Neuroscience Foundations for Human Decision Making in Information Security: A General Framework and Experiment Design

Bin Mai[1], Thomas Parsons[1], Victor Prybutok[1], Kamesh Namuduri[1]
[1]University of North Texas, Denton, U.S.A
{bin.mai, thomas.parson, victor.prybutok, Kamesh.namuduri@unt.edu}

Abstract: In this paper, we propose a conceptual model for information security (InfoSec) decision making that is based on cognitive science and neuroscience, and present a comprehensive framework of InfoSec decision making process. In addition, we illustrate a specific experiment design that could be used to investigate how specific automatic affective processes would impact specific components of the InfoSec decision making process.

Keywords: information security, decision making, Neuroscience, NeuroIS, conceptual framework, affective executive control, cognitive executive control, experiment design

1. Introduction

The main focus of this paper is to present a basic framework for applying neuroscience concepts, theories, and tools to studying human decision making in information security situations. Information security (InfoSec) has been a significant issue in the society, exacerbated by the current "big data" environment in today's global society [1]. By the very nature of information security, this field has been an intersection among engineering technology, economic incentive design, and human behavior [2]. Among the various aspects of InfoSec issues, human decision making during real InfoSec situations remains one of the most critical and under-investigated issues in InfoSec [3, 4]. After all, it is human decision making that ultimately determines the outcomes of InfoSec planning and implementation. By understanding the details how individuals make such decisions and how various factors could influence these decision making processes, we would be able to design better information systems artifacts, develop better policies and regulations, provide better training / education, construct a better culture and environment, all from the perspectives of facilitating the individuals to make better InfoSec decisions and thus achieve more desirable InfoSec outcomes.

Traditionally, IS researchers interested in the determinants of behavior have emphasized controlled (conscious) processing of perceptions and intentions over automatic (unconscious) processing of information. Quite often, researchers have studied InfoSec's controlled decision making processes by analyzing data collected through

mostly surveys and interviews, constructing empirical models for decision making process, and developing analytical and quantitative models to derive optimal decision strategies, all based on the standard assumption of the decision makers being rational agents [5-7]. While this stream of research has yielded valuable insights towards InfoSec decision making, there exist significant gaps which are not well explained by the current methodologies [8].

Recently IS research has begun to emphasize the role that habit plays in the post-adoption stage of usage, in which the behavior turn out to be more automatic and may be performed with a reduced amount of controlled (conscious) processing. Researchers have also studied the role of habit in InfoSec contexts [9-11]. However, one concern for current approaches to studying InfoSec decision making is that the use of self-report methods are insufficient for assessing user mental state given the profound limitations of survey methods for measuring relatively automatic (unconscious) heuristics and biases as they are less accessible to introspection [12]. Moreover, in search for more objective and comprehensive approaches to studying InfoSec decision making, researchers are increasingly embracing advances in neuroscience theories, techniques, and tools, such as psychophysiological metrics and neuroimaging techniques, because they offer promise in alleviating the limitations found in subjective self-reports through more direct and objective measurement of automatic processes [13]. Still, what are lacking in the InfoSec literature include a general framework to facilitate the investigation of InfoSec decision making with these new approaches, and some concrete examples for implementing this framework.

In this paper, following the NeuroIS Research Framework proposed by [14], we formulate our research question as: how can we systematically incorporate relevant neuroscience theories, techniques, and tools into the study of InfoSec decision making to make it more objective, accurate, and realistic? In addressing this question, we make three contributions to the literature of InfoSec decision making. First we propose a general framework for InfoSec decision making that is based on cognitive science and neuroscience. Second, in our propose framework, we explicitly emphasize the different roles played by controlled cognitive processes and automatic affective processes. And last but not least, we describe a specific experiment design that could be used to investigate how specific automatic affective processes would impact specific components of the InfoSec decision making process.

2. A General Framework for Neuro-scientific InfoSec Decision Making

InfoSec decision making is one specific type of general decision making. However, there are two components that are particularly significant in the InfoSec decision making context: risk and uncertainty [15]. Within InfoSec context, risk often refers to the likelihood that information assets are insufficiently protected against certain types of

damages or loss [16]; and uncertainly usually refers to one form of manifestation of information asymmetry [17]. Traditionally, a widely accepted model for decision making has been the Observe–Orient–Decide–Act (OODA) Loop proposed by [18]. It is a model originally design for understanding decision making processes adopted by military commanders to enhance command and control. However, as [19] pointed out, the OODA model "has a number of problems as a framework of human decision making" including the failure to account for the "necessary dependence of perception on preexisting knowledge and concepts" during decision making. To address the deficiencies of the OODA paradigm, [19] proposed a cognitive science based framework of decision making, the CECA (Critique, Explore, Compare, Adapt) framework to model individual decision making. Although both OODA and its extension CECA originated within a military context, their acceptance and application have since gone beyond the military decision making situations, and have become an important decision model in a wide range of decision making scenarios including emergency response [20], system safety development [21], and significantly, InfoSec [3], in which it is pointed out that OODA and CECA "could be a usable framework for the security manager's decision process" (p.60). In addition, the CECA framework specifically addresses the issues of risk and uncertainty. Therefore, in this paper we integrate this CECA paradigm with the OODA framework elements to model InfoSec decision making processes. The overall framework for the InfoSec decision making can thus be illustrated by the following figure:

