

An upcoming second online survey of the project is focused on getting a snapshot of security culture using the proven Information Security Culture Assessment [31] and looking at compliance, self-efficacy, and competing values [32] in order to support change management within the SMEs. Finally, awareness measurements before and after testing the developed learning scenarios and trainings, coupled with management surveys, will assess the instruments of the current project for critical evaluation. One purpose of the project is to make all the results and tools available free of charge at the end of the project in 2023.

7. Acknowledgments

We thank the Federal Ministry for Economic Affairs and Climate Action (BMWK) for funding the project “Awareness Lab SME Information Security/ALARM Informationssicherheit.” We would also like to acknowledge the anonymous reviewers for their helpful critical comments. Many thanks, too, to Simon Cowper for his detailed and professional proofreading of the text. Finally, we would like to express our gratitude for the opportunity to expand our LICE conference paper 2022 for publication in this journal.

8. References

- [1] Bitkom. (2018). Bitkom Digital Office Index 2018: Eine Studie zur Digitalisierung von Büro- und Verwaltungsp Prozessen in deutschen Unternehmen [Berlin, 28. Juni 2018]. <https://www.bitkom.org/sites/default/files/file/import/180813-Studienbericht-Bitkom-Digital-Office-Index-2018.pdf> (Access Date: 4 March 2022).
- [2] Bundesministerium für Wirtschaft und Technologie (Ed.). (2012). IT-Sicherheitsniveau in kleinen und mittleren Unternehmen: Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie [2011/2012]. Deutschland. <https://www.it-sicherheit-inderwirtschaft.de/ITS/Redaktion/DE/Publikationen/Studien/it-sicherheitsniveau-in-kleinen-und-mittleren-unternehmen.pdf> (Access Date: 6 July 2021).
- [3] WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (Ed.). (2017). Aktuelle Lage der IT-Sicherheit in KMU [2017]. <https://www.it-sicherheit-inder-wirtschaft.de/ITS/Redaktion/DE/PDF-Anlagen/Studien/aktuelle-lage-der-it-sicherheit-in-kmu-langfassung.pdf> (Access Date: 3 November 2021).
- [4] Verizon. (2022). Data Breach Investigations Report (DBIR) 2022. <https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf> (Access Date: 27 July 2022).
- [5] Menges, U., Hielscher, J., Buckmann, A., Kluge, A., Sasse, M. A., and Verret, I. (2022). Why IT Security Needs Therapy. In S. Katsikas, C. Lambrinouidakis, N. Cuppens, J. Mylopoulos, C. Kalloniatis, W. Meng, S. Furnell, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, and M. A. Sotelo Monge (Eds.), *Lecture Notes in Computer Science (LNCS): Vol. 13106, Computer Security: Esorics 2021 International Workshops. Revised Selected Papers* (pp. 335–356). Springer.
- [6] Bundesamt für Sicherheit in der Informationstechnik (Ed.). (2021). Die Lage der IT-Sicherheit in Deutschland 2021. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3 (Access Date: 17 December 2021).
- [7] Bundesamt für Sicherheit in der Informationstechnik (Ed.). (2021, January 26). IT Grundschatz. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschatz/it-grundschatz_node.html (Access Date: 23 April 2021).
- [8] Bundesamt für Sicherheit in der Informationstechnik (Ed.). (n.d.). BSI-Standards. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschatz/BSI-Standards/bsi-standards_node.html (Access Date: 29 December 2021).
- [9] Bada, M., Sasse, A. M., and Nurse, J. R. C. (2016). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In *International Conference on Cyber Security for Sustainable Society (ICT4SS)*. <https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf> (Access Date: 29 December 2021).
- [10] Ertan, A., Crossland, G., Heath, C., Denny, D., and Bjerg Jensen, R. (2018). Everyday Cyber Security in Organisations: Literature review. <https://arxiv.org/ftp/arxiv/papers/2004/2004.11768.pdf> (Access Date: 29 December 2021).
- [11] Bada, M., and Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security*, 27(3), 393–410. DOI: 10.1108/ICS-07-2018-0080 (Access Date: 31 August 2022).
- [12] Wilson, M., and Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. NIST special publication: 800-50 (October). U.S. Government Printing Office. <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf> (Access Date: 29 December 2021).
- [13] Scholl, M. C. (2019). Raising Information Security Awareness in the Field of Urban and Regional Planning. *International Journal of E-Planning Research*, 8(3), 62–86. DOI: 10.4018/IJEPR.2019070104 (Access Date: 31 August 2022).
- [14] Gugerell, K., and Zuidema, C. (2017). Gaming for the energy transition. Experimenting and learning in co-designing a serious game prototype. *Journal of Cleaner Production*, 169, 105–116. DOI: 10.1016/j.jclepro.2017.04.142 (Access Date: 31 August 2022).
- [15] George P. Pavlidis, and Stella Markantonatou. (2018). Playful Education and Innovative Gamified Learning Approaches. In *Handbook of Research on Educational Design and Cloud Computing in Modern Classroom*

Settings (pp. 321–341). IGI Global. DOI: 10.4018/978-1-5225-3053-4.ch015 (Access Date: 31 August 2022).

[16] Maor, D. (1999). Teachers-as-learners: The role of a multimedia professional development program in changing classroom practice. *Australian Science Teacher's Journal*, 45(3) August.

