

Singapore Management University

Institutional Knowledge at Singapore Management University

Research Collection School Of Information
Systems

School of Information Systems

11-2011


Profit-Maximizing Firm Investments in Customer Information Security

Yong Yick LEE
Arizona State University

Robert J. KAUFFMAN
Singapore Management University, rkauffman@smu.edu.sg

Ryan SOUGSTAD
Augustana College - Sioux Falls

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research

 Part of the [Business Commons](#), and the [Information Security Commons](#)

Citation

LEE, Yong Yick; KAUFFMAN, Robert J.; and SOUGSTAD, Ryan. Profit-Maximizing Firm Investments in Customer Information Security. (2011). *Decision Support Systems*. 51, (4), 904-920. Research Collection School Of Information Systems.

Available at: https://ink.library.smu.edu.sg/sis_research/2181

This Journal Article is brought to you for free and open access by the School of Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email library@smu.edu.sg.

Profit-maximizing firm investments in customer information security

Yong Jick Lee ^{a,*}, Robert J. Kauffman ^b, Ryan Sougstad ^c

^a W. P. Carey School of Business, Arizona State University, Tempe, AZ, 85287, United States

^b School of Information Systems, and Lee Kong Chian School of Business, Singapore Management University, Singapore 178902, and Glassmeyer-McNamee Center for Digital Strategies, Tuck School of Business, Dartmouth College, Hanover, NH, 03755, United States

^c Business Administration, Augustana College, Sioux Falls, SD, 57917, United States

A B S T R A C T

When a customer interacts with a firm, extensive personal information often is gathered without the individual's knowledge. Significant risks are associated with handling this kind of information. Providing protection may reduce the risk of the loss and misuse of private information, but it imposes some costs on both the firm and its customers. Nevertheless, customer information security breaches still may occur. They have several distinguishing characteristics: (1) typically it is hard to quantify monetary damages related to them; (2) customer information security breaches may be caused by intentional attacks, as well as through unintentional organizational and customer behaviors; and (3) the frequency of such incidents typically is low, although they can be very costly when they occur. As a result, predictive models and explanatory statistical analysis using historical data have not been effective. We present a profit optimization model for customer information security investments. Our approach is based on *value-at-risk methods* and *operational risk modeling* from financial economics. The main results of this work are that we: (1) provide guidance on the trade-offs between risk and return in customer information security investments; (2) define the range of efficient investments in technology-supported risk indemnification for sellers; (3) model how to handle government-dictated levels of investment versus self-regulation of investments in technology; and (4) characterize customer information security investment levels when the firm is able to pass some of its costs on to consumers. We illustrate our theoretical findings with empirical data from the Open Security Foundation, as a means of grounding our analysis and offering the reader intuition for the managerial interpretation of our theory and main results. The results show that we can narrow the decision set for solution providers and policy-makers based on the estimable risks and losses associated with customer information security. We also discuss the application of our approach in practice.

Keywords:

Customer information
Financial economics
Information security
Managerial decision-making
Operational risks
Risk management
Value-at-risk

1. Introduction

The ubiquity of the Internet, the expansion of data storage space, and revolutionary increases in computing power have enabled firms to collect and analyze massive amounts of wide-ranging customer information at very low costs. Extensive personal information can be gathered either with or without the customer's knowledge, when the person interacts with a firm. Such information is gathered to profile users and provides targeted services, such as tailored advertisements, discount offers and so on. Significant risks are associated with handling such private information about customers, and firms are responsible for the proper treatment of

customers when they use their information. When the firm misuses customer information or it falls into the hands of other intruders who misuse it, this may have a significant impact on the firm's reputation, and also may result in large financial losses. Various sources [31,38] confirm that the number of customer information security breaches has been increasing over time, and more and more individuals are being affected. Firms that collect personal information from consumers should consider the costs and risks of customer information privacy protection, and strive to offer technology solutions and the security policies associated with them to create effective support.

Customer information security breaches have unique characteristics. First, it is hard to quantify the monetary damages that may be involved, even though the severity of the information security breach may be perceived to be high. Firms that suffer from information security breaches face the prospect of customer losses, reputational problems, and fines, while the contingent liabilities often lead to the downgrading of the firm's stock value [12,16]. Some of the losses may occur over the long term, and, thus, recovery also will take time. The

* Corresponding author at: W. P. Carey School of Business, Department of Information Systems, Arizona State University, PO Box 874606, Tempe, AZ 85287-4606, United States. Tel.: +1 480 965 3252; fax: +1 480 727 0881.

E-mail addresses: leeyj@asu.edu (Y.J. Lee), robkauffman@smu.edu.sg (R.J. Kauffman), rsougstad@augustana.edu (R. Sougstad).

long-term effects also may make it difficult to estimate the related monetary damages accurately. Second, unlike other security intrusions,¹ the cause of customer information security breaches may arise due to intentional attacks, as well as unintentional organizational and individual behaviors. The Open Security Foundation [31] has reported that about a half of past information security breaches are due to intentional attacks such as hacking, while accidents under normal operations, such as lost or stolen computers and documents, account for the rest. This wide range of causes makes it hard for a firm to establish effective information security strategy; technical and non-technical means of protection mechanisms are necessary, but may not be easy to implement effectively. Last, although the total number of customer information security breaches has increased over time in the economy, the frequency of such incidents is still low for individual firms. Moreover, there is not much historical data that is publicly available (in part because firms often do not wish to make their information security issues public knowledge), so statistical analysis of historical data is not very feasible.

Since such information security breaches may have a significant negative financial impact, many firms now deploy technology and security policy-based safeguards to protect their customers' private information to prevent becoming victims of such breaches [27]. A firm may implement several information security methods to its customers to reduce the risk of information security breaches. They include software and hardware solutions known as *privacy-enhancing technologies* and other non-technical information security policies. Examples of software protection methods include intrusion detection add-ons, encryption software, secure socket-layer connections, public-key infrastructure, and anti-virus software. Random-number generators, smart cards and fingerprint readers are examples of hardware solutions for privacy protection. Besides such software and hardware solutions, firms also offer other means of information security to their customers. Examples of non-technical means include providing opt-out choices while collecting personal information, conducting transactions through third-party payment systems such as PayPal or Google Checkout, and using one-time auto-generated credit card numbers that are not linked to personal information. A firm can choose to hire staff to manage use of customer privacy information, too, with a chief privacy officer leading the effort.

Firms face the risks of improper access to, errors with, and theft of their customers' personal information [40]. As a firm invests more in information security, such risks will likely be reduced. However, due to the unforeseen nature of such risks, they may not be controlled completely, even if a firm implements all of the possible technological and security policy protections. Moreover, the firm may not choose to use all of these methods due to customer preferences and incompatible environments, and due to concerns about profit maximization [2]. Previous research suggests that some customers are sensitive about information security, but others are less concerned [8]. Different computing environments also prevent customers from adopting all of the possible methods of protection. Some methods require high-powered computing with advanced technology, some are dependent

on the operating systems that customers have implemented, and some require nearly expert knowledge of computing.

Therefore, it is important for a firm to understand the factors affecting the value of its decision to invest in information security. Public policy and regulatory studies have identified several external factors that affect information security strategy [12,26,39]. Government regulations and self-regulations are key components that affect an organization's information security strategy [11]. Privacy concerns now have become a major obstacle to attracting customers to e-commerce [19]. However, Hui et al. [21] suggest that the consumers are not fully cautious about sharing their personal information with online merchants even though they are concerned about privacy. Studies by Ashrafi and Kuilboer [2] and Schwaig et al. [39] have revealed that firms selectively adopt the available information security mechanisms based on their own competitive circumstances. Prior research has overlooked the need to understand customer privacy protection more fully in economic terms though. Generally, although firms should respect their customers' rights for information privacy, economic theory predicts that it may not be optimal for a firm to protect them fully – which may be truly unfortunate in some cases.

Providing protection methods for customers may reduce the risk of misuse or the loss of private information, but at the same time, it will impose some costs on the firm, as well as on its customers. Some protection methods involve direct costs to customers. One is the use of hardware solutions that may require users to purchase technology to access services securely. An example is PayPal, which sells a small keychain device – a *security fob* – that provides a frequently-updated login code that enables the validation of a user's login, and blocks password phishing [36]. Other solutions may not involve direct monetary costs to customers, but some indirect costs may occur. The required time and installation effort, the learning costs for use, and the costs of dealing with malfunctions of software solutions are examples of such indirect costs. Customers' perceptions about the value of information security may vary too. So customers may choose to use protection services to different degrees, depending on how much they value privacy and how much the services cost.

Firms, on the other hand, incur implementation costs to provide customer information security. Although the result of mishandling private information can be costly, most firms will choose to implement only some of the available customer information security protections. In most cases, implementing all of the available protections will be prohibitively expensive. So firms must balance the costs and risks associated with customer information security breaches against the investment required to find a profit-maximizing level of privacy protection.

We will answer the following questions: What are the value-maximizing investment options for firms to protect customer information security? What are the factors that drive firms to invest in information security protection? How can we identify which investment level choices are optimal? We develop a profit optimization model for information security technology investments that considers the risks associated with implementation. We use a *profit-at-risk approach* based on *value-at-risk methods*, and *operational risk modeling* from financial economics. We show that the optimal investment choice is based on the control and expected mitigation of risks due to implementing information security technology solutions, and is affected by other concerns as well. We also provide model-based evidence as to why firms may not choose to implement full protection for their customers, and related empirical evidence of the model findings.

2. Literature review

Various studies on consumer information privacy have identified several factors that are likely to affect the privacy strategy of an organization. We classify such studies according to three different stakeholders with information privacy interests. *Individuals* provide their personal information to a number of *organizations* (businesses,

¹ We define *information security* in terms of the broader concept of *information privacy*. Information privacy issues arise whenever data are exchanged or processed, and are explicitly related to individuals. They also typically are a matter of the law and business ethics. Information security issues, in contrast, deal with the loss, theft, and unauthorized use of data in information systems [32], and are typically matters that are operational, financial and managerial in nature. Information security issues also arise with respect to sensitive data that do not constitute sensitive personal information. Although security is required to achieve privacy, information security emphasizes protection mechanisms involving technological and non-technological solutions. We focus on protecting a consumer's information security, which is also a subset of information privacy issues. Protecting a firm's operational data is solely an information security issue; implementing authentication methods to protect a customer's bank account information, for example, may be an information privacy issue, as well as an information security issue.

non-profits, and government agencies) that not only use such information themselves but often share it with other organizations. *Standard-setters and regulatory agencies* prescribe how organizations must protect the personal information they collect from individuals and may impose limits on its subsequent dissemination. Each stakeholder affects an organization's privacy strategy either directly or indirectly. Table 1 summarizes the main thrust of the literature based on the role of each stakeholder in an organization's customer information security strategy.

2.1. The privacy concerns of individuals

The nature of the relationship among privacy concerns, risk perceptions, and trust remains unclear. Some studies have shown that privacy concerns increase risk perceptions [35,44], but others have found that the riskiness of divulging personal information increases privacy concerns [13]. Similarly, there is evidence that privacy concerns reduce trust [28], but also evidence that trust decreases concerns about privacy [35].

Evidence about the effects of privacy concerns on actual behavior has been mixed. Milne et al. [30] have indicated that privacy concerns predict self-reported levels of engaging in privacy-protecting behaviors. Pavlou et al. [35] showed that increased concerns about privacy are negatively related to online purchasing behavior. Risk perceptions appear to affect *intent to provide personal information* [3,13,28] and *willingness to transact with e-retailers* negatively [44]. Perceived risk also reduces trust [13], which is important because trust is positively related not only to intent to share personal information [44], but also to the actual sharing of such information with an online merchant [17] and purchase behavior [44].

2.2. Organizational cost-benefit analysis and risk assessment

Some studies have also focused on the direct economic and financial effects on the firm resulting from privacy violations [1,6]. Contrary to other problems where the value of information is well defined, the value of protecting against customer information loss is difficult to quantify [1]. Nevertheless, losses from information security breaches can be potentially significant and their recovery may require an unspecified length of time [7].

Risk management studies analyze costs and benefits for privacy strategies. Gordon and Loeb [17] use an economic model to determine the optimal investment required to protect a firm's information. They report two key results. They show that optimal investment decision-making should focus on protecting information assets with mid-range vulnerability, since the protection of highly-vulnerable information is

so expensive. Second, they offer evidence that it never pays to invest to protect information completely; instead, maintaining some vulnerability is optimal. Hoo [20] formulates a similar decision analysis approach to provide evidence for the value of different information security safeguards based on the *annual loss expectancy value*, in the presence of perfect and imperfect information on loss-generating events.