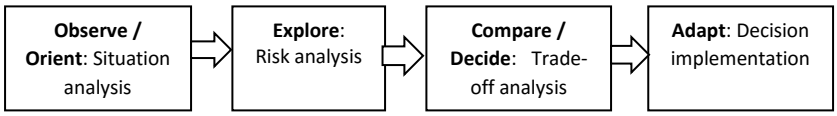

Fig. 1. The framework for InfoSec decision making

More specifically, the InfoSec decision making process would include the following procedures:

1. Situation analysis – (Observe / Orient)
   a. Recognizing whether this is an infosec situation (formulate questions/identify info needs, define security mission/develop security goals)
2. Risk analysis (Explore)
   a. Threat analysis (what are the threats; the probability of the threats being realized; the damage if the threats are realized)
   b. Counter measure analysis (what are the counter measures; the effectiveness of the counter measures; the costs for implementing the counter measures)
3. Trade-off analysis (Compare / Decide)
   a. Alternatives analysis (what are the available alternatives of actions to take)

b. Mental algebra (compute and compare the overall expected payoffs/costs of each alternative)
c. Decide on which alternative to take

4. Implement the decision (Adapt)
   a. Actually implement the decision once it is made.

The above framework places significant emphasis on the role of information collection in each of the steps during decision making process, and thus focus more on the factors of controlled cognitive processes and their influence on the decision making process. However, as pointed out in previous section, the uncontrolled and automatic processes also play a significant role in influencing each of the steps of the decision making process. We need to extend the above framework to explicitly incorporate such factors to complement the existing controlled processes and provide a more comprehensive picture of InfoSec decision making.

One field that holds great promise in contributing to the above goal of InfoSec decision making framework is neuroscience, which is the science that explains how human brain works. A component missing from most InfoSec scenarios research is the reality that controlled decision making may include affective recognition and evaluation of stimuli. Affective stimuli are particularly potent distracters that can reallocate processing resources and impair attentional performance [22]. In addition to the cognitive appraisal of a stimulus, affective reactions are characterized by psychophysiological changes (e.g., alterations in skin conductance and heart rate; as well as behavioral approach or avoidance) and involve a number of subcomponents occurring in frontal subcortical circuits [23-25]. According to models of neurovisceral integration, autonomic, attentional, and affective systems are simultaneously engaged in the support of self-regulation [26, 27].

Based on the above neuroscience findings, we expand the above general InfoSec decision making process model via the inclusion of a dual-process approach to modeling decision making, in which both automatic affective and cognitive processes perform essential roles in controlled decision making: 1) automatic processing is reflexive, rapid, and led by heuristics and biases. They operate automatically, intuitively, involuntarily, and effortlessly; and 2) controlled cognitive processing refer to the people's reflective, logical, and rational decision making.

Therefore, our proposed general framework for neuro-scientific InfoSec decision making can be illustrated by the following figure:

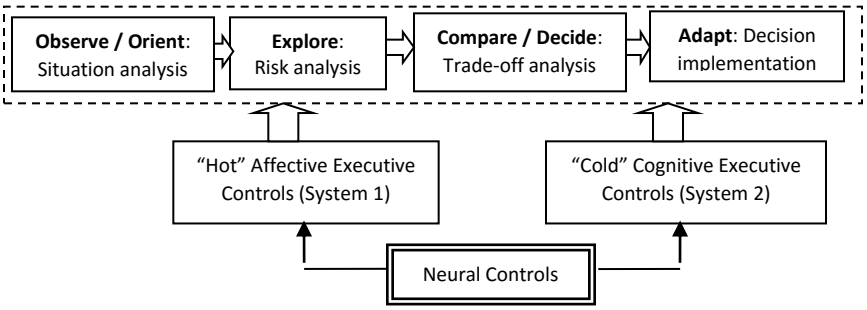

Fig. 2. A general framework for neuro-scientific InfoSec decision making

Based on our propose framework, we lay out the foundation for the following tasks: (i) investigate and determine the neural correlates (brain areas) of automatic and controlled decision making during InfoSec situations; (ii) investigate and develop comprehensive models for automatic, as well as controlled, human decision making during InfoSec situations, aiming to incorporate/map the neural correlates of decision making processes; (iii) identify possible automatic affective and cognitive biases and associated neural processes during the controlled infoSec decision making; and (iv) design and develop mechanisms, based on theoretical foundations for decision making, to influence human decision making during information security situations, in order to overcome identified affective and cognitive biases and achieve optimal information security outcomes.

