(\gamma_2\) | 33.4056 | 29.4362 | 24.2264 | 19.1794 | 15.1032 | 12.9005 |
| \(\beta_1^*(t)\) | 4.4832 | 4.4819 | 4.4849 | 4.4968 | 4.5180 | 4.5452 |
| \(\beta_2^*(t)\) | 4.2832 | 4.3375 | 4.4144 | 4.4968 | 4.5713 | 4.6324 |
| \(\gamma_1^*(t)\) | 0.2584 | 0.5181 | 0.7726 | 1.0064 | 1.2049 | 1.3643 |
| \(\gamma_2^*(t)\) | 1.4336 | 1.3250 | 1.1713 | 1.0064 | 0.8575 | 0.7533 |
| \(\Pi_1^*(t)\) | 20.0807 | 24.3851 | 31.1062 | 39.3452 | 47.6231 | 54.9805 |
| \(\Pi_2^*(t)\) | 68.2448 | 60.1974 | 49.6241 | 39.3652 | 31.0639 | 24.9163 |
| \(\hat{x}_1\) | 0.2076 | 0.2809 | 0.3866 | 0.5000 | 0.5999 | 0.6784 |
| \(\hat{x}_2\) | 0.7924 | 0.7191 | 0.6184 | 0.5000 | 0.4001 | 0.3216 |
| \(\Pi_1\) | 31.440 | 35.307 | 40.636 | 46.489 | 52.269 | 57.626 |
| \(\Pi_2\) | 73.982 | 65.595 | 55.551 | 46.489 | 39.237 | 33.605 |
the resulting integral profits for both firms over the sensitivity parameter of the pricing rate of firm 1, \( b_1 \), as shown in Table 2. One can discover from Table 2 that as \( b_1 \) increases, the pricing rate of firm 1 decreases, whereas the pricing rate of firm 2 increases. With a higher \( b_1 \), there is a greater negative effect on the consumer demand rate of firm 1 and a greater positive effect on that of firm 2. Firm 1 restricts its pricing rate to maintain its consumer demand rate, whereas firm 2 improves its pricing rate to obtain a higher profit. Firm 1 reduces the negative effect of a higher \( b_1 \) on its change in the consumer demand rate through negative feedback in Equation (3) by decreasing its rates of security investment and information sharing, because both can increase firm 1’s consumer demand rate; see Fig. 3. Firm 2 does not need to invest more in information security to attract consumers, due to the positive effect of \( b_1 \) on its consumer demand rate. However, it can be observed that as \( b_1 \) increases, firm 2 shares more security information, implying that firm 2 focuses on enlarging the consumer demand rate for the entire industry. A higher \( b_1 \) has a positive effect on firm 2 and therefore always improves firm 2’s integral profit. It is interesting that \( b_1 \) does not always harm firm 1’s integral profit, despite its negative effect. A possible explanation is that when \( b_1 \) increases from an initial low value, firm 1’s expenditure rates for security investment and information sharing decrease, and such cost reductions prevail over the loss in the consumer demand rate.

![Figure 2](image1.png)

**Figure 2.** Security investment rates with \( a_t \) for (a) firm 1 and (b) firm 2.

Assume that \( a_1 = a_2 = 1, b_1 = b_2 = 0.1, l_1 = 1, d = 0.1 \). Table 3 gives the change in feedback equilibrium solutions and resulting integral profits for both firms over the consumer demand loss coefficient of firm 1, \( l_1 \). One can find that as \( l_1 \) increases, firm 1 decreases its pricing rate to alleviate the negative effect of hacker attacks. Noting that the positive effect of firm 1’s pricing rate on firm 2’s consumer demand rate decreases, firm 2 needs to decrease its pricing rate to maintain its consumer demand rate. At first glance, it seems economically plausible that as \( l_1 \) increases, firm 1 would increase both its security investment rate and its information sharing rate to improve its consumer demand rate. However, one can observe from Fig. 4 that firm 1’s rates of security investment and information sharing decrease over \( l_1 \). In reality, each firm’s consumer demand rate serves as a double-edged sword, which can contribute to its profit and meanwhile can strengthen the negative effect of targeted attacks. The negative effect prevails in this situation, and firm 1 does not need to invest more and share more to reduce such an effect. Firm 2 invests more in this situation to increase its consumer demand rate, as \( l_1 \) has no negative effect on it. It follows that firm 2’s information sharing rate first decreases and then increases.

