ADOPTION OF INFORMATION SECURITY AS DECISION-MAKING UNDER UNCERTAINTY: A BEHAVIOURAL ECONOMICS APPROACH

Research in Progress

Egorova, Kristina, National University of Singapore, Singapore, kristina.egorova@nus.edu.sg

Abstract

In this study, we consider the question of adoption of information security technologies at individual level as a problem of decision-making under uncertainty and analyse it using a behavioural economics approach. We highlight the importance of the security adoption question for individuals outside of the organizational setting. In our model, we assume that an individual faces two sources of uncertainty, namely, environmental uncertainty and product uncertainty. An experiment is proposed to derive the utility function by testing personal perceptions toward varying levels of environmental and product uncertainties. Expected results are derived analytically and future research directions are discussed.

Keywords: Information Security Adoption, Decision-Making under Uncertainty, Behavioural Economics, Experiment.

1 Introduction

Given the ubiquitous nature of Information Technology (IT), individuals' adoption of protective technologies outside of the organizational setting remains an important issue. First, outside of the organization, individuals are not protected by corporate information security infrastructures and may not be aware of information security threats and appropriate means of protection. Second, even those individuals, who are concerned about information privacy or security and have the intention to protect themselves, frequently fail to actually do so, meaning that intention may not be predicting actual behaviour in this case (Goes, 2013). Paradoxically, even individuals with high privacy concerns towards the personal details (Acquisti and Grossklags, 2005) admit that they frequently disclose personal data. The aim of our study is to examine the information security adoption process at the individual level outside of the organizational context, since the existing approaches do not allow us understand the decision-making process and predict the outcomes. By conducting this study we hope to help individuals and policy makers to make better decisions, and to contribute to literature on information security adoption, broader IS acceptance literature and to behavioural economics.

From the perspective of behavioural economics, we conceptualized the process of adoption as decision-making under uncertainty. First, we model adoption of protective technology as a conscious process (Anderson and Agarwal, 2010). Second, we model individuals as facing two separate sources of uncertainty – environmental uncertainty and product uncertainty. Environmental uncertainty captures the (subjective) probability of different threats, which corresponded to *risk perception* in prior behavioural models. Product uncertainty emerges from three sources, including product performance uncertainty, description uncertainty and seller uncertainty, and corresponds to *perceived product quality* in prior behavioural models (Dimoka et al., 2012). Finally, we modelled these two sources of uncertainty as acknowledged and separable, which allowed us to model the sources of uncertainty as conditional small worlds (Chew and Sagi, 2008).

In order to verify our model, we design an experiment, in which we propose a way to test individuals' perceptions towards different sources of uncertainty. We expected individuals to recognize the different sources of uncertainty and report reasonable willingness-to-pay prices for the information security software upon the decision. We analyse the expected results in terms of utility models and suggest potential future research directions.

2 Literature Review

The adoption of protective technologies has been investigated by two research perspectives in the information security literature – 1) a behavioural perspective, which is a sub-stream of the mature domain of IS acceptance, and 2) an economics perspective relating to investments in information security.

2.1 Information Security Adoption

From a behavioural perspective, researchers have investigated the adoption of protective technologies at both organizational and individual levels. Most studies assume *conscious use* of the protective technologies. Here, conscious use implies that agents are engaged in a cognitive process of decision-making regarding information security; however a difference was observed between organizational and non-organizational settings. Outside the organizations, individuals may not be exposed to and benefit from security-related training and are unlikely to have security professionals take care of home-owned information systems (Dinev and Hu, 2007, Anderson and Agarwal, 2010). As a result, the decision to protect information assets is voluntary, and only some IS users would consider adopting security software.