2.3. Standard-setters and regulatory agencies

Several external forces regulate organizations' use of private information. The U.S. Privacy Act of 1974 documented what constitutes Fair Information Practices, which are widely recognized and used for self-regulation in the United States [11]. They offer guidelines for firms' self-regulation practices, as well as for the role of governmental legislation [14]. The Fair Information Practices also provide guidelines for a firm to control access to the private information of its customers. However, U.S. legislation has maintained a patchwork approach that is fragmented and discontinuous, and usually targets specific sectors or prevents specific abuses.

Little support has been found to support the assertion that regulation increases compliance with policies [9]. These findings suggest that self-regulatory efforts have been largely ineffective. Ashrafi and Kuilboer [2] examined the way privacy is treated in the context of the Fair Information Practices. They surveyed 500 companies in the U.S., and found that retailers and travel agencies have been complying fairly well with the principles. However, they also reported that few firms spend enough resources on privacy protection so that their compliance would be viewed as "full."

The presence of government regulation does not exclude self-regulation. However, self-regulation lacks enforcement mechanisms and sanctions. Research indicates that full compliance with such guidelines doesn't always happen [2,37]. Schwaig et al. [39] found that firms in different industries use different information practices that are considered fair, even though they may not address information privacy and information security in the same ways. The sensitivity of consumer information also differs by industry. As a result, some industries are subject to government regulations, as is the case with individual information privacy in healthcare and education, which makes managing stakeholders' privacy especially challenging.

3. Theory

We next discuss operational risk and a profit-at-risk approach based on value-at-risk theory from financial economics.

Table 1
Major stakeholders with information security interests.

Stakeholders	Factors	Citations	Findings
Individuals	Privacy concerns Risk perceptions Trust	Awad and Krishnan [3] Dinev and Hart [13] Hui et al. [21] Malhotra et al. [28] Pavlou et al. [35] Van Slyke et al. [44]	The nature of the relationship between privacy concerns, risk perceptions, and trust remains unclear. Evidence about the effect of privacy concerns on actual behavior has been mixed.
Organizations	Cost-benefit analysis Risk assessment	Acquisti et al. [1] Cavusoglu et al. [6] Crothers [7] Gordon and Loeb [17] Hoo [20]	The value of protecting against customer information loss is difficult to quantify. Optimal investment decision-making should focus on protecting information assets with "mid-range" vulnerability. Maintaining some vulnerability is optimal.
Standard-setters and regulatory agencies	Regulations Guidelines	Ashrafi and Kuilboer [2] Culnan [9] Culnan and Bies [11] PriceWaterhouseCoopers [37] Schwaig et al. [39]	Little evidence has been found to support the idea that regulation increases compliance with policies. Some industries are subject to government regulations (e.g., HIPAA for healthcare), which makes managing privacy challenging.

3.1. Operational risk and value-at-risk

Operational risk is the risk of monetary loss due to inadequate or failed internal processes, people and systems, or from external events [4]. Operational risk is often assessed in the financial services industry, though the term is generic and can be applied to any other industry [34]. Unlike other types of risk, where firms may seek out risk to create the basis for subsequent reward, operational risk originates at the business process level and only generates financial losses [23]. Thus, managing to identify and eliminate sources of risk is important. Losses due to the risks associated with the firm's choices about its customer information security practices can be classified as an operational risk. The issues arise from an inadequate handling of private information (the misuse or unauthorized access to the information, ineffective privacy policy, and the loss of equipment and documents), or an external attack. Frequency and severity of financial losses associated with information security breaches are two key factors that are used to measure the losses due to operational risk, according to Jorion [23]. Typically, the occurrence of such events is infrequent, but sometimes their impacts may be severe to the extent that it may cause a firm to become bankrupt. Moreover, recovery may be timely and costly, and may also require radical changes in the organization's business processes and operations.

Jorion [23] suggested using *value-at-risk methods* to model the operational risk in the financial services industry. Value-at-risk methods are widely used in finance to model market and credit risks also. They estimate the maximum loss in a financial portfolio with a given level of confidence. Value-at-risk methods have been applied in financial services to evaluate asset portfolios in the presence of risk factors as well. The method provides comprehensive risk measurement and can deal with risks from any sources. Unlike conventional financial forecasts that only consider point estimates of the most likely cases, value-at-risk provides the worst-case scenario for a given level of confidence that managers determine is appropriate. Such worst-case scenarios can identify the range of expected loss values considering the risk. Thus, a financial manager can have a better idea of the trade-offs between the risk and the expected value of the portfolio.

Value-at-risk is typically calculated for a single time period to gauge the likelihood of loss at the 95% or 99% confidence level [5]. The *confidence level* of 95% indicates that, on average, there is a 95% chance of the expected loss of an asset being lower than the value-at-risk value that is calculated. Risk in a value-at-risk model is represented by the volatility of the underlying costs or revenues and the resulting expected value outcome. It is expressed using the standard deviation. This permits the minimum and maximum possible values of the portfolio in the presence of risk to be estimated.

Jorion [23] described the computation of value-at-risk of a portfolio in five steps. First, the analyst estimates the current *mark-to-market* (MTM) value of the portfolio in dollar terms (e.g., \$100 million). Second, she measures the variability of the portfolio value by establishing the risk factor r (e.g., 15% per annum). In financial market operations, this is typically done on the basis of observations of market value over time. For many operational settings, the risk factor must be estimated, since no historical information will be available, or it will be prohibitively expensive to capture. Third, the analyst selects a time horizon or the holding period t for the analysis (e.g., 10 days, annualized based on the assumption of 252 trading days in a year, so $t = 10/252$).² Fourth, she sets the

confidence level α (e.g., 99%), which yields a confidence coefficient c of 2.33, assuming a normal distribution of potential losses. Last, she reports the worst potential loss by processing all the preceding information into a probability distribution of revenues, which is summarized by the *VaR* measure. This can be stated, for example, as a portfolio value of \$7 million at the 99% confidence level, as follows:

$$VaR = MTM \cdot r \cdot \sqrt{t} \cdot c = \$100,000,000 \cdot 15\% \cdot \sqrt{\frac{10}{252}} \cdot 2.33 = \$7,000,000 \quad (1)$$

In Eq. (1), \$7 million represents the value of the current portfolio in the worst-case scenario, with a confidence level of 99%, while the MTM value of \$100 million is the maximum expected value of the portfolio. In practice, one can expect the value to be somewhere between \$7 million to \$100 million. This enables management to plan an investment strategy that is sensitive to assumptions about risk.

Wang et al. [45] built a model of information security investments and showed how a firm can evaluate different investment trade-offs based on value-at-risk analysis. They provide simulation results based on historical data and managerial estimations of the costs associated with an information security breach. In addition, Paleologo [33] applied value-at-risk methods in the context of pricing IT services on demand and introduced the *price-at-risk* approach to address uncertainty in services pricing decisions. He argues that the price-at-risk approach improves on traditional cost-plus pricing methods. Kauffman and Sougstad [24] extended the price-at-risk methodology in the context of information technology (IT) service contract design, and introduced the concept of *profit-at-risk*, the maximum expected profit that can be achieved in the presence of risk.

We apply a similar construct, *price-at-risk* from Kauffman and Sougstad [24], for estimating the maximum expected profit that a firm can earn from customer information security protection, in the presence of the risk of the misuse of customers' personal information. They focused on pricing IT service contracts together in a portfolio, and on optimizing profit in the presence of uncertainty. Our methodology extends the idea of the set of services as a portfolio. However, we will focus on modeling optimal investment decision-making for information security investments in the presence of the risk of information security breach incidents and external regulatory actions.

4. Model development

We next introduce a model that can be used to value information security technology solution investment decisions. Our model utilizes a risk management modeling technique suggested by Jorion [23]. Through its use, we are able to evaluate the risk associated with customer information security breaches, based on the idea of profit-at-risk.

4.1. Model parameters and assumptions

Our model's parameters are defined in Table 2. We assume that the firm offers a chosen mix of information security protection services or technology investment from a known pool of such opportunities. Customers prefer to transact with firms that implement effective means to protect the privacy of their personal information. Likewise, the firm will select an information security level, subject to a pre-set level of risk which it may need to endure, to maintain an acceptable level of profitability. In effect, its aim is to protect itself against disabling financial losses.

4.1.1. Information security level S

In our model, we will assume that there are a number of information security and protection methods available. The information security level S that a firm chooses to implement can be

² Risk is measured by the standard deviation of unexpected outcomes. The *mean*, or expected return, and the *variance* increase linearly with time. The *risk*, represented by the standard deviation, grows with the square root of time, however. It is assumed that the returns follow a *random walk*, and are uncorrelated over time. Thus, adjustments of risk for different time horizons can be based on a factor involving the square root of time. All parameters are measured on an annualized basis.

Table 2
Modeling notation and definitions.

Notation	Description
S	A proportion defining the information security protection level with $0 \leq S \leq 1$, and $S=0$ indicating no protection and $S=1$ indicating full protection.
R	Firm revenue in the presence of choices about information security investments. R^{PassOn} indicates firm revenue in the presence of choices about information security investments, inclusive of the recovery of their costs from customers in the form of a higher price that the firm passes on.
π	Profit, based on firm revenue, reduced by information security implementation costs and customer information-related expected losses when a security breach occurs.
PaR	Value of profit-at-risk; the minimum expected profit at a given confidence level.
α	Confidence interval for profit-at-risk.
$C(S)$	Overall implementation cost (purchase plus deployment) to provide the level of information security protection S .
$x, E[x]$	Loss severity x stated in financial loss terms for the firm when an information security breach event occurs; and the expected value of the same.
$n, E[n]$	Frequency of information security breaches in period t ; and its expected value.
$z, E[z]$	Observed total financial losses in a period considering the expected loss severity and the expected security breach frequency; and expected total financial losses.
$g(x)$	Probability distribution function for customer information security breach-related losses related to an information security breach event x .
$f(n)$	Probability distribution function for customer information security breach frequency n .
$h(z)$	Probability distribution function of total financial losses considering both the frequency and the loss severity of information security breaches, $h(z) = h(f(n), g(x))$.
$\lambda(S)$	Expected total financial losses for information security protection level S , with $\lambda(S) = E[z]$.
$z(S, \alpha)$	Total financial losses z for information security protection level S at confidence level α .
t	Period when information security technology investment is to occur. ^a
k	Minimum targeted profit at a given confidence level for period t .
S^*	Information security protection level that yields maximum profit, $S^* = \arg\max(\pi)$.
S^*	Information security protection level that yields maximum PaR , $S^* = \arg\max(PaR)$.
<i>SelfReg, GovReg, UnderEst, PassOn</i>	Indicators for self-regulation, government regulation, under-estimation of risk, and pass-on of implementation costs for information security.

Note: We use the notation PaR when we refer to modeling values in our analysis of this problem, and reserve the term *profit-at-risk* for the higher-level concept and the methodology.

^a In the baseline case, we assume that the time horizon will be one year. Thus, we use $t=1$ for our examples. However, depending on the actual data set and its time horizon, one can adjust t accordingly.

thought of as being continuous from a low percentage to a high percentage of security, or $0 \leq S \leq 1$.³ The firm chooses a security level $S=1$ when it provides information security as much as possible, based on current methods of information security auditing. An information security level $S=0$ implies no spending on services or technologies to protect customer information

³ In reality, each information security method in the known pool of services and privacy-enhancing technology investments may not be weighted equally. The cost of implementation and the reduced risk associated with the approaches will be different. Thus, S should not be considered as the *number of services implemented* or the *expenditures on information security technologies*. Rather, it should be considered as the *level of information security achieved* from these things. It is reasonable to assume that there is an implementation sequence representing a best-known approach among those that most firms follow in practice. So we expect that most firms will choose to implement information security services in a sequence that they think is logical. This helps to ensure that one firm's information security level is the same as another firm's information security level when they both invest in the same proportional protection.

security. The customer should not expect full protection; there is likely to be some opportunity for security breaches that will compromise a customer's personal information.

Kauffman and Sougstad [24] demonstrated an approach that is useful in this context. They employed a *profit-at-risk constraint* in their analysis of IT service contracts. Their methodology considers the lowest acceptable level of profit within a given confidence level over a given time period. We view the managerial problem for protecting customer information security in terms of a portfolio of financial assets, which makes it amenable to analysis with value-at-risk methods. We consider the set of information security services as a portfolio that a firm can build. Information security level S , this way, represents the proportion of information security services chosen among the possible protection services.

