To Calculate or To Follow Others: How Do Information Security Managers Make Investment Decisions?

Xiuyan Shao
University of Oulu
xiuyan.shao@oulu.fi

Mikko Siponen
University of Jyväskylä
mikko.t.siponen@jyu.fi

Seppo Pahnila
University of Oulu
seppo.pahnila@oulu.fi

Abstract

Economic models of information security investment suggest estimating cost and benefit to make an information security investment decision. However, the intangible nature of information security investment prevents managers from applying cost-benefit analysis in practice. Instead, information security managers may follow experts' recommendations or the practices of other organizations. The present paper examines factors that influence information security managers' investment decisions from the reputational herding perspective. The study was conducted using survey questionnaire data collected from 106 organizations in Finland. The findings of the study reveal that the ability and reputation of the security manager and the strength of the information about the security investment significantly motivate the security manager to discount his or her own information. Herding, as a following strategy, together with mandatory requirements are significant motivations for information security investment.

1. Introduction

As information security incidents grow in frequency, there has been an increase in recent years in the costs of managing and mitigating breaches. It is estimated that cybercrime is costing organizations, on average $11.7 million per organization [1]. Budgeting for information security expenditures is a crucial resource allocation decision in organizations. The budgeting question of information security investment is often addressed via two main research streams. One research stream analyzes the budgeting question through traditional decision analysis. This approach compares the risk and return of investments. The return on an information security investment does not come from increased revenues or decreased costs but from reducing security risks [2]. Such risk analysis is based on the measurement of security risk = (likelihood of a loss event) × (cost of a loss event) [3] or more complex variations, such as the value-at-risk approach [4]. The most influential work in this research stream is by Gordon and Loeb [5]. By comparing the cost of investment and the potential loss caused by possible security breaches, they found that the optimal security investment would be far less than (with a theoretical maximum of less than 40% of) the potential loss if a security breach does happen, and that the optimal security investment does not necessarily increase with system vulnerability. Another research stream employs game theory to view information security investments based on the actions and reactions between a firm and the attackers [6, 7, 8]. From the methodological perspective, the game theory approach is best suited for modeling the outcome of a specific security technology with limited rounds (often two or three) of actions and reactions between a limited number of players (often, the firm and the attacker).

However, due to uncertainty in information security, it is difficult to apply cost-benefit analysis in practice. First, an information security investment has intangible benefits [2]. Estimating the expected costs related to information security activities is difficult because organizations cannot get historical data to make predictions. But estimating the expected benefits is even harder, as estimating the expected benefits requires managers to have information on potential losses from security breaches and the probability of such breaches. Second, there are no reliable actuarial loss statistics [9]; therefore, it is not possible to estimate the future benefits expected to be derived from information security investments [10]. However, although game theory is suitable from a methodological perspective, applying game theory requires estimating the attacker's utility parameters, which is much more difficult, if not impossible, than estimating those of the targeted firm.

In practice, information security managers usually intend to follow the decisions of other experts and best practices. For example, information security managers have noted that the expenditure budgeted for information security for their organizations is largely driven by best practices in the industry [10]. As a concrete example, ISO-IEC 27002 recommends having employee security awareness training programs; in 2014, 51% of respondent companies were reported to have security awareness and training programs, and 57% of respondent companies required

URI: https://hdl.handle.net/10125/59926
ISBN: 978-0-9981331-2-6

employees complete training on privacy policies [11]. Occasionally, organizations may adopt information security technology by following the practices of other organizations. Studies have shown that organizations tend to chase the hottest IT [12]. For example, anti-virus software, network access control software, identity management technology, and encryption of desktop PCs are popular applications among organizations [13].

The present paper examines the strategy adopted by managers in information security investment. The objective of the present paper is to explore factors that influence an information security manager's investment decision. This paper makes several potential theoretical and empirical contributions in this regard.

2. Theoretical framework

2.1. Reputation-based herding behavior

Different from the rational assumption in neoclassical economics, which assumes that decision-makers gather complete information, design all possible alternatives, compare, and choose an alternative [14], herding behavior was originally used to describe the behavior of investment decision-makers who follow the decisions of earlier adopters [15, 16]. Herding behavior has also been found in IT adoption, for example, downloading popular software products [17], adopting wiki systems [18], and general purchase decision-making [19].

Scharfstein and Stein [20] developed the reputational herding model, in which they suggested that managers with good reputations are more conservative in bucking the consensus and herd to protect their current status. Sun [18] developed two new concepts to describe herding behavior in technology adoption: imitating others and discounting own information. Imitating others describes the degree to which a person follows others' decisions when adopting a technology, and discounting own information concerns the degree to which a person disregards his or her own beliefs about a particular technology when making an adoption decision.