Prior research on voluntary adoption of protective measures focused on intention toward the adoption of protective technologies. The work of Dinev and Hu (2007), which was based on the Theory of Planned behaviour, was empirically tested with both university students and IS professionals and found that awareness of protective technology was a strong predictor of the intention to adopt protective measures, whereas classical constructs from the technology acceptance model (i.e., perceived ease of use (PEoU) and perceived usefulness (PU)) were no longer significant in this context. More importantly, the authors controlled for the IT background of the respondents, and found that respondents with basic skills exhibited a stronger relationship between technology awareness and intentions to adopt protection measures, as compared to IT professionals with more advanced skills, for whom awareness led to seek protective solutions from their social circles. Further, Dinev et al., (2008) extended this model by incorporating Hofstede's cultural dimensions as moderators of the relationships between the determinants and behavioural intention. The extended model was supported by data collected in the US and Korea.

Lastly, Herath et al., (2014) studied the intention towards adoption of email authentication service as a form of threat coping behaviour. The authors developed a model based on the Technology Acceptance Model and Technology Threat Avoidance Theory, which was validated through a survey distributed among US university undergraduate students. The results showed that individuals' *perceptions toward risks* in email communication were predictive of intention to adopt email authentication services, and that perceived risk also influenced the perceived usefulness of the protective technology.

Given the importance of security, researchers proposed the idea of influencing intentions towards security precautions with persuasive messages that describe the positive potential consequences of adopting of protective technologies, or conversely, negative outcomes of security rule violations. For example, in the organizational setting, Johnston and Warkentin (2010) found that negatively framed messages (i.e., fear appeal) were effective in improving individuals' compliance with information security policies. This result was somewhat contrasting to those obtained by Anderson and Agarwal (2010), who found, through an experiment conducted with home users, that positive messages had a stronger effect and thus might be more persuasive than negative ones in promoting the use of infor-

mation security software. Given that the Johnston and Warkentin (2010) study was conducted in a non-voluntary context; this might explain the opposite results.

Unfortunately, even influencing intentions toward the adoption of information security measures may not be enough to ensure a desirable secure state since intention may not effectively predict behaviour, as it is typically assumed in general IS adoption models. For example, as pointed out by Goes (2013, p.vii), "… while most individuals are genuinely concerned about security and protecting their privacy, they don't act appropriately to do so." Furthermore, behaviour models (e.g. fear appeal models) do not fully capture the mechanisms of decision making, leaving room for additional experimental-based and/or neural research (Crossler et al., 2013). Therefore, we believe that a focus on the decision-making is warranted in order to help individuals make better important security-related decisions.

2.2 Investments in Information Security

From the economics perspective, studies conducted at organizational level focused on determining the optimal amount of investment, given information security characteristics, such as vulnerability of the assets and the potential losses imposed if a breach occurs (Gordon and Loeb, 2002). Since both vulnerability and potential losses are contingent on the assessment of information security risks, researchers suggested several ways of incorporating existing information into the assessment in order to obtain more precise estimates and proposed approaches such as using value-at-risk (Wang et al., 2008), real options with Bayesian post audit (Herath and Herath, 2008), and game theoretic models (Cavusoglu et al., 2008). From a strategy perspective, Kwon and Johnson (2014) compared proactive and reactive investments, and found that proactive investments were more efficient in the healthcare context.

Even though the adoption of information security is different for general individuals compared those in organizational contexts, the literature on investments helps to understand the complex nature of the information security problem and provides a starting points for analysis, since we need to understand the relationship between the major constructs a decision-maker needs to consider. These constructs include the information assets, security risks and threats, and the security software. Information assets, which are the objects to be protected, need to be assessed so that they may be prioritized. However, this might be challenging due to the intangible nature of IT artefacts. Security risks are contingent on the information assets (e.g., vulnerabilities in the software) and the environment (e.g. probability of attacks). Next, security threats, which are contingent on the information security risks, exhibit varying levels of severity. Finally, for the assessment of the effectiveness of the information security investments, one needs to reveal true value of the security software, which is inherently difficult because security software is credence good (Ekelund et al., 1995).