4.1.2. Revenue R

We assume that a firm cannot price its products or services differently based on the total costs of providing a given level of protection to its customer. Implicit in this assumption is that consumers will be indifferent to information security protection and the reparations the firm pays out in terms of legal settlements or other approaches to restore value. The more customer information security the firm invests in, the more the costs of implementation will be, while revenue R will be roughly constant. In other words, the revenues associated with high-variance expected losses from less complete information security will be the same as those for the revenues with lower-variance losses associated with more complete information security protection.⁴ When a firm provides more information security, its transactions will be less risky from its customers' point of view, but the firm's costs will increase as information security becomes more complete.

4.1.3. Implementation costs $C(S)$ and estimated losses $\lambda(S)$

We assume total costs are of two types: implementation costs $C(S)$ and the severity of estimated losses $\lambda(S)$ at a given confidence level associated with information security breaches that permit customer information to be exploited. We use the words *estimated losses* for financial losses directly associated with the firm's legal obligations and remediation measures for restoring information security, as well as any estimated indirect costs, such as loss in reputation and trust. Implementation costs are costs related to development and deployment of the services to provide information security to customers, and are not subject to uncertainty. Instead, implementation costs tend to be known by the firm, so it is more a matter of whether they choose to incur them, and how much they will spend. We also assume that implementation costs are increasing as S increases.

We also expect that the customer information security spending is subject to variance in its capacity to provide effective protection. Consider an e-commerce transaction. From accepting an order from a customer to the final delivery, a firm faces a number of potentially harmful outcomes with respect to the use of its customers' information that need to be dealt with to thwart their occurrence. Although there are no certain outcomes in financial transactions, it may be possible for the firm's managers to estimate the extent of the financial losses that may occur with different levels of probability.

We assume that the probability distribution of losses at any level of S has "fat tails," which means the probability of a very large loss occurring is low, but still non-zero. As S increases though, the probability of loss decreases, so the probability distribution will shrink toward 0. The maximum loss at a given confidence level is represented as a deviation

⁴ We acknowledge that more information security protection provided to customers ought to increase their trust and the firm's reputation. Also, more trust and reputation will generally have a positive effect on customer demand [25], but not if delivering these costs them more. To obtain our initial results though, we only require that the revenue function be non-decreasing in the level of investment in information security S and be concave.

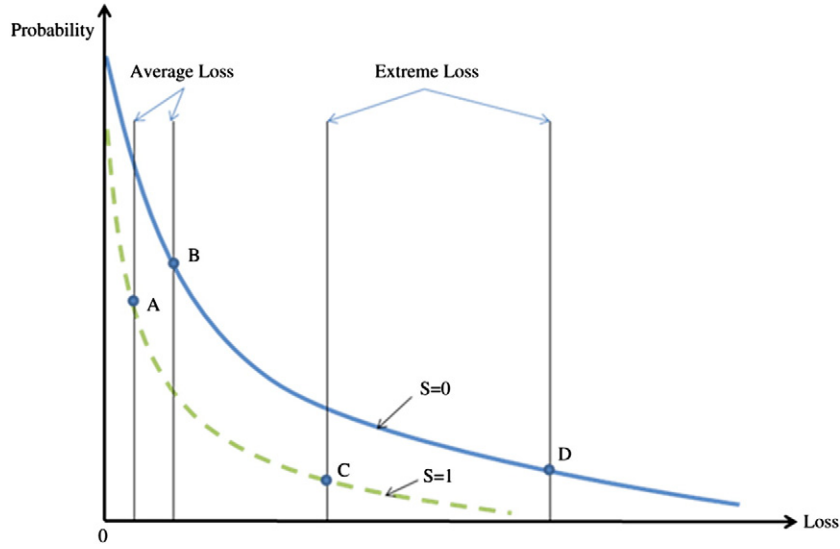


Fig. 1. Probability distribution of financial losses.

from the expected loss. Fig. 1 shows the probability distribution of losses for no protection ($S=0$), and at full protection ($S=1$).

With the profit-at-risk approach, we focus on the occurrence of an *extreme loss*, the maximum loss that occurs at a given confidence level. The two right vertical lines in Fig. 1 represent the maximum loss at 95% confidence on the probability distribution, marked by Points C and D at $S=0$ and $S=1$. In conventional approaches to profitability analysis, only the expected values would be considered. Thus, if we only consider revenue in an expected sense, without considering the distribution of losses, then the case of no information security ($S=0$) will always be preferred, as the immediate costs will be the least. Of course, this breaks down as soon as information security breach-driven losses are considered, and so our recommendation is to consider revenues and costs in a more sophisticated manner.

4.1.4. Frequency, severity and variance

The operational risk modeling literature [23,34] suggests two parameters that are useful in modeling losses due to operational risk. *Frequency* is the number of information security breaches that occurs in period t , and *loss severity* is a measure of the size of the related financial loss that occurs. One can derive a probability distribution function of total losses based on the frequency and loss severity distributions, as we will shortly show. In practice, historical data from an organization's own information security breaches or relevant others in a similar industry can be used to derive the necessary information to support figuring these things out. The *risk of total financial losses* associated with customer information security breaches and the related misuse of customers' personal information are associated with investments made by the firm to protect information security. This is what the firm will face when it is not able to protect its customers' information security fully.

Consider the following elements that we will use to construct a model for information security technology investment choices. First, let $f(n)$ be the probability distribution function for the frequency $n \geq 0$ of customer information security breaches during a period of time t . Next, define $g(x)$ as the probability distribution function for the severity of the financial losses $x (x \geq 0)$, specified in terms of the dollar amount of losses, that occur as a result of a customer information security breach. It is reasonable to assume that $f(n)$ is decreasing in n , so that information security breaches are less likely to occur with an increasingly high rate of frequency than with a low rate of frequency in a period. Similarly, $g(x)$ is also decreasing in x , so that higher-severity, higher dollar-loss customer information security breaches are less likely to occur than lower-severity, lower dollar-loss incidents. Assuming that the distributions of information security breach-

related frequency n and severity x are independent, the expected total loss $E[z]$ in period t will be a function of the random loss severity x over a random number of breaches n .

For example, suppose that in a representative period t , a firm faces the risk of a customer information security breach. The firm's probability distribution for breach frequency and loss severity are represented in Tables 3a and 3b. This information permits a manager to compute the expected frequency of an information security breach as $E[n]=0.5$ and the expected loss severity as $E[x]=\$23,500$ for period t . Assuming that breach frequency and loss severity are independent, the expected total financial loss within the period will be the product of the expected breach frequency and loss severity, which is $E[n] \cdot E[x]=0.5 \cdot \$23,500$ in this example. More generally, the *probability distribution function of total financial losses* that occur in period t due to the joint effects of breach frequency and breach-related loss severity can be written as $h(z)=h(g(x),f(n))$.⁵ Since $g(x)$ and $f(n)$ are both decreasing in x and n , $h(z)$ also will be decreasing in z , which represents the possible combinations of x and n weighted by the likelihood of their joint occurrence. Note that z also is a function of investments in information security, S . This permits us to write expected total financial losses as $\lambda(S)=E[z]$, reflecting the benefits that S will create by reducing the loss severity of information security breaches, as well as their frequency.

We assume that the expected total losses will decrease in S , so $d\lambda/dS < 0$. This is a reasonable assumption: there is no incentive for a firm to invest in information security protection if it increases expected financial losses. For the illustrations that we will offer hereafter in this article, we assume that the diminution in expected losses decreases in S , and the marginal benefit from investing in more information security decreases as

⁵ To calculate the expected value of total loss out of frequency and severity distribution, computing the product of the expected values of breach frequency and loss severity is sufficient. However, in order to derive value-at-risk, we need to recover the full distribution [23]. To derive the probability distribution function of $h(z)$, it is necessary to recognize that it is based on two independent distribution functions, $g(x)$ and $f(n)$, which can be estimated in practice with a variety of forecasting and control methods. The simplest way to construct the total loss severity distribution is by tabulating all of the possible combinations of frequency and loss severity that are identified. This should not be too onerous a task in practice, since only a limited set of outcome probabilities will need to be assessed for severity and frequency. Alternatively, one can also derive the $h(z)$ distribution by fitting the probability distribution functions for the loss frequency and the loss severity from a known parametric distribution. For the modeling we do in this research, we do not require any specific form of the loss severity distribution in our model, so long as the distributional assumption that $h(z)$ is decreasing in S . For additional discussion of these issues, the interested reader should see Jorion [23].

Table 3
Sample security breach frequency and loss severity probability distribution.

(a) Breach frequency distribution		(b) Loss severity distribution	
Breach frequency (n)	Probability	Loss severity (x)	Probability
0	60%	\$1,000	50%
1	30%	\$10,000	30%
2	10%	\$100,000	20%
Note: The expected value of an information security breach is 0.5 times per period.		Note: The expected value of the typical security breach-related loss severity is \$23,500.	

well.⁶ So, beyond some point, adding more protection will not improve the level of security for customer information very much, if at all. Also, since we have assumed fixed revenues for the firm at any level of S , total cost is the only factor that will affect its profit.

The distribution of total costs also should become narrower as S increases. Fig. 1 (presented earlier) shows a probability distribution function for $S=0$, with risk depicted as the distance between the expected loss (Point B) and the maximum loss at the 95% confidence level (Point D). We see that this distance is wider than in the case of maximum protection ($S=1$, Points A and C). So, even though profit is decreasing in S , PaR is affected by the information security investments made to reduce risk. We further note that the profit associated with the average value of total costs is always greater than profit-at-risk when the maximum loss is considered at a given confidence level for any value of S , with $0 \leq S \leq 1$.

Fig. 2 shows implementation costs, expected total losses and total costs for the information security protection interval $0 \leq S \leq 1$. We assume that increases in S are likely to reduce the frequency and severity of the financial losses (or both), and so $f(n)$ or $g(x)$ (or both again) will decrease as S increases. We further expect that the distribution of total financial losses due to information security breaches in a period, $h(z)$, will follow an exponential distribution with parameters for information security breach frequency and loss severity. The function $\lambda(S)$ denotes the expected losses z in the presence of information security protection S . Similarly, $z(S, \alpha)$ denotes the total loss severity for information security protection level S at a given confidence level α , which describes the worst case scenario (VaR).

Expected losses, $\lambda(S)$, for a given level of severity for customer information breach-induced financial losses and the associated extreme losses, $z(S, \alpha)$, will be decreasing in S and convex. The total costs are subject to the interaction between the expected losses and implementation costs. With a continuous and convex total cost function, the profit function will be continuous and concave. From this, we can derive the profit-maximizing information security investment level S . The first-order condition is $-dC(S)/dS - d\lambda(S)/dS = 0$; profit will be at a maximum when the marginal cost of implementation is equal to the marginal diminution in expected financial losses.

4.2. The baseline model

Recent information security breaches reveal that the payoffs for customer information security investments can be large. Once an information security breach occurs, a firm is exposed to direct costs

⁶ We assume that the rate of diminution of expected losses associated with investment in information security technology initially will be positive and increasing ($d^2\lambda/dS^2 > 0$), but then after some point ($d^2\lambda/dS^2 = 0$) the gains will tail off ($d^2\lambda/dS^2 < 0$). When the rate of diminution in expected returns is positive ($d^2\lambda/dS^2 > 0$), the marginal total costs will always be increasing. So, marginal profit will always decrease in this interval. However, in the interval where the marginal benefit from investing in more information security decreases, marginal total costs also will always decrease, and so we can expect maximum profit to occur within this interval. We will only focus on the interval in which the diminution in expected losses decreases in S .

for investigating its customer's personal information losses and advising its customers about the breach. A firm may also face indirect costs for settlements and legal actions that will need to be dealt with later. Also, loss of trust and reputation is hard to restore without enduring additional costs. Thus, even though the probability may be low, customer information security breaches are perceived to be very risky in organizations across many different industries. Our information security technology investment decision-making model, representing this setting, is formulated as follows:

$$\begin{aligned} \text{Max } \pi &= R - C(S) - \lambda(S) \\ \text{s.t. } PaR &= R - C(S) - z(S, \alpha) \sqrt{t} \geq k (0 \leq S \leq 1), \end{aligned} \quad (2)$$

where $\lambda(S)$ is the expected total losses considering the frequency and severity of customer information security breaches in period t , and $z(S, \alpha)$ represents the extreme losses associated with the confidence level α , considering the extent of the information security protection investments that are made by the firm. We also assume that the firm will only consider positive expected profit, where $R > C(S)$, and thus will have no incentive to invest when costs exceed revenues. Moreover, we assume that the firm will prefer the *highest minimum profit level at a given confidence level*. Thus, it will prefer more over less profit-at-risk.

