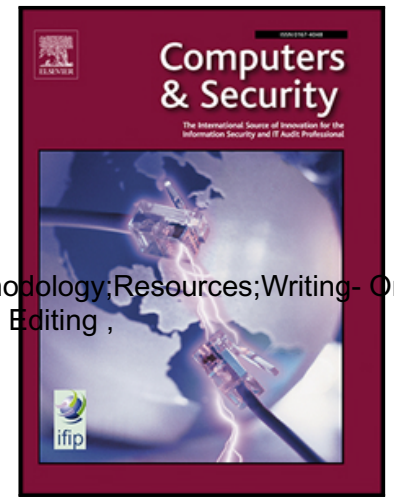

Shall We Follow? Impact of Reputation Concern on Information Security Managers' Investment Decisions

Xiuyan Shao Conceptualization;Model development;Data collection;Methodology;Resources;Writing- Original draft
Mikko Siponen Conceptualization;Data collection;Writing- Reviewing and Editing ,
Fufan Liu Data analysis

PII: S0167-4048(20)30237-6
DOI: https://doi.org/10.1016/j.cose.2020.101961
Reference: COSE 101961

To appear in: *Computers & Security*

Received date: 3 February 2020
Revised date: 8 June 2020
Accepted date: 13 July 2020

Please cite this article as: Xiuyan Shao Conceptualization;Model development;Data collection;Methodology;Resour
Mikko Siponen Conceptualization;Data collection;Writing- Reviewing and Editing ,
Fufan Liu Data analysis , Shall We Follow? Impact of Reputation Concern on Information Security Managers' Investment Decisions, *Computers & Security* (2020), doi: https://doi.org/10.1016/j.cose.2020.101961

Shall We Follow? Impact of Reputation Concern on Information Security Managers' Investment Decisions

Xiuyan Shao
School of Economics and Management, Southeast University, Nanjing 211189, Jiangsu, China

Mikko Siponen
Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, FI 40014, Finland

Fufan Liu
Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, FI 40014, Finland

Information about corresponding author:
Name: Xiuyan Shao
Email: xiuyan_shao@163.com
Full postal address: School of Economics and Management, Southeast University, Nanjing 211189, Jiangsu, China
Tel. +8615759860982

E-mail addresses: xiuyan_shao@163.com (X. Shao), mikko.t.siponen@jyu.fi (M. Siponen), fuliu@student.jyu.fi (F. Liu)

Keywords: Information security investment; decision making; uncertainty; discount own information; reputational herding

Shall We Follow? Impact of Reputation Concern on Information Security Managers' Investment Decisions

Abstract: Information security (infosec) is important for organizations. While budgeting for infosec is a crucial resource allocation decision, infosec managers may choose to follow other fellow experts' recommendations or baseline practices. The present paper uses reputational herding theory to explain the decision made by infosec managers to use a "let's follow others" strategy in this context. Based on a sample of 106 organizations in Finland, we find that infosec managers' ability to accurately predict the benefit of infosec investment, as well as their reputations, have significant effects on motivating them to discount their own information. Infosec managers' discounting of their own information, together with the strength of information that relates to infosec investment and mandatory requirements, motivates infosec investment. Our empirical results highlight the "let's follow others" strategy as an important alternative to cost–benefit analysis in terms of budgeting for infosec investment.

Keywords: Infosec investment; decision making; uncertainty; discount own information; reputational herding

1. Introduction

Information security (infosec) has become an important issue for organizations (Von Solms & Van Niekerk 2013). The cost of managing and mitigating security breaches is estimated at $11.7 million per year per affected organization (Cost of Cybercrime Study 2017[1]). Many studies also report that infosec events have a statistically significant effect on organizations' stock prices (Spanos and Angelis 2016).

How to budget for infosec is a topic frequently mentioned in the literature. To determine how much to invest, previous studies propose the use of expected utility theory (e.g., Gordon and Loeb 2002, Huang et al. 2014) and game theory (e.g., Cavusoglu et al. 2008, Qian et al. 2018) to estimate the optimal investment level. To assess the efficiency of infosec investment, previous studies develop analytical tools, like net present value (NPV) and return on investment (ROI), to facilitate security investment decision making (e.g., Kumar et al. 2008). Whichever approach is selected, the existing research relating to infosec budgeting involves estimating the costs and benefits of such activities.

However, these studies, although they provide a quantitative basis with which infosec managers can weigh the costs and benefits of investment, are difficult to apply in organizations (Weishäupl et al. 2018). This is mainly because the benefits of infosec investment are uncertain and intangible. Typically, infosec investment is done neither for revenue generation nor cost reduction (Baskerville 1991). Organizations allocate resources for infosec to prevent security threats, and often the best outcome is that "nothing happens" (Menon and Siponen 2019). Besides, generally, there is a lack of reliable statistics on actuarial loss (Baskerville 1991; Wood and Parker 2004). Therefore, quantifying the benefits of infosec investment and applying such cost–benefit in practice is confronted with many difficulties in practice.

Further, previous studies on infosec investment have mainly focused on providing analytical tools for estimating the optimal level of infosec investment and evaluating its efficiency. However, they fail to investigate how organizational and psychological factors may influence decision making in this context. It is noted that, in practice, when making infosec investment decisions, managers often follow "smart cookies," such as other infosec experts and their recommendations; thus, the infosec budget may be driven by best practices in the industry instead of formal quantifications of its benefits (Gordon and Loeb 2006). For example, following the recommendations from ISO-IEC 2700, 51% of respondent companies implemented security awareness and training programs (Global State of Information Security Survey 2015)[2]. Managers may also follow other organizations' practice in adopting infosec technology, driven by a tendency to chase the hottest information technology (IT; Wang 2010).

---

1 https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

2 http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf

In order to address these limitations and thereby enrich our understanding of infosec managers' following decision in infosec investment, this study develops two research questions: *Under what conditions does following decision occur in infosec investment? How does following decision influence infosec investment?* To approach these research questions, this study will present a research model based on a reputational herding model. Our empirical results support that the "let's follow others" strategy is an important alternative to cost–benefit analysis in budgeting for infosec investment. Our results also reveal the factors that influence following intention.

The next section reviews the literature on budgeting for infosec investment and discusses the uncertain nature of such investment. The third section develops our research model, and the fourth outlines our methodology. These sections are followed by a discussion of the findings of this study. The final section provides conclusions and avenues for future research.

2. Previous work on budgeting for infosec investment

2.1 Estimating the optimal level of infosec investment

Studies have proposed decision-theoretic and game-theoretic approaches to estimating how much to invest in infosec. A decision-theoretic approach compares the risk and return of infosec investments. The risk is usually measured by the likelihood of a loss event and the cost of such an event (Schechter 2005). For example, Gordon and Loeb (2002) suggest comparing the cost of infosec investment with the potential loss from a security breach to analyze the optimal level of investment in infosec for a risk-neutral organization. Several studies extend the Gordon and Loeb model by relaxing or modifying some restrictive assumptions (e.g., Cremonini and Nizovtsev 2006; Hausken 2006; Ogut et al. 2005). Nevertheless, the core of the model, comparing cost with the potential loss of security breaches, remains unchanged. Similarly, Huang et al. (2008) propose adopting the expected utility theory, which considers corporate wealth and the potential loss due to security breaches. Expected utility theory is also adopted by other studies (e.g., Mayadunne and Park 2016).

