A Social Cognitive Neuroscience Approach to Information Security

Robert West, Kaitlyn Malley, Bridget Kirby
DePauw University

Qing Hu
Baruch College – The City University of New York

White Paper submitted for A Decadal Survey of the
Social and Behavioral Science for National Security

June 12, 2017

Contact Information:

Robert West, PhD
Department of Psychology & Neuroscience
DePauw University
7 E. Larabee Street
Greencastle, IN 46135

Email: robertwest@depauw.edu

Information security (InfoSec) represents a significant challenge for private citizens, corporations, and government entities. Breaches of InfoSec, may lower consumer confidence (Yayla & Hu, 2011), shape national and international politics (Groll, 2017), and represent a significant threat to the world economy (e.g., estimated costs of breaches related to cybercrime were $3 trillion in 2015; Cybersecurity Ventures). Significant progress has been made in the context of developing and refining hardware and software infrastructure to thwart cybercrime (Ayuso, Gasca, & Lefevre, 2012; Choo, 2011). However, much less attention has been devoted to understanding the factors that lead individuals within an organization to compromise the digital assets of a company or government entity (Posey, Bennett, & Roberts, 2011; Warkentin & Willison, 2009). The need to for a greater understanding of the causes of insider threat becomes readily apparent when one considers that roughly 50% of security violations result from the activities of individuals within an organization (Richardson, 2011). Additionally, in a recent survey 89% of respondents felt that their organizations were at risk from an insider attack, and 34% felt very or extremely vulnerable (Vormetric Data Security, 2015). In this paper we describe our program of research that examines the neural basis of individual decision making related to InfoSec, and is grounded in a social cognitive neuroscience approach. We also consider evidence from studies examining the effects of individual and cultural differences on decision making related to InfoSec. Together this evidence may serve to motivate future research that integrates theories from neuroscience and the social and behavioral sciences in order to deepen our understanding of the factors that lead individuals to compromise InfoSec.

Two commentaries have called for the expansion of work in the behavioral and social sciences that is designed to enhance our understanding of Information Systems (Dimoka et al., 2011) and InfoSec (Crossler et al., 2013), and grounded in the theories and methods of neuroscience. Dimoka et al. describe how advances in the emerging field of Neuro-Information Systems (NeuroIS) could increase our understanding of user interactions with information systems. They identify seven research opportunities (i.e., localize the brain areas associated with IS constructs, capture hidden processes, complement existing sources of data, identify antecedents of IS constructs, test consequences, infer causality, and challenge IS assumptions) for the NeuroIS field. In a

second commentary, Crossler et al. focus on recent advances and potential discoveries related to “separating insider deviant behavior and insider misbehavior, unmasking the mystery of the hacker world, improving information security compliance, and cross-cultural InfoSec research.” One of the common themes in these reviews represents the need to develop novel measurement or assessment tools that circumvent problems related to participant subjectivity, social desirability, and method variance that contribute to limitations in the Information Systems and InfoSec literatures. As has been demonstrated in a study by Hu et al. (2015), we believe that a social cognitive neuroscience approach to the study of InfoSec holds significant promise in both addressing many of the limitations inherent in the extant literature, and in providing significant insight into the research opportunities identified in these commentaries.

In our program of research we have sought to use event-related brain potentials (ERPs) to examine the time course and spatial distribution of neural activity related to decision making while participants consider scenarios describing violations of InfoSec policies and practices that vary in severity (Hu et al., 2015). Obtaining valid physiological data related to decision making in this domain presents a number of methodological challenges. First, to reduce social desirability we had participants make decisions as if s/he were an IT employee at a fictitious company rather than report their own intentions. Additionally, a deception manipulation with a monetary incentive was used to encourage participants to offer realistic decisions. Importantly for those with ethical concerns related to the use of deception in research, a recent study reveals that this manipulation is not necessary to obtain the relevant behavioral or neurophysiological effects (Budde & West, 2017). Second, to isolate neural activity time-locked to the decision process, framing information for each decision was separated from a shorter decision prompt (see Hu et al., 2015 Table 1). Individuals also completed a set of control trials with the same format, but that did not include an ethical violation. The control trials allowed us to isolate neural activity related to ethical decision making from that related to more general aspects of information processing.