Next, consider the PaR function in Fig. 3.

The PaR function is concave since the maximum total costs at a given confidence level in Fig. 2 are convex and continuous. By definition, $z(S, \alpha) > \lambda(S)$ at any point in S , and, thus, $PaR(S) < \pi(S)$ holds for all S . At point S^* , where PaR is maximized, $d\pi(S^*)/dS^* < 0$. Thus, the point of maximum service level, $PaR(S^*)$, will be greater than the profit-maximizing value S^* :

$$PaR(S^*) < \pi(S^*) \quad (3)$$

4.3. Inefficient and efficient information security levels

We next offer two propositions that enable us to characterize the efficiency of information security associated with a given information security protection technology choice. We distinguish between the *inefficient protection interval* and the *efficient protection level*, as follows:

- **Proposition 1 (Inefficient protection interval).** When $(d\pi/dS)/(dPaR/dS) > 0$, there is always a better customer information security investment choice available that will maximize profit and profit-at-risk. This is the inefficient protection interval.
- **Proposition 2 (Efficient protection interval).** When $(d\pi/dS)/(dPaR/dS) < 0$, so that profit is decreasing while PaR is increasing, investments in customer information security at level S are subject to tradeoffs between profit and risk. We define this interval as the efficient protection interval.

For the proofs of these and all of the other propositions in this article, see Appendix 1.

A firm will not choose to invest in information security in the interval $0 \leq S < S^*$ in Fig. 3, as it does not satisfy profit-maximizing strategy of the firm; both profit and profit-at-risk are increasing in the interval. So, investments in information security in this interval are inefficient: there is always a better investment level S that yields more profit with less risk. This is similar to the idea of an efficient frontier in portfolio management for financial assets. Similarly, $S^* < S \leq 1$ is inefficient; both profit and profit-at-risk are decreasing in this interval. Thus, the information security investment level S clearly matters in terms of efficiency. In the interval of $S^* \leq S \leq \hat{S}$, a firm may

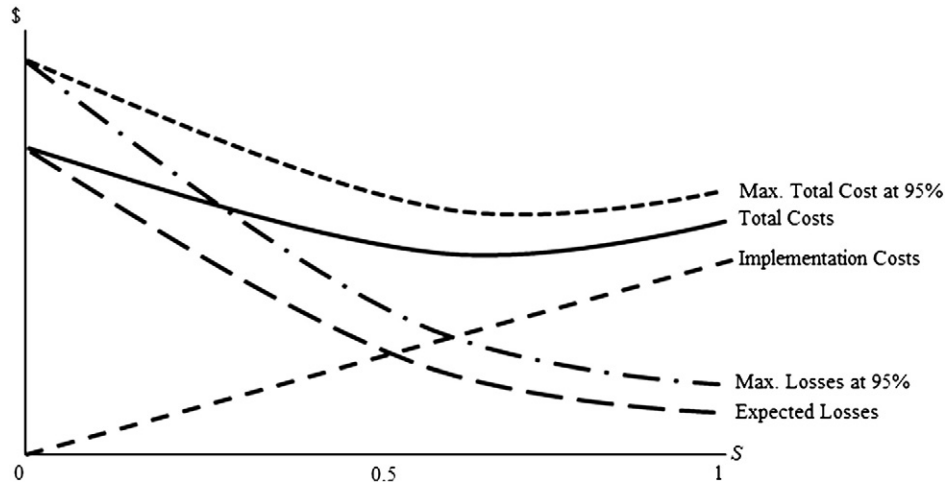


Fig. 2. Implementation costs and financial losses, $0 \leq S \leq 1$.

choose more profit with more risk S^* , or less profit with less risk \hat{S} , or position its investment somewhere in the middle, so $S^* < S < \hat{S}$.

4.4. Illustrative example

We next provide a numerical example to ground our model and provide additional insights to the reader. Consider a business-to-consumer e-commerce firm in the retail industry. It faces two customer information security investment choices to indemnify against fraudulent access to customer information. A prime example of a fraud event for this kind of firm is unauthorized access to customer or employee records that leads to subsequent misuse of personal information. Recent examples of such private information breaches include Capital One, Nationwide Financial and Alaska Air Group [31].

The first investment the firm considers is a set of system-wide controls that will reduce the expected probability of a customer information security breach. The second alternative involves parsing

customer databases, so that no more than one million records can ever be compromised on a given day. The second of these two investment choices is likely to result in a change in the financial loss distribution for a security breach in our model. We further assume that these two investments are mutually exclusive, and that the firm is interested in a three-month (one quarter) time horizon for the computation of value-at-risk.

The Web site of the Open Security Foundation (www.dataloss.org) is the source of sample data for our simulation. These data have limitations with their reporting intervals, granularity and completeness. Nevertheless, it is helpful for supporting an illustrative example. We selected data from June 1, 2008 to June 1, 2010, representing two years of customer information security breaches. The Open Security Foundation coded the events as “fraud breaches,” marked as “Fraud-SE” on the Web site. Fig. 4 shows the actual distribution of information security-related losses that occurred, based on a cross of the number of customer data records lost and the frequency of occurrence of a customer information security break.

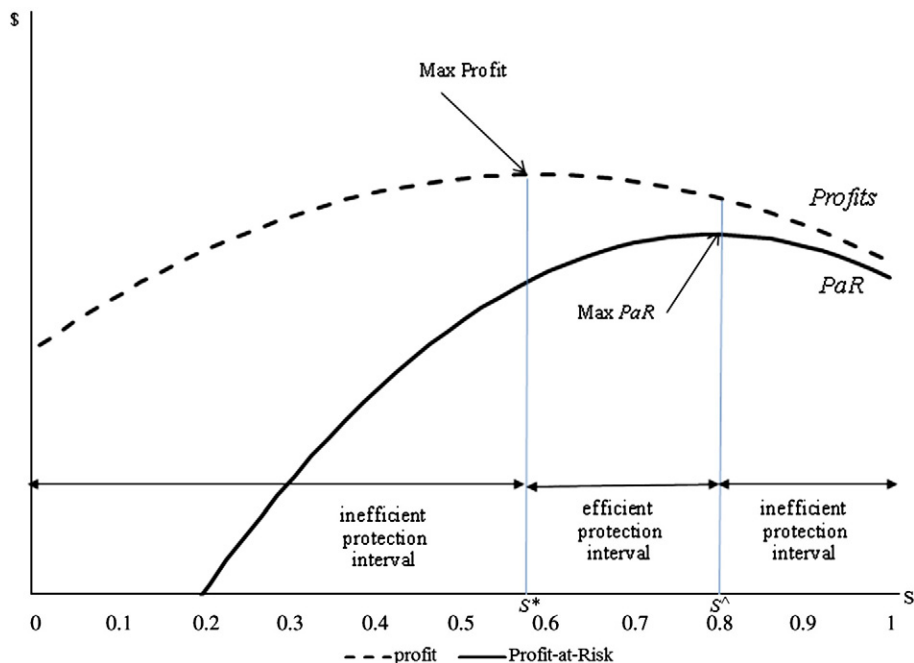


Fig. 3. Profit and PaR for $0 \leq S \leq 1$.

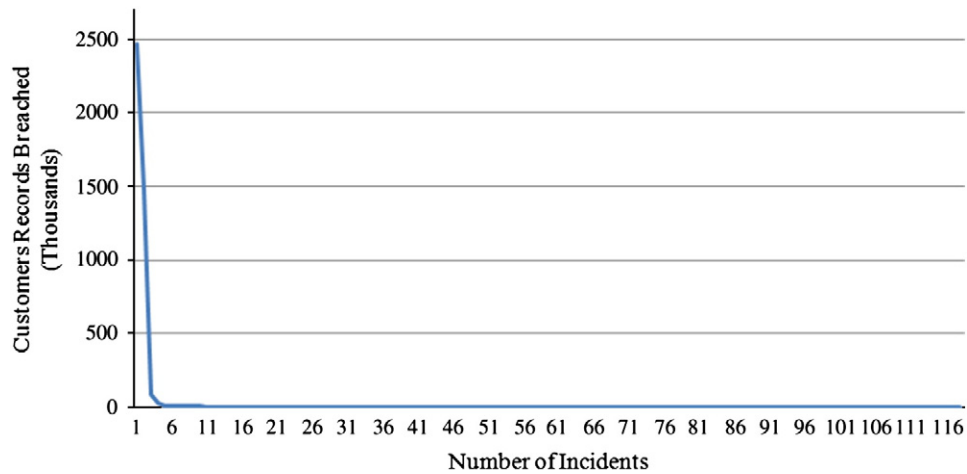


Fig. 4. Financial loss distribution for customer information security breaches.

Note that the distribution is highly skewed, with a mean loss of 37,507 records per security breach, but a median loss of only seventy records for each event.

We can approximate the financial losses associated with the number of customer records that have been compromised in a security breach based on a linear mapping. This is a simplification, of course. Indeed, it is very likely that the relationship between the number of customer records that have been accessed and the dollar value of the losses is not linear. Still, this captures the essential impact of the distribution of losses. For our illustration, we will assume a baseline likelihood of 10% for one information security breach over a three-month period that involves some number of customer data records which, in turn, can be tied to some level of severity of financial loss. Although this may seem like a high likelihood, the Open Security Foundation data surprisingly indicate that there was a 64% chance of an information security breach across the reporting firms in a similar time period. If we further assume that our hypothetical firm has a significant market presence, then 10% is a reasonable likelihood for the occurrence of a customer information security breach.

We constructed our simulation results on the basis of outcomes that occurred in 1,000 simulated quarters. Table 4 shows the expected loss and value-at-risk (based on the maximum loss that might occur at a 98% confidence level). It also shows the profit-at-risk (*PaR*) for each scenario. We assume that the revenue level from client Web interactions with the firm in its normal business will be unaffected at \$5,000,000, regardless of the customer information security investment choice the firm makes. We further assume that the technology investment costs the firm on the order of \$1,000,000.

Table 4 illustrates the trade-offs managers must make between the risks they face and the profit-at-risk associated with the customer information security technology investment. We observe that a new technology investment that reduces the likelihood during the period of a major customer information security breach to 5% (the middle column in the table) yields a higher expected profit in comparison to the alternative that caps the number of records lost at 1,000,000, with the associated financial losses. In contrast though, the second alternative – the investment that caps the loss of customer data records – yields a higher profit-at-risk (*PaR*). Interestingly, both of these investments would be considered “efficient” according to the Inefficient Protection Interval Proposition (P1): so neither investment choice dominates the other. Managers then must decide, based on their own risk tolerance, which investment is more attractive. Our illustration suggests that this may not always be the profit-maximizing investment, which is in line with the theory we have put forward.

5. Analysis

We next analyze information security investments under alternative circumstances: (1) when there is selective adoption and underestimation of risk; (2) when regulations or standards are implemented; and (3) when a firm is able to pass on implementation costs to its customers. A firm’s information security investment level reflects its managers’ boundedly-rational understanding about the known sources of threats.

Table 4
Three simulated scenarios for information security investments analyzed with a value-at-risk model.

Value-at-risk model parameters	Baseline scenario before an addition technology investment	Technology investment diminishes expected frequency of breach	Technology investment diminishes expected loss severity
Probability of one information security breach in the quarter involving all the firm’s customers’ data records	10%	5%	10%
Loss severity distribution	Unaffected	Unaffected	Financial losses diminished by an information security technology investment that caps the firm’s security breach to include no more than 1,000,000 records, which diminishes the loss severity
Expected financial losses (for the quarter)	\$343,826	\$162,560	\$178,740
Value-at-risk (maximum loss at a 98% confidence level)	\$1,576,756	\$1,497,726	\$1,001,715
Expected profit	\$4,656,174	\$4,837,440	\$4,821,260
Profit-at-risk (<i>PaR</i>)	\$3,423,244	\$3,502,274	\$3,998,285

5.1. Moral hazard, selective adoption and underestimation of risk

In the base case, we assumed every customer has homogeneous perceptions about the value of privacy protection. So we only considered their concerns about how well privacy protection works on average. There is a wide spectrum of attitudes among customers though. Some value privacy more, no matter what improvements in a firm's services are offered. Others, by the same token, may disclose their private information even though they express concerns about privacy [8]. Prior studies have shown that if consumers believe their information is safe, they may be reckless in their behavior [10]. For example, they may choose poor passwords, or leave their home wireless networks insecure. This is a form of *moral hazard*, and is endemic to insurance markets [29,41] and settings involving principals and agents [18]. Some customers might choose not to take advantage of the protection mechanisms that a firm provides, either because they are ignorant of information security risks, or because they simply don't want to be bothered by using those solutions. For example, customers who have a slow Internet connection might refuse to use protection mechanisms that would slow their transactions.