Game theory models the possible outcomes of actions and reactions between a limited number of players. In contrast to the decision-theoretic approach, the game-theoretic approach takes the behavior of attackers into account, considering that an organization's infosec investment would influence the behavior of attackers and vice versa. Methodologically, game theory is better suited for modeling decision making about infosec investment, because infosec investment involve actions and reactions between the organization and the attack (Huang et al. 2014). A number of studies have applied the game-theoretic approach. Cavusoglu et al. (2008) compare it to decision-theoretic approaches and suggests that the sequential game results in the maximum payoff for the firm. Considering that hackers may disseminate security knowledge within a hacker population over time, Gao et al. (2013) apply a simultaneous and sequential differential game, finding that the firm invested the most in the sequential differential game. The game-theoretical approach is also employed in modeling the actions and reactions of two allied firms. Studies show that when two firms share substitutable knowledge, they fall into a prisoners' dilemma and invest lower than is optimal in infosec (Liu et al. 2011; Qian et al. 2018).

2.2 Evaluating the efficiency of infosec investment

After determining the optimal level of investment, the next question to answer is where to invest, which can be viewed as a process of selecting and prioritizing security countermeasures. To select infosec countermeasures, Viduto et al. (2012) propose a risk assessment and optimization model. Moreover, Sawik (2013) formulates the selection problem based on the countermeasures' effectiveness, costs, and attack probabilities. Huang and Behara (2013) consider heterogeneous attacks with distinct characteristics and propose an analytic model for the allocation of a fixed budget for infosec investment. Prioritizing security measures can be viewed as assessing the effectiveness of such investment. From this point of view, traditional management and financial tools, such as cost–benefit analysis (Gordon and Loeb 2006), ROI, NPV, and internal rate of return, are often applied (e.g., Bojanc and Blazic 2008; Gupta et al. 2008; Pursor 2004; Tsiakis and Stephanides 2005). In addition, analytical frameworks have been proposed. By adopting the analytic hierarchy process (AHP), a rating method that employs pairwise comparisons among different security technologies, Bodin et al. (2005) determine the allocation of infosec investment budget. Soo Hoo (2000) proposes a decision analysis framework based on a risk-management approach to evaluate various IT security policies (see also Kinnunen et al. 2020). Based on a threat-scenario approach, Schechter (2005) identifies the strengths and forecasted the risks in security software. In addition, Arora et al. (2004) propose to associate the bypass rate[3] with the infosec technologies.

2.3 The uncertain nature of infosec investment

Infosec investments usually do not generate economic benefits in the sense of revenue generation or cost reduction. The value of infosec investment lies in "preventing something from happening" rather than "making something happen" (Huang et al. 2007, p. 55). When no security attacks occur, it is sometimes difficult to determine whether the investment is working or the organization is simply enjoying good luck. Therefore, it is difficult to quantify the benefits of security investments in a reliable manner.

Furthermore, the cost of infosec breaches is also often ambiguous. Lee et al. (2011) argue that it is difficult to quantify monetary damages related to customers. When an organization's system is hacked, it is difficult to know with absolute certainty who the hacker is and what information was accessed. The density of network traffic can be used to estimate the amount of data affected, but it is difficult to precisely identify the leaked data and anticipate how it will be used. The difficulties do not end here. Often, the value of leaked or damaged information is difficult to estimate in financial terms, especially before the risk is realized. If, for example, hackers break one's password, can one determine an exact monetary loss? If some data ends up with unauthorized parties, it may be highly difficult to quantify such damages. Scholars have suggested that the benefits and costs of infosec are based on guesswork (Baskerville 1991; Wood

[3] A bypass rate is the rate at which an attack results in observable damage to the organization (Arora et al. 2004)

and Parker 2004).

The tools proposed by previous literature (expected utility theory, cost–benefit analysis, financial analysis tools, analytical frameworks, and game theory) to budget for infosec investment all involve estimating the risks, the costs of countermeasures, and the probabilities of attack to conduct a cost–benefit analysis. Applying game theory requires knowledge of attacker's utility parameters, which is much more difficult to obtain. The uncertain nature of infosec investment thus prevents the use of the analytical tools proposed by previous scholarship for decision making. We postulate that an infosec investment decision is not always made through cost–benefit analysis; in contrast, "following" may be a good alternative. In the next section, we present the theoretical framework derived from reputational herding theory.

3. Theoretical development

3.1 Reputation-based herding behavior

Herding behavior is a term originally used to describe investment decision makers who follow the decisions of earlier adopters due to a lack of information (Kauffman and Li 2003; Swanson and Ramiller 2004). It has been observed in situations such as software adoption (Duan et al. 2009; Sun 2013), financial forecasting (Bernhardt et al. 2009), management fashion (David and Strang 2006), and general purchasing decision making (Shen et al. 2014). As one type of herding behavior, **reputation-based herding behavior**, describes the situation wherein managers with good reputations herd to protect their current status (Scharfstein and Stein 1990).

It is necessary to distinguish how reputation-based herding behavior from other similar concepts, namely network externality, subjective norm, and information cascades. *Network externality* refers to an effect whereby "the value of a technology increases as the number of its users increases" (Li 2004, p. 94). When the number of users increases, the earlier users receive increased payoffs. To differentiate reputational herding from network externalities, it is first noted that value adding is not necessary in reputational herding. The main motivations for reputational herding are overcoming uncertainty and maintaining reputation. At the same time, the two concepts share different theoretical backgrounds. Reputational herding originates from an agency problem, while network externalities are rooted in economies of scale.

A *subjective norm* defines a person's perception that most people who are important to him think he should or should not perform the behavior (Fishbein and Ajzen 1975, p. 320). Reputational herding behavior differs from subjective norms regarding where and how the information is accessed. First, a subjective norm comes from other people who are important to a person, while reputational herding behavior accesses information from broader sources, for example, other companies' security investment decisions. Second, subjective norms depend primarily on *messages* received from others, while reputational herding behavior depends on *observations* of other people's behavior (Sun 2013).

The concept of *information cascades* is another notion that can be confused with reputational herding. An information cascade refers to an infinite sequence of individuals ignoring their private information when making a decision (Anderson and Holt 1997). This differs from reputation herding behavior in a couple of ways (Celen and Kariv 2004). First, reputational herding includes

reputational concerns, compared with an information cascade for which reputation is not necessarily a factor. In turn, in reputational herding, individuals' behaviors may still provide information. When acting according to reputational herding, the behavior is fragile in the sense that a strong signal may cause the behavior to shift. In contrast, an information cascade is stable; that is, no signal can cause a change in the pattern of behavior.

3.2 Research model and hypotheses

To build a research model for reputation-based herding behavior in an infosec investment, this study refers to Scharfstein and Stein's (1990) work on reputational herding theory. The main aspect of reputational herding theory is that, when an investment decision maker is uncertain about their ability to decide on an investment, the investor may see conforming to other investment professionals as a good choice. The reputational herding theory is chosen as the theoretical lens mainly because it assumes that there are systematically unpredictable components of the investment value, which is consistent with the uncertain nature of infosec investment, as discussed in section 2.3.

There are three primary conditions under which reputation-based herding behavior can occur: uncertainty about the decision, observation of others' actions, and concern about reputation. First, people are more likely to herd when they are uncertain about the decision being made due to incomplete information (Bikhchandani and Sharma 2000). Second, observing that many people have made the same decision promotes feelings of security and allows reputational herding behavior to occur (Bikhchandani et al. 1992). Third, managers' concern about their reputation also leads to herding intentions (Scharfstein and Stein 1990).