In this paper, we explore factors that motivate decision-makers to discount their own information and how discounting own information affects information security investments.

Network externalities, information cascades, and herding behavior are similar (but still different) concepts that have been used to study imitative behavior. Network externality emphasizes that "the value of a technology increases as the number of its users increases" [21]. Network externalities tend to reward herding decisions with increased payoffs to those who associate themselves with the majority. The rewards of such marginal increases in value go to previous members of the herd, not to the member who just joined. There are two ways to differentiate reputational herding from network externalities. First, a value-adding mechanism is not necessary in reputational herding. The main motivations for reputational herding are to overcome uncertainty and maintain reputation. Second, the two are based on different theoretical backgrounds. Reputational herding results from the agency problem (which comes from information asymmetry), while network externalities are based on economies of scale.

Information cascade refers to when a decision-maker ignores his or her own private information, which is overwhelmed by publicly observable information, and instead, mimics others' actions [22]. Information cascade theory is also associated with the theory of institutional mimetic isomorphism, in which institutions tend to imitate each another in technology adoption decision-making [16, 23, 24]. Reputational herding theory and information cascade theory share the characteristics peer influences and uncertainty in decision-making. Reputational herding differs from an information cascade in that the former includes managers' reputational concerns in addition to the latter. Information cascade theory shows that herding behavior can be tracked back to information asymmetries and the problems associated with observational learning. However, the reputational herding model demonstrates that herding may be caused by managerial incentive problems. Therefore, the reputational herding model connects agency theory and rational observational learning.

2.2. Research model and hypotheses

To understand information security investment decision-making in organizations, reputational herding theory [20] is used as the basis for our theoretical model (Figure 1). Reputational herding theory claims that if an investment manager is uncertain about his or her ability to decide on an investment, conformity with other investment professionals is a good choice [20]. This is because of the following key assumptions of the theory: i) There are systematically unpredictable components of the investment value, and ii) smart managers make similar decisions. If managers make the same decision as others, they will be evaluated more favorably because they can share the blame. Reputational herding theory emphasizes the unpredictability of the value of decisions; therefore, the theory explains decision-

making under uncertainty very well. We expect this theory to be well suited for explaining information security investment, which also involves unpredictability of the value.

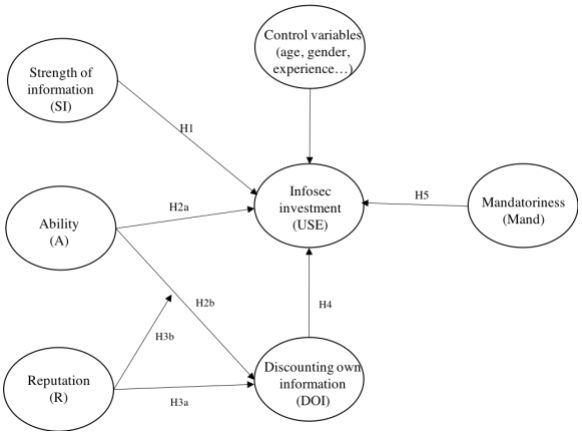

Figure 1. Research model

2.2.1. Strength of the information. In the reputational herding model, previous information [20] refers to information that has previously been made public and shows a probability of deriving profit from an investment. The reputational herding model suggests that when previous information is strong and consistent with the majority's actions, the decision-maker tends to follow the actions of the majority. Here, following Hirshleifer [25], we define the strength of information as the extremeness of public information that shows the probability of deriving profit from an information security investment. Based on this, we construct our first hypothesis:

H1: The strength of the information is positively associated with information security investment.

2.2.2. Ability to analyze an investment decision. When a person has incomplete information, he or she perceives inability to predict something accurately [26]. In the information security investment context, it is usually difficult for information security managers to predict when hackers' next attack will occur, especially successful, expensive, and destructive attacks (state of uncertainty). The damage from an information security breach (or attack) is difficult for information security managers to assess (effect uncertainty). It is also difficult to guarantee that the information security investment will efficiently prevent all security breaches (response uncertainty). Consequently, it is difficult to accurately predict the value of the information security investment.[1] Previous research has shown that when people feel uncertain about a decision, they are likely to follow others [18, 27, 28, 29]. Therefore, we construct the following hypotheses:

H2a: A manager's ability to accurately predict the value of an information security investment is positively associated with the information security investment.

H2b: A manager's ability to accurately predict the value of an information security investment is negatively associated with discounting his or her own information.