Moreover, the information security-enhancing technologies that a firm chooses to offer to its customers may not be as effective as expected. Because of differences in customer preferences for technology, not all customers will wish or have time to adopt all such technologies. The Fair Information Practices guidelines recommend that firms provide opt-out choices to their customers when collecting unnecessary personal information for transactions. In this case, even if a firm provides opt-out choices, customers who do not choose to opt out might still face some risks. Thus, the overall risk associated with a firm's consumer information security issues might not be as controlled as customers expect.

Likewise, some protection methods may be incompatible with customers' computer operating systems or software and hardware set-ups. Some privacy-enhancing technology solutions require software to be installed. Protection solutions written with ActiveX controls cannot be installed on Mac or Linux systems, for example. So those solutions would not protect customers who have systems that run OSX or Linux. Such limitations might shift the loss function associated with customer information security breach and loss severity risks as a result [40].

Now, let us revisit the information security optimization problem. (See Fig. 5.) If the solutions a firm decides to implement do not protect all its customers, then the effects of the firm's efforts to control and diminish risk for its customers will be smaller than might be expected, but its implementation costs would remain the same. Thus, we propose:

- **Proposition 3 (Underestimation of risk).** *Due to a lack of technical capacity or differences in preferences, not all customers will adopt the information security protection mechanisms suggested by a firm, resulting in the protection mechanisms being less effective than expected. As a result, the estimated risk will be less than the actual risk, and such under-estimation will result in a lower protection level.*

The difference between the *maximum profit* and *maximum PaR* is derived from the presence of the severity of loss distribution $z(S, \alpha)$. Under-estimating the risk that is present will reflect a belief that there is a smaller variance in x , thus reducing the efficient protection interval. Fig. 5 shows an example with a smaller variance in x . Compare this to Fig. 3, the base case. The efficient interval is narrower with a smaller variance in x . Though S^* does not change, S^\wedge is lower in Fig. 5 than in Fig. 3. So underestimating the anticipated risk level will result in a lower customer information security protection level, with less of an investment in technology that is made.

5.2. Self-regulation versus government regulation

The efficacy of two different approaches, self-regulation and government regulation, has been a subject of debate for some time [11]. Government regulations force firms to follow strict rules when handling the sensitive personal information of their customers, and require the implementation of different policies and privacy-enhancing technologies. In many cases, government regulations are accompanied by severe penalties for failure to comply. In the U.S., for example, state and federal legislatures have passed many regulations that impose civil or criminal penalties for the failure to protect consumer privacy. Although the regulations offer detailed privacy protection guidelines, they are sometimes either too broad in their context of application and do not consider specific industries' characteristics, or not specific enough to be

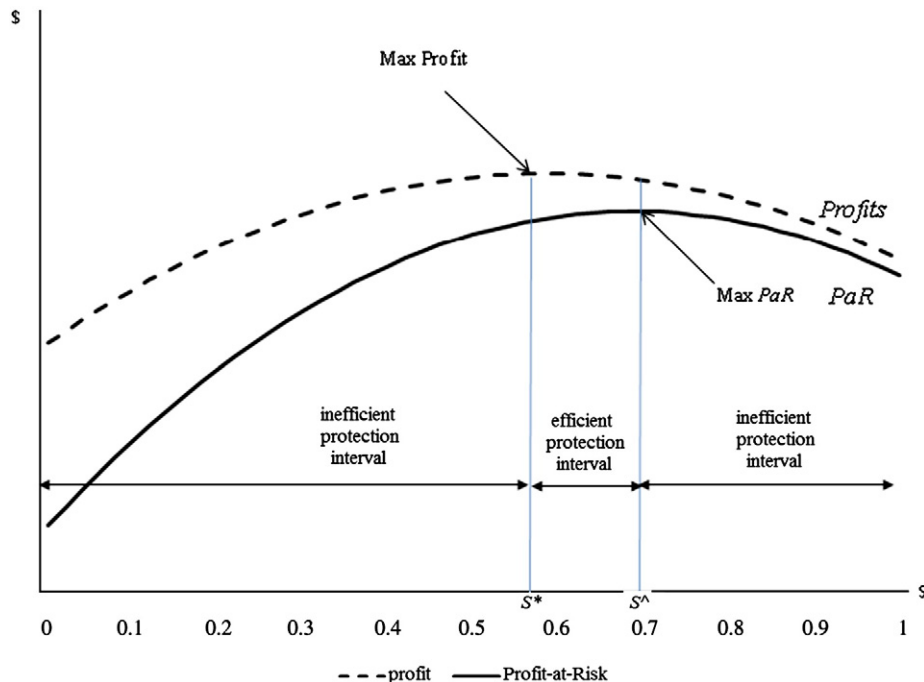


Fig. 5. The effects of under-estimation of the risk of an information security breach.

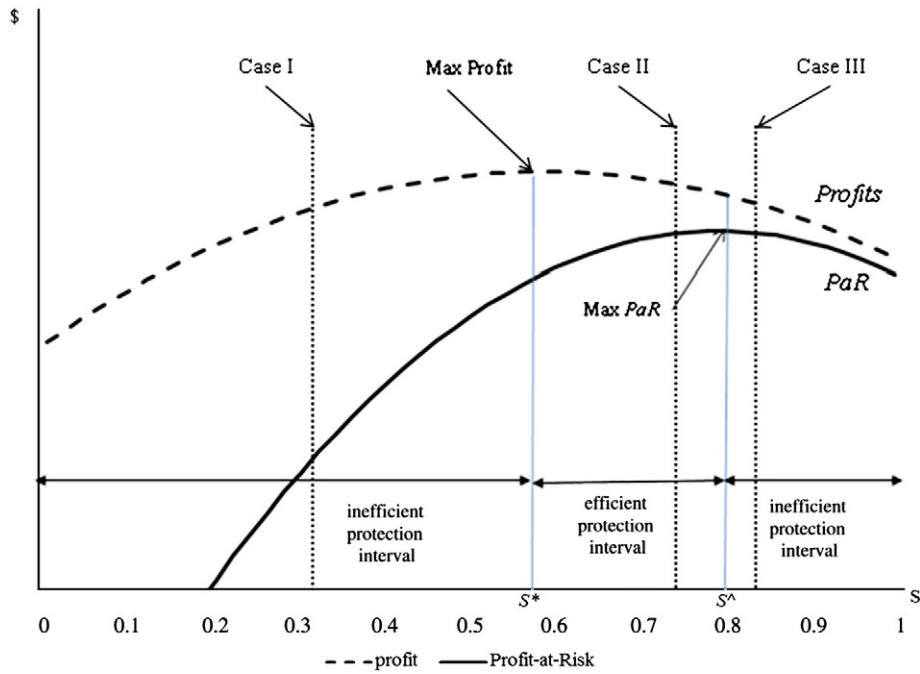


Fig. 6. Effects of government regulation on firm profit from information security investments.

enforceable [39]. Because of growing concerns about consumers' privacy and an increase in the number of privacy regulations in the U.S. economy, however, firms are increasingly expected to maintain higher standards of online privacy.

On the other hand, self-regulation policies impose no penalties; instead, firms can use them as guidelines to help reduce the risk of misuse to a reasonable level when fully adopted. But self-regulation is not always feasible, and firms will act to self-regulate only within the bounds of their limited resources. Studies that treat these issues suggest that it is not enough to adhere to self-regulation because firms typically will choose to adopt the level of privacy protection that suits their own circumstance, rather than the needs of their customers [37]. Because self-regulation does not force full adoption of the guidelines, most countries use government regulations to set the minimum level of protection, even if they still encourage self-regulation in practice.

Next, let us revisit our information security protection interval analysis results with this broader discussion in mind. First, we will assume that only government regulation exists, and examine several different cases (See Fig. 6).

5.2.1. Case I: Government regulation for information security protection that is insufficient

If the level of government regulation is at the left inefficient interval, both profit and PaR increase as S increases, and there is always a better information security investment choice available which will maximize profit and PaR . Thus, any firm would choose a customer information security protection level above the level the government sets. In this case, then, the government's regulations will be ineffective.

5.2.2. Case II: Government regulations enforce information security protection inside the efficient interval

What if the government regulations enforce the minimum level of information security protection inside the efficient interval? Firms that comply with those regulations would choose to set their information security protection level between the minimum level set by the government and PaR . Thus, those government regulations will narrow the efficient protection interval, effectively increasing the minimum information security protection level, so that customers overall are better protected. Firms that take risks would expect lower profits. Depending on

the penalty that accompanies these regulations, however, some firms may choose to set their information security protection level below the government's regulations to maximize their profit. To prevent this from happening, the regulations should impose a penalty that is greater than or equal to the firms' expected gain in profit. If the minimum level of protection is set adequately, and is accompanied by a proper penalty, then regulation will increase the protection level for consumers, which will decrease the risk of privacy breaches, while still allowing firms to generate reasonable profits as they remain on the efficient interval.

5.2.3. Case III: Government regulation sets a privacy protection above the level consistent with PaR

The last case is where the level of information security protection set by the government exceeds the protection level at PaR . The information security protection level at PaR is defined as the level that will maximize profit while controlling most of the possible risks associated with information security breaches, excluding some extreme cases. In other words, at PaR , most of the probable causes of information security breaches will have been addressed. Beyond that level, implementation costs will exceed the costs of the risk that the firm faces; thus the firm will have no reason to go beyond this point. From the security perspective of customers alone, more information security is preferred and full protection is beneficial.

The reality, however, is different. From an economic standpoint, efficient information security protection might mean less-than-best or full protection.⁷ Firms must consider the implementation costs, as well as the costs associated with the risk. We have seen that the costs

⁷ It is appropriate for us to comment on another situation in which personal information privacy regulations by the government might require firms to invest above PaR to protect their customers, even though we have not sought to model this. In cases where national security interests are an issue, the government might insist on full protection as a means of addressing the most extreme cases that are possible [22]. Full information security protection investment levels might be inefficient from an economic perspective, but this would be in the national interest and justifiable because of the risks association with cyber-penetration into a defense contractor systems, for example. Social welfare interests dominate efficiency in expectational terms. We have recently seen indications of the severe risks that are present due to the increasing capacity of China-based Internet attackers, and their ability to mimic U.S. Department of the Air Force and other defense community memoranda [15].

outweigh the benefits at some specific point S^* in the analysis. Thus, if the level of information security protection that the regulations enforce is in this region, it might seem that customers will be well-protected; but in reality, little is gained because the additional protection will only cover rare and extreme cases. Regulations that require this level of protection only sacrifice firm profit if they are enforced. Thus, from a financial economics perspective, there is no reason for the government's regulations to go beyond the protection level above the information security level that is established in connection with PaR . We now offer two additional propositions:

- **Proposition 4 (Proper penalty for government regulation).** *To encourage firms to follow the regulations for information security protection, the penalty imposed under the regulation should be at least equal to the difference between the maximum profit level and the profit at the desired level of information security protection.*
- **Proposition 5 (Effective interval for government regulation).** *To be effective, the level of government regulation should be within the efficient protection interval, which is between the level of information security protection that yields the maximum profit and that which yields the maximum PaR .*

Now, consider the role of self-regulation. Unlike government regulations, which are accompanied by appropriate penalties for enforcement in most cases, self-regulation has no specific means of enforcement. Thus, an information security protection level suggested by self-regulation set below government regulations has practical meaning. Similarly, a level of information security beyond PaR is inefficient from both the government regulation and self-regulation standpoints. As a result, the effective region for self-regulation lies above the government's regulation level, and below the level at PaR . However, self-regulation tends to provide enough information security protection to cover the most probable causes of the security breaches, so it can serve as a "reasonable" maximum protection level. So we argue that the most effective self-regulation will be a level of information security protection that is equal to the protection level at

PaR . Interestingly, this finding agrees with prior empirical research [2], which shows that most firms do not implement plans to achieve full privacy protection, even though we cannot ascertain from the data alone that the observed patterns of firm information security investments are due to firms' efforts to optimize their investments. We propose:

- **Proposition 6 (Effective interval for self-regulation).** *To be effective, the selected level of self-regulation should be greater than the level of government regulation within the efficient protection interval, preferably at the level of PaR .*

5.3. Recovering investment costs by passing them on to customers

Competitive conditions in some parts of the marketplace may permit a firm to pass the costs of protecting customers' information security on to the customers' themselves. For example, some banks ask customers to purchase an authentication certificate to indicate their earnestness and willingness to divulge their identities in order to permit them to use the banks' online payment services. We wrote earlier of a keychain device that PayPal sells to its members, and that this is an example of a firm that is passing the costs of information security on to its customers. Many justifications for investing in information security-enhancing technologies have been suggested. Most studies, however, relate the protection of people's privacy to building trust and reputation [40]. This is an incomplete view based on how we have conceptualized this problem — there are some important economic relationships that need to be sketched.