**Table 2.** The effect of \( b_1 \)

| \( b_1 \) | 0.025 | 0.05 | 0.075 | 0.1 | 0.125 | 0.15 |
|---|---|---|---|---|---|---|
| \( \beta_1 \) | 23.1825 | 22.1088 | 21.116 | 20.1858 | 19.3260 | 18.5269 |
| \( \gamma_1 \) | 22.0768 | 21.0380 | 20.0799 | 19.1794 | 18.3492 | 17.5781 |
| \( \beta_2 \) | 15.6072 | 17.2887 | 18.8077 | 20.1658 | 21.4415 | 22.5899 |
| \( \gamma_2 \) | 14.5778 | 16.2296 | 17.7761 | 19.1794 | 20.4582 | 21.6280 |
| \( p_{11}(t) \) | 4.8770 | 4.7691 | 4.6736 | 4.5885 | 4.5121 | 4.4431 |
| \( p_{12}(t) \) | 4.5282 | 4.5514 | 4.5731 | 4.5885 | 4.6037 | 4.6171 |
| \( x_{21}(t)/\sqrt{x_{22}(t)} \) | 0.9840 | 0.9237 | 0.8704 | 0.8230 | 0.7806 | 0.7425 |
| \( x_{21}(t)/\sqrt{x_{22}(t)} \) | 0.9437 | 0.8972 | 0.8575 | 0.8230 | 0.7927 | 0.7658 |
| \( x_{21}(t) \) | 52.7264 | 48.3055 | 44.8676 | 41.8718 | 39.2436 | 36.9227 |
| \( x_{22}(t) \) | 27.7281 | 33.2840 | 37.9295 | 41.8718 | 45.2601 | 48.2046 |
| \( x_{11} \) | 0.5742 | 0.5484 | 0.5236 | 0.5000 | 0.4777 | 0.4567 |
| \( x_{12} \) | 0.4258 | 0.4516 | 0.4764 | 0.5000 | 0.5223 | 0.5433 |
| \( \Pi_1 \) | 51.016 | 53.199 | 54.158 | 54.300 | 53.891 | 53.119 |
| \( \Pi_2 \) | 43.750 | 47.799 | 51.264 | 54.300 | 57.003 | 59.438 |

**Table 3.** The effect of \( l_1 \)

| \( l_1 \) | 0.25 | 0.5 | 0.75 | 1 | 1.25 | 1.5 |
|---|---|---|---|---|---|---|
| \( \beta_1 \) | 87.2908 | 44.9135 | 28.571 | 20.1858 | 15.2385 | 12.0508 |
| \( \gamma_1 \) | 84.8141 | 43.2462 | 27.3214 | 19.1794 | 14.4035 | 11.2304 |
| \( \beta_2 \) | 18.9983 | 18.3968 | 19.1402 | 20.1858 | 21.2491 | 22.2374 |
| \( \gamma_2 \) | 18.4752 | 17.6615 | 18.2571 | 19.1794 | 20.1497 | 21.0631 |
| \( p_{11}(t) \) | 4.0385 | 4.6324 | 4.5557 | 4.4968 | 4.4503 | 4.4128 |
| \( p_{12}(t) \) | 5.0466 | 8.3327 | 5.8275 | 4.9498 | 3.6660 | 3.0962 |
| \( x_{21}(t)/\sqrt{x_{22}(t)} \) | 2.4767 | 1.6673 | 1.2587 | 1.0064 | 0.8350 | 0.7114 |
| \( x_{21}(t)/\sqrt{x_{22}(t)} \) | 0.5231 | 0.7533 | 0.8885 | 1.0064 | 1.0994 | 1.1743 |
| \( x_{21}(t) \) | 172.1049 | 88.5957 | 55.8335 | 39.3652 | 29.6420 | 23.9092 |
| \( x_{22}(t) \) | 37.4735 | 36.0583 | 37.3919 | 39.3652 | 41.9988 | 43.3005 |
| \( x_{11} \) | 0.5927 | 0.5760 | 0.5381 | 0.5000 | 0.4661 | 0.4372 |
| \( x_{12} \) | 0.4073 | 0.4240 | 0.4619 | 0.5000 | 0.5339 | 0.5628 |
| \( \Pi_1 \) | 42.5170 | 41.3000 | 73.0200 | 46.4900 | 33.3300 | 25.7300 |
| \( \Pi_2 \) | 143.0300 | 76.5800 | 55.7700 | 46.4900 | 41.6800 | 39.0100 |
with $l_1$. It is straightforward to understand that as $l_1$ increases from a high value, firm 2 is ready to share security information to increase its consumer demand rate. When $l_1$ increases from an initial low value, firm 1’s information sharing rate remains high even though it is decreasing. Firm 2 decreases its information sharing rate out of consideration for free riding. Furthermore, one can observe that consistent with common sense, the integral profit of firm 1 decreases with $l_1$. Interestingly, the integral profit of firm 2, however, also decreases with $l_1$, although its long-run market share rate increases. The reason for this behavior may be that an increase in $l_1$ results in a drastic decrease in firm 2’s pricing rate.