2.2.3. Managers' reputation. Reputation can be important to managers because it brings autonomy, power, and career success [30]. Reputation shows a manager's ability. From the agency theory perspective, a manager's reputation also indicates that his or her behavior is predictable, and no close monitor is needed for a manager's actions. As managers gain a good reputation, they also gain power [31, 32], which may be derived from not only formal but also informal authority; the authority to delegate tasks is an example of this power. Reputation also has the ability to affect performance evaluations, promotions, and compensation [33].

A manager's reputation is updated when the labor market checks whether he or she makes smart decisions. A smart decision can be evaluated in terms of whether it is a profitable decision for the organization or whether the decision is similar to those made in other organizations [20]. If reputation is important to managers, they may generally avoid making dumb decisions. For instance, Brandenburger and Polak [34] suggested that a firm can have a reputational incentive to make investment decisions that are consistent with a previous belief regarding the profitability of a project, even if the firm has superior information than public.

As we discussed above, the difficulty of accurately predicting the value of an information security investment results in difficulty evaluating whether managers' decisions are profitable. Therefore, managers 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:

[1] IS studies that focused on uncertainty related to IS complexity, IS performance and quality operationalize uncertainty so as to represent the level of *uncertainty anxiety* experienced by users related to a change, which refers to the psychological uncertainty and the associated stress. Our ability construct does not need to measure the anxiety, but only measure if the manager is able to calculate cost and benefit related with information security investment.

H3a: A manager's reputation is positively associated with herd behavior.

H3b: Reputation enhances the relationship between ability and information security investment.

2.2.4. Impact of discounting own information on information security investment. Previous researchers suggested two main reasons why investment managers mimic the investment decisions of other managers. First, managers mimic others to avoid the risk of being considered incapable [20, 28]. Second, if a manager makes an unprofitable investment by following others, "sharing the blame" with others who made the same decision makes the mistake more acceptable. Herding is considered a legitimate strategy for people with good reputations to protect their status [28]. In the context of information security investment, a manager may imitate others in making an 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 also accepted or rejected an efficient information security investment. Thus, this potentially spares the manager his or her own reputation. Such a positive association with herd behavior leads to the construction of the following hypothesis:

H4: Discounting one's own information is positively associated with a manager's information security investment decision.

2.2.5. Mandatory requirements. As more people have realized the value of information, governments have enacted various laws to secure information in cyberspace, such as the Gramm-Leach-Billy Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act Security Rule, the Sarbanes-Oxley Act, and the recent EU General Data Protection Regulation (GDPR) in May 2018. Security managers are faced with the complex challenge of meeting the multiple compliance requirements of a growing array of federal, state, and industry standards. Given this aim, we sought to determine whether mandatory requirements ensure compliance. This investigation led to the formulation of the following hypothesis:

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

3. Research method and data analysis

3.1. Operationalization of constructs

This study utilized instruments that were validated in previous studies. For example, the items used to measure discounting one's own information were adopted from Sun [18], items assessing reputation were adopted from Zinko et al. [30], items assessing mandatory requirements were adopted from Boss et al. [35] and items assessing use of information security management standards were adopted from Beaudry and Pinsonneault [36]. We adopted previous measures after carefully considering the information security investment context. All items were assessed using a seven-point Likert scale.

Because there were no previously validated instruments for assessing ability and the strength of information, we developed new instruments in this study to assess ability and strength. We followed the procedure from Mackenzie et al. [37]. The instrument development process resulted in four items for assessing ability and three items for assessing the strength of the information. Content validity for all measures was established through a literature review and a content validity expert panel that comprised eight researchers (faculty and doctoral students) who were skilled in quantitative research methods.

3.2. Pretest

A pretest survey was conducted at one university in Finland. A total of 32 responses were collected. An open question was included to allow the participants to comment on the wording, content, and length of the questionnaire. The questionnaire was revised using the responses. To assess the reliability of the scales, Cronbach's alpha [38] was used. Items with high "Cronbach's alpha if item deleted" statistics, or small standard deviation scores (and thus, low explanatory power) were deleted, bearing in mind the content validity.

3.3. Survey administration

The main field study was conducted among information security managers in Finland, a developed country in which a number of organizations are increasingly aware of information security investment issues. The survey was sent to the 1,042 Finnish companies. A research assistant called these companies and asked for the name of the chief information security officer (CISO) or a similar title. The survey was mailed to them. As an incentive to participate, we offered to provide the organizations a report of the findings upon conclusion of the study. Out of the 1,042 surveys distributed to these organizations, 110 responses were obtained. Respondents returned the completed surveys by using

envelopes with pre-paid postage. We conducted a structured data screening process. First, we dropped 4 respondents who did not answer a large portion of the questions. The number of missing values for each variable was 0.92%, which means we could use the rest of the respondents. We then replaced the missing values with a median value. The variance of each respondent ranged from 0.5 to 2.2, showing that respondents did not answer arbitrarily. The skewness and kurtosis values were between –1 and 1, showing the normality of the data. No outlier values were found in the data.

