Asia Pacific Journal of Information Systems
Vol. 26 No. 2 (JUNE 2016), 290-298

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
http://dx.doi.org/10.14329/apjis.2016.26.2.290

Cognitive Bias and Information Security Research: Research Trends and Opportunities

Jongpil Park[a,*], Chang-Gyu Oh[b]

[a] *Assistant Professor, College of Economics and Commerce, Department of e-Business, Kyungnam University, Korea*
[b] *Professor, College of Economics and Commerce, Department of e-Business, Kyungnam University, Korea*

A B S T R A C T

Human cognition and decision-making related to information systems (IS) is a major area of interest in IS research. Among these areas, cognitive bias rooted in behavioral economics is gaining considerable attention from researchers. In the present study, we identify the role of cognitive biases and discuss how they shape the information security behavior. We also seek research opportunities to provide directions and implications for future research.

Keywords: Cognitive Bias, Behavioral Economics, Information Security, Affect Heuristics, Goal Framing, Optimistic Bias

Ⅰ. Introduction

Information security research focuses on the human factor, as well as technical aspect. This is because humans are considered to be information security's weakest link (Crossler et al., 2013). In particular, information security research needs to understand 'how to boost individuals' security behavior.' Therefore, it is critical to understand how individuals internalize to shape security-related decision making (Tsohou et al., 2015).

One particular phenomenon based upon psychology perspective that is related to human decision-making is gaining attention in IS research - the so called cognitive bias rooted in behavioral economics. The cognitive bias has much potential to information security research (Fleischmann et al., 2014; Goes, 2013; Tsohou et al., 2015).

However, little is known about the role of cognitive bias in the discipline of information security research. In present study, we identify the role of cognitive biases and discuss these biases how to shape information security behavior. Further, we seek to research opportunities on behalf of cognitive biases

*Corresponding Author. E-mail: jpark@kyungnam.ac.kr Tel: 82552492461

<Table 1> Two Modes of Thinking (Slovic et al., 2004)

Analytic system	Experiential system
1. Analytic	1. Holistic
2. Logical: reason oriented	2. Affective: pleasure-pain oriented
3. Logical connections	3. Associationistic connections
4. Behavior mediated by conscious appraisal of events	4. Behavior mediated by "vibes" from past experiences
5. Encodes reality in abstract symbols, words, and numbers	5. Encodes reality in concrete images, metaphors, and narratives
6. Slower processing: oriented toward delayed action	6. More rapid processing: oriented toward immediate action
7. Requires justification via logic and evidence	7. Self-evidently valid: "experiencing is believing"

for further research.

Therefore, in the present study, we aim to address research trends and opportunities, and thus close a gap in the research on cognitive biases in IS security. Specifically, we investigate the two primary research questions. First, what is the current state of research on cognitive biases in IS security? Second, what are the research opportunities for future research on cognitive biases in IS security?

To do so, this study intends to provide grounded avenues and directions for future research. Therefore, we believe that these attempts contribute to have further advance the explanatory and predictive capabilities of IS security research.

Ⅱ. Cognitive Bias in IS Security

2.1. The Role of Biases in Human Cognition and Decision-making

Human cognition and decision-making related to information systems have been served as one of major areas in IS research. Although it has been premised that humans are rational, humans often hesitate and make decisions not entirely based on rationality (Goes, 2013). Therefore, humans' decision-making is subject to psychological biases which make them interpret information in various ways (Camerer and Loewenstein, 2004).

Research have revealed that there are two modes of human thinking (Tsohou et al., 2015). Slovic, Finucane, Peters, and MacGregor (2004) used the term the "Experiential System" and "Analytic System". Kahneman and Frederick (2002) named them "System 1" and "System 2".

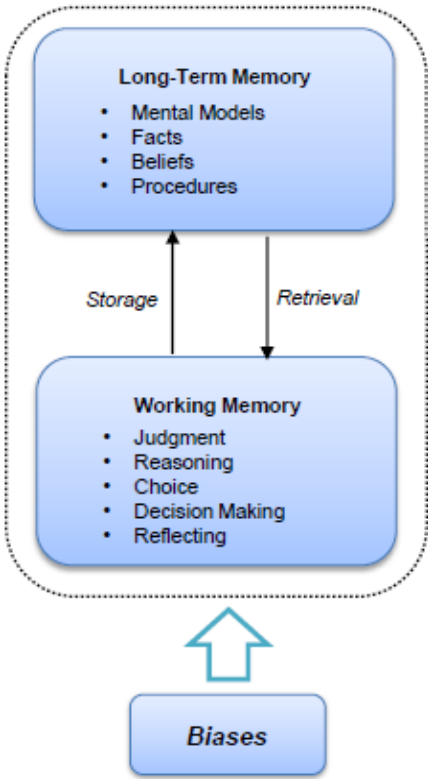
The experiential system depends primarily on heuristics and guides to biased decisions. On the other hand, the analytic system is oriented towards algorithmic processing and seeks for the best option (refer to <Table 1>, for more details).