Letting $a_1 = 1.1, a_2 = 1, l_1 = 0.9, l_2 = 1, b_1 = b_2 = 0.1$, we can obtain the change in feedback equilibrium solutions and resulting integral profits for both firms over the density of hacker attacks, $d$, shown in Table 4. Here, we simply define the superior firm as the one with more favorable model parameters; i.e., a higher efficiency in the security investment rate and a lower consumer demand loss coefficient than those of the inferior firm. That is, firm 1 is superior, and firm 2 is inferior. One can see that as $d$ increases, both firms decrease pricing rates to increase their respective consumer demand rates. Figure 5 shows that the security investment rates of both firms decrease with $d$, meaning that the firms seem reluctant to defend against hackers. Actually,
to deter the hacker, a firm requires an enormous security budget to employ better access control policies, complex cryptographic protocols, advanced firewalls and IDSs, better system evaluation tools, and the perfect code design. In contrast, hackers only need to exploit one drawback in order to successfully intrude into a firm’s information system (Anderson and Moore, 2006). One can observe that as $\Delta$ increases, both firms will share less security information. The reason for this behavior may rest with the fact that after decreasing information sharing rates, both firms would decrease the negative effect of hacker attacks by decreasing their consumer demand rates. It can be observed that the integral profits of both firms decrease with $\Delta$, even though the consumer demand rate of the superior firm, firm 1, increases.

In this subsection, we examine the effects of key model parameters using numerical methods, due to the extreme difficulty in analytical tractability. Nevertheless, we are able to obtain some analytical results in Appendix A, which, together with the numerical results above, are summarized in Table 5.

5. The cooperative scenarios

As discussed above, many information sharing organizations have been established that can intervene in firms’ decisions on information security so that their rates of security investment or/and information sharing may be specified in a centralized fashion. Moreover, there has been rapid growth in serious security threats from hackers. Underground hacker industry chains have emerged that involve purchasing attack tools from hacking experts, selling information assets stolen from firms, disseminating attacking knowledge among the hacker population, and training fresh hackers. To curb such serious threats, firms sometimes need to cooperate in a series of security measures to prevent hacker attacks and satisfy their own security requirements. This section studies how feedback equilibrium strategies and resulting integral profits for both firms change when security investment rates, information sharing rates, or both are regulated cooperatively. Naturally, the purpose of both firms is to maximize the sum of their integral profits when they behave cooperatively.

5.1. Equilibrium solution when firms cooperate in security investment

It is not difficult to observe in Appendix B that one of the two firms has a zero rate of security investment in this partially cooperative situation. Without loss of generality, we assume that firm 2 has a zero security investment rate in this subsection.

Proposition 3. When the firms choose security investment rates cooperatively but information sharing rates non-cooperatively:

(a) the feedback equilibrium solution for each firm is

$$p_1^*(t) = \frac{1}{2l_1d} \left[1 - b_1(\beta_{z1} - \gamma_{z1})\right], s_2^*(t) = \frac{c_1}{\beta} (\beta_{z1} + \gamma_{z1}),$$

$$z_{21}^*(t) = \frac{a_1}{\alpha} (\kappa_1 - \kappa_2) \sqrt{x_2^2(t)}, z_{22}^*(t) = 0,$$  \hspace{1cm} (12)

provided that they are positive, and the parameters $\beta_{z1}, \gamma_{z1},$ and $\kappa_i$ satisfy the equations:

$$r_1\beta_{z1} = \frac{1}{4l_1d} \left[1 - b_1 (\beta_{z1} - \gamma_{z1})\right]^2$$

$$r_2\gamma_{z1} = -\frac{a_1^2}{2\alpha} (\kappa_1 - \kappa_2)^2 + \frac{a_1^2}{\alpha} (\beta_{z1} - \gamma_{z1}) (\kappa_1 - \kappa_2)$$

$$+ \frac{b_2}{2l_2d} (\beta_{z1} - \gamma_{z1}) \left[1 - b_2 (\beta_{z2} - \gamma_{z2})\right],$$

$$r_2\beta_{z2} = -\frac{b_1}{2l_1d} (\beta_{z2} - \gamma_{z2}) \left[1 - b_1 (\beta_{z1} - \gamma_{z1})\right]$$

Table 5. A brief summary of the obtained analytical and numerical results

| $a_1$ | $b_1$ | $l_1$ | $d$ | $p_1^*(t)$ | $p_2^*(t)$ | $z_1^*(t)$ | $z_2^*(t)$ | $s_1^*(t)$ | $s_2^*(t)$ | $\dot{x}_1$ | $\dot{x}_2$ | $\Pi_1$ | $\Pi_2$ |
|------|------|-------|-----|------------|------------|------------|------------|-------------|-------------|------------|------------|--------|--------|
| ↑    | ↓    | ↑     | ↓   | ↑          | ↑          | ↓          | ↓          | ↑           | ↑           | ↑          | ↑         | ↓      | ↑      |