Prior research relied on the assumption of rationality in decision-making, which is proven to be systematically violated in many research fields such as psychology, marketing, and behavioural economics. The irrationality of decision-making (Ariely, 2009) has several implications in the context of information security, since, as pointed out by (Schneier, 2008), security in general, and information security in particular, is both a feeling and a reality. The reality of information security is mathematical in nature and could be assessed in terms of probabilities, whereas security as a feeling is driven by psychological reactions to risks and perceptions towards used countermeasures and their effectiveness. At the same time, information security is a trade-off between the resources individual can invest (including not only time, money and effort, but also convenience, capabilities, and liberties) and gains in perceived and real security. Schneier (2008) emphasized that due to dual nature of security and human bounded rationality, the real and subjective trade-off of information security might diverge on five aspects. These five aspects include the assessment of severity and probability of information security risks, the assessment of magnitude of the costs of countermeasure implementation, the assessment of the effectiveness of the countermeasure at mitigating the risk and, finally, it might not be clear how well disparate information security threats and countermeasure costs can be compared.

It is rather clear that the aforementioned aspects will have different implications in different contexts. For instance, the incorrect assessment of the security risks will lead to under- or over- investment in

security infrastructure at an organization, and consequent monetary losses if confidentiality, availability and (or) integrity of information is violated. Similarly, individuals' incorrect perception towards the information security threats is likely to lead to smaller monetary, but still unpleasant losses caused by information corruption, loss, or temporal unavailability. Therefore, the divergence between real and perceived trade-offs is potentially dangerous because investments and losses are real (as often measured in monetary terms), whereas security decisions are driven by subjective assessment.

Thus, we conclude from this review that economic models of investments are useful for understanding the problem at first approximation but do not incorporate the psychological factors and the imperfect nature of human-decision making. Since these factors are important in the process of information security adoption, we adopt the methods, models and findings from behavioural economics in order to model the decision-making and account for the characteristics of the information security context.

3 Research Methodology

3.1 Decision-Making under Uncertainty and Source Reference Model

We focus on conscious users of protective technologies – i.e., those who voluntary decided to protect themselves using specialized security software – and assume that users have to make this decision under at least two sources of uncertainty, namely, environmental uncertainty and product uncertainty. Environmental uncertainty captures the (subjective) probability of different information security risks, which might occur and result in violation of information confidentiality, integrity and availability. The subjectivity of the probability arises from the individuals' dual perception of security (Schneier, 2008). From the perspective of behavioural models, environmental uncertainty can be seen as *risk perception*, which can be operationalized through lack of information.

Product uncertainty arises from three sources – i.e., product performance uncertainty, description uncertainty and seller uncertainty (Dimoka et al., 2012). If we think about information security *product performance*, we see that it cannot be revealed unless product fails; therefore information security products are credence goods (Ekelund et al., 1995). Further, *description uncertainty* arises from multiple sources. First, the user might not understand the product description due to her limited ability, knowledge or experience; a seller might not be willing to honestly [fully] describe the product characteristics due to a moral hazard problem; finally, the seller might be not aware of the full product characteristics of the product himself due to a fast changing nature of the technology. Finally, *seller uncertainty* is the perception towards seller reputation, which might be resolved by licensing or by another way of signalling about the quality (e.g. marketing efforts). Altogether, product uncertainty should be interpreted as *perceived quality* of the product.

In order to model the decision-making process, we adopt one of the axiomatic models of decision making under uncertainty, developed by Chew and Sagi (2008), which is a sophisticated version of expected utility (EU) model. The original EU model allows one to understand and predict individual preferences towards choices which have uncertain outcomes. Individuals' preferences can be assessed in terms of probabilities. The model of Chew and colleagues relaxes the rationality assumptions and helps to model more complicated cases.