The reputational herding theory is revised in two ways to build our research model. First, we use the managers' ability to accurately predict the value of an infosec investment to represent uncertainty about the decision. We made this change because the studies that focus on uncertainty mostly relate to systems' complexity, performance, and quality (Lee and Joshi 2017). Thus, uncertainty is usually operationalized to represent the level of uncertainty anxiety experienced by users related to a change, which refers to psychological uncertainty and associated stress. In contrast, our reputational herding model does not include anxiety; rather, it considers whether the manager is able to calculate the costs and benefits associated with the infosec investment. Second, the observation of others' actions was replaced with the strength of the information, which shows how the decision maker interprets their observation. Our research model is shown in Figure 1.

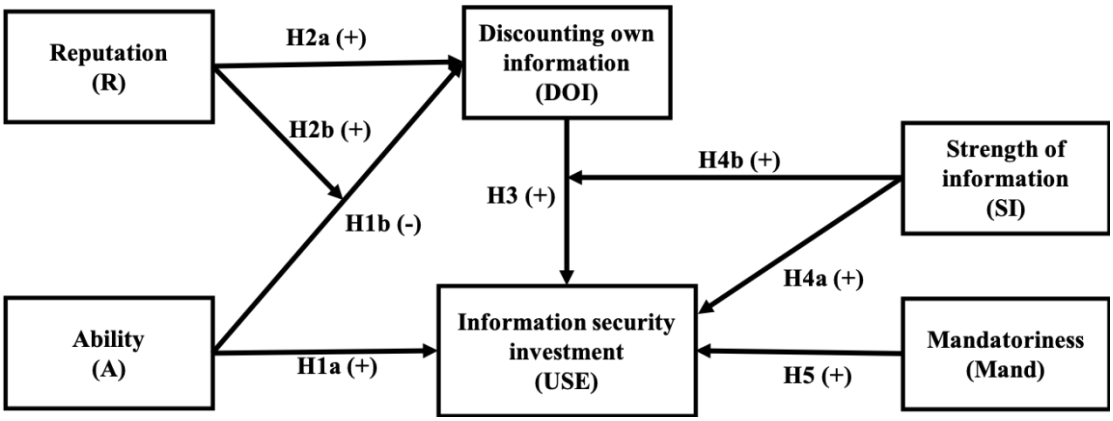

Figure 1. Research model.

3.2.1 Ability to predict the value of infosec investment

With incomplete information, a person may perceive an inability to make an accurate prediction on a certain topic (Milliken 1987). In the infosec investment context, there are several unpredictable components, which are as follows: (i) it is usually difficult to predict when hackers' next attacks will occur, especially in terms of successful, expensive, and destructive attacks, (ii) it may be difficult to assess the damage caused by an infosec breach or attack, and (iii) it is difficult to guarantee that the infosec investment will efficiently prevent the intended breaches. Previous research in other contexts has shown that, when people feel uncertain about a decision, they are likely to discount their own information (Sun 2013) and follow that procured by others (Bikhchandani and Sharma 2000; Graham 1999; Zwiebel 1995). We suggest that the same applies to the infosec investment context in the following hypotheses:

H1a: A manager's ability to accurately predict the value of an infosec investment is significantly associated with the infosec investment.

H1b: A manager's ability to accurately predict the value of an infosec investment is negatively associated with discounting their own information.

3.2.2 Reputation

When managers gain a reputation, they may also gain autonomy, power, and career success (Gioia and Sims 1983; Pfeffer 1992; Zinko et al. 2012). Reputation also affects performance evaluations, promotions, and compensation (Ferris et al. 2003); therefore, managers intend to maintain a good reputation to secure these benefits.

According to reputational herding theory, a manager's reputation is accessible in the labor market by checking whether a manager makes smart decisions. A smart decision is usually evaluated in terms of whether it is either a profitable decision for the organization or one similar to those made in other organizations (Scharfstein and Stein 1990). Thus, managers who have reputation concerns generally avoid making unwise decisions. For example, Brandenburger and Polak (1996) suggest that a manager with a reputation incentive may make investment decisions that are consistent with a previous belief regarding the profitability of a project, even if the firm has superior information compared with that available to the public.

The uncertain nature of an infosec investment prevents the accurate prediction of its benefits; therefore, it is difficult to evaluate whether a manager's decisions are profitable. Under such circumstances, infosec managers or decision makers who have reputational concerns tend to make decisions that are consistent with others' decisions to maintain their reputations. Based on this, we construct the following hypotheses:

H2a: A manager's reputation is positively associated with discounting their own information.

H2b: Reputation enhances the relationship between the ability of a manager and their decision to discount their own information.

3.2.3 Effect of discounting one's own information on infosec investment

Discounting one's own information refers to the notion that a decision maker relies less on their initial beliefs in forming a new, adjusted belief (Sun 2013). The reputational herding model suggests that managers may imitate others by discounting their own information to avoid being considered incapable (Graham 1999; Scharfstein and Stein 1990). Consequently, herding is considered a legitimate strategy for people with good reputations to protect their status (Graham 1999). In the context of infosec investment, a manager may rely less on their initial beliefs and choose to imitate others in making an infosec investment decision. Even if the decision turns out to be inefficient, the manager is not alone in having made the wrong decision, and thus shares the blame with others who have also accepted or rejected an efficient infosec investment. Thus, this strategy will potentially spare the manager's reputation. Based on this, we construct the following hypothesis:

H3: Discounting one's own information is significantly associated with a manager's infosec investment decisions.

3.2.4 Strength of the information

As one of the three conditions for reputation-based herding behavior, observation of others' action refers to the information that shows a probability of deriving profit from an investment (Scharfstein and Stein 1990). The reputational herding model suggests that, when such information is strong, the decision maker is more inclined to discount their own information and make the same decision as the majority. We take Hirshleifer's (2001) conceptualization and define the strength of information as the extremeness of information showing the probability of deriving profit from an investment. Based on this, we construct the following hypotheses:

H4a: The strength of the information is positively associated with infosec investment.

H4b: The strength of the information enhances the relationship between discounting one's own information and infosec investment.

3.2.5 Mandatory requirements

Since people have increasingly realized the importance of information, governments have enacted laws to protect it, such as the Gramm–Leach–Billy Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act's Security Rule, the Sarbanes–Oxley Act, and the EU General Data Protection Regulation. The complexity and challenges faced by infosec managers result in multiple types of compliance with requirements from industry, state, and federal bodies. Research has suggested that mandatory requirements ensure security compliance (e.g., Boss et al. 2009). When infosec vendors provide products that comply with mandatory requirements, infosec managers are more likely to invest in those products. This finding in the literature leads to the formulation of the following hypothesis:

H5: Mandatory requirements are positively associated with a manager's infosec investment.

4. Research method

4.1 Measures and pilot test

Appendix B lists the measures utilized in this study. Wherever possible, we utilized instruments that were previously validated. The items for discounting one's own information were adopted from Sun (2013), items for reputation were adopted from Zinko et al. (2012), items to measure mandatory requirements were adopted from Boss et al. (2009), and items to measure infosec management standards application were adopted from Beaudry and Pinsonneault (2010). We adopted previous instruments after carefully considering the infosec investment context. The items were assessed using a 7-point Likert scale.

Since there are no previously validated instruments for ability and strength of information, we developed new instruments for them. Appendix A describes in detail how the instruments were developed, following the procedure set forth by Mackenzie et al. (2012). The instrument development process resulted in three items for ability and three items for strength of information (see Appendix B). Content validity was first checked through a literature review, followed by a content validity expert panel formed by eight researchers who are skilled in quantitative research methods.