↑ denotes increase; ↓ denotes decrease; □ denotes first increase and then decrease; ∪ denotes first decrease and then increase.
\[ r \gamma_2 = \frac{a_1^2}{\alpha} (\beta_2 - \gamma_2) (\kappa_1 - \kappa_2) + \frac{1}{4l_1d} [1 - b_2 (\beta_2 - \gamma_2)] [1 + 3b_2 (\beta_2 - \gamma_2)] \]

\[ r \kappa_1 = \frac{1}{4l_1d} [1 - b_1 (\beta_1 - \gamma_1)] \times [1 + b_1 (\beta_1 - \gamma_1) - 2(\kappa_1 - \kappa_2)] \]

\[ r \kappa_2 = \frac{a_1^2}{2\alpha} (\kappa_1 - \kappa_2)^2 + \frac{1}{4l_1d} [1 - b_2 (\beta_2 - \gamma_2)] \times [1 + b_2 (\beta_2 - \gamma_2) + 2(\kappa_1 - \kappa_2)]. \]  

(b) The integral profits for both firms are

\[ \Pi_{i1} = \frac{1}{4l_1d} \left[ 1 - b_i^2 (\beta_1 - \gamma_1)^2 \right] \times \left( \frac{F_i}{O_{i1} + O_{i2} + r} + \frac{G_i}{r^2} + \frac{H_{i1}}{r} \right) - \frac{a_i^2}{2\alpha} (\beta_1 - \gamma_1)^2 \]

\[ \Pi_{i2} = \frac{1}{4l_1d} \left[ 1 - b_i^2 (\beta_2 - \gamma_2)^2 \right] \times \left( \frac{F_i}{O_{i1} + O_{i2} + r} + \frac{G_i}{r^2} + \frac{H_{i2}}{r} \right) - \frac{c_i^2}{2\beta r} (\beta_2 + \gamma_2)^2 \]

with \( O_{i1}, F_i, G_i, \) and \( H_{i1} \) being given in Appendix B.

Note that the feedback equilibrium strategies and resulting integral profits for both firms are independent of \( a_2 \). Although it is quite difficult to derive the necessary condition to ensure the positive feedback equilibrium solution in Proposition 3 (as well as the following Propositions 4 and 5), we find that the equilibrium solution is always positive for a wide range of parameters. Considering that our aim here is to compare the equilibrium solution in such a situation with that in the completely independent situation above, in this section and the following sections, we borrow the parameter values listed in Table 4 to examine the effect of the density of hacker attacks, \( d \), with firm 1 being the superior firm and firm 2 the inferior one. The feedback equilibrium solutions and resulting integral profits are given in Table 6 and Fig. 6.

5.2. Equilibrium solution when firms cooperate in information sharing

When firms choose security investment rates non-cooperatively but information sharing rates cooperatively, the following results can be obtained.

Proposition 4. When the firms choose security investment rates non-cooperatively but information sharing rates cooperatively:

(a) the feedback equilibrium solution for each firm is

\[ \rho_{i1}(t) = \frac{1}{2l_1d} [1 - b_i (\beta_i - \gamma_i)], \]

\[ \gamma_i(t) = \frac{a_i}{\alpha} (\beta_i - \gamma_i) \sqrt{x_{i3-i}}, \quad s_i^*(t) = \frac{c_i}{\beta} (\rho_i + \rho_{i2}) \]  

(b) Table 6. The effect of \( d \) with cooperative security investment rates

| \( d \) | 0.025 | 0.05 | 0.075 | 0.1 | 0.125 | 0.15 |
| --- | --- | --- | --- | --- | --- | --- |
| \( \beta_{i1} \) | 129.4493 | 67.0045 | 45.9979 | 35.3765 | 28.9254 | 24.5702 |
| \( \beta_{i2} \) | 127.0816 | 64.7700 | 43.8780 | 33.5363 | 26.9927 | 22.7511 |
| \( \gamma_{i1} \) | 72.8416 | 34.8527 | 22.3023 | 16.0997 | 12.4279 | 10.0157 |
| \( \gamma_{i2} \) | 74.9889 | 36.8724 | 24.2127 | 17.9555 | 14.1610 | 11.6757 |
| \( \kappa_1 \) | 202.2908 | 101.8572 | 68.3002 | 51.7662 | 41.5333 | 34.5859 |
| \( \kappa_2 \) | 202.0705 | 101.6424 | 68.0907 | 51.2718 | 41.5378 | 34.9908 |
| \( \rho_{i1}(t) \) | 16.9607 | 8.6283 | 5.8731 | 4.4332 | 3.5855 | 3.0166 |
| \( \rho_{i2}(t) \) | 24.2946 | 12.0197 | 7.9403 | 5.0979 | 4.6932 | 3.8867 |
| \( \gamma_{i1}(t) / \sqrt{x_{i3-i}(t)} \) | 0.2423 | 0.2363 | 0.2305 | 0.2248 | 0.2196 | 0.2146 |
| \( \gamma_{i2}(t) / \sqrt{x_{i3-i}(t)} \) | 0 | 0 | 0 | 0 | 0 | 0 |
| \( \Pi_{i1} \) | 256.5309 | 131.7745 | 89.8759 | 68.7328 | 55.9181 | 47.2833 |
| \( \Pi_{i2} \) | 147.8305 | 71.7251 | 46.3550 | 34.0152 | 26.5898 | 21.6914 |
| \( \Pi_{i3-i} \) | 1416.500 | 362.700 | 164.400 | 94.000 | 61.000 | 42.900 |
| \( \Pi_{i3-i} \) | 97.7010 | 240.470 | 105.240 | 58.530 | 36.600 | 25.220 |