The main component of the sophisticated model is a *conditional small world*, which is a "*set of possible states with known composition, typically referred to as risk*" (Chew et al., 2013). The model has two attractive characteristics, which would allow us to analyse the individual decision about the adoption of information security software. First, the model allows for probabilistic sophistication of a decision maker, which means that an individual's choices are based on probabilistic beliefs about events. The probabilistic sophistication property of the model is critical in the context of information security: security is a state of being and feeling safe from threats, contingent both on knowledge and perception about the threats and their subjective probability (Schneier, 2008). We conjecture that a decision maker, considering the choice of information security software, assigns probabilistic beliefs to events (or set of events), and makes decisions based on these beliefs. Second, the model has the property of re-

duction of compound lotteries. This means that individuals are indifferent between the ways in which uncertainty is resolved. This property is also essential in our setting due to the credence nature of information security goods. We further make two assumptions about a decision maker's attitude about the way the uncertainty is resolved – 1) *Before an information security breach*, we assume that a consumer is indifferent whether or not she knows the true probability to resolve environmental uncertainty and product uncertainty at the time she is making the decision, or between the order in which this information is provided – the only thing that matters is the perception formed towards the environmental and product uncertainty; and 2) *after the information security breach*, we assume that a consumer is also indifferent between how uncertainty is resolved – since the breach already occurred, there is no longer any product uncertainty, and the only uncertainty which remains is environmental uncertainty (e.g., when will the next attack arrive).

3.2 Experiment Setting

To test the individuals' perceptions towards the two sources of uncertainty and understand whether these sources of uncertainty exhibit the properties of conditional small world events, we propose a 3x3 between-subject experiment. During the experiment, subjects will be shown a textual vignette of the information security landscape and of hypothetical information security software, after which subjects will be asked to fill in a questionnaire. The textual vignettes operationalize three levels of environmental and product uncertainty (See Appendix for actual text vignettes to be used for the treatments). In order to reveal the utility function, subjects will be asked to indicate their *willingness to pay (WTP)* for the information security software.

The manipulations will be verified as follows. For environmental uncertainty, which corresponds to risk perceptions, the *risk perception* construct (Herath et al., 2014) is adapted to test whether the three uncertainty levels correspond to differences in risk perception, whereas for product uncertainty, which corresponds to perceived product quality, the *product quality* construct (Wells et al., 2011) is adapted to test whether the three uncertainty levels correspond to different perceptions of product quality.

We expect subjects to have different levels of knowledge about information security risks and protection mechanisms, as well as different valuation of the information assets. Therefore, we would adapt and use the following measures to capture this.

- Security risks awareness – based on ***Awareness*** construct (Hong and Thong, 2013)
- Security protection awareness – based on ***Technology Awareness*** construct (Dinev and Hu, 2007)
- Valuation of information assets – based on ***PERVAL*** scale (Sweeney and Soutar, 2001)

Finally, we also collect demographic data for controls.

3.3 Expected Results

The analysis of expected results is shown in Table 1. We begin our analysis with one extreme outcome P1E1 – the situation of the (subjectively) complete information, followed by the analysis of all remaining cases up to and E3P3 – the situation of the (subjectively) incomplete information.

In the situation of the subjective complete information, an individual has information about probabilities of information security risks and information about security software failure. We expect the subject to engage in her own risk assessment, and form a subjective probability belief basing on her knowledge and experience, given the information security resources she wants to protect.

In this case, utility can be expressed in a form of subjective expected utility in the following way:

$$U(f) = \Sigma_{i=1} u(x_i) \times P(x_i), \quad (1)$$

where $u(x_i)$ is the utility of the outcome, which depends on characteristic of the information set (i.e., loss conditioned on a breach occurring, λ), characteristics of the information security software (i.e., cost of adoption, β), and the user's demand for feeling / being secure (γ) (Gordon and Loeb, 2002, Cavusoglu et al., 2005); $P(x_i)$ is the subjective (Bayesian) probability formed by individual based on the

information provided and private information.

If the environmental and product uncertainties are independent events, then:

$$P(x_i) = P(E_1) \times P(P_1) \quad (2)$$

In case of two outcomes – x_1 – breach occurs vs. x_2 – breach does not occur – the utility becomes:

$$U(f) = [-u(\lambda) \times P(x_1) - \beta] + [u(\gamma) \times P(x_2) - \beta] \quad (3)$$

In both cases, an individual is paying cost of information security adoption β, which includes the software price and disutility from software installation and use. In case of information security breach (x_1), an individual experiences a disutility λ from the loss conditioned on the breach occurring. In case the information security breach does not occur, or is not discovered (x_2), an individual gains the utility from the feeling / being secure γ.

