SPECIAL SECTION: Cybersecurity Decision Making

Introduction to Special Issue of the *Journal of Cognitive Engineering and Decision Making* Special Issue Focus: Cybersecurity Decision Making

BACKGROUND

In the past 2 years cybersecurity breaches have made the national headlines almost weekly. Many *Journal of Cognitive Engineering and Decision Making* (*JCEDM*) readers were personally affected by breaches of credit card information at Target, Home Depot, Michaels, and Staples, or through intrusions into the information systems of national banks such as JP Morgan Chase. We hope that few of you succumbed to the "ransomware" criminals who encrypt your personal files, such as digital photos, and decrypt them only upon payoff. The major attack on Sony Pictures, while fascinating to many, revealed that no email can truly be considered private and any business can be significantly disrupted both technically and culturally by cyber attacks.

Each of these breaches was possible because of human decisions: a credit card company's senior management made a conscious decision to slow-roll a transition to less vulnerable smart cards; a computer network defender decided to ignore the alerts signaling an intrusion into Target; a network security operator failed to apply double authentication to a JP Morgan Chase server; an individual employee at Sony chose to move confidential records to an unauthorized system; and everyday users like us decide to not check the safety of the apps we download and not use strong passwords on all our devices because it doesn't appear to be worth the effort.

Journal of Cognitive Engineering and Decision Making
2015, Volume 9, Number 2, June 2015, pp. 115–116
DOI: 10.1177/1555343415581166

When we first issued the Call for Papers for this special issue, we asked that the research community consider all types of cybersecurity decisions when submitting papers. We recognized that cognitive engineers are drawn to studying the complex work domain of computer network defense (CND)—that is, the cadre of specialists who decide the levels of security to be applied to computing systems, trade off security against availability of computing systems and networks, decide what is normal or anomalous for computing systems and networks, and decide how to respond to a security incident. Thus, we expected a majority of paper submissions to be related to CND. But we also sought research reflecting strategic decisions made by Chief Information Security Officers (CISOs), who consider security risks, policies, resource investments, and the impact of a security breach; and decisions made by individual users—home computer users, office workers, students, and soldiers—about password usage, personal firewalls, and policy compliance.

We are very pleased to present three papers that are primarily focused on what influences the decisions of the latter group. The Parsons et al. (2015) paper provides insight into how an organization's information security culture can affect the security decisions made by an individual worker's compliance with security policy and ultimately the organization's risk to cyber attack. Nehmadi and Meyer's (2015) paper addresses the factors that contribute to whether people choose to use authentication methods such as strong passwords to increase the security of their computing activities or whether they prefer to bypass authentication in favor of ease and efficiency. (When reading this paper, keep in mind that "computing" does not just refer to what you

do on your workstation or laptop but extends to your cell phone, tablet, and gaming systems.) Chen, Gates, Li, and Proctor's (2015) paper sheds light on how framing a decision based on safety versus risk affects our decisions on which cell phone apps to download. Each of these papers contributes to our understanding of how nonexperts are influenced in how they make decisions that affect the cybersecurity posture of their work and home environments. They also inform us as end-users about how we can improve our own security risk profiles.

In putting together this special issue, we also discovered that although there are many ongoing studies of the decision-making processes of computer network defenders, these studies are still in a nascent state. Most of the papers we received on this topic were in a preliminary form, limited by experimental conditions or number of participants who were representative of cybersecurity experts. All of the papers in this special issue were reviewed by both experts in cognitive engineering and experts in cybersecurity. We found that the cybersecurity experts were most concerned about the ecological validity of studies that attempted to represent the complex environment and various roles of CND in a laboratory environment. In contrast, the cognitive engineering experts, while sensitive to the need for ecological validity, were also insistent on the need for rigorous study design and methodology and appropriate use and interpretation of statistical techniques. In combination, our reviewers placed a high standard for what good research in the cybersecurity domain should look like, which we believe is as it should be. We are pleased to say that the three papers in this special issue successfully met all these high criteria.

We believe there remains opportunity for more cognitive engineering research in the cybersecurity domain that melds the standards of rigor of the cognitive engineering community with the demands for relevance and ecological validity of the cyber defense community (which after all is a hallmark of cognitive engineering research). One clear avenue is for cognitive engineering researchers to collaborate more fully with cybersecurity experts to produce research on CND decision making that is both experimentally sound and truly representative of the CND domain. There is also opportunity for more cross-discipline dialogue that would benefit both communities. We hope that this special issue has made an important first step in that direction.

We hope you enjoy this special issue on cybersecurity decision making and look forward to many more submissions on the topic in the future.

Anita D'Amico
Secure Decisions
Emilie M. Roth
Roth Cognitive Engineering

REFERENCES

Chen, J., Gates, C. S., Li, N., & Proctor, R. W. (2015). Influence of risk/safety information framing on Android app-installation decisions. *Journal of Cognitive Engineering and Decision Making, 9*(2), 149–168.

Nehmadi, L. & Meyer, J. (2015). Effects of authentication method and system properties on authentication decisions and performance. *Journal of Cognitive Engineering and Decision Making, 9*(2), 130–148.

Parsons, K. M., Young, E., Buravicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making, 9*(2), 117–129.