Our study was pretested by ten faculty members and graduate students to ensure that the questions matched the selected theories and that the questions were readable. After that, the survey instrument was pilot tested by 32 responses at one university in Finland. Our pilot study used a paper-based questionnaire that consisted of questions and a section in which respondents could leave remarks and feedback about the questions asked. We used these responses to ascertain the validity of the questions and to identify any points of confusion within the survey. We assessed the reliability of measurement items for each construct by using Cronbach's α; we assessed convergent and discriminant validity by using factor loadings. Measurement items with unacceptably low Cronbach's α were rephrased or dropped.

4.2 Data collection

The final data were collected from infosec managers in Finland, a developed country in which an increasing number of organizations are aware of infosec issues. The survey was administrated in Finnish, as it is the primary language of all the participants in our study.

We called companies from a company list provided by the Finnish Business Administration, and we asked for the name of the chief information security officer or a similar individual responsible for infosec management. We sent paper-based surveys to these infosec managers. As an incentive to participate, we offered to provide them with a report of our findings upon conclusion of the study.

We used infosec management standard implementation to represent infosec investment in our survey. On the one hand, applying guidelines from infosec management standards involves several steps, including: establishing the context, scope, and objective for infosec management; conducting a risk assessment for the organization; implementing controls for mitigating risks; conducting staff awareness training; and reviewing, monitoring, and conducting an internal audit.

All the steps involve time and effort, which can be treated as intangible investments in infosec. On the other hand, to obtain a certification in infosec management standards, an organization can consider paying, which can be treated as a tangible investment in infosec.

At the beginning of the survey, we asked the participants to think about one infosec management standard (for example ISO-IEC 27001, ISO-IEC 27002, or guidelines based on these standards; Siponen & Willison, 2009; Von Solms 1999) that they had applied in their organizations. In doing so, this survey situated participants in the context of applying infosec management standards. Participants were then asked to provide answers regarding the constructs used in our research model. They returned the completed surveys using envelopes with pre-paid postage.

The survey was sent to 1,042 infosec managers or persons responsible for infosec management. In total, 110 responses were obtained, four of which did not answer a large portion of the questions and were dropped. The proportion of missing values for each variable amounted to 0.92%, showing that the rest of the responses could be used. Missing values were replaced with a median value. The variance for each respondent ranged from 0.5 to 2.2, demonstrating that the respondents did not answer the questions arbitrarily. The skewness and kurtosis values were between -1 and 1, revealing the normality of the data. No outliers were found in the data. We used this final dataset of 106 respondents for our analysis. According to Barclay et al.'s (1995) "rule of ten" heuristic, the required sample size for our model was 60. Therefore, we deem this sample size large enough.

The survey was anonymous: no identifying information of any kind was gathered from the participants. It was also clearly communicated to the respondents that independent university researchers would analyze the results of their surveys. Our respondents' average experience in infosec management was over 10 years, showing that they had firsthand knowledge of infosec management. Table 1 summarizes the respondents' education level and the sizes of their organizations, and these results suggest that the sample was heterogeneous.

Table 1. Descriptive Statistics of the Respondents

Education	Frequency (%)	Size of organization (# of employees)	Frequency (%)
Vocational	7 (6.60)	1–100	9 (8.49)
College level	19 (17.92)	101–249	14 (13.20)
Bachelor's degree	28 (26.42)	250–499	20 (18.87)
Master's degree	49 (46.23)	500–999	19 (17.92)
Ph.D.	3 (2.83)	1,000+	44 (41.51)

4.3 Data analysis and results

4.3.1 Measurement model

To validate the measurements, we tested convergent validity and discriminant validity. First, all our item loadings were significant at a p-value < 0.001 (see Table C1 in Appendix C), exhibiting convergent validity (Gefen and Straub 2005; Gefen et al. 2011). We also examined the cross-loadings, and each loading for a latent variable was substantially higher than those for other latent variables (see Table C1 in Appendix C), which also indicates convergent validity (Kock 2010). To establish discriminant validity, we first determined that there was no significant overlap of factor loadings between the constructs (see Table C1 in Appendix C; Gefen and Straub 2005; Gefen et al. 2011). We also examined the square roots of the average variance extracted against the latent variable correlations (see Table C2 in Appendix C; Gefen and Straub 2005; Gefen et al. 2011). The results also showed strong discriminant validity.

Since all the data was collected using a single questionnaire, the common-method bias problem needs to be examined. Each method developed for testing common-method bias has limitations (Chin et al. 2012); therefore, we used two approaches. First, we used Harmon's factor analysis test. This approach produced 19 factors, the largest of which only accounted for 51% of the variance, showing a low likelihood of common-method bias. The second approach we used was examining the correlation matrix of the constructs. The correlations were all below the 0.90 threshold, which proves a low likelihood of common-method bias.

To establish reliability, we examined the composite reliability of the constructs and Cronbach's α. Both the composite reliability and Cronbach's α coefficients were above 0.7 (see Table C3 in Appendix C), showing that all of our constructs exhibited high levels of reliability (Hair et al., 2012). To summarize, our model data meets the validation standards expected in behavioral research (Gefen and Straub 2005; Gefen et al. 2011; Straub et al. 2004).

4.3.2 Structural model

To test our structural model, we performed both partial least squares (PLS, using SmartPLS version 3.0) and covariance-based structural equation modeling (SEM) using R 3.5.2 and its lavaan 0.6-3 package (Rosseel 2012). Covariance-based SEM is more conservative than the PLS method. As the results from both methods were somewhat similar with no large differences, we report the findings from the covariance-based modeling. We generated a bootstrap with 500 resamples for the PLS-based model. Table 2 reports the results of the structural model (see section 5); these results are obtained from the more conservative test afforded through covariance-based SEM. For the results, the overall model fit indices were within the expected parameters, which

were as follows: $\chi^2_{df\ (92)}$ = 130.32**, χ^2/df = 1.42, root mean square error of approximation (RMSEA) = 0.063 (90% confidence interval 0.035–0.086), CFI = 0.966, TLI = 0.955, and SRMR = 0.077 (*p < .05;** p < .01;*** p < .001). Although the model χ^2 test was significant, the normed χ^2/df (Wheaton et al. 1977) was within the range of good fit (Hooper 2008, p. 54). According to Kline (2011, pp. 204–210) and Hooper (2008), all other fix indexes (RMSEA, CFI, TLI, SRMR) indicate a fairly good fit. In addition, the standardized residuals did not suggest any substantive misspecification.

5. Discussion

5.1 Summary of findings

Seven of the eight hypotheses were supported by our analysis. Although both the dependent variables have significant paths leading to them, the amount of explained variance differs greatly between them. While 54.5% of the variance in infosec investment was explained by our model, only 20.2% of the variance in discounting one's own information was explained. Table 2 summarizes these findings.

Table 2. Summary of the Results

Hypothesis	Coef.	*t*	*p*	Result
H1a: Ability → Information security (infosec) investment	0.388	4.51	0.000	Supported
H1b: Ability → Discounting own information	−0.138	1.14	0.021	Supported
H2a: Reputation → Discounting own information	0.481	4.09	0.000	Supported
H2b: Reputation moderates: Ability → Discounting own information	0.303	2.69	0.001	Supported
H3: Discounting own information → Infosec investment	0.236	3.04	0.001	Supported
H4a: Strength of information → Infosec investment	0.189	2.35	0.019	Supported
H4b: Strength of information moderates: Discounting own information → Infosec investment	0.059	0.42	0.679	Not Supported
H5: Mandatoriness → Infosec investment	0.217	2.69	0.001	Supported

When infosec managers make decisions about investments, the ability to accurately predict the benefit of the investment is central to the decision-making process. This ability positively influences the infosec investment (H1a) and negatively influences security managers' intention to discount their own information (H1b). Reputation also plays an important role during this process: infosec managers with a better reputation are more inclined to discount their own information (H2a), especially those who have lower ability to predict the benefit from infosec investment (H2b).