3. A Research Experiment Design

In this proposed project, we aim to establish an approach to cognitive (task engagement) and affective (arousal) state estimation for cyber threat detection. Based on our proposed model, this is a topic of the impacts of System 1 and 2 factors on the observe/orient process of InfoSec decision making. The psychophysiological signals from users could be logged as participants experience various stimulus modalities aimed at assessing automatic and controlled cognitive and affective processing. Psychophysiological metrics and event-related potentials (ERP) have been used to infer various aspects of an individual such as personality, memory and preferences. More specifically, the following methodologies can be adopted:

- ***Psychophysiological Metrics for Establishing Indices of Arousal (System 1):*** Psychophysiological techniques (e.g., cardiovascular reactivity, skin conductance response, respiration, EEG source models of connectivity) allow for enhanced understanding of the ways in which emotion and cognition interact [28, 29]. In addition to autonomic measures and EEG spectral power and waveforms, interactions between pairs of EEG oscillations – such as phase synchronization and coherence –

have also been implicated in affective states of hedonic arousal [30].

- ***Psychophysiological Metrics for Establishing Indices of Cognitive Control (System 2):*** Using psycho-physiological metrics to measure cognitive processing has been widely used. Results suggest that autonomic and EEG engagement reflects information gathering, visual processing, and attention allocation [31].
- ***Data Analytics:*** The psychophysiological data could then be filtered to get separate frequency bands to train cognitive-affective classifiers with classification techniques such as support vector machines, naïve Bayes, and k nearest neighbors [32].

A "Psychophysiological Baseline" would be established for each participant. To establish each participant's "Psychophysiological Baseline" (minimum brain wave and autonomic activity) participants would be told "to relax and try not to think about anything" as they stare at a blank screen for 2:00 minutes. Next, the participant would take part in the following cognitive workload and arousal tasks to establish maximal physiological responses: 1) a "Two Picture Cognitive Task" would be used to establish a cognitive workload signature for the user [33]; 2) the International Affective Picture System (IAPS) would be used to establish the affective load signature of the user; and 3) the cyber threat scenario. Task presentation order would be counter-balanced across participants.

To assess psychophysiological reactivity to the cyber threat scenario, we would compute reactivity scores for cognitive workload and affective load by 1) subtracting "Psychophysiological Baseline" values from the cyber threat scenario; and 2) comparing Cognitive and Arousal indices to values from the insider threat scenario.

Due to length limit of the paper. We omit the description of our data analysis process.

4. Conclusion

In this paper, we proposed a general framework for neuro-scientific InfoSec decision making. The framework is based on cognitive science and incorporates two important categories of neural controls that would impact the InfoSec decision making processes: automatic affective executive controls and controlled cognitive executive controls. We illustrate how this proposed framework can be the foundation for the development of a comprehensive model of neuro-scientific InfoSec decision making, and discuss some specific research questions that can be addressed through our framework. In addition, we provide a detailed description of a scientific research experiment project that is based on our proposed conceptual framework.

The immediate next step would be to embellish details of our basic framework, and accordingly identify specific automatic and controlled executive controls significant in InfoSec decision making behaviors. We would then hypothesize the functioning mechanisms of those controls in terms of how they impact the InfoSec decision making, and conduct lab experiment to empirically investigate those mechanisms.

References

1. Wang, H., Jiang, X., Kambourakis, G.: Special issue on Security, Privacy and Trust in network-based Big Data. Inf. Sci. 318, 48-50 (2015)
2. Chatterjee, S., Sarker, S., Valacich, J.S.: The behavioral roots of information systems security: Exploring key factors related to unethical IT use. Journal of Management Information Systems 31, 49-87 (2015)
3. Pettigrew III, J.A., Ryan, J.J.: Making Successful Security Decisions: A Qualitative Evaluation. IEEE Security & Privacy 60-68 (2012)
4. Schneier, B.: The psychology of security. Progress in Cryptology–AFRICACRYPT 2008, pp. 50-79. Springer (2008)
5. Arora, A., Nandkumar, A., Telang, R.: Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. Information Systems Frontiers 8, 350-362 (2006)
6. Fang, F., Parameswaran, M., Zhao, X., Whinston, A.B.: An economic mechanism to manage operational security risks for inter-organizational information systems. Information Systems Frontiers 16, 399-416 (2014)
7. Hsu, J.S.-C., Shih, S.-P., Hung, Y.W., Lowry, P.B.: The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness. Information Systems Research 26, 282-300 (2015)
8. Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. IEEE Security & Privacy 26-33 (2005)
9. Ng, B.-Y., Kankanhalli, A., Xu, Y.C.: Studying users' computer security behavior: A health belief perspective. Decision Support Systems 46, 815-825 (2009)
10. Pahnila, S., Siponen, M., Mahmood, A.: Employees' behavior towards IS security policy compliance. In: System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on, pp. 156b-156b. IEEE, (Year)
11. Vance, A., Siponen, M., Pahnila, S.: Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management 49, 190-198 (2012)
12. Woodside, A.G.: Overcoming the illusion of will and self-fabrication: Going beyond naïve subjective personal introspection to an unconscious/conscious theory of behavior explanation. Psychology & Marketing 23, 257-272 (2006)
13. Pavlou, P., Davis, F., Dimoka, A.: Neuro IS: the potential of cognitive neuroscience for information systems research. ICIS 2007 Proceedings 122 (2007)