provided that they are positive, and the parameters \( \beta_{i3-i}, \gamma_{i3-i} \), and \( \rho_i \) satisfy the following equations:

\[ r \beta_{ii} = \frac{1}{4l_1d} [1 - b_i (\beta_i - \gamma_i)]^2 \]

\[ - \frac{a_i^2}{\alpha} (\beta_{i3-i} - \gamma_{i3-i}) \]

\[ r \gamma_{ii} = \frac{a_i^2}{2\alpha} (\beta_{i3-i} - \gamma_{i3-i}) + \frac{b_{3-i}}{2l_3d} (\beta_{i3-i} - \gamma_{i3-i}) \times [1 - b_{3-i} (\beta_{i3-i} - \gamma_{i3-i})] \]

\[ r \rho_i = \frac{1}{4l_1d} [1 - b_i (\beta_i - \gamma_i)] \times [1 + b_i (\beta_i - \gamma_i) - 2(\rho_i - \rho_{3-i})] \]

\[ - \frac{a_i^2}{2\alpha} (\beta_{i3-i} - \gamma_{i3-i})^2 \]

\[ - \frac{c_{3-i}}{\alpha} (\rho_i - \rho_{3-i}) (\beta_{i3-i} - \gamma_{i3-i}). \]

Figure 6. Firm T’s security investment rate with cooperative security investment rates.
Proposition 5. We are now in a position to discuss the fully cooperative condition in Proposition 1. The feedback equilibrium solutions are provided that they are positive, and the parameters $\beta_i, \gamma_i$, and $\sigma$ satisfy the following: 

\[
p_{b1}(t) = \frac{1}{2l_d} \left[ 1 - b_1(\beta_{b1} - \gamma_{b1}) \right],
\]

\[
z_{b1}(t) = \frac{a_1}{\alpha} (\sigma_1 - \sigma_2) \sqrt{x_2(t)},
\]

\[
z_{b2}(t) = 0, s_{b1}(t) = \frac{c_i}{\beta} (\sigma_1 + \sigma_2)
\]

\[
(r_{b1}) = \frac{1}{4l_d} \left[ 1 - b_1(\beta_{b1} - \gamma_{b1}) \right]^2
\]

\[
r_{b2} = -\frac{a_1^2}{2\alpha} (\sigma_1 - \sigma_2)^2 + \frac{a_2^2}{\alpha} (\beta_{b1} - \gamma_{b1}) (\sigma_1 - \sigma_2)
\]

\[
+ \frac{b_2}{2l_d} (\beta_{b1} - \gamma_{b1}) \left[ 1 - b_2(\beta_{b2} - \gamma_{b2}) \right]
\]

\[
r_{\gamma_{b1}} = \frac{1}{4l_d} \left[ 1 - b_2(\beta_{b2} - \gamma_{b2}) \right] \left[ 1 + 3b_2(\beta_{b2} - \gamma_{b2}) \right]
\]

\[
r_{\gamma_{b2}} = \frac{1}{4l_d} \left[ 1 - b_1(\beta_{b1} - \gamma_{b1}) \right]
\]

\[
r_{\sigma_1} = \frac{1}{4l_d} \left[ 1 - b_1(\beta_{b1} - \gamma_{b1}) \right] \times \left[ 1 + b_1(\beta_{b1} - \gamma_{b1}) - 2(\sigma_1 - \sigma_2) \right]
\]

\[
r_{\sigma_2} = \frac{a_1^2}{2\alpha} (\sigma_1 - \sigma_2)^2 + \frac{1}{4l_d} \left[ 1 - b_2(\beta_{b2} - \gamma_{b2}) \right] \times \left[ 1 + b_2(\beta_{b2} - \gamma_{b2}) + 2(\sigma_1 - \sigma_2) \right]
\]

with $O_i$, $F_i$, $G_i$, and $H_i$ being given in Appendix C.

Comparing Equation (9) and Equation (16) yields that positive pricing rates and positive security investment rates in such a partially cooperative situation can be guaranteed under the condition in Proposition 1. The feedback equilibrium solutions and resulting integral profits in this partially cooperative case are given in Table 7 and Fig. 7.

### 5.3 Equilibrium solution when firms cooperate in both security investment and information sharing

We are now in a position to discuss the fully cooperative situation, in which rates of both security investment and information sharing are determined centrally. We assume again that firm 2 has a zero security investment rate without loss of any generality.