The two systems work in parallel and complement one another. However, the two systems often trigger irreconcilable or even opposing results. Further, certain cases lead to systematic errors. The systematic errors are referred as 'cognitive biases'.

2.2. Cognitive Bias

Cognitive biases are defined as systematic errors in human cognition and decision-making. Cognitive biases lead objectively irrational decisions or suboptimal results (Wilkinson and Klaes, 2012). In particular, cognitive biases can be effectively utilized in risk-perceiving decisions (Tsohou et al., 2015).

We identify several cognitive biases in information security research, such as affect heuristic, goal framing, and optimistic bias. These biases affect in-



<Figure 1> Cognition Model (Brown and Parsons, 2012)

dividuals' judgment, choice and decision-making, as shown in <Figure 1>. Specifically, Browne and Parsons (2012) proposed the cognition model. According to the cognition model, individuals' biases affect one's working memory (i.e., one's judgment, reasoning, choice, decision-making, and reflecting). Then, ultimately, one's working memory forms the long-term memory (i.e., one's mental models, facts, beliefs, and procedures). Therefore, the cognition model depicts a role of biases toward individuals' mentality.

2.1.1. Affect Heuristic

The affect heuristic refers to a mental shortcut by using individuals' affective impression (Tsohou et al., 2015). In other words, the affect heuristic enables individuals to make a decision based upon an affect rather than rational judgment.

In particular, the affect heuristic promotes to the "risk du jour" mentality (Tsohou et al., 2015). For example, Finucane et al. (2000) argued that affect heuristic can be an important cue to make risk-related decision-making. Pfleeger and Caputo (2012) described if users noticed little risk on IS security, the system should have an effective security design that encourages users to perceive higher risk by using affect heuristic.

2.1.2. Goal Faming

Kaheman and Tversky (1979) proposed a schema for how people frame economic outcomes as gains and losses. They found that individuals have a response to losses that is more extreme than the response to gains. It is referred to as goal framing.

Goal framing arises when alternative framing of contextually same information produces different decisions. Therefore, individuals react differently to the same information that has been presented in varying manners by the use of different wordings, contents and other presenting types (Tversky and Kahneman, 1981).

A number of studies have demonstrated the influence of goal framing on decision making behaviors. Among them, in the domain of IS security, Anderson and Agarwal (2010) employed the concepts of goal framing to develop the most effective message cues for enhancing home computer security attitudes and behaviors. Specifically, the study was conducted a laboratory experiment using gain- and loss-frame. They found that goal framing partially influence on home computer security attitudes and behaviors.

<Table 2> Primary Research on Cognitive Bias in IS Security

Cognitive Bias	Descriptions	Research
Affect Heuristic	The bias is a mental shortcut that enables individuals to make judgments and decisions hesitantly based upon affective impressions	·Finucane et al. (2000) ·Pfleeger and Caputo (2012)
Goal Framing	The bias occurs as alternative descriptions of choice and its outcomes. Either one as gains or as losses and may lead to different reactions.	·Anderson and Agarwal (2010)
Optimistic Bias	The bias refers that individuals believe they are less at risk of experiencing a negative event compared to others.	·Rhee et al. (2005) ·Rhee et al. (2012)

2.1.3. Optimistic Bias

The optimistic bias refers to as a cognitive bias that individuals believe they are less at risk of experiencing a negative event compared to others (Warkentin et al., 2013). Optimistic bias has been variously referred to as 'unrealistic bias' or 'self-favoring bias' (Hoorens, 1995; Rhee et al., 2012). Optimistic bias has been mainly studied in the area of health and crime. For example, individuals who smoke believe that they are less likely to have diseases or lung cancer than other smokers. This is because individuals tend to believe that they are less at risk of experiencing a negative event.

In the context of information security, a recent field survey conducted by AOL (American Online) and NCSA (National Cyber Security Agency) (2004) empirically demonstrated optimistic bias of users. Surprisingly, the study reported that users believe that they are less at risk of computer virus infection. In addition, Rhee et al. (2005) examined that general users have an optimistic bias associated with information security. Rhee et al. (2005) found that general users perceive that their risk is significantly lower than their friends and average other users. More recently, Rhee et al. (2005) also investigated that MIS (management information systems) executives have optimistic bias. Rhee et al. (2012) found that the MIS executives perceived the information security of their companies risk significantly lower than that of their comparison targets, such as their business partners and general companies.