When infosec managers observe a considerable number of organizations that have made the same infosec investments, the managers are more likely to make that investment decision (H4a). We find that the strength of the information does not enhance the relationship between discounting one's own information and infosec investment (H4b). Finally, we find that mandatory government or industry requirements strongly affect infosec investments (H5).

Based on our empirical results, we next highlight two findings. First, we explore factors other than cost–benefit analytical tools influencing infosec investment decisions. We find that discounting one's own information is significantly associated with infosec investments (H3). The observation of many organizations making the same infosec investments increases the likelihood of a manager making that investment decision (H4a). This result supports our assertion that there are other motivations for infosec investment than benefit-driven interests determined via financial analytical tools.

The second finding is that when the uncertain nature of infosec investment encourages managers to apply a herding strategy, reputational concern plays a role in the process. This effect is illustrated in our theoretical model (H2a, H2b) and shown in detail in Table 2. When facing uncertainty in infosec investment, managers with better reputations and lower analytical ability are more willing to follow others. Finally, there is a strong effect of mandatory government or industry requirements on infosec investments (H5).

5.2 Implications for research

Our results highlight a number of opportunities for future research on infosec investment decision making. First, due to the uncertain nature of infosec investment, theories that address decision making under conditions of uncertainty can be used to examine influential factors other than reputation. For example, Black (1986, p. 529) suggests, "Noise in the sense of a large number of small events is often a causal factor much more powerful than a small number of large events can be." In stock markets, when investment managers (or individual stock buyers) are uncertain about the results of one stock and lack necessary information for analyzing its potential benefits (or losses), they may invest based on noise. The advice of gurus can be deemed as one example of such noise (Shleifer and Summers 1990). Evidence shows that investors do tend to follow experts' opinions (Menkhoff 1998). In infosec investment, managers may be more willing to invest in implementing infosec investment standards that are deemed to be the best practice by experts (see von Solms 1999; Wood and Parker 2004). Future research is needed to study whether this assertion is supported.

Second, we study generic investment decision making for infosec. Research can further study investment decisions related to specific types of infosec investment. For example, an investment

decision related to infosec technology involves not only financial calculations, but also consideration of technological features, compliance requirements, and user acceptance. Furthermore, an investment decision related to infosec training may need to consider employees' security-related stress (D'Arcy et al. 2014). An infosec training program is beneficial for improving employees' security awareness (Karjalainen et al. 2020), but if the security training program causes task conflicts, employees may feel stressed and less motivated to comply with infosec requirements. All those factors will add contextual richness to infosec investment research.

Third, our reputation-based herding model shows that when it is difficult to accurately calculate the costs and benefits of infosec investment, following others is an alternative strategy for infosec managers. From the perspective of saving time, the herding strategy works better than the cost–benefit analysis. Future research can explore if infosec investment decisions based on herding can actually prevent and reduce organizational risk.

Finally, by exploring the effect it has on managers discounting their own information on infosec investment, the study determined that the strength of the information has a minimal influence on the model's ability to predict infosec investment. This is a surprising finding that emphasizes the need for future research on observable information that affects infosec investment decision making.

5.3 Implication for practice

Our results highlight several managerial implications. First, practitioners should observe that it is difficult, if not impossible, to accurately estimate the optimal level of infosec investment due to the uncertainty related to it. In practice, infosec investment managers should switch from pondering the quantitative amount of an infosec investment to paying attention to what influences the actual decision-making process. Organizations must understand that using only cost–benefit analysis may lead to errors in infosec investment decision making. One alternative approach is paying attention to the practices followed by other companies and then making investment decisions based on them.

Second, our results show that both ability and reputation are important in infosec investment decision making. If possible, infosec managers would like to rely on their ability in their decision making (i.e., accurately calculating the costs and benefits of infosec investment). However, since the benefits of infosec investment are uncertain and intangible, and cognitive limitations are inevitable in any kind of decision making, infosec managers may make an investment decision based on reputational concerns. This represents an agency problem. We suggest that senior management and supervisors should communicate more about the work of infosec investment managers. In this way, the agency problem between supervisors and managers could be eliminated.

Our results support the view that mandatory government or industry requirements strongly affect infosec investments. In general, organizations still need to spend time and resources on privacy and security issues to comply with the complex requirements from a growing array of federal, state, and industry standards (Kayworth and Whitten 2010, p. 165).

5.4 Limitations and future research

Sources of model misfit may include non-normality, missing data, specification errors, and the sensitivity of the test to large samples (Kaplan 1990). Regarding normality, the skewness and kurtosis values were between -1 and 1, revealing the normality of the data. As for missing data, we obtained 110 responses, of which four did not answer a large portion of the questions and were dropped. The proportion of missing values for each variable amounted to 0.92%, showing that the rest of the responses could be used. Missing values were replaced with a median value. Regarding model misspecification, we examined the standardized residuals to check the difference between the model-implied covariances and empirical covariances. The standardized residuals did not suggest any substantive misspecification. Therefore, our model does not exhibit a misfit problem.

However, our model may have some limitations that call for future research. A key limitation of the paper is the sample, which was collected from Finnish organizations. National culture has been found to have a substantial effect in infosec studies (Leidner and Kayworth 2006); therefore, caution should be taken in generalizing these results to other cultures. The sample size, although it was acceptable in general, is still small. A larger sample size would have been desirable to increase the statistical power of the study. Another limitation is that the study was conducted using a single method for both dependent and independent variables. Common-method bias was tested using multiple tools, and fortunately it was not found to be significant.

Also, we study generic investment in infosec instead of a specific type of infosec investment, such as investment in infosec technology and/or employees' infosec training. This may also have posed some limitations. Investment decision making regarding infosec technology may involve more contextual factors than the model proposed in this study. Future research can address this limitation by looking into a specific type of infosec investment decision making.

6. Conclusions

The uncertain nature of infosec investment makes applying economic models and financial indicators to infosec management difficult. In practice, infosec managers tend to follow experts' recommendations, best practice suggestions, and the practices adopted by other organizations. This study aims to answer how the uncertain nature of infosec investment affects managers' decision making and what factors influence their choices. This study proposes and tests a model explaining the factors influencing infosec managers' application of a herding strategy. Seven of the eight hypothesized relationships were supported. Our model demonstrates that the infosec managers' ability to accurately predict the benefit of infosec investment and infosec managers' reputation have significant effects on motivating infosec managers to discount their own information. Infosec managers' choices to discount their own information, together with the strength of the information relating to infosec investment and mandatory requirements, motivate infosec investment. Our empirical results highlight the "let's follow others" strategy as an important alternative to cost–benefit analysis in terms of budgeting for infosec investment.

Researchers can make use of the theoretical model based on reputational herding theory, and they can develop new models using this perspective. Researchers can also explore other theories explaining decision making under conditions of uncertainty, which suits the uncertain nature of

infosec investment. Practitioners could stop worrying about the exact number of infosec investments and instead switch to focus on other issues, like eliminating agency problems in infosec investment decision making.