Proposition 5. When the firms choose rates of both security investment and information sharing cooperatively:

\[
\frac{\partial p_{b1}(t)}{\partial t} = \frac{a_1^2}{2\alpha} (\beta_{b1} - \gamma_{b1})^2 \left( \frac{F_{b1}}{O_{b1} + O_{b2} + r} \right) + \frac{G_{b1}}{r^2} \left( H_{b1} + \frac{H_{b2}}{r} \right)
\]

\[
- \frac{c_i^2}{2\beta r} (\sigma_1 + \sigma_2)^2
\]

\[
\frac{\partial z_{b1}(t)}{\partial t} = \frac{a_1}{\alpha} (\sigma_1 - \sigma_2) \sqrt{x_2(t)}
\]

\[
\frac{\partial z_{b2}(t)}{\partial t} = 0, s_{b1}(t) = \frac{c_i}{\beta} (\sigma_1 + \sigma_2)
\]

\[
\Pi_{b1} = \frac{1}{4l_d} \left[ 1 - b_1(\beta_{b1} - \gamma_{b1}) \right] \left( \frac{F_{b1}}{O_{b1} + O_{b2} + r} \right) \left( \frac{G_{b1}}{r^2} + \frac{H_{b1}}{r} \right)
\]

\[
- \frac{a_1^2}{2\alpha} (\sigma_1 - \sigma_2)^2 \left( \frac{F_{b2}}{O_{b1} + O_{b2} + r} \right) \left( \frac{G_{b2}}{r^2} + \frac{H_{b2}}{r} \right)
\]

\[
- \frac{c_i^2}{2\beta r} (\sigma_1 + \sigma_2)^2
\]
Table 8. The effect of $d$ with cooperative rates of both security investment and information sharing

| $d$ | $P_{b1}$ | $P_{b2}$ | $P_{s1}$ | $P_{s2}$ |
|-----|---------|---------|---------|---------|
| 0.025 | 129.4943 | 67.0045 | 45.9979 | 35.3765 |
| 0.05 | 127.0816 | 64.7700 | 43.8780 | 33.3563 |
| 0.075 | 72.8416 | 34.8527 | 22.3023 | 16.0997 |
| 0.1 | 74.9889 | 36.8724 | 24.2127 | 17.9155 |
| 0.125 | 202.2908 | 101.8572 | 68.3002 | 51.4762 |
| 0.15 | 202.0705 | 101.6424 | 68.0967 | 51.2783 |

\[
\Pi_{b1} = \frac{1}{4b_1d} \left( 1 - b_1^2(b_2 - \gamma_2) \right) \left( \frac{F_{b1}}{O_{bi} + O_{s2} + r} + \frac{G_{s2}}{R} + \frac{H_{b2}}{R} \right) - \frac{c_2^2}{2b_2} (\sigma_1 + \sigma_2)^2 \tag{20}
\]

with $O_{bi}$, $F_{b1}$, $G_{s2}$, and $H_{b2}$ being given in Appendix D.

The feedback equilibrium solutions and resulting profits are shown in Table 8 and Fig. 8.

5.4 Comparison between non-cooperative and cooperative scenarios

One can find that Equation (9) for $\beta_i$ and $\gamma_i$ in Proposition 1 is equivalent to Equation (16) for $\beta_1$ and $\gamma_1$ in Proposition 4, implying that $p_2^i(t) = p_2^s(t)$. Similarly, it is clear that $\beta_{2i}$, $\gamma_{2i}$, and $\kappa_{1}$ in Equation (13) in Proposition 3 are equal to $\beta_{b1}$, $\gamma_{b1}$, and $\sigma_i$ respectively, in Equation (19) in Proposition 5, implying that $p_{2i}^s(t) = p_{bi}^s(t)$.

Proposition 6. $p_{b1}^i(t) = p_{b1}^s(t), p_{s1}^i(t) = p_{s1}^s(t)$.

The results of Proposition 6 are independent of which firm is superior. Proposition 6 implies that when both firms choose security investment rates independently, each firm’s pricing strategy remains unchanged whether they behave non-cooperatively or cooperatively in determining the information sharing rates. In addition, provided that both firms choose the security investment rates cooperatively, each firm’s pricing rate is still independent of whether they choose information sharing rates independently or cooperatively. We next compare rates of security investment and information sharing based on the presented numerical results.

Observation 1:

(a) When security investment rates are chosen cooperatively, the inferior firm always has a zero security investment rate whether both firms’ information sharing rates are determined cooperatively or non-cooperatively.

(b) The security investment rate of the superior firm when information sharing rates are determined cooperatively is always higher than that when information sharing rates are determined non-cooperatively, whether both firms’ security investment rates are determined cooperatively or non-cooperatively.

(c) Information sharing rates of both firms in the fully cooperative situation are the highest, whereas those in the independent situation are the lowest.

The security investment rate of a firm aims to attract its rival’s consumers by improving its relative security level; that is, investing in information security is a competitive strategy. When security investment rates are chosen in a centralized fashion, there would be investment waste if both firms have positive security investment rates. The inferior firm can only create a minor security improvement in the case of a positive security investment rate, which finally decreases its security investment rate to zero, as illustrated by Observation 1(a). Observation 1(b) shows that the security investment rate seems to be more effective when the information sharing rates are chosen cooperatively than when they are chosen independently. Consistent with common sense, Observation 1(c) implies that the free-riding effect of information sharing rates is more remarkable when they are determined non-cooperatively. That is, individual optimization in more likely to bring the effect of free riding on information sharing.