The behavioral data for our InfoSec paradigm represents the decisions offered by participants indicating whether they would take an action, and the response times associated with the decisions. Regardless of whether or not deception is utilized in the

paradigm (Budde & West, 2017; Hu et al., 2015), individuals are more likely to endorse control scenarios than minor or major ethical violations and are also significantly less likely to endorse major violations than minor violations. The response time data revealed a different pattern. Here individuals are slower to decide for minor violations than either control scenarios or major violations. Additionally, individuals low in self-control respond more quickly than individuals high in self-control for control scenarios and major violations and are somewhat more likely to accept minor violations than those with high self-control. These data reveal a general behavioral profile that is expected, and show that the task is sensitive to individual differences in self-control, a variable that is known to be a significant predictor of violations of InfoSec (Hu, Xu, Dinev, & Ling, 2011; Hu, Zhang, & Xu, 2012).

The ERP data elicited during the InfoSec paradigm in Hu et al. (2015) reveal a number of findings that are relevant to the seven opportunities identified by Dimoka et al. (2011) as well as the scope of the decadal survey. Importantly, considering either minor or major violations of InfoSec is associated with ERP activity localized to the medial and lateral prefrontal cortex (Hu et al., 2015). This finding converges with evidence from studies using functional MRI to examine the functional neuroanatomy of moral decision making in more traditional paradigms (Greene, 2015; Oliveira-Souza, Zahn, & Moll, 2015) and reveals some of the brain areas underpinning InfoSec constructs. Qualitatively different modulations of the ERPs are consistently observed when individuals are considering either minor or major violations of InfoSec. This finding leads to the suggestion that somewhat different neural systems are involved in processing violations with moderate or more severe consequences. Individual differences in self-control also have quantitative and qualitative effects on the neural correlates of decision making related to InfoSec. Low self-control is associated with a reduction in the amplitude of neural activity related to major violations. In contrast, high and low self-control is associated with qualitative differences in neural recruitment when individuals are considering minor violations. Together these findings provide insights that not readily apparent in the behavioral data alone, and that may advance our understanding of InfoSec by indicating that different neural systems are recruited when individuals consider various types of violations. Additionally, the interaction between

individual differences in self-control and the type of violation may reveal that different strategies could be required to either reduce biases in decision making or mitigate insider threat depending upon the characteristics of the situation or the individual.

A number of InfoSec scholars have recognized the importance of considering individual and cultural differences when examining the adoption and violation of InfoSec policy. As an example, low self-control has been linked to an increase in the intention to violate information security policy when individual consider hypothetical scenarios (Hu et al., 2011) and to also predict actual exploratory and exploitive hacking behavior (Hu et al., 2012). The effect of self-control on the intention to offend may be mediated by the perceived benefits and risk of sanctions, with low self-control enhancing the perception of benefits and attenuating the perception of formal sanctions (Hu et al., 2012). There is also some evidence that stronger moral belief serves to reduce the likelihood of hacking behavior that is engaged in for a variety of reasons including revenge, justice, survival or profit (Hu et al., 2012). Future work could explore the neural foundation of the moderating effect of moral belief on the influence of self-control on decision making related to InfoSec. For instance, ERP or fMRI methods could be used to examine variation in activation of the reward circuit during InfoSec decision making as related to individual differences in self-control and moral belief.

In today's geo-political climate, it is important not only to understand the motives of national security threats from inside the United States but also those arising from other countries. Most research regarding InfoSec has focused on western, educated, industrialized, rich, and democratic (WEIRD) subjects, a description that does not fit many of the threats currently faced by the United States. Related to the potential effect of culture on InfoSec, one study revealed differences between individuals in the United States and South Korea in terms of the variables that predicted intentions to adopt protective information technology (Dinev et al., 2009). Subjective norms were a significant predictor of intentions in Korea, but not the United States, while the effect of attitudes toward adopting protective technology was similar in the two cultures. A number of factors that differ across cultures including individualism, collectivism, the level of uncertainty avoidance, and power distance may affect the likelihood that an individual compromises InfoSec (Crossler et al., 2012). For example, in cultures with

lower power distance individuals are less likely to accept unequally distributed power (Crossler et al. 2012); that may make them feel more inclined to violate security measures against a figure of authority. Given this initial evidence and conceptual work, it seems clear that a greater understanding of cultural differences as related to InfoSec from a neurocognitive perspective has the potential to advance our fundamental knowledge in building capacity to inform challenges of national security.