The required sample size for evaluating the model was 60, according to the "rule of ten" heuristic [39]. Given the difficulty of reaching CISOs in large companies, this response rate is acceptable. More importantly, the returned surveys were completed by managers with firsthand knowledge of their companies' information security management, as evidenced by their position and the length of time in which they have held their position. Table 1 summarizes the demographic information, which suggests that the sample was heterogeneous.

Table 1. Descriptive statistics of the respondents

	Frequency (%)
Gender	
Male	92 (86.79)
Female	14 (14.77)
Age	Average = 45.16
Experience (years)	Average = 10.73
Education	
Vocational	4 (4.55)
College level	17 (19.32)
Bachelor's degree	21 (23.86)
Master's degree	45 (51.14)
Ph.D.	1 (1.14)
Previous experience	
Yes	57 (64.77)
No	31 (35.23)
Size of organization (number of employees)	
1–100	8 (9.10)
101–249	11 (12.5)
250–499	11 (12.5)
500–999	10 (11.36)
1,000+	48 (54.55)

4. Data analysis

Data analysis was performed using SmartPLS, version 3.0 [40]. A partial least squares (PLS) technique was selected to test the hypotheses, because PLS is more suitable than the covariance-based approach for conducting exploratory research [41]. The primary focus of this research is understanding each specific path coefficient and variance explained rather than the overall model fit. Thus, PLS is a more appropriate method for this research, relative to covariance-based tools.

4.1. Measurement validation

The latent variables show good reliability. Table 2 shows the Cronbach's alpha, composite reliability, and average variance extracted (AVE) of each construct and shows the internal consistency of the model. All constructs have a Cronbach's alpha value higher than 0.7 and thus, display convergent validity [42]. Furthermore, they all show a composite reliability greater than the proposed threshold of 0.7 that literature considers good for explanatory purposes [43]. In addition, the AVE of all constructs is higher than the proposed threshold of 0.5 [44], which means that the error variance does not exceed the explained variance [42].

Table 2. Construct reliability and validity

	Cronbach's Alpha	Composite Reliability	AVE
A	0.722	0.721	0.565
DOI	0.756	0.725	0.584
Mand	0.925	0.93	0.822
R	0.893	0.894	0.679
SI	0.899	0.904	0.764
USE	0.857	0.86	0.675

To assess discriminant validity, we use the Heterotrait-Monotrait (HTMT) ratio, as Henseler et al. [45] argued it is superior to the Fornell and Larcker criterion [46]. Table 3 shows that all HTMT ratios are below the strict cutoff value of 0.85 proposed by Kline [47] which indicates good discriminant validity.

Table 3. HTMT ratios to assess discriminant validity

	A	DOI	Mand	R	SI	USE
A	1					
DOI	0.227	1				
Mand	0.279	0.535	1			
R	0.713	0.388	0.226	1		
SI	0.613	0.235	0.259	0.637	1	
USE	0.735	0.547	0.521	0.531	0.526	1

To assess common method bias, we chose the statistical approach suggested by Podsakoff et al. [48] and applied by Liang et al. [49]. As suggested, we

created the PLS model and included a common method factor that linked to all the single-indicator constructs that were converted from the observed indicators. Because the method factor loadings were not statistically significant and the indicators' substantive variances were substantially greater than their method variances, we concluded that common method bias is unlikely to be a serious concern.

4.2. Structural model testing

Given that the data displayed factorial validity and did not display common method bias, the structural model was tested. The results of the structural model are presented in Table 4. We used bootstrapping with 1000 samples to determine whether the relations between the constructs were statistically significant and supported the hypotheses. The table shows that all hypotheses are supported. We determined the effect size f-squared of each variable according to the formula by Hair et al. [50]. Effect sizes are considered small if they are above 0.02, medium if they are above 0.15, and large if they are above 0.35 [51]. Table 4 shows the effect sizes of the variables. It reveals that A (ability) has the highest influence on USE (information security investment) and R (reputation) has the highest influence on discounting own information (DOI). Meanwhile, A also has a large influence on DOI, and R also has a large influence on USE. Strength of information (SI) and Mandatory requirements (Mand) have only a small positive influence (although statistically significant) on USE. The moderation effect between A and R has a large influence on DOI.