[17] Lombardi, M. M. (2007). Authentic Learning for the 21st Century: An Overview. *Educause Learning Initiative*(1: 2007 (May)). https://www.researchgate.net/publication/220040581_Authentic_Learning_for_the_21st_Century_An_Overview (Access Date: 28 July 2022).

[18] Rolloff, M. (2010). A constructivist model for teaching evidence-based practice. *Nursing Education Perspectives*, 31(5), 290–293.

[19] Trybus, Jessica. (2014). Game-Based Learning: What it is, Why it Works, and Where it's Going. <https://www.newmedia.org/game-based-learning--what-it-is-why-it-works-and-where-its-going.html> (Access Date: 12 April 2015).

[20] Hart, S., Margheri, A., Paci, F., and Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers and Security*, 95, 101827. DOI: 10.1016/j.cose.2020.101827 (Access Date: 31 August 2022).

[21] Pokoyski, D., Matas, I., Haucke, A., and Scholl, M. (2021). Qualitative Wirkungsanalyse Security Awareness in KMU: Tiefenpsychologische Grundlagenstudie im Projekt "Awareness Labor KMU (ALARM) Informationssicherheit. Technische" Hochschule Wildau, Wildau. <https://alarm.wildau.biz/static/d6490e49f8d31adfa35259134b8d1b9d/220316-alarm-studie-final.pdf> (Access Date: 16 March 2022).

[22] Tippelskirch, H. von, Schuktomow, R., Scholl, M., Walch, M. C., Hubertus v. Tippelskirch, Regina Schuktomow, Margit Christa Scholl, and Marie Christin Walch. (2022). Report zur Informationssicherheit in KMU: Sicherheitsrelevante Tätigkeitsprofile [Report 1: Ergebnisse einer Umfrage im Rahmen des Projektes Awareness Labor KMU (ALARM) Informationssicherheit, Technische Hochschule Wildau, Wildau]. DataCite. <https://alarm.wildau.biz/static/20b6d15448c0ba23729e0f45daa20650/alarm-informationssicherheit-report-1.pdf> (Access Date: 2 August 2022).

[23] Porst, R. (2008). Fragebogen: Ein Arbeitsbuch. Lehrbuch zur Praxis der Fragebogenerstellung. SpringerLink Bücher. VS Verlag für Sozialwissenschaften. DOI: 10.1007/978-3-531-90897-7 (Access Date: 20 August 2021).

[24] Wirtschafts- und Sozialwissenschaftliches Institut (WSI), Hans-Böckler-Stiftung (Ed.). (2021). Homeoffice: Was wir aus der Zeit der Pandemie für die zukünftige Gestaltung von Homeoffice lernen können [WSI Report Nr. 65, April 2021]. https://www.boeckler.de/pdf/p_wsi_report_65_2021.pdf (Access Date: 6 July 2021).

[25] Winkler, I. (2017). 7 elements of a successful security awareness program: Action items for CSOs looking to

bolster their security awareness programs. *CSO Online. CSO Magazine*. <https://www.csoonline.com/article/2133408/network-security-the-7-elements-of-a-successful-security-awareness-program.html> (Access Date: 9 August 2022).

[26] Brüggemann, R., Carlsen, L., and Wittmann, J. (2014). Multi-indicator Systems and Modelling in Partial Order. Springer New York. DOI: 10.1007/978-1-4614-8223-9 (Access Date: 31 August 2022).

[27] Lee, K. C., Ma, J. D., Hudmon, K. S., and Kuo, G. M. (2012). A train-the-trainer approach to a shared pharmacogenomics curriculum for US colleges and schools of pharmacy. *American Journal of Pharmaceutical Education*, 76(10), 193. DOI: 10.5688/ajpe7610193 (Access Date: 3 August 2021).

[28] Paullet, K., Pinchot, J., and Mishra, S. (2017). Implementing a Successful Train-The-Trainer Program in Mobile forensics and Security. *Issues in Information Systems*, Volume 18(Issue 1, October 2017), 173–179. https://www.researchgate.net/profile/sushmamishra/publication/339460664_implementing_a_successful_train-the-trainer-program-in-mobile-forensics-and-security/links/5ecfd5f245851529451b28b9/implementing-a-successful-train-the-trainer-program-in-mobile-forensics-and-security.pdf (Access Date: 3 August 2022).

[29] Wilson, B. G. (2017). Constructivism for active, authentic learning. In B. Reiser and J. Dempsey (Eds.), *Current Trends in Instructional Design and Technology*. Pearson Prentice Hall. https://www.academia.edu/download/38422000/Wilson_-_Constructivism_2017.pdf (Access Date: 9 August 2022). Draft Chapter.

[30] Volkamer, M., Sasse, M. A., and Boehm, F. (2020). Analysing Simulated Phishing Campaigns for Staff. In *European Symposium on Research in Computer* (pp. 312–328). Springer. DOI: 10.1007/978-3-030-66504-3_19 (Access Date: 31 August 2022).

[31] da Veiga, A. (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information and Computer Security*, 26(5), 584–612. DOI: 10.1108/ICS-08-2017-0056 (Access Date: 31 August 2022).

[32] Karlsson, F., Karlsson, M., and Åström, J. (2017). Measuring employees' compliance – the importance of value pluralism. *Information and Computer Security*, 25(3), 279–299. DOI: 10.1108/ICS-11-2016-0084 (Access Date: 31 August 2022).