Acknowledgements

This work was supported by Zhishan Youth Scholar Program of Southeast University, Jiangsu Specially-Appointed Professor Program (No. 3051107219003), and National Social Science Foundation of China (No. 6614000050).

Reference

Anderson LR, Holt CA. Information Cascades in the Laboratory. American Economic Review 1997; 87(5): 847-862.

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

Barclay D, Higgins C, Thomson R. The Partial Least Squares Approach (PLS) To Causal Modeling, Personal Computer Adoption and Use as An Illustration. Technology Studies 1995; 2(2): 285- 309.

Baskerville R. Risk analysis: an interpretive feasibility tool in justifying information systems security. European Journal of Information Systems 1991; 1(2): 121-130.

Beaudry A, Pinsonneault A. The other side of acceptance: studying the direct and indirect effects of emotions on information technology use. MIS Quarterly 2010; 34(4): 689- 710.

Bernhardt D, Campello M, Kutsoati E. Who Herds? Journal of Financial Economics 2009; 80(3): 657-675.

Bikhchandani S, Sharma S. Herding behavior in financial markets: A review. IMF Working Paper No. 00/48, 2000.

Black F. Noise. The Journal of Finance 1986; 41(3): 529-543.

Bodin LD, Gordon LA, Loeb MP. Evaluating information security investments using the analytic hierarchy process. Communications of the ACM 2005; 48(2): 79-83.

Bojanc R, Blazic BJ. Towards a standard approach for quantifying an ICT security investment. Computer Standards & Interfaces 2008; 30(4): 216-222.

Boss SR, Kirsch LJ, Angermeier I, Shingler RA, Boss RW. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. European Journal of Information Systems 2009; 18(2): 151–164.

Brandenburger A, Polak B. When managers cover their posteriors: Making the decisions the market wants to see. Rand Journal of Economics 1996; 27(3): 523-541.

Cavusoglu H, Raghunathan S, Yue WT. Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. Journal of Management Information Systems 2008; 25(2): 281-304.

Celen B, Kariv S. Distinguishing informational cascades from herd behavior in the laboratory. American Economic Review 2004; 94(3):484–497.

Chin WW, Thatcher JB, Wright RT. Assessing common method bias: problems with the ULMC technique. MIS Quarterly 2012; 36(3): 1003-1019.

Cremonini M, Nizovtsev D. Understanding and influencing attackers' decisions: Implications for security investment strategies. The Fifth Annual Workshop on Economics and Information Security. Cambridge, UK. 2006

Cronbach LJ. Essentials of Psychological Testing. New York: Harper and Row, 1970.

David RJ, Strang D. When Fashion Is Fleeting: Transitory Collective Beliefs and the Dynamics of TQM Consulting. Academy of Management Journal 2006; 49(2): 215-233.

Dor D, Elovici Y. A model of the information security investment decision-making process. Computers & Security 2016; 63: 1-13.

Duan W, Gu B, Whinston AB. Information cascades and software adoption on the Internet: An

empirical investigation. MIS Quarterly 2009; 33(1): 23-48.

D'Arcy J, Herath T, Shoss MK. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. Journal of Management Information Systems 2014; 31(2): 285-318.

Ferris GR, Blass FR, Douglas C, Kolodinsky RW, Treadway DC. Personal reputation in organizations. In: J. Greenberg (Ed.), Organizational behavior: The state of the science (2nd ed) Mahwah, NJ: Lawrence Erlbaum, 2003.

Fishbein M, Ajzen I. Beliefs, Attitude, Intention and Behavior: an Introduction to Theory and Research, Reading, MA: Addison-Wesley, 1975.

Fornell C, Bookstein F. Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory. Journal of Marketing Research 1982; 19: 440-452.

Gao X, Zhong W, Mei S. Information Security Investment When Hackers Disseminate Knowledge. Decision Analysis 2013; 10(4): 352-368.

Gefen D, Rigdon EE, W. Straub DW. An update and extension to SEM guidelines for administrative and social science research. MIS Quarterly 2011; 35(2): iii–xiv.

Gefen D, Straub DW. A practical guide to factorial validity using PLS-Graph: tutorial and annotated example. Communications of the AIS 2005; 16 (5): 91-109.

Gioia DA, Sims HP. Perceptions of managerial power as a consequence of managerial behavior and reputation. Journal of Management 1983; 9(1): 7- 26.

Gordon LA, and Loeb MP. The economics of information security investment. ACM Transactions on Information and System Security (TISSEC) 2002; 5(4): 438-457.

Gordon LA, Loeb MP. Budgeting process for information security expenditures. Communications of the ACM 2006; 49(1): 121-125.

Gordon LA, Loeb MP. Return on information security investments: myths vs. realities. Strategic Finance 2002; 84(5):26-31.

Graham JR. Herding among Investment Newsletters: Theory and Evidence. The Journal of Finance 1999; 54(1): 237-268.

Gupta M, Banerjee S, Agrawal M, Rao HR. Security analysis of internet technology components enabling globally distributed workplaces – A framework. ACM Transactions on Internet Technology 2008; 8(4): 1-38.

Hausken K. Income, interdependence, & substitution effects affecting incentives for security investment. Journal of Accounting and Public Policy 2006; 25(6): 629-665.

Hirshleifer D. Investor psychology and asset pricing. Journal of Finance 2001; 56(4): 1533- 1597.

Hoo K. How much is enough? A risk-management approach to computer security. Consortium for Research on Information Security Policy (CRISP) Working Paper. Stanford University, Stanford, Calif., June. 2000.

Hooper D, Coughlan J, Mullen M. Structural Equation Modelling: Guidelines for Determining Model Fit. The Electronic Journal of Business Research Methods 2008; 6(1): 53-60.

Huang CD, Behara RS, Goo J. Optimal information security investment in a Healthcare Information Exchange: An economic analysis. Decision Support Systems 2014; 61: 1-11.

Huang CD, Behara RS, Hu Q. Economics of information security investment. In: Handbooks in Information Systems 2007; 53–69.

Huang CD, Behara RS. Economics of information security investment in the case of simultaneous attacks. International Journal of Production Economics 2013; 141(1): 255-268.

Huang CD, Hu Q, Behara RS. An economic analysis of the optimal information security investment in the case of a risk-averse firm. International Journal of Production 2008; 114(2): 793-804.

Kaplan D. Evaluating and modifying covariance structure models: A review and recommendation. Multivariate Behavioral Research 1990; 25(2): 137-155.

Karjalainen M, Siponen M, Sarker S. Toward A Stage Theory of the Development of Employees' Information Systems Security Behavior. Computers & Security 2020; 93: 1-18.

Paananen H, Lapke M, & Siponen M. State of the art in information security policy development. Computers & Security 2020; 88: 1-14.

Kauffman RJ, Li X. Payoff Externalities, Informational Cascades and Managerial Incentives: A Theoretical Framework for IT Adoption Herding. In: Working Paper WP 03-18, Management Information Systems Research Center, University of Minnesota, 2003.

Kayworth T, Whitten D. Effective Information Security Requires a Balance of Social and Technology Factors. MIS Quarterly Executive 2010; 9(3): 2012-2052.

Kline RB. Principles and Practice of Structural Equation Modeling, (3rd ed.), Methodology in the Social Sciences, New York: Guilford Press. 2011.

Kock N. Using WarpPLS in E-collaboration studies: an overview of five main analysis steps. International Journal of e-Collaboration 2010; 6(4): 1-11.

Kumar RL, Park S, Subramniam C. Understanding the value of countermeasure portfolios in information security. Journal of Management Information Systems 2008; 25(20): 241-279.