In summary, we identified several cognitive biases applied in information security research, as shown in <Table 2>.

Ⅲ. Research Opportunities

Recent research on cognitive bias in information security research have been extending their scopes. Through extensive literature reviews, we found that the cognitive bias research are applying into new research areas, such as designing in security awareness stimulus, developing software update notices for users' security protection, and neurosecurity.

3.1. Cognitive Bias and Security Awareness Stimuli

Recently, cognitive bias has been applying into designing security awareness stimulus (Tsohou et al., 2015). For example, as shown in <Figure 2>, the security awareness poster on password use and management provided by ENISA (European Network and Information Security Agency) highlights the 'use of strong password' posters in a common way. On the other hand, the poster proposed

by Minnesota State College and Universities is combined with an affect heuristic stimulus, as shown in <Figure 3>. Comparing to those security awareness stimuli, the security poster proposed by Minnesota State College and Universities is more effective than ENISA's poster due to the emotional stimulus from the affect heuristic.

<Figure 2> Neutral Poster for Strong Password (ENISA)

3.2. Cognitive Bias and Software Security Protection

Recent research on cognitive bias have been utilizing in developing software update notices. For example, Fleischmann, Grupp, Amirpur, and Hess (2015) tested the acceptance of software update notices for security protection in professional and private IS usage. Specifically, they employed the concept of goal framing and examined the effects of gaining and loosing features in professional and private IS usage. As a result, they found that expert and novice users showed different reactions to software updates. Specifically, novice users showed a significant higher continuance intention when gaining the feature. On the other hand, experts showed a significant lower continuance intention when gaining the feature through software updates. Therefore, this study attempts to explains the psychological mechanism based upon cognitive bias (i.e., goal framing).

<Figure 3> Affect-appealing Poster for Strong Password (Minnesota College and State University)

3.3. Cognitive Bias and Neurosecurity

Recent research on cognitive bias have been extended to Neurosecurity. Neurosecurity refers to as the application of neuroscience to behavioral information security to better understand and improve users' security behaviors (Anderson et al., 2014). Neurosecurity offers new insights into cognitions and individual behaviors in the context of information security research.

The potential of neurosecurity has been recognized

by security researchers. Research methodologies have begun using neurophysiological methods to investigate security behavior (Anderson et al., 2014). Specifically, neurosecurity methodologies include eye and mouse cursor tracking, electroencephalography (EEG) and functional magnetic resonance imaging (fMRI) (refers to <Figure 4>). These tools enable to reveal the "black box" of individual cognition and behaviros (Anderson et al., 2014).

By using those neurophysiological methods, neurosecurity research are seeking to better understand and improve individuals' security cognitions and behaviors. For example, Anderson et al. (2015) used fMRI to investigate the problem of attenuated attention to security warning messages. Anderson et al. (2015) focused on the repetition suppression bias which affects individuals' cognition and developed a polymorphic security message composed of the visual variations. Through a laboratory experiment based upon fMRI, they demonstrated the polymorphic warning was effective to be reduced habituation to security warnings.

<Figure 4> Electroencephalography (EEG) Test

In addition, Anderson et al. (2015) investigated the effect of gender's cognition differences in user responses to security messages. As a result, Anderson et al. (2015) attempted to have an empirical evidence that significant gender-based differences exist in the brain. They employed an electroencephalography (EEG) laboratory experiment and acquired convincing evidence that gender plays an important role in how users process security messages. Therefore, the findings indicate it is useful in designing security messages that adapt to gender's cognitive characteristics.

To summarize, these neurosecurity studies offer new insights into cognitions and individual behaviors.

Ⅳ. Concluding Remarks

This study provides research trends and opportunities on cognitive biases in information security research. In particular, we identified the role of cognitive biases in IS security, such as affect heuristic, goal framing, and optimistic bias. Further, we attempted to seek research opportunities for future research.

These attempts seek to the current state of research as well as the promising avenues for future research on cognitive biases in the discipline of IS security. Therefore, this study provides a comprehensive theoretical background for further research on the role of cognitive biases in IS security.

In addition, this study provides a set of practical guidelines for enhancing the design and implementation of security. Specifically, we identified prominent cognitive biases (i.e., affect heuristic, goal framing, and optimistic bias) that have been proven to influence users' intention to comply with IS security. Therefore, our study provide a practical implication how security standards and practices can

be adapted to provide more effective guidance for designing and implementing security, taking into consideration the role of cognitive biases.