Table 4. Path coefficients and effect sizes

Hypothesis		Path coefficients	T statistics	P value	Supported	R square included	R square excluded	Effect size	
H1	**SI -> USE**	0.045	2.206	0.028	**Yes**	0.751	0.748	0.012	Small
H2a	**A -> USE**	0.633	5.157	0.000	**Yes**	0.751	0.548	0.815	**Large**
H2b	**A -> DOI**	-0.393	2.153	0.029	**Yes**	0.336	0.134	0.304	**Large**
H3a	**R -> DOI**	0.820	4.053	0.000	**Yes**	0.336	0.044	0.440	**Large**
H3b	**A*R -> DOI**	0.460	2.692	0.007	**Yes**	0.336	0.137	0.300	**Large**
H4	**DOI -> USE**	0.359	2.749	0.006	**Yes**	0.751	0.672	0.317	**Large**
H5	**Mand -> USE**	0.139	2.898	0.004	**Yes**	0.751	0.740	0.044	Small

The adjusted R-squared of the model is 0.722 (USE as a dependent variable), and 0.369 (DOI as a dependent variable). The constructs of USE explain 72.2% of its variance, and the constructs of DOI explain 36.9% of its variance.

5. Discussion and implication

5.1. Discussion of the results

This study developed a model to understand how information security managers make investment decisions. First, the findings demonstrate that when managers make decisions about information security investments, the ability to accurately predict the net benefit of the decision is important for security managers. This ability positively influences the information security investment decision (H2a) and negatively influences security managers' intention to discount their own information (H2b). During this process, a security manager's reputation plays an important role. A security manager who has a higher reputation is more conservative and therefore, tends to discount his or her own information more (H3a). Reputation also enhances the relationship between a security manager's ability and his or her intention to discount his or her own information. When a security manager with a high reputation cannot accurately predict the net benefit of a security investment decision, he or she has more intention to discount his or her own information (H3b). In addition, when information security managers observe a considerable number of organizations that have made the same information security investments, the managers are more likely to make the same decision (H1). To sum up, the factors above influence an information security manager's intention to discount his or her own information (therefore, adopt a herding strategy) in making information security investment decisions.

This model also shows that discounting one's own information is statistically significantly associated with information security investments (H4). Although this is the first application of reputational herding theory to information security investment research, previous studies in other fields have shown that reputational herding theory is an effective strategy in making decisions under uncertainty. Take Graham

[28], for example, who studied herding behavior among investment newsletters. By using the data of analysts who published investment newsletters, he found that if the analyst's reputation is high, if the analyst's ability is low, or if the signal correlation is high, the analyst is likely to follow investment newsletter's recommendation.

In addition, the present results show that mandatory government or industry requirements strongly affect information security investments (H5). The result is consistent with information security literature. Kayworth and Whitten ([52], p. 165) claimed that "security managers are faced with the complex challenge of meeting multiple compliance requirements from a growing array of federal, state, and industry standards." For example, in 2018, the EU GDPR replaced the Data Protection Directive 95/46/EC and aims to reshape the way organizations across the region approach data privacy. The EU GDPR requires organizations have clear language to explain their privacy policies, obtain affirmative consent from users before their data can be used, clearly inform users about data transfers, collect and process data only with a well-defined purpose and inform users about new purposes for processing the data, and inform users whether the decision is automated and provide users with the possibility of contesting it. In general, organizations must spend more time and resources on privacy and security issues to comply with the EU GDPR. From all the discussion above, we conclude that when the perceived net benefit is difficult to accurately predict, an information security manager may adopt a herding strategy to make information security investment decisions.

5.2. Implications for research and practice

This is the first study that provides more motivations than benefit-driven via financial analytical tools for information security investments. Previous studies developed economic models or financial indicators to estimate the optimal level of information security investment. However, economic models do not work well because actuarial data is lacking. This empirical study explored and tested influential factors that were not included in previous economic models, for example, information security managers' ability to accurately calculate the costs and benefits of information security investment, information security managers' reputation, etc.

5.2.1. Implications for research. The primary contribution of this study is to suggest herding as managers' strategy in information security investment and to investigate the influential factors of a herding strategy. As information security investment managers are uncertain about the intangible costs and benefits of information security investments, applying an economic model or financial indicator is impossible. Therefore, information security managers employ supplementary strategies. This study also encourages that other supplementary strategies that can be utilized in information security investment decision-making be investigated in future research.

The intangible nature of information security investment limits information security managers' ability to accurate estimate the costs and benefits of information security investments [53]. Therefore, theories that address the concern of making decisions under uncertainty may be relevant. For example, Black [54] suggested, "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" ([54], p 529). In stock markets, when investment managers (or individual stock buyers) are uncertain about the results of one stock and lack necessary information to analyze potential benefits (or losses), they might invest based on noise. Shleifer and Summers [55] pointed to the advice of financial gurus as one example of noise. In line with that idea, Menkhoff [56] showed that investors tend to follow experts' opinions. For example, information security investment managers are more willing to invest in implementing information security investment standards that are deemed by experts to be the best practice.