Lavaan RY. An R Package for Structural Equation Modeling. Journal of Statistical Software 2012; 48(2): 1-36.

Lee K, Joshi K. Examining the use of status quo bias perspective in IS research: need for reconceptualizing and incorporating biases. Information Systems Journal 2017; 27(6): 733-752

Lee YJ, Kauffman RJ, Sougstad R. Profit-maximizing firm investments in customer information security. Decision Support Systems 2011; 51(4): 904-920.

LeidnerD, KayworthT. A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict. MIS Quarterly 2006; 30(2): 357-399.

Li X. Informational Cascades in IT Adoption. Communications of the ACM 2004; 47(4): 93-97.

Liu D, Ji Y, Mookerjee V. Knowledge sharing and investment decisions in information security. Decision Support Systems 2011; 52(1): 95-107.

Lohmöller J-B. Latent Variable Path Modeling with Partial Least Squares, Heidelberg: Physica-Verlag. 1989.

Mackenzi SB, Podsakoff PM, Podsakoff NP. Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. MIS Quarterly 2011; 35(2): 293-334.

Mayadunne S, Park S. An economic model to evaluate information security investment of risk-taking small and medium enterprises. International Journal of Production Economics 2016; 182: 519-530

Menkhoff L. The noise trading approach - Questionnaire evidence from foreign exchange. Journal of International Money and Finance 1998; 17(3): 547-564.

Menon N, Siponen M. Executives' Commitment to Information Security: Interaction between the Preferred Subordinate Influence Approach (PSIA) and Proposal Characteristics. The Data Base for Advances in Information Systems 2019; In Press.

Milliken FJ. Three Types of Perceived Uncertainty about the Environment: State, Effect, and Response Uncertainty. The Academy of Management Review 1987; 12(1): 133-143.

Ogut H, Menon N. Cyber insurance and IT security investment: impact of interdependent risk, Fourth Workshop on the Economics of Information Security, Cambridge, Mass, June 2-3 2005.

Pfeffer J. Managing with power: Politics and influence in organizations. Boston: Harvard Business School Press, 1992.

Pursor S. A Practical Guide to Managing Information Security. Artech House, 2004.

Qian X, Liu X, Pei J, Pardalos, PM. A new game of information sharing and security investment between two allied firms. International Journal of Production Research 2018; 56(12): 4069-4086.

Sawik T. Selection of optimal countermeasure portfolio in IT security planning. Decision Support Systems 2013; 55(1): 156-164.

Scharfstein DS, Stein JC. Herd Behavior and Investment. The American Economic Review 1990; 80(3): 465-479.

Scharfstein DS, Stein JC. Herd Behavior and Investment. The American Economic Review 1990; 80(3): 465-479.

Schechter SE. Toward econometric models of the security risk from remote attacks. IEEE Security & Privacy 2005; 3(1): 40-44.

Shen XL, Zhang KZK, Zhao SJ. Understanding Information Adoption in Online Review Communities: The Role of Herd Factors. In Proceedings of the 47th Hawaii International Conference on System Science 2014; 604-613.

Shleifer A, Summers LH. The Noise Trader Approach to Finance. Journal of Economic Perspectives 1990; 4(2): 19-33.

Simon HA. The New Science of Management Decision. New York: Harper & Row. 1960.

Siponen MT, Willison R. Information security management standards: Problems and solutions. Information & Management 2009; 46(5): 267-270.

Soo Hoo K, How much is enough? A risk-management approach to computer security. Working Paper, Consortium for Research on Information Security and Policy 2000, Stanford University, USA.

Spanos G, Angelis L. The impact of information security events to the stock market: A systematic literature review. Computers & Security 2016; 58: 216-229.

Straub DW, Boudreau M, Gefen D. Validation guidelines for IS positivist research. Communications of the AIS 2004; 13(24): 380–426.

Sun H. A longitudinal study of herd behavior in the adoption and continued use of technology. MIS Quarterly 2013; 37(4): 1013-1041.

Swanson EB, Ramiller NC. Innovating Mindfully with Information Technology. MIS Quarterly 2004; 28(4): 553-583.

Tsiakis T, Stephanides G. The economic approach of information security. Computers & Security 2005; 24 (2): 105-108.

Viduto V, Maple C, Huang W, Lopez-Perez D. A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. Decision Support Systems 2012; 53(3): 599-610.

Von Solms R. Information security management: why standards are important. Information Management & Computer Security 1999; 7(1): 50-57.

Von Solms, R., Van Niekerk, J. (2013) From information security to cyber security. Computers &

security 38, 97-102

Wang P. Chasing the hottest IT: Effects of IT Fashion on Organizations. MIS Quarterly 2010; 34(1): 63-85.

Weishäupl E, Yasasin E, Schryen G. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. Computers & Security 2018; 77: 807-823.

Wheaton B, Muthen B, Alwin DF, Summers GF. Assessing Reliability and Stability in Panel Models. Sociological Methodology 1977; 8(1): 84-136

Wood CC, Parker DB. Why ROI and similar financial tools are not advisable for evaluating the merits of security projects. Computer Fraud & Security 2004; 5: 8-10.

Zinko R, Ferris GR, Humphrey SE, Meyer CJ, Aime F. Personal reputation in organizations: Two-study constructive replication and extension of antecedents and consequences. Journal of Occupational and Organizational Psychology 2012; 85(1): 156- 180.

Zwiebel J. Corporate conservatism and relative compensation. Journal of Political Economy 1995; 103(1): pp. 1-25.

Appendix A. Scale development procedure

The new measures for ability (A) and strength of information (SI) were developed following the procedure suggested by Mackenzie et al. (2012). First, conceptual definitions of the constructs were developed based on existing literature on reputational herding theory. The definition of A focuses on the accurate prediction of the costs and benefits related to using information systems (IS) security management standards, and the definition of SI focuses on the extremeness of information that predicts the costs and benefits of using IS security management standards. Both A and SI are constructed as first-order reflective constructs.

Once the constructs of interest were well defined, seven items for measuring A and nine items for measuring SI were created based on their definitions. Seven-point Likert scales were used for A items, with 1 representing "strongly disagree," 4 "neutral," and 7 "strongly agree." Furthermore, 7-point Likert scales were used for SI items, with 1 representing "extremely negative," 4 "neutral," and 7 "extremely positive."

The initial items for measuring A and SI were examined for content validity. First, we constructed a matrix in which definitions of constructs were listed at the top of the columns and the items were listed in the rows. Next, we recruited 12 raters (including IS researchers and doctoral students at a Finnish university). Each rater was provided with instructions and paper-based matrixes. Each respondent was asked to rate how well each item (row) corresponded to each construct definition (column) on a scale from 1 to 7 (1 = strongly disagree; 7 = strongly agree). Then, one-way repeated measures analysis of variance (ANOVA) was used for assessing whether an item's mean rating on one definition differed significantly from its ratings on other definitions. The next step in the survey development process was the specification of the measurement model. As we constructed A and SI as first-order constructs, we fixed a path between the latent construct and one of its indicators at 1.0.