<References>

[1] Anderson, C.L. and Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643.

[2] Anderson, B.B., Vance, A., Kirwan, B., and Eargle, D. (2014). *How users perceive and respond to security messages: A neuroIS research agenda and empirical Study*. Working paper, Brigham Young University, USA.

[3] Anderson, B.B., Kirwan, C.B., Jenkins, J.L., Eargle, D., Howard, S., and Vance, A. (2015). How polymorphic warnings reduce habituation in the brain insights from an fMRI study. In *Proceedings of CHI*.

[4] AOL/NCSA. (2004). *AOL/NCSA online safety study*; Research Report, American Online and the National Cyber Security Alliance.

[5] Browne, G.J. and Parsons, J. (2012). More enduring questions in cognitive IS research. *Journal of the Association for Information Systems, 13*(12), 1000-1011.

[6] Camerer, C.F., and Loewenstein, G. (2004). *Behavioral Economics: Past, Present Future*, in: Advances in Behavioral Economics, Princeton University Press.

[7] 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, 32*(1), 90-101.

[8] ENISA. (2010). *The new users' guide: How to raise information security awareness*. Retrieved from, http://www.enisa.europa.

[9] Finucane, M.L., Alhakami, A., Slovic, P., and Johnson, S.M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making*, *13*(1), 1-17.

[10] Fleischmann, M., Amirpur, M., Benlian, A., and Hess, T. (2014). Cognitive biases in information systems research: A scientometric analysis. In: *Proceedings of the 22nd European Conference on Information Systems, Tel Aviv, Israel*.

[11] Fleischmann, M., Grupp, T., Amirpur, M., and Hess, T. (2015). Gains and losses in functionality: An experimental investigation of the effect of software updates on users' continuance intentions. In: *Proceedings of the 36th International Conference on Information Systems, Fort Worth, USA*.

[12] Goes, P.B. (2013). Editor's comments: Information systems research and behavioral economics. *MIS Quarterly*, *37*(3), iii-viii.

[13] Hoorens, V. (1995). Self-favoring biases, self-presentation, and the self-other asymmetry in social comparison *Journal of Personality*, 63(4), 793-817.

[14] Kahneman, D. and Frederick, S. (2002). *Representativeness revisited: Attribute substitution in intuitive judgment*. In: Heuristics and biases. Cambridge University Press.

[15] Kahneman, D. and Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263-291.

[16] Pfleeger, S.L., and Caputo, D.D., (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*, 597-611.

[17] Rhee, H.S., Ryu, Y.U., and Kim, C.T. (2005). I am fine but you are not: Optimistic bias and illusion of control on information security. In: *Proceedings of the 26th International Conference on Information Systems, Las Vegas, NV, USA*.

[18] Rhee, H. S., Ryu, Y. U., and Kim, C. T. (2012). Unrealistic optimism on information security management. *Computers & Security*, *31*(2), 221-232.

[19] Slovic, P., Finucane, M.L., Peters, E., and MacGregor, D.G. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis, 24*(2), 311-322.

[20] Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems, 24*(1), 38-58

[21] Tversky, A., and Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science, 211*(4), 453-458.

[22] Warkentin, M., Xu, Z., and Mutchler, L.A. (2013). I'm safer than you: The role of optimism bias in personal IT risk assessments. In: *Proceedings of IFIP Security Research Workshop, Niagara, NY, USA.*

[23] Wilkinson, H., and Klaes, M. (2012). *An Introduction to Behavioral Economics*. Palgrave, New York, NY.

◆ About the Authors ◆

Jongpil Park

Dr. Jongpil Park is an assistant professor in the Department of e-Business at Kyungnam University. He received a Ph.D. in Management Information Systems from Yonsei University, Seoul, Korea. He holds an M.S from New York University. His works have been published in International Journal of Information Management (IJIM), Asia Pacific Journal of Information Systems (APJIS), Information Systems Review (ISR), and so forth. His research primarily focuses on Behavioral IS security and Neuro-security applied in cognitive science.

Chang-Gyu Oh

Dr. Chang-Gyu Oh is a Professor in the Department of e-Business at Kyungnam University. He holds a Ph.D. in Management Information Systems from Pusan National University. He was a visiting scholar at the University of Texas at Dallas. His current research interests focus on the technology acceptance issues related to pervasive informatics. Especially his passion for making people happier in all aspects of IT happiness flows through in the ICT industry coverage he provides. His work has been published in various kinds of IS journals.

Submitted: January 28, 2016; 1st Revision: May 20, 2016; Accepted: May 30, 2016