ENHANCING DECISION MAKING BY CYBERSECURITY EMPLOYEES

Reeshad S. Dalal

Chair, Department of Psychology, George Mason University

Email: rdalal@gmu.edu

Website: http://psychology.gmu.edu/people/rdalal

June 2017

As a part of its decadal surveys of the social and behavioral sciences for national security, the Second Call for White Papers by the National Academies of Sciences, Engineering, and Medicine identifies several broad areas of research interest. This white paper supports the following areas:

- **Building analytic skill sets** (i.e., workforce development, **selection, training,** human-technology interactions, performance management)
- **Strategies and techniques for avoiding errors and biases in decision making**
- **Building coordination and improving communication (i.e., between** researchers, analysts, policy and/or **decision makers and among teams)**

(**emphasis** added to reflect the specific areas of contribution of the current white paper).

Government agencies, militaries, corporations, and non-profits the world over are busily establishing or enlarging Security Operations Centers (SOCs) and Cybersecurity Incident Response Teams (CSIRTs) to detect and mitigate cyber threats. Over the course of their work shifts, employees staffing these SOCs/CSIRTs must sift through large volumes of incoming data (the "eyes on glass" problem), quickly determine which events constitute incidents warranting mitigation efforts, and, for each such incident, quickly engage in a decision-making process that involves how and with the assistance of whom to effectively resolve the incident (Tetrick et al., 2016; Zaccaro et al., 2016).

These problems are not purely technological in nature: social and behavioral science (SBS) approaches are needed. SBS approaches in this domain can involve employee selection, employee training, the use of cognitive prompts, and the use of mnemonics (Tetrick et al., 2016).

Selecting Good Decision Makers

SOCs/CSIRTs could aim to select (i.e., hire) analysts who are inherently good decision makers. One approach involves identifying specific *skills* that aid in decision-making: for instance, critical thinking, problem sensitivity, and information ordering (Peterson et al., 2001). A second approach involves assessing the role of the fundamental decision-making *styles* of rationality and intuition (Phillips et al., 2016).

Tasks for future SBS research involve refining the measurement of these decision-making skills and styles, examining the relative importance of these skills and styles in predicting performance in cybersecurity jobs, and examining the conditions under which the importance of each skill or style is high versus low. For example, although extant research suggests that a rational decision-making style generally leads to better decisions than an intuitive decision-making style (Alaybek et al., 2017; Phillips et al., 2016), it is conceivable that intuition is beneficial when the decision is familiar, frequent, and low in severity (Alaybek et al., 2017).

Training Better Decision-Making

Among the many techniques suggested as ways to train people to make better decisions in naturalistic settings are expert modeling, critical thinking training, guided self-correction, structured troubleshooting training, and after-action reviews (Steinke et al., 2015; Tetrick et al., 2016). Each of these training techniques has previously been shown to be at least somewhat effective.

However, due to the different research designs and criteria for success used in extant research studies, the head-to-head effectiveness of these techniques cannot yet be determined. Moreover, extant research on these techniques has not devoted much attention to the common problem of "fade out" (namely, the declining effectiveness over time of training interventions) and to potential solutions (e.g., the frequency of "booster doses" of the training). Nor has the effectiveness of most of these training techniques yet been systematically examined specifically in a cybersecurity setting. Finally, in addition to the benefit (effectiveness) of each training technique, its costs in money and time must also be determined and compared. Costs can be thought of in terms of costs associated with the *development* (or adaptation to a cybersecurity setting) of the training protocol and costs associated with the *implementation* of the training (Tetrick et al., 2016). These, then, represent areas for future SBS research.

Using Cognitive Prompts to Reduce Biased Decision-Making

The use of relatively simple cognitive prompts may facilitate less heuristical thinking and, accordingly, less biased decision-making. For example, in a "pre-mortem" (Klein, 2007), respondents are prompted to: (a) imagine that they had already made and implemented the decision in question and that it had gone horribly wrong, and (b) speculate as to why this might have happened. As another example, in a "five-why" analysis (Heath et al., 1998) respondents who provide a diagnosis of a problem are repeatedly asked "why" in an effort to help them arrive at root causes. As in the case of training techniques, here too head-to-head comparisons between various cognitive prompts are needed in a cybersecurity setting with the same research design, the same criteria for success, the same attention to the frequency of prompts, and an examination of costs as well as benefits.

Using Mnemonics to Enhance Mental Models

Mnemonics such as SBAR (Situation, Background, Assessment, and Recommendations) and SHARED (Situation, History, Assessment, Risks, Events, and Documentation) have been developed for use in other settings (e.g., healthcare, aviation; Steinke et al., 2015). Future SBS research should compare the

effectiveness and cost of various mnemonics applied to various aspects of the cybersecurity decision process. For instance, although mnemonics are likely to be somewhat helpful when a cybersecurity analyst is making a decision on his or her own, mnemonics may be even more helpful when incorporated into formal handoff and escalation protocols because in such cases they are likely to facilitate the development of a common mental model across analysts.

Putting it All Together

Finally, a major area for future SBS research is to examine the *interplay* between selection, training, cognitive prompts, and mnemonics vis-à-vis cybersecurity employees. For example, might selecting employees who are already good decision makers reduce the need for training—or, conversely, might good decision makers be better able than bad decision makers to make use of decision-making training? Might the use of mnemonics, when integrated into formalized decision protocols, reduce the need for cognitive prompts? Might the effectiveness of training techniques be enhanced by incorporating mnemonics into the training protocols? Questions such as these suggest that opportunities abound for SBS research aimed at optimizing the decision-making of cybersecurity employees.

References

Alaybek, B., Dalal, R. S., Wang, Y. Dubrow, S., & Boemerman, L. (2017). The criterion-related validity of rationality and intuition on job performance and attitudes: A meta-analysis. Manuscript in preparation.

Heath, C., Larrick, R. P., & Klayman, J. (1998). Cognitive repairs: How organizational practices can compensate for individual shortcomings. *Review of Organizational Behavior, 20,* 1-37.

Klein, G. (2007). Performing a project premortem. *Harvard Business Review*, *85*, 18-19.

Peterson, N. G., Mumford, M. D., Borman, W. C., Jeanneret, P. R., Fleishman, E. A., Levin, K. Y., Campion, M. A., Mayfield, M. S., Morgeson, F. P., Pearlman, K., Gowing, M. K., Lancaster, A. R., Silver, M. B., & Dye, D. M. (2001). Understanding work using the Occupational Information Network (O*NET): Implications for practice and research. *Personnel Psychology*, *54*, 451-492.

Phillips, W. J., Fletcher, J. M., Marks, A. D., & Hine, D. W. (2016). Thinking styles and decision making: A meta-analysis. *Psychological Bulletin, 142,* 260-290.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., Zaccaro, S. J., Dalal, R. S., & Tetrick, L. E. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. *IEEE Security & Privacy, 13,* 20-29.

Tetrick, L. E., Zaccaro, S. J., Dalal, R. S., Steinke, J. A., Repchick, K. M., Hargrove, A. K., Shore, D. B., Winslow, C. J., Chen, T. R., Green, J. P., Bolunmez, B., Tomassetti, A. J., McCausland, T. C., Fletcher, L., Sheng, Z., Schrader, S. W., Gorab, A. K., Niu, Q. & Wang, V. (2016). *Improving social maturity of cybersecurity incident response teams.* Fairfax, VA: George Mason University. Retrieved from http://calctraining2015.weebly.com/the-handbook.html

Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Steinke, J. A. (2016). *Psychosocial dynamics of cyber security.* New York, NY: Routledge.