Once the measurement model was formally specified, the next step of the scale development was the pretesting of the instrument. For the pretest, we created a survey including instructions for the participants. In total, 114 responses were collected. We assessed convergent, nomological, and discriminant validity. Items were modified or deleted if they had non-significant loadings on the hypothesized construct; squared, completely standardized loadings that were less than .50; large and significant measurement error covariances with other measures; or large and significant cross-loadings on non-hypothesized subdimensions. With the pretest data, we purified and refined the scales by using SPSS and AMOS to perform the statistical tests, including the following: (1) goodness of fit; (2) the average variance extracted (AVE); (3) the internal consistency reliability (Cronbach's alpha); (4) Fornell and Larcker's (1981) index of construct reliability; (5) the individual indicator validity and reliability; and (6) elimination of problematic indicators (nonsignificant loadings, squared completely standardized loadings less than .50, large and significant measurement error covariances with other measures). In total, nine items were deleted (A1, A2, A3, A7, SI4, SI5, SI6, SI7, SI8, SI9). Following this, we gathered data from new samples to reexamine the purified scales.

Next, we inspected the item loadings. All item loadings ranged between 0.72 and 0.93; these findings indicated a high level of convergent validity. We then cross-validated our results. We

collected data from a new sample comprising 104 respondents, and all the fit indexes were in line with the recommended cutoff values, indicating that the measurement model fit was good.

The final step included developing norms for the new scales. When developing norms for new scales, it is important to consider that the scales could vary across research contexts and time. We only tested our conceptualization and survey instrument in the context of infosec management in Finland using cross-sectional data. Future studies could extend the scope and develop further norms. Still, given our results, we think it is reasonable to say that the scales are stable in the context of our work.

Appendix B. Measurement items

Questionnaire items translated from the Finnish version used in this study

Construct and definition	**Statement**
Ability (A): The degree to which one is able to accurately predict the issues related to using IS security management standards (CR=0.72).	A4: I know accurately about the benefit of using this information security management standard.
	A5: I know accurately what benefit we can get from using this information security management standard.
	A6: My predictions for the benefit of using information security management standards are usually accurate.
Discounting own information (DOI): The degree to which a person disregards his or her own beliefs about a particular IS security management standard when making a decision (CR=0.76).	DOI1: My use of this information security management standard is not totally based on my own preferences.
	DOI4: I didn't make the decision about using the information security management standard totally based on my own preferences.
	DOI6: It is not my own preferences that select this information security management standard.
Mandatoriness (MAND): Using information security standards is required by regulations (CR=0.93).	MAND1: Regulation requires information security management standards be used in my organization.
	MAND2: Legislation requires information security management standards be used in my organization.
	MAND3: Our organization is required to use information security management standards according to the regulations.
Reputation (R): The extent to which IS security managers are perceived by others as performing their jobs competently (CR=0.89).	R1: I am regarded highly in managing information security in my organization.
	R2: I have a good reputation for managing information security in my organization.
	R5: I have a reputation for producing good results in information security management.
	R6: I have a reputation for producing a high-quality performance in information security management.
Strength of information (SI): The extremeness of information that predicts the possible outcomes of using IS security management standards (CR=0.90).	SI1: I know information about this information security management standard, which is: (Extremely negative)1 2 3 4 5 6 7 (Extremely positive)
	SI2: I have information about this information security management standard, which is: (Extremely negative)1 2 3 4 5 6 7 (Extremely positive)
	SI3: There is information about this information security management standard, which is:

	(Extremely negative)1 2 3 4 5 6 7 (Extremely positive)
Use (U): The use of the information security standard can be seen as a sort of investment (CR=0.86).	U1: To what extent do you apply the information security management standard in your current organization?
	U2: I apply all parts of the information security management standard in my current organization.
	U3: How extensive do you apply the information security management standard in your current organization? (0% Not at all) 1 2 3 4 5 6 7 (All 100%)

Appendix C. Construct validity assessment

Table C1. Correlations of latent variable scores against the indicators and significance of loading values on the latent variable

Item	A	DOI	Mand	R	SI	USE	P-value
A4	0.789	0.096	0.151	0.533	0.615	0.512	<0.001
A5	0.808	0.082	0.246	0.328	0.341	0.532	<0.001
A6	0.807	0.29	0.195	0.596	0.311	0.451	<0.001
DOI2	0.102	0.831	0.248	0.288	0.215	0.3	<0.001
DOI4	0.08	0.854	0.28	0.264	0.139	0.333	<0.001
DOI6	0.249	0.762	0.611	0.275	0.157	0.53	<0.001
MAND1	0.324	0.508	0.96	0.278	0.28	0.528	<0.001
MAND2	0.112	0.446	0.882	0.097	0.147	0.322	<0.001
MAND3	0.298	0.633	0.951	0.234	0.253	0.545	<0.001
R1	0.647	0.298	0.237	0.899	0.53	0.459	<0.001
R2	0.605	0.316	0.148	0.817	0.503	0.402	<0.001
R5	0.498	0.304	0.175	0.86	0.496	0.412	<0.001
R6	0.614	0.346	0.206	0.904	0.556	0.497	<0.001
SI1	0.665	0.227	0.202	0.583	0.937	0.57	<0.001
SI2	0.571	0.24	0.26	0.617	0.952	0.493	<0.001
SI3	0.39	0.125	0.218	0.448	0.84	0.305	<0.001
U1	0.572	0.477	0.399	0.501	0.481	0.885	<0.001
U2	0.553	0.437	0.411	0.273	0.352	0.849	<0.001
U3	0.665	0.505	0.481	0.526	0.477	0.915	<0.001

Table C2. Assessing discriminant validity using AVEs

	A	DOI	Mand	R	SI	USE
A	**0.72**					
DOI	0.13	**0.95**				
Mand	0.31	0.24	**0.87**			
R	0.55	0.26	0.2	**0.72**		
SI	0.32	0.18	0.23	0.52	**0.9**	
USE	0.55	0.26	0.45	0.45	0.38	**0.93**

Table C3. Construct reliability

	Cronbach's Alpha	Composite Reliability
A	0.722	0.844
DOI	0.756	0.857
Mand	0.926	0.952
R	0.893	0.926
SI	0.9	0.936
USE	0.859	0.914

Biographical sketch

Xiuyan Shao, Southeast University, China Xiuyan Shao is an assistant professor in School of Economics and Management at Southeast University, China. Her degrees include Ph.D. in Management Information Systems; M.Sc. in Economics; and B.Sc. in Economics. Her main research interests cover fields of behavioral issues of IT security investment, information security management, and economics of information security.

Mikko Siponen, University of Jyvaskyla, Finland Mikko Siponen is a professor of Information Systems at the University of Jyväskylä. He holds a Ph.D. in philosophy from the University of Joensuu, Finland, and a Ph.D. in Information Systems from the University of Oulu, Finland. His research interests include IS security, IS development, computer ethics, and philosophical aspects of IS. Mikko has published more than 70 articles in journals such as MIS Quarterly, Journal of the Association for Information Systems, Information & Management, European Journal of Information Systems, Information & Organization, Communications of the ACM, IEEE Computer, IEEE IT Professional, and others. He has received over 10 million EUR of research funding from corporations and numerous funding bodies. He has been a track chair for the International Conference on Information Systems and the European Conference on Information Systems three times. His other editorial board experiences include positions with Journal of the Association for Information Systems, European Journal of Information Systems, Information & Management, and Communications of the Association for Information Systems.

Fufan Liu, University of Jyvaskyla, Finland Fufan Liu is a PhD candidate in the Faculty of Information Technology at the University of Jyväskylä. He holds a Master's in cognitive psychology and his research interests lie in media exposure and risk perception in security communication.

CRediT author statement:
Xiuyan Shao: Conceptualization, Model development, Data collection, Methodology, Resources, Writing- Original draft preparation.
Mikko Siponen: Conceptualization, Data collection, Writing- Reviewing and Editing
Fufan Liu: Data analysis

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.