Next, we have the situation of the (subjectively) partially incomplete information. In this case, subjects are either provided with some information, or not provided with any information about the probabilities of the risks and software failure. Therefore, we expect subjects to understate the risks (since they are not personalized) or exaggerate them (if the description provokes the memories about recently announced information security threats), and these probability beliefs will be the basis for their WTP. However, since the probabilities of the risk and/or software failure are not known, we cannot use the subjective expected utility to derive the utility function. Instead, we assume that both events are conditional small world events, and proceed as follows: we model the increasing levels of product and environment uncertainty as intervals of partial interval ambiguity, where $n_i=0$, $i \in [1, 2]$ refers to the case of subjectively complete information (P1E1), and where $n_i=1$, $i \in [1, 2]$ refers a case of subjectively incomplete information (P3E3). For the small world of product uncertainty, the lottery induced becomes:

$$U_p(f) = (1 - n_1) \times \delta_{c1} + n_1 \times \delta_{d1}, \quad (4)$$

where d is certainty equivalent for unknown domain, $d_1=CE_u$, c is certainty equivalent for known domain $c_1=CE_c$. Similarly, for the small world of environment uncertainty:

$$U_e(f) = (1 - n_2) \times \delta_{c2} + n_2 \times \delta_{d2}, \quad (5)$$

where d is certainty equivalent for unknown domain, $d_2=CE_u$, and c is certainty equivalent for known domain, $c_2=CE_c$. Thus, we would have 3×3=9 different conditions, which are summarized below.

	E1: No uncertainty	**E2: Low uncertainty**	**E3: High uncertainty**
P1: No uncertainty	$n_1 = 0$ $n_2 = 0$ $U_p = \delta_{c1}$ $U_e = \delta_{c2}$	$n_1 = 0$ $0 < n_2 < 1$ $U_p = \delta_{c1}$ $U_e = (1\text{-}n_2) \times \delta_{c2} + n_2 \times \delta_{d2}$	$n_1 = 0$ $n_2 = 1$ $U_p = \delta_{c1}$ $U_e = \delta_{d2}$
P2: Low uncertainty	$0 < n_1 < 1$ $n_2 = 0$ $U_p = (1 - n_1) \times \delta_{c1} + n_1 \times \delta_{d1}$ $U_e = \delta_{c2}$	$0 < n_1 < 1$ $0 < n_2 < 1$ $U_p = (1 - n_1) \times \delta_{c1} + n_1 \times \delta_{d1}$ $U_e = (1 - n_2) \times \delta_{c2} + n_2 \times \delta_{d2}$	$0 < n_1 < 1$ $n_2 = 1$ $U_p = (1 - n_1) \times \delta_{c1} + n_1 \times \delta_{d1}$ $U_e = \delta_{d2}$
P3: High uncertainty	$n_1 = 1$ $n_2 = 0$ $U_p = \delta_{c1}$ $U_e = \delta_{c2}$	$n_1 = 1$ $0 < n_2 < 1$ $U_p = \delta_{c1}$ $U_e = (1 - n_2) \times \delta_{c2} + n_2 \times \delta_{d2}$	$n_1 = 1$ $n_2 = 1$ $U_p = \delta_{c1}$ $U_e = \delta_{d2}$

Table 1 Analysis of Expected Results

4 Conclusion

In this study, we analyse the problem of individual adoption of information security software as decision making under uncertainty. We focus on two main sources of the uncertainty – i.e., environment uncertainty (or perceived information security risks) and product uncertainty (or perceived software quality) – and model them as conditional small worlds. We propose an experiment in order to obtain preliminary results pertaining to individuals' decision making in the context of information security.