To maintain profitability while properly protecting customer information security, a firm may wish to pass on its implementation costs to its customers by increasing its prices. We will assume that there is no diminution in demand based on the change in prices associated with the costs of additional information security protection that the firm offers, which is reasonable in the short run because customers are able to obtain additional insurance that their personal information will remain private. A price increase may even enable a firm to offer a higher level of protection than it did before, charge more than before, and engender more trust and a stronger reputation

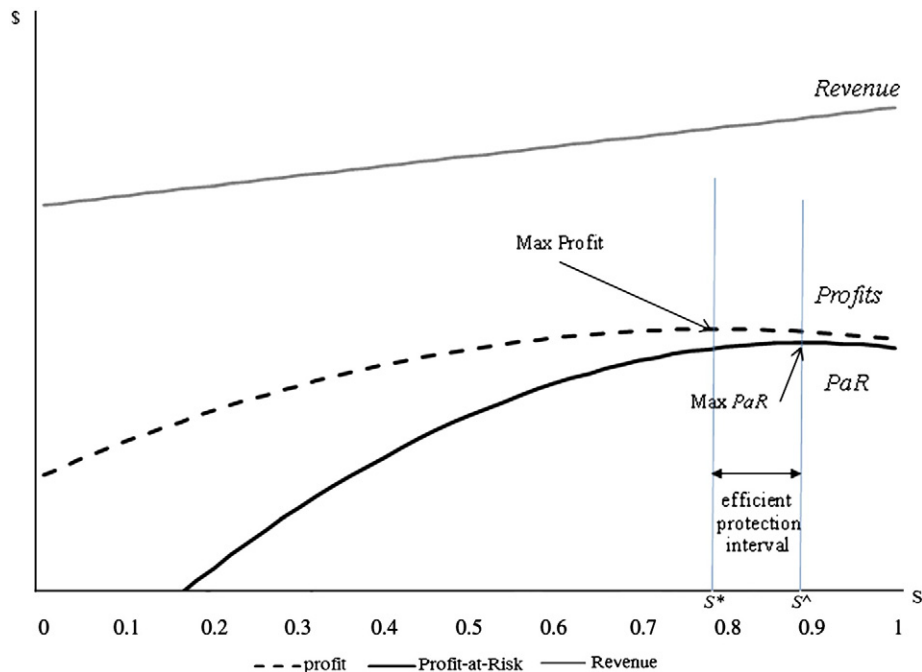


Fig. 7. Pass-on of 50% of implementation costs for information security investments.

in the market than it had before. Instead though, our modeling approach is to limit the benefit from the price premium to investment cost recovery rather than as a means to build higher revenues. We will discuss this limitation further when we conclude.

Consider two scenarios. The first occurs when a firm passes on some of the implementation costs of enhanced information security to its customers. Fig. 7 shows the changes in *PaR* and profit when the firm can recover 50% of the information security implementation costs from its customers. A second scenario is to pass 100% of those costs on to customers, as shown in Fig. 8.

Let us compare Figs. 7 and 8 to our base case in Fig. 3. Note that Fig. 8 shows the case in which a firm passes all of its implementation costs on to its customers at the point of maximum profit and maximum profit-at-risk; this is $S = 1$, or *full investment*. Thus, the firm incurs no losses or additional costs for implementing this level of information security. Further note that, even at the 50% investment level as shown in Fig. 8, the efficient protection interval is right-shifted so that $S \rightarrow 1$.

From the above discussion, we propose:

- **Proposition 7 (Pass-on of implementation cost effect).** *When possible, passing on the implementation costs for privacy protection to a firm's customers will increase information security protection at both the minimum and maximum level for the efficient protection interval.*

Another related observation is that the efficient protection interval will start out higher than in the base case, and will be narrower, too. This is because the firm suffers less from the costs associated with providing protection services. However, it is important to keep in mind that the amount of implementation costs that a firm can pass on to its customers without diminishing their demand will be limited beyond some price premium level. Even if customers don't figure this out right away, they will figure it out eventually, and so the price elasticity of their demand will be useful to consider. If the implementation costs are large, and the price premium from added trust and enhanced reputation that can be charged in the market is small, then the firm will be unable to pass all of the implementation costs on to its customers.

6. Discussion

We next will offer some clarifications about the boundary conditions of the model we have proposed. We also seek to highlight some of the applications that will be most beneficial to firms and consumers. We will discuss where these risk management techniques should not be used, and the potential dangers that may accompany misuse. We first discuss some issues with the technical assumptions of the model, as a basis for providing full disclosure on what we know about the approach we have developed.

6.1. On the assumptions and boundary conditions for the model

Our model assumes that the loss distributions can be estimated in terms of both loss severity and breach frequency. Managers must have some point of historical reference to make estimates in quantitative or qualitative terms about the loss distribution. Wang et al. [45] proposed a value-at-risk model for financial information services. They utilized historical data to simulate event frequencies, and made managerial estimates of the potential losses. The key take-away from their work is that the approach will only be as sound as the robustness of the estimation of the underlying loss severity and frequency distributions. Moreover, any implementation of this model should be subject to frequent testing and checking to see whether the parameter assumptions are in synch with the evolution of the risks of loss in the related managerial environment.

A value-at-risk model can be tested and validated by *back-testing*, a process that involves the systematic comparison of historical *PaR* measures with the subsequent returns [23]. Given the confidence level α , one can test such a model by counting how many times the actual loss exceeds the model's *PaR*, after counting the number of exceptions in the total sample size. When the total sample size is large enough, a standard *t*-test can be applied to derive Type I error for rejecting a correct model or Type II error for accepting an incorrect model. To validate the model, one should consider both error types. Even if the Type I error is low, a high Type II error will mean that the model's accuracy can be improved by increasing the confidence level. A manager can then adjust the model according to previous data. In addition to providing information on the model's accuracy, back-testing may also provide useful information about

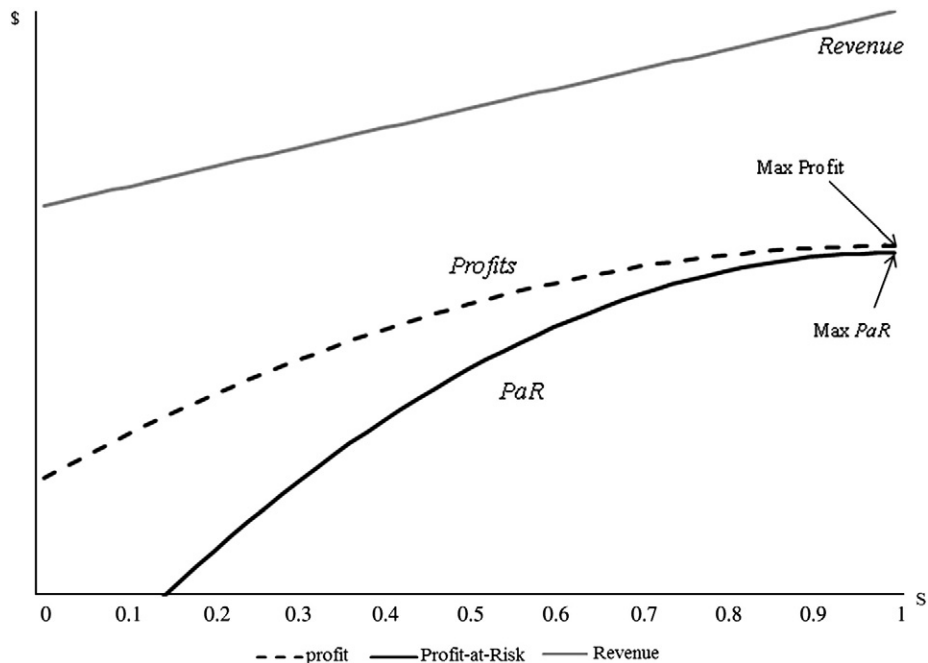


Fig. 8. Pass-on of 100% of implementation costs for information security investments.

the firm's data collection initiatives. This will help managers to understand better the domain to which this approach is best suited, and what metrics provide the most effective decision support.

In the analysis, we assumed continuous normal distributions with “fat tails” for the loss function. In reality, it's not clear whether this will be the case. However, as long as the probability distribution shrinks as technology investments S increase, our model will produce valid results with any other distributional assumptions. This assumption is reasonable because there is no need to implement information security protection mechanisms that do not diminish the risks associated with information security breach-related losses. Further, our model does not require the loss function to be continuous. In the case of a discrete loss function — which may be all that is possible to estimate, a manager can consider using percentiles instead of confidence levels (at the 95th percentile instead of the 95% confidence level) when applying the model. Each discrete case should be compared separately to find the optimal PaR , and the optimal PaR then should be compared with the maximum profit level for accuracy.

6.2. Consumer preferences, managerial strategies and public policy perspectives

One of the central questions we examined in this article is who pays for information security protection. The consumer may have strong preferences to protect their personal information, and may be on the lookout for opportunities to transact with firms that offer information security services that create better protection. Consumers are likely to have some expectation of privacy, and thus all sellers will be forced to make investments in information security as a “cost of doing business.” On the Internet today especially, a firm will not be able to operate effectively in the market without doing this. In the end, consumers will foot the bill, but an interesting question arises as to whether a firm will be able to obtain competitive advantage or to reap extra profits through information security investments.

Anecdotal evidence shows that there are companies whose entire business models are centered on information security services for other firms. These firms, such as LifeLock (www.lifelock.com), TrustedID (www.trustedid.com) and Identity Guard (www.identityguard.com), specialize in identity theft protection. It is clear that they employ technologies to reduce the risk of customer identity theft, but they also offer some interesting financial remedies in the event that an intrusion occurs, and customers' personal information is lost. For example, LifeLock touts a \$1 million dollar guarantee to cover certain expenses associated with an individual's identity theft. Most of these services also offer tiered-pricing with different technologies that enhance information security, and different levels of remedies. The technical services often involve notification, which serves to ensure that a participant is informed in a timely manner that there has been some form of identity theft.

It still is unclear what the base level of information security is that most consumers expect, and beyond that, what more they might be willing to pay for. Our earlier example of PayPal's decision to foist upon consumers the perceived need to further protect intrusion into their PayPal accounts through the application of a code-generating keychain device for which they must pay is a case in point. Indeed, the spectrum of different offerings and pay-for-harm remedies associated with identity theft bears this out. Although we have demonstrated a modeling mechanism in this research to deal with such managerial choice problems, the problem, nevertheless, may be best addressed by the formation of public policy related to it. Similar to other settings in which insurance policies need to be evaluated, consumers may not be able to accurately assess the value of protecting their private personal information. Firms, then, may have little incentive to provide the means to protect consumers, and the resulting under-investment in protection of personal information may lead to an overall loss of welfare to society. Although self-regulation is often attractive, we question whether it will work in this instance. Instead, it may make more sense for government policy-makers to be the pivotal agents who are charged with figuring out what value of social welfare gains will

accompany the balancing of costs, risks and expected financial loss trade-offs that we modeled.

6.3. Black swan risks

Another aspect of the problem we have studied that is worthy of further consideration involves the classes of risks that cannot be estimated or predicted with accuracy. Such risks may be characterized as “black swan” events, as the popular business risks writer Nassim Taleb [43] calls them. They include such things as the September 11, 2001 terrorist attacks on the World Trade Center in New York City, and the likelihood of an earthquake in San Francisco, California or Seattle, Washington of the magnitude that occurred in Haiti in January 2010. In the context of information security breaches, there are also analogous “black swan” risks, and they fall outside the risk boundaries and analytical capacity of our model. Managers should be aware of this, and perhaps should look to other kinds of extreme value analysis from economics, risk and insurance.