14. vom Brocke, J., Liang, T.-P.: Guidelines for neuroscience studies in information systems research. Journal of Management Information Systems 30, 211-234 (2014)
15. West, R.: The psychology of security. Communications of the ACM 51, 34-40 (2008)
16. Straub, D.W., Welke, R.J.: Coping with systems risk: security planning models for management decision making. Mis Quarterly 441-469 (1998)
17. Grossklags, J., Christin, N., Chuang, J.: Secure or insure?: a game-theoretic analysis of information security games. In: Proceedings of the 17th international conference on World Wide Web, pp. 209-218. ACM, (Year)
18. Boyd John, R.: A Discourse on Winning and Losing. Air University document MU43947, briefing 1, (1987)
19. Bryant, D.J.: Rethinking OODA: Toward a Modern Cognitive Framework of Command Decision Making. Military Psychology 18, 183 (2006)
20. Romanowski, C., Raj, R., Schneider, J., Mishra, S., Shivshankar, V., Ayengar, S., Cueva, F.: Regional response to large-scale emergency events: Building on historical data. International Journal of Critical Infrastructure Protection 11, 12-21 (2015)
21. Trotter, M.J., Salmon, P.M., Lenne, M.G.: Impromaps: Applying Rasmussen's Risk Management Framework to improvisation incidents. Safety science 64, 60-70 (2014)
22. Dolcos, F., McCarthy, G.: Brain systems mediating cognitive interference by emotional distraction. The Journal of Neuroscience 26, 2072-2079 (2006)
23. Bonelli, R.M., Cummings, J.L.: Frontal-subcortical circuitry and behavior. Dialogues in clinical neuroscience 9, 141 (2007)
24. Pessoa, L.: How do emotion and motivation direct executive control? Trends in cognitive sciences 13, 160-166 (2009)
25. Ray, R.D., Zald, D.H.: Anatomical insights into the interaction of emotion and cognition in the prefrontal cortex. Neuroscience & Biobehavioral Reviews 36, 479-501 (2012)
26. Critchley, H.D.: Neural mechanisms of autonomic, affective, and cognitive integration. Journal of Comparative Neurology 493, 154-166 (2005)
27. Thayer, J.F., Lane, R.D.: A model of neurovisceral integration in emotion regulation and dysregulation. Journal of affective disorders 61, 201-216 (2000)
28. Okon-Singer, H., Hendler, T., Pessoa, L., Shackman, A.J.: The Neurobiology of Emotion-Cognition Interactions: Fundamental Questions

and Strategies for Future Research. Frontiers in Human Neuroscience 9, (2015)
29. Wu, D., Courtney, C.G., Lance, B.J., Narayanan, S.S., Dawson, M.E., Oie, K.S., Parsons, T.D.: Optimal arousal identification and classification for affective computing using physiological signals: virtual reality Stroop task. Affective Computing, IEEE Transactions on 1, 109-118 (2010)
30. Wyczesany, M., Grzybowski, S.J., Barry, R.J., Kaiser, J., Coenen, A.M., Potoczek, A.: Covariation of EEG synchronization and emotional state as modified by anxiolytics. Journal of Clinical Neurophysiology 28, 289-296 (2011)
31. Parsons, T.D., Courtney, C.G., Dawson, M.E.: Virtual reality Stroop task for assessment of supervisory attentional processing. Journal of clinical and experimental neuropsychology 35, 812-826 (2013)
32. Wu, D., Lance, B.J., Parsons, T.D.: Collaborative filtering for brain-computer interaction using transfer learning and active class selection. PloS one 8, e56624 (2013)
33. McMahan, T., Parberry, I., Parsons, T.D.: Modality specific assessment of video game player's experience using the Emotiv. Entertainment Computing 7, 1-6 (2015)