Observation 2:

(a) The superior firm enjoys the highest integral profit in the fully cooperative situation and the lowest integral profit in fully non-cooperative situations.

(b) The inferior firm almost always obtains the highest integral profit with cooperative security investment rates and always gains the lowest integral profit in the fully cooperative case.

Observation 2 shows that the superior firm prefers the organizational structure where both firms cooperate in choosing rates for both security investment and information sharing, whereas in most cases, the inferior firm prefers the situation where both firms cooperate solely in choosing security investment rates. There are two factors that can explain why the superior firm enjoys the highest integral profit in the fully cooperative case. First, the positive effect of security investment for the superior firm is greater because its competitor, the inferior firm, does not invest at all at equilibrium. Second, the free ride obtained by the inferior firm is weaker and can effectively
improve both firms’ consumer demand. The inferior firm benefits least in the fully cooperative situation for opposite reasons, namely, ineffective security investment and insignificant free ride effect. It can be concluded that although the inferior firm tends to cooperate in security investment, the superior firm should offer some economic incentive, such as a subsidy, to the inferior firm so that both of them can cooperate in information sharing as well. Moreover, it is not difficult to observe that social welfare, measured by the sum of the two firms’ integral profits, is highest when both firms cooperate in security investment and information sharing. Hence, it is in the interest of the whole of society to encourage and even to require different firms to cooperate in both security investment and information sharing.

6. Concluding remarks

This article constructs a differential game framework in which the effects of security investment, information sharing as well as pricing are taken into account. In particular, we characterize targeted attacks by hackers as a negative effect on consumer demand and assume that firms’ information assets can be changed via an endogenous determination of pricing. The differential game established here allows us to derive feedback equilibrium solutions for rates of pricing, security investment, and information sharing. We demonstrate that a firm’s higher efficiency in security investment leads to higher rates for both security investment and information sharing. There exists a U-shaped relationship between this firm’s pricing rate and such efficiency. We indicate that a higher consumer demand loss coefficient, caused by targeted attacks, leads to lower pricing rates for both firms. Furthermore, we demonstrate that a higher hacker attack density always decreases both firms’ pricing rates, security investment rates, information sharing rates, and finally their integral profits. We reveal that as the density of hacker attacks increases, both firms are not always willing to cooperate in either security investment or information sharing. In particular, we reach the conclusion that the superior firm prefers the fully cooperative situation, whereas the inferior firm almost prefers the situation where only cooperative security investment occurs.

Despite these contributions on information security economics, there are still several limitations in our article, which will be left for our future research. First, although the differential game constructed in this article leads to feedback equilibrium solutions, complete analytical results regarding the comparative statics of key model parameters and the comparisons between the four forms of situations are quite difficult to obtain. The robustness of the related results needs further validation. Second, for the analytical expression of feedback equilibrium solutions, we only consider targeted attacks by hackers. Although targeted attacks constitute an increasingly important type of cyber-attack, one can construct alternative models that also include mass attacks and examine the effects of the two main types of cyber-attacks. Third, we assume that decisions regarding rates of pricing, security investment, and information sharing are determined in a single stage, for mathematical tractability; one can generalize our model into a two-stage differential game, in which both firms choose rates of security investment and information sharing in the first stage and then choose pricing rates in the second stage. Fourth, the model under current study assumes that the demand loss and hackers’ attack density are completely exogenous and independent of firms’ security decisions. In reality, when a firm invests more in its security, the improved security should deter hackers, make attacks more costly, or decrease the demand loss from a successful attack. Making the demand loss and hackers’ attack density endogenous implies that hackers are strategic in their choice of attacking activities, which requires a model extension from our differential game model between two competitive firms into a more interesting but complex differential game model between hackers and these firms. Fifth, the information a firm receives from information sharing arrangements may provide critical insights on the threats the firm is facing and significantly influence the firm’s cybersecurity investment decisions. Gordon et al. (2015) demonstrate that a firm’s information sharing practice may impact both the timing and expected value of its cybersecurity investments. Hence, our assumption that security investments and information sharing are independent of each other does not always hold. Although formally modeling the relation between information sharing and cybersecurity investments could cause loss of mathematical traceability, this issue deserves further investigation. Finally, the results of our article are obtained based on a differential game, which need to be empirically evidenced by realistic cases in the field of information security.

Acknowledgements

The authors thank the editorial board and the anonymous referees for their valuable suggestions that helped to substantially improve the quality and presentation of this article.

Funding

This study was supported by the National Natural Science Foundation of China (grant no. 71501041, grant no. 71371050).

Notes on contributors

Xing Gao is a Lecturer at the Southeast University in China. His research interest is information systems economics. He has published research articles in journals such as Decision Analysis, Journal of the Operational Research Society, and Information Systems Frontiers.