We do not wish to argue, however, that firms cannot invest in technologies that will provide risk indemnification against “black swan” events. In fact, the record shows that many financial firms located in the World Trade Centers were able to recover their systems after the 9/11 attacks due to prior investments in disaster recovery services [42], and the loss of customer information in the process was never a major issue. One cannot predict the frequency or magnitude of these events related to information security losses with any real accuracy though. Thus, it will be hard to develop any kind of meaningful empirical data to formulate appropriate loss distributions that would permit an analyst to use our modeling approach for the “black swan” class of customer information security risks. Instead, we advocate a much simpler approach: subsuming the risks of extraordinary disaster into a model that calibrates the impacts of loss distributions for the more-frequently encountered risks that might be present at the 1% likelihood level — but nothing less.

7. Conclusion

We developed a model based on current theoretical perspectives in financial risk management to analyze how information security investments result in tradeoffs between expected financial losses and the firm's risk mitigation efforts on behalf of its customers. Our model has the potential for real-world application in a variety of scenarios where information security breach frequency and financial loss severity distributions can be estimated qualitatively or quantitatively. In addition to our contributions in this research, we also highlight several limitations of our modeling approach that will help information security managers and information privacy theorists to gauge its range of application and potential effectiveness.

7.1. Contributions

Our main contribution is to model the information security investment decision-making process using operational risk management and value-at-risk methods in financial economics that support a profit-at-risk approach to evaluate the optimality of firm-level decisions to protect the personal information of customers. It is well known that there is a trade-off between security costs and desirable levels of information security, but little work has been done to analyze the risk-return trade-offs for information security enhancement investments. Even though the probability of an information security breach may be low for most firms, the associated risk still may be quite high because of potentially extreme losses. Thus, firms will need to invest in information security services to reduce their exposure to these risks. It is unclear how much a firm should invest though. Spending too much will cause an undue financial burden, while spending too little will expose the firm to unpredictable and unacceptable losses. We addressed this issue, and provided an in-depth analysis of the dynamics of information security investments with analytical methods from financial risk management.

Our model can be implemented in a real-world decision support system, because the underlying analytical methods can be readily represented and embedded in risk analysis routines that can guide information security investments. As such a model is tested, managers will see the benefits of gathering customer information security-related data, and sharing it among firms – in much the same way that we see benchmarks that have been created for risk management in commercial lending and financial services, IT outsourcing and services contracts, and other settings. This also will inform information security professionals' efforts to develop new metrics to improve their internal controls.

We have shown that optimal investment decisions for information security protection depend on the tradeoff between the cost to implement the information security service and the concomitant risk mitigation that is achieved. Practitioners may benefit from our model, since it is directly applicable in operational settings and business processes for which customer information security is an issue. By applying reasonable values to each attribute, it is possible to come up with approximations of the investment choices that will be effective for the firm. The profit-at-risk method allows the assignment of a confidence interval that the manager thinks appropriate. Managers also can test the effects of small changes in each attribute by performing sensitivity analysis on the model's elements. This approach will add richness to the analysis process to justify the necessary technology investments to enhance information security for customers.

We have also shown that there is a minimum information security protection level that the firm will need to achieve to make its investment in customer privacy protection effective. We called this the *inefficient protection interval*, and within it a firm incurs higher costs of implementation and operations relative to the associated risk reduction that the information security protection services provide.

Due to the ambiguity in understanding what constitutes effective privacy protection, many firms tend to under-estimate the risks. When a manager believes that the risk is likely to be low, the firm will invest less. Another factor that affects the investment level is the cost of implementing and operating the protection. Our model confirms that the lower the concern about risk, then the optimal value of *profit-at-risk*, PaR , will occur at a lower level of customer information security protection. This implies that proper evaluation of expected risk is necessary to set the confidence level associated with security breaches.

Our model also confirms why firms do not fully invest in customer information security protection. The risks that companies and their customers face with changing technology developments include intentional attacks on private customer information, and changing levels of effectiveness of firm-level information security. It is likely that a firm's and its customers' personal information may not be completely secure, even if the firm invests fully in relevant information security. Thus, investing to achieve the maximum level of protection often is not an optimal strategy. Firms are better off when they consider maximizing profit-at-risk instead, and then they should invest in protection accordingly, albeit at a lower level than fully.

One way to manage profitability in the presence of information security investments is for the firm to pass all or some of its security-related implementation and operational costs on to its customers. Although this is rarely the first thing that most managers think about – just as it is not the first thing we have considered in our base model for customer information security investments – it is a necessary consideration in today's marketplace. Consumers are likely to be willing to pay for this protection to some degree, so this is worthwhile for managers to explore. Our model shows that firms should provide more information security when they share the costs of information protection investments with their customers. This may not always be true, of course. Other factors, such as high price competition, price elasticity of market demand, and so on, should be considered during the decision-making process. We have only scratched the surface of

the complex issues that need to be modeled and evaluated in greater depth.

7.2. Limitations

We conclude by pointing out some caveats and limitations. In our model, all of the information security protection services are weighted equally. Adding any services will incur the same proportional costs. Only the quantity of services matters in the model that we have specified. Some service elements, in reality, may not cost the same amount though. Examples include the provision of payment services using secure third-party payment methods, opt-out choices on promotional mailing lists, and opt-out choices to preclude the retention of customers' private information used during transactions. Different kinds of protection will cause the firm to incur different implementation costs. For the analysis we have conducted, this issue does not affect our results. Our model deals with the average costs that are incurred with information security protection technology investments. It will only be implementation costs which deviate significantly from average costs that will affect our policy recommendations and results.

A second limitation is that we have assumed there is not an endogenous relationship between the extent of a firm's investments in information security on behalf of its customers and the possibility that such investments promote new demand-driven revenue from consumers. Instead, we focused only on variations in the severity and frequency of information security breaches. Future research should explore what will happen with changes in consumer demand for a firm's products or services if it gains an increasingly strong reputation with respect to the protection of customer information privacy, while its competitors may be less successful. Finally, our model relies on estimates of the frequency and magnitude of future losses. We expect firms to build predictive models based on historical data to estimate future losses when customer information is compromised. Third-party firms that provide security benchmarks, auditors, and standards bodies may be good sources of such data.

Acknowledgments

An earlier version of this paper appeared at the 2009 Hawaii International Conference on Systems Science, Waikoloa, HI, January 2009 under a different title. We thank Yabing Jiang, Avi Seidmann and the anonymous DSS reviewers for their input, and Jennifer Zhang for her creative guidance with the refinement of our modeling approach. We appreciated earlier input from Michel Benaroch, Qizhi Dai, Haluk Demirkan, Michael Goul, Gezinus Hidding, Paul Maglio, Paul Steinbart, Marilyn Prosch, three anonymous reviewers at HICSS, and the participants of the CIS 791 Doctoral Seminar at the W.P. Carey School of Business, Arizona State University. Rob Kauffman thanks the W. P. Carey Chair, the Shidler School of Business at the University of Hawaii, and the Research Center for Contemporary Management at the School of Economics and Management of Tsinghua University in Beijing, China for generous support.

Appendix 1. Proof of propositions

A. Proof of Proposition 1 (Inefficient protection interval)

Let $S^* = \text{argmax}(\pi)$ and $\hat{S} = \text{argmax}(PaR)$. From Eq. (3), we know that $PaR(\hat{S}) < \pi(S^*)$. We assume that $d\lambda(S)/dS < 0$, $dz(S, \alpha)/dS < 0$ and $dC(S)/dS > 0$. We further assume that π and PaR are continuous, so the first-order condition for $\pi(S^*)$ is $dC(S^*)/dS^* = -d\lambda(S^*)/dS^*$, and the first-order condition for $PaR(\hat{S})$ is $dC(\hat{S})/d\hat{S} = -dz(\hat{S}, \alpha)/d\hat{S}$. By definition, $d\lambda(S)/dS < dz(S, \alpha)/dS$. Also, since $dC(S)/dS > 0$, $S^* < \hat{S}$. Therefore, $dC(S^*)/dS^* < dC(\hat{S})/d\hat{S}$. To satisfy the condition $d\pi/dS/dPaR/dS > 0$, it is necessary that $d\pi/dS$

$dS > 0$ and $dPaR/dS > 0$ (Case A-1) must hold, or that $d\pi/dS < 0$ and $dPaR/dS < 0$ (Case A-2) must hold.

Case A-1. $d\pi/dS > 0$ and $dPaR/dS > 0$

Since $PaR(\hat{S}) < \pi(S^*)$, the interval which satisfies the conditions $d\pi/dS > 0$ and $dPaR/dS > 0$ is $[0, S^*]$. Within $[0, S^*]$, $\max(\pi)$ is at S^* since $d\pi/dS > 0$, and $\max(PaR)$ is also at S^* since $dPaR/dS > 0$. Therefore, for any point S^+ within $[0, S^*]$, $\pi(S^*) > \pi(S^+)$ and $PaR(S^*) > PaR(S^+)$.

Case A-2. $d\pi/dS < 0$ and $dPaR/dS < 0$

Since $PaR(\hat{S}) < \pi(S^*)$, the interval that satisfies both $d\pi/dS < 0$ and $dPaR/dS < 0$ is $[\hat{S}, 1]$. Within $[\hat{S}, 1]$, $\max(\pi)$ will be at \hat{S} since $d\pi/dS < 0$, and $\max(PaR)$ also will be at \hat{S} since $dPaR/dS < 0$. Therefore, for any point S^+ within $[\hat{S}, 1]$, we know that $\pi(\hat{S}) > \pi(S^+)$ and $PaR(\hat{S}) > PaR(S^+)$. \square

B. Proof of Proposition 2 (Efficient protection interval)

We assume that both $d\pi/dS$ and $dPaR/dS$ are decreasing and continuous. Also, from Eq. (3), we know that $PaR(\hat{S}) < \pi(S^*)$, where \hat{S} and S^* are the points where PaR and π are maximized. To satisfy the condition $(d\pi/dS)/(dPaR/dS) < 0$, $d\pi/dS$ and $dPaR/dS$ must be $d\pi/dS < 0$ and $dPaR/dS > 0$. Since $PaR(\hat{S}) < \pi(S^*)$, the interval which satisfies both $d\pi/dS < 0$ and $dPaR/dS > 0$ is $[S^*, \hat{S}]$. Within $[S^*, \hat{S}]$, $\max(\pi)$ will occur at S^* since $d\pi/dS < 0$, and $\max(PaR)$ will occur at \hat{S} since $dPaR/dS > 0$. Thus, at any point S^+ within $[S^*, \hat{S}]$, $\pi(S^*) > \pi(S^+)$ and $PaR(\hat{S}) < PaR(S^+)$. Thus, investments in customer information protection at level S within $[S^*, \hat{S}]$ will be subject to tradeoffs between π and PaR . \square

C. Proof of Proposition 3 (Under-estimation of risk)

Let x^{UE} be the information security loss severity distribution x for under-estimation (*UnderEst*), $\pi^{UnderEst}$ be the profit associated for under-estimation, and \hat{S} the protection level S which maximizes PaR . The level of profit will remain the same as in the base case. This is because under-estimation only affects the severity of the total financial loss distribution, $z(S, \alpha)$. Thus, $\max(\pi) = \max(\pi^{UnderEst})$. However, since $dz/dS < 0$, $dz^{UnderEst}/dS < 0$, and with $dz/dS < dz^{UnderEst}/dS$ from Eq. (1), it also will be the case that $dPaR/dS < dPaR^{UnderEst}/dS$. Therefore, $S^{UnderEst} = \arg\max(PaR) < \hat{S}$. \square

D. Proof of Proposition 4 (Proper penalty for government regulation)

Let us assume that government regulation (*GovReg*) requires some minimum information security protection level S^{GovReg} , with $S^* < S^{GovReg} < \hat{S}$. Since $d\pi/dS < 0$ and $PaR(\hat{S}) < \pi(S^*)$ within the *efficient protection interval* (from the proof of Proposition 2), $\pi(S^*) > \pi(S^{GovReg}) > PaR(S^{GovReg})$. Thus, in order to enforce the government's regulation effectively, the penalty associated with the regulation should be greater than $\pi(S^*) - \pi(S^{GovReg})$. For the case of $0 < S^{GovReg} < S^*$ and $\hat{S} < S^{GovReg} < 1$, see Proposition 5's proof. \square

E. Proof of Proposition 5 (Effective interval for government regulation)

Case E-1. $0 < S^{GovReg} < S^*$

Since $d\pi/dS > 0$ within this interval, $\pi(S^*) > \pi(S^{GovReg})$. Thus, government regulation in this interval will be ineffective.