In addition to the theory discussion above, different theories in behavioral economics (such as cognitive biases, heuristics, and investor's sentiment) can be applied to explain and predict the issues in this research stream. Testable theories in terms of explaining and predicting [57] can be built with variance or factor models.

5.2.2. Implications for practice. Two potential practical implications can be highlighted from the present results. First, practitioners should observe that it is not possible to accurately estimate the optimal level of information security investment due to the intangible nature of information security investment. In practice, information security investment managers should switch from pondering the quantitative amount of an information security investment to paying attention to what influences information security investment decision-making. Organizations must understand that using only cost-benefit analysis may lead to errors in information security investment decision-making. However, it may be more realistic to pay attention to the practices followed by other companies and then make investment decisions.

Second, cognitive limitations are inevitable in any kind of decision-making. In practice, information security managers can investigate whether these cognitive limitations have affected their decision-making. Regarding the reputational concern of information security investment managers, we suggest that senior management and supervisors should communicate more about the work of information security investment managers. Therefore, the agency problem between supervisors and managers could be eliminated.

6. Conclusion

Because of the intangible nature of information security investment, and thus, the difficulty of accurately assessing the benefits of information security investment, economic models and financial indicators are not applicable in information security management. In practice, information security managers tend to follow experts' recommendations, best practice suggestions, and the practices followed in other organizations. This study attempted to provide an alternative strategy in information security investment decision-making from a reputational herding perspective. The proposed model was examined, and the research results provide insights into making information security investment decisions.

However, this study has certain limitations. First, as is the case with most IS research, data was collected from within a single country. It may be that the results of this study cannot be applied generally to other countries and cultures. A much-needed avenue of future research is to examine the effects across cultures. Another limitation is the use of field studies as the only methodology. Although field studies offer the benefits of generalizability by examining professionals in actual organizational settings, there are several weaknesses, such as poor internal validity due to an inability to control the independent variables [58]. A longitudinal survey or an experiment could be used to provide evidence of causal effects.

Appendix

Questionnaire items translated from the Finnish version used in this study

	Definition of construct	**Statement**	**Source**
A1	The degree to which one is able to accurately predict the issues related to using IS security management standards.	I know accurately about the benefit of using this information security management standard.	Self-developed
A2		I know accurately what benefit we can get from using this information security management standard.	
A3		My predictions for the benefit of using information security management standards are usually accurate.	
DOI1	The degree to which a person disregards his or her own beliefs about a particular IS security management standard when making a decision.	My use of this information security management standard is not totally based on my own preferences.	[18]
DOI2		I didn't make the decision about using the information security management standard totally based on my own preferences.	
DOI3		It is not my own preferences that select this information security management standard.	
MAND1	Using information security standards is required by regulations.	Regulation requires information security management standards be used in my organization.	[35]
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.	
R1	The extent to which IS security managers are perceived by others as performing their jobs competently.	I am regarded highly in managing information security in my organization.	[30]
R2		I have a good reputation for managing information security in my organization.	
R3		I have a reputation for producing good results in information security management.	
R4		I have a reputation for producing a high-quality performance in information security management.	
SI1	The extremeness of information that predicts the possible outcomes of using IS security management standards.	I know information about this information security management standard, which is: Extremely negative — Neutral — Extremely positive 1 2 3 4 5 6 7	Self-developed
SI2		I have information about this information security management standard, which is: Extremely negative — Neutral — Extremely positive 1 2 3 4 5 6 7	

SI3		There is information about this information security management standard, which is: Extremely negative — Neutral — Extremely positive 1 2 3 4 5 6 7	
U1	The use of the information security standard can be seen as a sort of investment, because it takes time and resources.	To what extent do you apply the information security management standard in your current organization?	[36]
U2		I apply all parts of the information security management standard in my current organization.	
U3		To what extent do you apply the information security management standard in your current organization?	

