2024 European Association for Research on Learning and Instruction (EARLI)
Special Interest Group (SIG) 01 Assessment and Evaluation
Barcelona, 26 - 28 June 2024

Development and Validation of a Situational Judgment Test on the Cyber Security Competencies in VET

Thomas Keller, Julia Warwas, Patricia Köpfer

Abstract

As a result of digital transformation, cybercrime is increasing steadily. Attacks become more sophisticated and target the human factor of enterprises, which is considered the weakest link in the information security chain. Thus, the professionals' awareness and skills to protect sensitive information from unauthorized access, loss, theft, or damage present one important component of their digital competences. We developed an online Situational Judgement Test (SJT) to assess cyber security competencies for widespread security threats in office work. A current validation study involves apprentices across various stages of commercial vocational training in Germany. After outlining the foundation of the competence model, we expound features of the test instrument and evaluate indicators of valid assessments. Finally, we discuss (a) how test scores can inform teachers and trainers on potential competence deficits, and (b) how the proposed competency structure model for cyber secure behavior can guide instructional methods to foster competence development.

Assessment, Cyber Security Competencies, Situational Judgement Tests, Vocational Education,

Digital transformation significantly impacts business processes (Sembill & Frötschl, 2017), changing workflows for commercial professions (Gerholz & Dormann, 2017) through enhanced human-machine interaction (Mütze-Niewöhner & Nitsch, 2020), and leading to new competency requirements for employees (Hammermann & Stettes, 2015). Vice versa, a lack of digital competencies among the professionals poses major barriers to digitalization in companies (Pfeifer et al., 2016). A downside of digitalization manifests in the form of increased cybercrime (BSI, 2022). Hacker attacks are becoming more sophisticated, with new and refined methods targeting the vulnerable 'human factor' to bypass security systems and steal sensitive information (Ahmad et al., 2019). Thus, the employee's awareness and skills to protect sensitive information from unauthorized access, loss, theft, or damage present one important component of the digital competences of professionals. However, while such competences are highly

recognized in information security research (Ali et al., 2021), their promotion and assessment in educational settings that prepare for professional activities have received little attention so far.

Due to the increasing vulnerability of companies and the growing landscape of security threats, the European Commission plans to strengthen cyber security competencies among employees and apprentices in companies through Security Education, Training, and Awareness (SETA) measures (Hu, Hsu & Zhou, 2022). Current empirical research on workplace cyber security is markedly influenced by models from social psychological theories, which serve to explain behaviors. However, these models often prove too generic and lack sufficiently contextualized items, tailored to specific threats (Siponen & Vance, 2014). Moreover, a reported intention to comply with information security policies in established questionnaires is often interpreted as actual security behavior.

Situational Judgement Tests (SJTs) can be used for a wide range of constructs (McDaniel et al., 2001), such as job-related knowledge and behavior (Christian et al., 2010; Polyhart & McKenzie, 2011). They are characterized by strong intuitive prompting, as trainees are asked to put themselves in a specific threat scenario (Stemler & Sternberg, 2006). SJTs confront participants with multiple response options for a given threat situation. Their task is then to select the most appropriate or effective response. Based on a competency structure model for cyber security behavior (Köpfer et al., 2023), we aim to develop and validate a comprehensive SJT for assessing specific cyber security competencies among apprentices for commercial professions in three distinct threat areas.

Password management

- Scenario 1: An employee creates an insecure new password.
- Scenario 2: An employee shares their password with colleagues.
- Scenario 3: An employee uses the same passwords for social media and work accounts.

Social engineering

- Scenario 1: An employee receives a suspicious email with a dangerous attachment.
- Scenario 2: An employee receives a suspicious text message with a dangerous link.

- Scenario 3: An employee receives a call from an unknown caller.

Handling sensitive data at the workplace

- Scenario 1: An employee leaves their computer unlocked while unattended.
- Scenario 2: An employee leaves sensitive documents unattended on their desk.
- Scenario 3: An employee leaves a meeting room with sensitive data on the desk.