Case E-2. $\hat{S} < S^{GovReg} < 1$

Since $dPaR/dS < 0$ within this interval, $PaR(\hat{S}) > PaR(S^{GovReg})$. Note that $PaR(\hat{S})$ is the maximum profit for the worst-case outcome. Let ε

be the probability of an information security breach at S^{GovReg} , where the confidence interval for $PaR(\alpha)$ is less than ε . From the first-order condition, $PaR(\hat{S}) - PaR(S^{GovReg}) > z(S, \alpha) - z(S^{GovReg}, \varepsilon)$ since $dPaR/dS < 0$ within $[\hat{S}, S^{GovReg}]$. Thus, government regulation in this interval also will not be effective. \square

F. Proof of Proposition 6 (Effective interval for self-regulation)

Let $S^{SelfReg}$ be the minimum level of information security protection that self-regulation *SelfReg* requires. Since self-regulation is not associated with any penalty, if $S^{SelfReg} < S^{GovReg}$, only government regulation *GovReg* will be effective. Thus $S^{SelfReg}$ must be greater than S^{GovReg} . For the case of $\hat{S} < S^{SelfReg} < 1$, see proof of Proposition 5. \square

G. Proof of Proposition 7 (Pass-on implementation cost effect)

Although we retain the assumption from Eq. (2) that the firm's revenue R is constant based on the quality of the information security offered to consumers, we include the firm's cost recovery of its technology investment by permitting the firm to charge a higher cost recovery-inclusive price. We capture such passed-on costs (*PassOn*) to customers in our analysis by rewriting revenue R inclusive of passed-on costs as R^{PassOn} . We further note that $R^{PassOn}(S)$ will be increasing in S ($dR^{PassOn}(S)/dS > 0$). Since $\pi^{PassOn}(S)/dS = \pi(S)/dS + dR^{PassOn}(S)/dS$, then $\pi(S)/dS < \pi^{PassOn}(S)/dS$. Similarly, we know that $PaR(S)/dS < PaR^{PassOn}(S)/dS$. Therefore, $\arg\max(\pi) < \arg\max(\pi^{PassOn})$ and $\arg\max(PaR) < \arg\max(PaR^{PassOn})$. \square

References

- [1] A. Acquisti, A. Friedman, R. Telang, Is there a cost to privacy breaches? An event study, in: D. Straub, S. Klein (Eds.), Proceedings of 27th Annual International Conference on Information Systems, Milwaukee, WI, 2006.
- [2] N. Ashrafi, J. Kuhlboer, Online privacy policies: an empirical perspective on self-regulatory practices, *Journal of Electronic Commerce in Organizations* 3 (4) (2005) 61–74.
- [3] N.F. Awad, M. Krishnan, The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization, *MIS Quarterly* 30 (1) (2006) 13–28.
- [4] Basel Committee on Banking Supervision, Operational Risk, Bank for International Settlements, Basel, Switzerland, 2001.
- [5] P.W. Best, Implementing Value at Risk, John Wiley and Sons, New York, NY, 1998.
- [6] H. Cavusoglu, B. Mishra, S. Raghunathan, The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers, *International Journal of Electronic Commerce* 9 (1) (2004) 69–104.
- [7] B. Crothers, Intel finds stolen laptops can be costly, *Nanotech – The circuits blog*, CNET News, San Francisco, CA, April 22, 2009, news.cnet.com/8301-13924_3-10225626-64.html?tag=mncol;title=current, March 1, 2011.
- [8] M.J. Culnan, How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use, *MIS Quarterly* 17 (3) (1993) 341–363.
- [9] M.J. Culnan, Protecting privacy online: is self-regulation working? *Journal of Public Policy and Marketing* 19 (1) (2000) 20–26.
- [10] M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, *Organization Science* 10 (1) (1999) 104–115.
- [11] M.J. Culnan, R.J. Bies, Consumer privacy: balancing economic and justice considerations, *Journal of Social Issues* 59 (2) (2003) 323–342.
- [12] M.J. Culnan, C.C. Williams, How ethics can enhance organizational privacy: lessons from the ChoicePoint and TJX data breaches, *MIS Quarterly* 33 (4) (2009) 673–687.
- [13] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions, *Information Systems Research* 17 (1) (2006) 61–80.
- [14] Federal Trade Commission, Self-regulation and privacy online, Prepared statement for the Subcommittee on Communications of the Committee on Commerce, Science and Transportation, United States Senate, Washington, DC, July 27, 1999, www.ftc.gov/os/1999/07/privacy99.pdf, current, March 1, 2011.
- [15] F-Secure, On-going targeted attacks against U.S. military contractors, blog post, San Jose, CA, January 18, 2010, www.f-secure.com/weblog/archives/00001859.html, current, March 1, 2011.
- [16] K.M. Gatzlaff, K.A. McCullough, The effect of data breaches on shareholder wealth, *Risk Management and Insurance Review* 13 (1) (2010) 61–83.
- [17] L.A. Gordon, M.P. Loeb, The economics of information security investment, *ACM Transactions on Information and System Security* 5 (4) (2002) 438–457.
- [18] V. Gurbaxani, S.J. Whang, The impact of information systems on organizations and markets, *Communications of the ACM* 34 (1) (1991) 59–73.

[19] I. Hann, K. Hui, S.T. Lee, I.P.L. Png, Overcoming online information privacy concerns: an information processing theory approach, *Journal of Management Information Systems* 24 (2) (2007) 13–42.

[20] K.J.S. Hoo, How much is enough? A risk management approach to computer security, Ph.D. dissertation, Graduate School of Engineering, Stanford University, Palo Alto, CA, 2000.

[21] K.L. Hui, H.H. Teo, S. Yong, S.Y.T. Lee, The value of privacy assurance: an exploratory field experiment, *MIS Quarterly* 31 (1) (2007) 19–33.

[22] Internet Security Alliance, Cyber security social contract, Arlington, VA, January 2010, www.isalliance.org/index.php?option=com_content&task=view&id=173&Itemid=335, current, July 10, 2010.

[23] P. Jorion, *Value at Risk: The Benchmark for Controlling Market Risk*, 3rd Ed. McGraw-Hill Professional Book Group, Blacklick, OH, 2007.

[24] R.J. Kauffman, R. Sougstad, Risk management of contract portfolios in IT services: the profit-at-risk approach, *Journal of Management Information Systems* 25 (1) (2008) 17–48.

[25] D.J. Kim, D.J. Ferrin, H.R. Rao, A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents, *Decision Support Systems* 44 (2) (2008) 544–564.

[26] J.K. Lee, H.R. Rao, Perceived risks, counter-beliefs, and intentions to use anti-counterterrorism Web sites: an exploratory study of government-citizens online interactions in a turbulent environment, *Decision Support Systems* 43 (4) (2007) 1431–1449.

[27] C. Liu, K.P. Arnett, An examination of privacy policies in Fortune 500 Web sites, *Mid-American Journal of Business* 17 (1) (2002) 13–21.

[28] N.K. Malhotra, S.S. Kim, J. Agarwal, Internet users' information privacy concerns: the construct, the scale, and a causal model, *Information Systems Research* 15 (4) (2004) 336–355.

[29] A. Mas-Colell, M.D. Whinston, J.R. Green, *Microeconomic Theory*, Oxford University Press, New York, NY, 1995.

[30] G.R. Milne, A.J. Rohm, S. Bahl, Consumers' protection of online privacy and identity, *Journal of Consumer Affairs* 38 (2) (2004) 217–232.

[31] Open Security Foundation, Data loss statistics, Glen Allen, VA, July 10, 2010, www.dataloss.org, current, March 1, 2011.

[32] B. Otjacques, P. Hitzelberger, F. Feltz, Interoperability of e-government information systems: issues of identification and data sharing, *Journal of Management Information Systems* 23 (4) (2007) 29–52.

[33] G.A. Paleologo, Price-at-risk: a methodology for pricing utility computing services, *IBM Systems Journal* 43 (1) (2004) 20–31.

[34] H.H. Panjer, *Operational Risks: Modeling Analytics*, John Wiley and Sons, Hoboken, NJ, 2006.

[35] P.A. Pavlou, H. Liang, Y. Xue, Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective, *MIS Quarterly* 31 (1) (2007) 105–136.

[36] PayPal, PayPal security key, San Jose, CA, www.paypal.com/cgi-bin/webscr?cmd=xpt/Marketing_CommandDriven/securitycenter/PayPalSecurityKey-outside, current, March 1, 2011.

[37] PriceWaterhouseCoopers, Safeguarding the new currency of business: findings from the 2008 Global State of Information Security Study, White paper, Security Advisory Services, New York, NY, 2008.

[38] Privacy Rights Clearinghouse, Chronology of data breaches: security breaches 2005-present, San Diego, CA, July 7, 2010, www.privacyrights.org/ar/ChrondataBreaches.htm, current, March 1, 2011.

[39] K.S. Schwaig, G.C. Kane, V.C. Storey, Compliance to the Fair Information Practices: how are the Fortune 500 handling online privacy disclosures? *Information Management* 43 (7) (2006) 805–820.

[40] H.J. Smith, S.J. Milberg, S.J. Burke, Information privacy: measuring individuals' concerns about organizational practices, *MIS Quarterly* 20 (2) (1996) 167–196.

[41] G.J. Stigler, The economics of information, *Journal of Political Economy* 69 (3) (1961) 213–225.

[42] Sungard Availability Services, Customer success story: the NYBOT wanted to improve its information availability capabilities to provide uninterrupted operations, Case study, Wayne, PA, 2008, www.availability.sungard.com/Documents/NYBOT%20CaseStudy.pdf, current, July 10, 2010.

[43] N.N. Taleb, *The Black Swan: The impact of the Highly Improbable*, Random House, New York, NY, 2007.

[44] C. Van Slyke, J.T. Shim, R. Johnson, J. Jiang, Concern for information privacy and online consumer purchasing, *Journal of the Association for Information Systems* 7 (6) (2006) 415–443.

[45] J. Wang, A. Chaudhury, H.R. Rao, A value-at-risk approach to information security investment, *Information Systems Research* 19 (1) (2008) 102–120.



Yong J. Lee is in the Information Systems Ph.D. program at the W. P. Carey School of Business at Arizona State University. He earned a B.A. in Computer Science and Engineering from Hongik University in Seoul, South Korea, and an MBA in Information Systems from the University of Washington. His research interest is information privacy and security issues in business and e-commerce. He has been working with financial economics, and a risk valuation approach known as value-at-risk. He has explored economic and financial perspectives on organizational strategy and decision-making for investments in IT and business processes that are used to protect consumer information security.



Robert J. Kauffman is a Visiting Professor of IS and Strategy at the School of Information and the Lee Kong Chian School of Business at Singapore University. He is also a Distinguished Visiting Fellow at the Glassmeyer-McNamee Center for Digital Strategies, Tuck School of Business, Dartmouth College. Previously, he served on the faculty at New York University, the University of Minnesota and Arizona State University. He also visited the University of Rochester and the Federal Reserve Bank of Philadelphia, and worked in international banking and finance in New York City prior to beginning his academic career. His graduate degrees are from Cornell University and Carnegie Mellon University, and his undergraduate degree is from the University of Colorado, Boulder. His research interests span the economics of IS, pricing and mechanism design on the Internet, competitive strategy, and theory development, modeling and empirical methods for IS and e-commerce research, all in contexts that emphasize senior management issues. His publications have appeared in *Management Science*, *Information Systems Research*, *MIS Quarterly*, the *Journal of Management Information Systems*, *Organization Science*, the *Review of Economics and Statistics*, *Decision Sciences*, and other journals.



Ryan Sougstad is an Assistant Professor of Business Administration at Augustana College in Sioux Falls, South Dakota, which he joined in 2009. He spent seven years with IBM in client sales and marketing, and at IBM Research's Business Informatics group. His research on the valuation and risk management of IT-enabled services has appeared in the *Journal of Management Information Systems* and *International Journal of Services Science*. He holds a B.A. degree from the University of Kansas, an MBA from the UT Dallas, and a Ph.D. in Information and Decision Sciences from the University of Minnesota.