We believe that this study can potentially contribute to the literature on information security adoption, to the broader IS acceptance literature, as well as to behavioural economics by providing a context where several potentially sources of uncertainty are separable.

We see several directions for the future research. First, it would be interesting to explore the extent to which individuals recognize product and environment uncertainty, and how far the *perceived* security trade-offs differ from *real* security trade-offs. Second, the testing of our assumption about reduction of compound lotteries could help researchers and practitioners better understand the mechanisms leading to the *perceived-real security trade-off discrepancies* and, hopefully, provide implications for improving the security practices. Third, future studies may focus on different contextual factors of information security adoption, such as different information security risks (e.g.. targeted vs. massive attacks), or different information security software (e.g., firewall vs. intrusion detection system). Finally, our theoretical discussion should benefit from the incorporation of the findings regarding longshot risks, since under some circumstances information security risks might be perceived as risks with very low probabilities of occurrence.

Appendix – Experimental Materials

The vignettes for the two uncertainty treatments (i.e., environmental uncertainty and product uncertainty) are as follows.

Environmental Uncertainty

1. No Uncertainty (E1)

In accordance with the Report on Information Security, the probability of experiencing the information security risk in first half of 2014 has dramatically increased: it remained in the medium range of getting 30% of experiencing attack in the same period in 2013, and rose up to 57% this year, meaning that more than one half of Internet users would be attacked.

2. Low Uncertainty (E2)

In accordance with the Report on Information Security, the probability of experiencing the information security risk in first half of 2014 has dramatically increased: now it is 1.9 times higher as compared to the same period in 2013. This implies more and more Internet uses would be attacked.

3. High Uncertainty (E3)

In accordance with the Report on Information Security, the probability of experiencing the information security risk in first half of 2014 has dramatically increased compared to the same period in 2013. This implies more and more Internet uses would be attacked.

Product Uncertainty

1. No Uncertainty (E1)

Please carefully read the description of information security software. These are the software functions: [1] controls incoming and outgoing network traffic [2] establishes a barrier between a trusted internal network and external non-secure network [3] monitors security events

[4] manages access rights

The assessment of the software company showed that the software, given the updates installation by end user, is able to protect him/her in 95% of cases.

The software is produced by a world's largest vendor of software security products, which is multi-national company with 35 regional offices worldwide. The company currently works in almost 150 countries. The company's products and technologies provide protection for over 170 million users worldwide and more than 150,000 corporate clients globally.

2. Low Uncertainty (E2)

Please carefully read the description of information security software.

These are the software functions:

[1] controls incoming and outgoing network traffic

[2] establishes a barrier between a trusted internal network and external non-secure network

[3] monitors security events

[4] manages access rights

The assessment of software quality showed that the software, given the updates installation by end user, is able to protect him/her.

The software is produced by a large vendor of software security products, which is multi-national company with several regional offices worldwide. The company's products and technologies provide protection individual users worldwide and corporate clients.

3. High Uncertainty (E3)

Please carefully read the description of information security software.

These are the software functions:

[1] controls incoming and outgoing network traffic

[2] establishes a barrier between a trusted internal network and external non-secure network

[3] monitors security events

[4] manages access rights

The assessment of software quality is performed on regular basis and it is recommended to install updates, released by vendor.

The software is produced by a vendor of software security products. The vendor has variety of products for individual and corporate clients.

References

Acquisti, A. and Grossklags, J. (2005), "Privacy and rationality in individual decision making," *IEEE Security & Privacy*, Vol. 2, pp. 24-30.

Anderson, C. L. and Agarwal, R. (2010), "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions," *MIS Quarterly*, Vol. 34, No. 3, pp. 613-643.

Arieli, D. (2009), *Predictably Irrational*, Harper Perennial, London.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2005), "The value of intrusion detection systems in information technology security architecture," *Information Systems Research*, Vol. 16, No. 1, pp. 28-46.

Cavusoglu, H., Raghunathan, S. and Yue, W. T. (2008), "Decision-theoretic and game-theoretic approaches to IT security investment," *Journal of Management Information Systems*, Vol. 25, No. 2, pp. 281-304.