7. References

1. https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
2. C.D. Huang, R.S. Behara, and Q. Hu, "Economics of information security investment", In: Handbooks in Information Systems, 2007, pp. 53-69.
3. S.E. Schechter, "Towards econometric models of the security risk from remote attacks", IEEE Security & Privacy, 3 (1), 2005, pp. 40-44.
4. J. Wang, A. Chaudhury, and H.R. Rao, "A Value-at-Risk Approach to Information Security Investment", Information Systems Research, 19(1), 2008, pp. 106-120.
5. L.A. Gordon, and M.P. Loeb, "The economics of information security investment", ACM Transactions on Information and System Security (TISSEC), 5(4), 2002, pp. 438-457.
6. H. Cavusoglu, and S. Raghunathan, "Configuration of Detection Software: A Comparison of Decision and Game Theory Approaches", Decision Analysis, 1(3), 2004, pp. 131-148.
7. H. Cavusoglu, B. Mishra, and S. Raghunathan, "A model for evaluating IT security investments", Communications of the ACM, 47(7), 2004, pp. 87-92.
8. H. Cavusoglu, B. Mishra, and S. Raghunathan, "The Value of Intrusion Detection Systems in Information Technology Security Architecture", Information Systems Research, 16(1), 2005, pp. 28-46.
9. C.C. Wood, and D.B. Parker, "Why ROI and similar financial tools are not advisable for evaluating the merits of security projects", Computer Fraud & Security, 5, 2004, pp. 8-10.
10. L.A. Gordon, and M.P. Loeb, "Budgeting process for information security expenditures", Communications of the ACM, 49(1), 2006 121-125.
11. http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf
12. P. Wang, "Chasing the hottest IT: Effects of IT Fashion on Organizations", MIS Quarterly, 34(1), 2010, pp. 63-85.
13. https://www.pwc.com/gx/en/consulting-services/information-security-survey/pwc-gsiss-2014-key-findings-report.pdf
14. H.A. Simon, "The New Science of Management Decision", New York: Harper & Row. 1960.
15. R.J. Kauffman, and X. Li, "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.
16. E.B. Swanson, and N.C. Ramiller, "Innovating Mindfully with Information Technology", MIS Quarterly, 28(4), 2004, pp. 553-583.
17. W. Duan, B. Gu, and A.B. Whinston, "Information cascades and software adoption on the Internet: An empirical investigation", MIS Quarterly, 33(1), 2009, pp. 23-48.
18. H. Sun, "A longitudial study of herd behavior in the adoption and continued use of technology", MIS Quarterly, 37(4), 2013, pp. 1013-1041.
19. X.L. Shen, K.Z.K. Zhang, and S.J. Zhao, "Understanding Information Adoption in Online Review Communities: The Role of Herd Factors", In Proceedings of the 47th Hawaii International Conference on System Science, (pp. 604-613), 2014.
20. D.S. Scharfstein and J.C. Stein, "Herd Behavior and Investment", The American Economic Review, 80(3), 1990, pp. 465-479.
21. X. Li, "Informational Cascades in IT Adoption", Communications of the ACM, 47(4), 2004, pp. 93-97.
22. L.R. Anderson, and C.A. Holt, "Information Cascades in the Laboratory", The American Economic Review, 87(5), 1997, pp. 847-862.
23. P.J. DiMaggio, and W.W. Powell, "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields", American Sociological Review, 48(2), 1983, pp. 147-160.
24. P. Tingling, and M. Parent, "Mimetic Isomorphism and Technology Evaluation: Does Imitation Transcend Judgment?", Journal of Association for Information Systems, 3(1), 2002, pp. 113-143.
25. D. Hirshleifer, "Investor psychology and asset pricing", Journal of Finance, 56(4), 2001, pp. 1533- 1597.
26. F.J. Milliken, "Three Types of Perceived Uncertainty about the Environment: State, Effect, and Response Uncertainty", The Academy of Management Review, 12(1), 1987, pp. 133-143.
27. S. Bikhchandani, and S. Sharma, "Herding behavior in financial markets: A review", IMF Working Paper No. 00/48, 2000.
28. J.R. Graham, "Herding among Investment Newsletters: Theory and Evidence", The Journal of Finance, 54(1), 1999, pp. 237-268.

