Developing a Situational Judgement Test for Cybersecurity in Healthcare: An important diagnostic prerequisite for fostering Cybersecurity Behavior among Hospital Staff

Thomas Keller (University of Hohenheim), Julia Warwas (University of Hohenheim) Florian Schütz (University of Goettingen), Florian Rampold (University of Goettingen)

In light of the increasing cyberattacks on critical infrastructure such as hospitals (IBM, 2023), and the associated data breaches, e.g. through insider leaks, loss, theft, or unintentional disclosure of sensitive patient data, there is an urgent need for job-specific training for hospital staff to mitigate these threats (Almulihi et al. 2022). However, there is a lack of knowledge of job-specific cybersecurity skill requirements and individual skill levels. Also, previous survey instruments that capture subjective perceptions, intentions, and self-reported behaviors often fail to adequately map and classify the complex conditions and demands for targeted action steps of real threat situations in a competence-oriented manner (Siponen & Vance, 2014). This study aims to close this gap by developing action-oriented, situational, authentic, and competence-oriented measurement instruments in the form of Situational Judgement Tests (SJT), based on the first two steps of the ECD framework (Mislevy et al., 2003).

Following the framework, a comprehensive *domain analysis* presents the starting point for assessment design., At this stage, job-specific threat vectors were identified through literature reviews and classification of security threats, through observational studies in hospitals, and through an extensive risk assessment and validation of threat vectors with experts in information security, (Rampold et al., 2024). The resulting *threat vectors*, consisting of asset and threat events (Schuetz et al. (2023) for detailed information), formed the content basis for the development of our SJT. On the other hand, a *competency structure model* for cyber security behavior (Köpfer et al., 2023), which encompasses seven dimensions of competence, provides a multi-faceted framework for assessing the necessary skills to effectively respond to potential threats.

Grounded on the domain and competency models, a *test model* could be developed. Its item universe consists of *testlets,* each covering a risk situation within the action field of hospitals and all seven competency dimensions for information-secure action. The planning and development phase resulted in testlets tailored to distinct professional profiles in hospitals, namely caregivers, physicians, and clerical workers. Finally, a total of 30 testlets with the highest criticality were developed. These testlets address critical threat vectors that are relevant in the respective activity profiles and vary depending on the degree of patient contact.

The study reported in the present abstract distributed the testlets via the panel providers Prolific and Clickworker with the aim of examining the functioning and quality of the test instrument. In particular, we analyzed response patterns, potential reported difficulties and feedback of the participants. Furthermore, analyses on difficulty parameters, item variance, and discriminatory power of the individual items were carried out (Kelava & Moosbrugger, 2008).

The study sample includes N = 607 people, consisting of physicians, caregivers, and clerical staff. Statistical analyses point to the tests' adequacy to differentiate between various competence levels. Moreover, the consistently positive feedback on the usability and authenticity of the test underscores its acceptance by the participants. The presentation will therefore outline how the test can be used to evaluate the effectiveness of training programs to foster cybersecurity behavior.

References

Almulihi, A. H., Alassery, F., Khan, A. I., Shukla, S., Gupta, B. K., & Kumar, R. (2022). Analyzing the implications of healthcare data breaches through computational technique. *Intelligent Automation & Soft Computing, 32*(3), 1763–1779. https://doi.org/10.32604/iasc.2022.023460

IBM. (2024, February 21). Identity comes under attack, straining enterprises' recovery time from breaches.

Kelava, A., & Moosbrugger, H. (2008). Deskriptivstatistische Evaluation von Items (Itemanalyse) und Testwertverteilungen. In H. Moosbrugger & A. Kelava (Eds.), *Testtheorie und Fragebogenkonstruktion* (pp. 73–98). Springer. https://doi.org/10.1007/978-3-540-71635-8_4

Köpfer, P., Warwas, J., Schütz, F., Rampold, F., Masuch, K., & Trang, S. (2023). A Competence-Based Screening of Instructional Designs in Trainings for IT-Security at the Workplace. AERA 2023, 1–11. https://doi.org/10.5281/zenodo.8300825

Mislevy, R. J., Almond, R., & Lukas, J. F. (2003). A brief introduction to evidence-centered design. *ETS Research Report Series, 2003*(1), i–29. https://doi.org/10.1002/j.2333-8504.2003.tb01908.x

Rampold, Florian & Heinsohn, Julia & Schütz, Florian & Klein, Julia & Keller, Thomas & Masuch, Kristin & Warwas, Julia. (2024). Custom Solutions for Diverse Needs: Laying the Foundation for Tailored SETA Programs in the Healthcare Domain.

Schütz, F., Rampold, F., Masuch, K., Köpfer, P., Mann, D., Warwas, J., & Trang, S. (2023). Bridging the Gap between Security Competencies and Security Threats: Toward a Cyber Security Domain Model. HICSS 2023 Proceedings, 6118–6127. https://doi.org/10.24251/hicss.2023.741

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems, 23*(3), 289–305.