Weijun Zhong is a Professor at the Southeast University in China. His current research interests include information security economics, management information systems, and management of technology and innovation. He has published research articles in various academic journals including Journal of Management Information Systems, Technological Forecasting and Social Change, Marketing Letters, and Operations Research Letters.

References

Anderson, R. and Moore, T. (2006) The economics of information security. Science, 314(5799), 610–613.
August, T., August, R. and Shin, H. (2014a) Designing user incentives for cybersecurity. Communications of the ACM, 57(11), 43–46.
August, T., Niculescu, M.F. Shin, H. (2014b) Cloud implications on software network structure and security risks. Information Systems Research, 25(3), 489–510.
August, T. and Tunca, T.I. (2006) Network software security and user incentives. Management Science, 52(11), 1703–1720.
Kim, S.H., Wang, Q. and Ulrich, J.B. (2012) A comparative study of cyber-attacks. Communications of the ACM, 55(3), 66–73.
Kolfal, B., Patterson, R.A. and Yeo, M.L. (2013) Market impact on IT security spending. Decision Sciences, 44(3), 517–556.
Krishnamoorthy, A., Prasad, A. and Sethi, S.P. (2010) Optimal pricing and advertising in a durable-good duopoly. European Journal of Operational Research, 200(2), 486–497.
Lambertini, L. and Mantovani, A. (2009) Process and product innovation by a multiproduct monopolist: a dynamic approach. International Journal of Industrial Organization, 27(4), 508–518.
Lambertini, L. and Mantovani, A. (2010) Process and product innovation: a differential game approach to product life cycle. International Journal of Economic Theory, 6(2), 227–252.
Lee, C.H., Geng, X. and Raghunathan, S. (2013) Contracting information security in the presence of double moral hazard. Information Systems Research, 24(2), 295–311.
Lee, M. and Lee, J. (2012) The impact of information security failure on customer behaviors: a study on a large-scale hacking incident on the Internet. Information Systems Frontiers, 14(2), 375–393.
Leeson, P. and Coyne, C.J. (2006) The economics of computer hacking. Journal of Law, Economics and Policy, 1(2), 511–532.
Liu, C.Z., Zafar, H. and Au, Y.A. (2014) Rethinking FS-ISAC: an IT security information sharing network model for the financial services sector. Communications of the Association for Information Systems, 34(2), 15–36.
Liu, D., Ji, Y. and Mookerjee, V. (2011) Knowledge sharing and investment decisions in information security. Decision Support Systems, 52(1), 95–107.
Marte, J. (2014) Are data breaches creating smarter consumers? Available from http://www.washingtonpost.com/news/get-there/wp/2014/10/20/are-data-breaches-creating-better-consumers/
Miyazaki, A. and Fernandez, A. (2000) Internet privacy and security: an examination of online retailer disclosures. Journal of Public Policy & Marketing, 19(1), 54–61.
Mookerjee, V., Mookerjee, R., Bensoussan, A. and Yue, W.T. (2011) When hackers talk: managing information security under variable attack rates and knowledge dissemination. Information Systems Research, 22(3), 606–623.
Mukhopadhay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukhan, S.K. (2013) Cyber-risk decision models: to insure IT or not? Decision Support Systems, 56, 11–26.
Png, I. and Wang, Q.H. (2009) Information security: facilitating user precautions vis-à-vis enforcement against attackers. Journal of Management Information Systems, 26(2), 97–121.
Prasad, A. and Sethi, S.P. (2004) Competitive advertising under uncertainty: a stochastic differential game approach. Journal of Optimization Theory and Applications, 123(1), 163–185.
Ransbotham, S. and Mitra, S. (2009) Choice and chance: a conceptual model of paths to information security compromise. Information Systems Research, 20(1), 121–139.
Ransbotham, S., Mitra, S. and Ramsey, J. (2012) Are markets for vulnerabilities effective? MIS Quarterly, 36(1), 43–64.
Ray, S., Ow, T. and Kim, S.S. (2011) Security assurance: how online service providers can influence security control perceptions and gain trust. Decision Sciences, 42(2), 391–412.
Román, S. (2007) The ethics of online retailing: a scale development and validation from the consumers’ perspective. Journal of Business Ethics, 72(2), 131–148.
Schenk, M. and Schenk, M. (2002) Defining the value of strategic security. Secure Business Quarterly, 1(1), 1–6.
Suh, B. and Han, I. (2003) The impact of customer trust and perception of security control on the acceptance of electronic commerce. International Journal of Electronic Commerce, 7(3), 135–161.
Wang, J., Chaudhury, A. and Rao, H.R. (2008) A value-at-risk approach to information security investment. Information Systems Research, 19(1), 106–120.
Yuan, H., Chen, G., Wu, J. and Xiong, H. (2009) Towards controlling virus propagation in information systems with point-to-group information sharing. Decision Support Systems, 48(1), 57–68.
Yue, W.T. and Cakanyildirim, M. (2007) Intrusion prevention in information systems: reactive and proactive responses. Journal of Management Information Systems, 24(1), 329–353.