29. J. Zwiebel, “Corporate conservatism and relative compensation”, Journal of Political Economy, 103(1), 1995, pp. 1-25.
30. R. Zinko, G.R. Ferris, S.E. Humphrey, C.J. Meyer, and F. Aime, “Personal reputation in organizations: Two-study constructive replication and extension of antecedents and consequences”, Journal of Occupational and Organizational Psychology, 85(1), 2012, pp. 156-180.
31. D.A. Gioia, and H.P. Sims, “Perceptions of managerial power as a consequence of managerial behavior and reputation”, Journal of Management, 9(1), 1983, pp. 7-26.
32. J. Pfeffer, “Managing with power: Politics and influence in organizations”, Boston: Harvard Business School Press, 1992.
33. G.R. Ferris, F.R. Blass, C. Douglas, R.W. Kolodinsky, and D.C. Treadway, “Personal reputation in organizations”, In: J. Greenberg (Ed.), Organizational behavior: The state of the science (2nd ed) Mahwah, NJ: Lawrence Erlbaum, 2003.
34. A. Brandenburger, and B. Polak, “When managers cover their posteriors: Making the decisions the market wants to see”, Rand Journal of Economics, 27(3), 1996, pp. 523-541.
35. S.R. Boss, L.J. Kirsch, I. Angermeier, R.A. Shingler, and R.W. Boss, “If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security”, European Journal of Information Systems, 18(2), 2009, pp. 151–164.
36. A. Beaudry, and A. Pinsonneault, “The other side of acceptance: studying the direct and indirect effects of emotions on information technology use”, MIS Quarterly, 34(4), 2010, pp. 689- 710.
37. S.B. Mackenzi, P.M. Podsakoff, and N.P. Podsakoff, “Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques”, MIS Quarterly, 35(2), 2011, pp. 293-334.
38. L.J. Cronbach, Essentials of Psychological Testing, New York: Harper and Row, 1970.
39. D. Barclay, C. Higgins, and R. Thomson, “The Partial Least Squares Approach (PLS) To Causal Modeling, Personal Computer Adoption and Use As An Illustration”, Technology Studies, 2(2), 1995, pp. 285-309.
40. C.M. Ringle, S. Wende, and J.-M. Becker, 2015. "SmartPLS 3." Boenningstedt: SmartPLS GmbH, http://www.smartpls.com.
41. C. Barroso, G. Cepeda Carrión, and J.L. Roldán, “Applying maximum likelihood and PLS on different sample sizes: Studies on SERVQUAL model and employee behavior model.” In V.E. Vinzi, W.W. Chin, J. Henseler, and H. Wang (eds.) Handbook of Partial Least Squares: Concepts, Methods, and Applications. Springer: Berlin, 2010, pp. 427-447.
42. G.D. Garson, Partial Least Squares: Regression and Structural Equation Models, Asheboro, NC: Statistical Associates Publishers. 2016.
43. J.F. Hair, C.M. Ringle, and M. Sarstedt, “Partial Least Squares: The Better Approach to Structural Equation Modeling?” Long Range Planning, 45(5–6), 2012, pp. 312–319 (doi: 10.1016/j.lrp.2012.09.011).
44. W.W. Chin, “The partial least squares approach to structural equation modeling,” Modern methods for business research, 295(2), 1998, pp. 295–336.
45. J. Henseler, C.M. Ringle, and M. Sarstedt, “A new criterion for assessing discriminant validity in variance-based structural equation modeling,” Journal of the Academy of Marketing Science, 43(1), 2015, pp. 115–135 (doi: 10.1007/s11747-014-0403-8).
46. C. Fornell, and D.F. Larcker, “Evaluating structural equation models with unobservable variables and measurement error,” Journal of marketing research, 1981, pp. 39–50.
47. R.B. Kline, Principles and practice of structural equation modeling, New York: Guilford publications. 2015.
48. P.M. Podsakoff, J.Y. Lee, and N.P. Podsakoff, “Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies”, Journal of Applied Psychology, 88(5), 2003, pp. 879-903.
49. H. Liang, N. Saraf, Q. Hu, and Y. Xue, “Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management”, MIS Quarterly, 31(1), 2007, pp. 59-87.
50. J. Hair, M. Sarstedt, L. Hopkins, and V.G. Kuppelwieser, “Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research,” European Business Review, 26(2), 2014, pp. 106–121 (doi: 10.1108/EBR-10-2013-0128).
51. J. Cohen, “Statistical power analysis for the behavioral sciences Lawrence Earlbaum Associates,” Hillsdale, NJ, 1988, pp. 20–26.
52. T. Kayworth, and D. Whitten, “Effective Information Security Requires a Balance of Social and Technology Factors”, MIS Quarterly Executive, 9(3), 2010, pp. 2012-2052.
53. M.T. Siponen and R. Willison, “Information security management standards: Problems and solutions”, Information & Management, 46(5), 2009, pp. 267-270.
54. F. Black, “Noise”, The Journal of Finance, 41(3), 1986, pp. 529-543.
55. A. Shleifer, and L.H. Summers, “The Noise Trader Approach to Finance”, Journal of Economic Perspectives, 4(2), 1990, pp. 19-33.
56. L. Menkhoff, “The noise trading approach—Questionnaire evidence from foreign exchange”, Journal of International Money and Finance, 17(3), 1998, pp. 547-564.
57. S. Gregor, “The Nature of Theory in Information Systems”, MIS Quarterly, 30(3), 2006, pp. 611-642.
58. E. Stone, Research Methods in Organizational Behavior, Glenview IL, Scott, Foresman, and Company, 1978.