A fundamental problem for InfoSec scholars is the identification of processes or programs that serve to reduce misconduct by individuals within or outside of an organization. Hu and colleagues (2010, 2011) have demonstrated that the certainty, severity, and swiftness of sanctions affects the perceived risk of violations of InfoSec, but that these factors do not, in turn, decrease the intention to commit a violation. This and other work (Crossler et al., 2013; Siponen & Vance, 2010), lead to the suggestion that the threat of punishment may not be an effective technique for reducing violations of InfoSec. In contrast, high levels of moral belief may serve to reduce hacking behavior (Hu et al., 2012). Furthermore, work in the area of behavioral economics demonstrates that mild, but widespread, cheating in a problem-solving task can be greatly reduced or possibly eliminated by priming an ethical frame of mind (Ariely, 2013). Given this, future research could explore how aspects of moral belief could be integrated into deterrence training programs.

In this review we have briefly explored the findings of an emerging program of research examining the neural basis of ethical decision making within the context of InfoSec, and examined some of the individual and cultural differences that may moderate the likelihood that individuals commit violations of InfoSec. Our prior studies reveal that incorporating methods from neuroscience can provide new insight into the processes underpinning decision making within this domain that may be less accessible with conventional behavioral and survey approaches used in the extant literature. Moving forward we anticipate that a social cognitive neuroscience approach, which integrates different levels of analysis (i.e., neural, cognitive, social, cultural), has the potential to provide insight into the causes of violations of InfoSec by organizational insiders and to also identify processes or procedures that may serve to mitigate insider threat to organizational InfoSec.

References

Ariely, D. (2013). The (Honest) *Truth About Dishonesty: How We Lie to Everyone-Especially Ourselves.* New York: HarperCollins Publishers.

Ayuso, P. N., Gasca, R. M., & Lefevre, L. (2013). A cluster-based fault-tolerant architecture for stateful firewalls. *Computers & Security, 31,* 524-539.

Budde, E., & West, R. (2017, April). *Neural correlates of ethical decision making related to information security.* Poster presented at the Midwestern Psychological Association, Chicago, IL.

Choo, K-KR. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30,* 719-731.

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

Cybersecurity Ventures (2017). Cybereconomy Infographic. http://cybersecurityventures.com/cybereconomy-infographic/.

de Oliveira-Souza, R., Zohn, R., & Moll, J. (2015). Neural correlates of human morality: An overview. In J Decety & T. Wheatley (Eds.), *The Moral Brain: A Multidisciplinary Perspective* (pp. 183-196). Cambridge, MA: The MIT Press.

Dimoka, A., Pavlou, P. A., & Davis, F. D. (2011). NeuroIS: The potential of cognitive neuroscience for information systems research. *Information Systems Research, 22,* 687-702.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behavior towards protective information technologies: The role of national cultural differences. *Information Systems Journal, 19,* 391-412.

Greene, J. D. (2015). The cognitive neuroscience of moral judgment and decision making. In J Decety & T. Wheatley (Eds.), *The Moral Brain: A Multidisciplinary Perspective* (pp. 197-220). Cambridge, MA: The MIT Press.

Groll, E. (2017, March 30). Russian interference went far beyond DNC hack, senate panel hears. Foreignpolicy.com.

Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems, 31,* 6-48.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54,* 55-60.

Hu, Q., Zhang, C., & Xu, Z. (2012, January). Moral beliefs, self-control, and sports: Effective antidotes to the youth computer hacking epidemic. Paper presented at 45th Hawaii International Conference on Systems Science. DOI: 10.1109/HICSS.2012.438

Posey, C., Bennett, R. J., Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security, 30,* 486-497.

Richardson, R. (2011). CSI computer crime and security survey. http://www.GoSCI.com.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34,* 487-502.

Vormetric Data Security. (2015). 2015 Vormetric Insider Threat Report. http://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf

Warkentin, M., & Wilson, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems. 18,* 101-105.

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM.* 56, 64-74.

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology, 26,* 60-77.