For the validation of the situational judgment tests, we conduct a study at a vocational education school in Germany. Participants in the validation study are apprentices in office and industrial professions, spanning the first, second, and third years of their vocational training. The content validity of the test is established through curricular analyses and its grounding in a Cyber Security Domain Model, which differentiates between Threat Event and Threat Area (Schuetz et. al., 2023). To ensure convergent validity, self-assessment scales from the Human Aspects of Information Security Questionnaire (Parsons et al., 2014) are implemented, focusing on threat areas that exhibit large overlap with our action-oriented test instrument, namely password management, email use, and information handling. To assess divergent validity, the self-assessment questionnaire social and methodical competencies is utilized (Frey & Balzer, 2005). Data collection is scheduled for April/May this year, and comprehensive results including comparisons between groups of learners at different stages of their professional development are available by the time of the conference.

Complementing the report of findings from the validation study, the presentation will discuss (a) how test scores can inform teachers and trainers on potential competence deficits of apprentices, and (b) how the proposed competency structure model for cyber security behavior can guide instructional methods to foster competence development.

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H. & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology 71 (8*), 939–953.

Ali, S. E. A., Lai, F.-W., Jan, A. A., Rahman, H. ur, Shah, S. Q. A., & Hamad, S. (2024). Does intellectual capital curb the long-term effect of information security breaches on firms' market value? *Quality & Quantity, 58*, 3673–3702. https://doi.org/10.1007/s11135-023-01797-3

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2022). Die Lage der IT-Sicherheit in Deutschland. Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6. Zugriff am 25.08.2024

Frey, A., & Balzer, L. (2005). Der Beurteilungsbogen smk: Ein Messverfahren für die Diagnose von sozialen und methodischen Fähigkeitskonzepten. In A. Frey, R. S. Jäger, & U. Renold (Hrsg.), *Kompetenzdiagnostik – Theorien und Methoden zur Erfassung und Bewertung von beruflichen Kompetenzen* (S. 31–56). Landau: Verlag Empirische Pädagogik.

Gerholz, K.-H. & Dormann, M. (2017). Ausbildung 4.0: Didaktische Gestaltung der betrieblich-beruflichen Ausbildung in Zeiten der digitalen Transformation. *bwp@ Berufs- und Wirtschaftspädagogik – online, 32*, 1-22.

Hammermann, A., & Stettes, O. (2016). Qualifikationsbedarf und Qualifizierung: Anforderungen im Zeichen der Digitalisierung. *IW-Policy Paper, 3/2016*. Institut der deutschen Wirtschaft Köln.

Hu, S., Hsu, C., & Zhou, Z. (2021). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems*, *62*(4), 752–764. https://doi.org/10.1080/08874417.2021.1913671

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

Mütze-Niewöhner, S. & Nitsch, V. (2020). Arbeitswelt 4.0. In Walter Frenz (Hrsg.), *Handbuch Industrie 4.0: Recht, Technik, Gesellschaft* (S. 1187–1217). Springer Vieweg.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Pfeiffer, S., Lee, H. & Ziring, Christopher, Suphan, Anne. (2016). *Industrie 4.0 – Qualifizierung 2025.*

Polyhart, R. E. & MacKenzie, W. I. (2011). Situational Judgement Tests: A Critical Review and Agenda for the Future. In S. Zedeck (Ed.), APA handbook of industrial and organizational psychology, Vol 2: Selecting and developing members for the organization (pp. 237-252). Washington: American Psychological Association.

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

Sembill, D. & Frotschl, C. (2017). Spannungsfelder digitalisierter Bildungswelten. In J. Schlicht & U. Moschner (Hrsg.), Berufliche Bildung an der Grenze zwischen Wirtschaft und Padagogik. Reflexion aus Theorie und Praxis (S. 159-178). Wiesbaden: Springer VS.

Siponen, M., Mahmood, M. & Seppo, P. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217–224.