Cherdantseva, Y. and Hilton, J. (2014), "Information security and information assurance: discussion about the meaning, scope, and goals," *Organizational, Legal, and Technological Dimensions of Information System Administration*, IGI Global, Hershey, PA, pp. 167-198.

Chew, S. H., Miao, B. and Zhong, S. (2013), "Partial ambiguity," Working Paper, National University of Singapore.

Chew, S. H. and Sagi, J. S. (2008), "Small worlds: Modeling attitudes toward sources of uncertainty," *Journal of Economic Theory*, Vol. 139, No. 1, pp. 1-24.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research," Computers *& Security*, Vol. 32, pp. 90-101.

DeVellis, R. F. (2003), Scale Development: Theory and Applications, 2nd ed. Sage Publication, Thousand Oaks, CA.

Dimoka, A., Hong, Y. and Pavlou, P. A. (2012), "On product uncertainty in online markets: Theory and evidence," *MIS Quarterly*, Vol. 36, No. 2, pp. 395-426.

Dinev, T., Goo, J., Hu, Q. and Nam, K. (2008), "User behaviour towards protective information technologies: The role of national cultural differences," *Information Systems Journal*, Vol. 19, No. 4, pp. 391-412.

Dinev, T. and Hu, Q. (2007), "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," *Journal of the Association for Information Systems*, Vol. 8, No. 7, Article 23.

Ekelund, R. B., Mixon, F. G. and Ressler, R. W. (1995), "Advertising and information: an empirical study of search, experience and credence goods," *Journal of Economic Studies*, Vol. 22, No. 2, pp. 33-43.

Goes, P. B. (2013), "Editor's comments: Information systems research and behavioral economics," *MIS Quarterly*, Vol. 37, No. 3, pp. iii-viii.

Gordon, L. A. and Loeb, M. P. (2002), "The economics of information security investment," *ACM Transactions on Information and System Security*, Vol. 5, No. 4, pp. 438-457.

Herath, H. S. B. and Herath, T. C. (2008), "Investments in information security: A real options perspective with Bayesian postaudit," *Journal of Management Information Systems*, Vol. 25, No. 3, pp. 337-375.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J. and Rao, H. R. (2014), "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service," *Information Systems Journal*, Vol. 24, No. 1, pp. 61-84.

Hong, W. and Thong, J. Y. L. (2013), "Internet privacy concerns: an integrated conceptualization and four empirical studies," *MIS Quarterly*, Vol. 37, No. 1, pp. 275-298.

Johnston, A. C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: An em-

pirical study," *MIS Quarterly*, Vol. 34, No. 3, 549-566.
Kwon, J. and Johnson, M. E. (2014), "Proactive versus reactive security investments in the healthcare sector," *MIS Quarterly*, Vol. 38 No. 2, p. 451-471.
Suby, M. (2014), "The 2013 (ISC)2 Global Information Security Workforce Study," https://www.isc2cares.org/giswsrsa2013/, ISC p. 27.
Moore, G. C. and Benbasat, I. (1991), "Development of an instrument to measure the perceptions of adopting an information technology innovation," *Information Systems Research*, Vol. 2, No. 3, pp. 192-222.
Schneier, B. (2008), "The psychology of security," *Progress in Cryptology–AFRICACRYPT 2008*, Springer, pp. 50-79.
Sweeney, J. C. and Soutar, G. N. (2001), "Consumer perceived value: The development of a multiple item scale," *Journal of Retailing*, Vol. 77, No. 2, pp. 203-220.
Wang, J., Aby, C. and Rao, H. R. (2008), "A value-at-risk approach to information security investment," *Information Systems Research*, Vol. 19, No. 1, pp. 106-120.
Wells, J. D., Valacich, J. S. and Hess, T. J. (2011), "What signals are you sending?: How website quality influences perceptions of product quality and purchase intentions," *MIS Quarterly*, Vol. 35, No. 2, pp. 373-396.