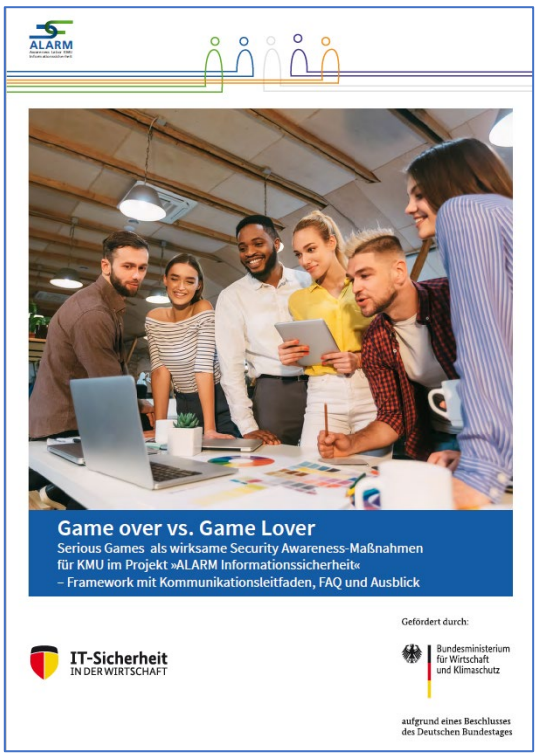
See also: https://www.researchgate.net/publication/373337618_Chapter_5_Findings_from_the_overall_scenario_and_the_three_studies_of_the_project_Awareness_Lab_SMEs_ALARM_Information_Security_followed_by_a_conceptual_outlook_translation_study_paper_forthcoming_in_

https://alarm.wildau.biz/ Studie 3 https://alarm.wildau.biz/en



Kapitel 5, Seiten 53-59

DOI: 10.13140/RG.2.2.12630.22082

Chapter 5
Findings from the overall scenario and the three studies of the project "Awareness Lab SMEs (ALARM) Information Security" followed by a conceptual outlook
(translation; study paper forthcoming in August 2023)

Margit Scholl

5.1 Summary in the context of further scientific literature

There is no doubt that cyberattacks can threaten the existence of small and medium-sized enterprises (SMEs), and information security is becoming increasingly important in German SMEs [1]. Companies around the world must increasingly give priority to information security management (ISM) [2]. The German Federal Office for Information Security (BSI) also regularly restates the fact that German SMEs must focus their business processes on their own IT security situation [3]. According to the study by the Germany's umbrella organization of industry and commerce (DIHK), the cyberattacks of the past year have shown that any company can become a target for hackers [4]. Therefore, SMEs are by no means excluded. However, previous measures to raise information security awareness and increase security-relevant behavior among employees have not had a long-lasting effect [5] [6]. German companies have recognized the dangers of various cyberattacks but only take *technical* precautions [4]. Without question, these are an important component of information security, but on their own they are not an adequate means to combat increasing cyber and real attacks such as social engineering [7]. By contrast, there was no significant increase in the *organizational* measures for information security, and only a third of the companies surveyed in the DIHK study have an action plan for emergencies [4]. This contradiction shows a paradox at work in German companies, with an evident lack of sustained implementation of awareness-raising measures, especially in SMEs.

No increase in organizational measures for information security in German SMEs means no awareness development and no awareness-raising measures for managers and employees. As a result, the employees of German SMEs are not sufficiently sensitized and trained, although this is explicitly required by the BSI standards [8] and the international family of standards ISO/IEC 2700X [9]. An operational information security management system (ISMS) is clearly incomplete without such awareness and training measures [10]. In addition, the economic interdependence is significant, and there are also clear indications from global studies that nonsecure behavior by employees poses a major threat and can undermine cybersecurity in companies [11]. To effectively counteract cyber threats, there can be no question that information security awareness (ISA) programs are an essential cornerstone of corporate security, and there are many ways to impart information security knowledge. But knowledge alone is not enough. Attention needs to be paid to the research results of many international studies, which indicate that the mere transfer of knowledge is not sufficient to achieve sustainable ISA [12]. In the project "Awareness Lab SMEs (ALARM) Information Security" funded by the German Federal Ministry of Economics and Climate Protection (BMWK) from 2020 to 2023, an overall scenario is being developed to explore new, human-centered ways of increasing information security on a long-term basis in German SMEs. In addition to extensive literature reviews on the situation in companies, the current status of ISA was observed in the project using a combination of different methods [1], [13].

This third study of the "ALARM Information Security" project rounds off the series of project studies, with desk research conducted by the subcontractor known_sense. In the first study [14] [15], the firm known_sense carried out in-depth psychological interviews with the participating pilot companies in order to understand the current status of information security in SMEs and used the information so obtained to identify the topics that are relevant for the development of suitable analog materials for raising awareness. These findings, coupled with an online survey (Report 1 [16]), were also used as a basis for developing the digital learning scenarios and "on-site attacks" that were integrated into the overall scenario. Right from the start, the goal of the project was to take the day-to-day operational work situation as the starting point for developing support tools for SMEs that would be both scientifically sound and highly practical. SMEs should be able to advance the establishment of awareness-raising measures for employees and thus contribute to increasing operational information security, thereby building an appropriate SME security culture and ultimately ensuring the increase in security levels in German SMEs.

The human factor has an increasingly important role to play in information security. User behavior is now widely recognized as a critical component of cybersecurity, and training is the method most frequently recommended as a means to ensure secure behaviors [17]. However, there is typically no input on methods and didactics, which would certainly be relevant. Since the digital age requires interaction with digital services (online services), ISA is becoming more important than ever for everyone. Yet, because ISA is now defined as a set of factors, it is not enough to simply increase knowledge [18]. This makes ensuring the efficiency of awareness-raising and training measures for information security extremely difficult. Given the significant role that individuals play in the security well-being of organizations, end users of IT systems are encouraged to see themselves as part of the information security solution and are expected to perform certain security functions (as a kind of "backend human firewall," for example). However, there is often a gap between the organization's expectations of the end users' part in information security and their functional role [19]. Actual security-relevant behavior does not simply follow in a linear manner from knowledge.

The intensive interviews conducted in the pilot SMEs made it clear [14] [15] that these are not new threats but well-known security problems, which German SMEs are still grappling with. In addition, the issues mentioned by the interviewees as being important in this connection revealed that the level of awareness can often be significantly expanded, with the well-known security problem areas of password security and phishing attacks at the top of the list [14] [15]. The eight problem complexes identified by SMEs were merged into seven topics, which formed the basis for developing seven analog and digital gamified learning scenarios (serious games) and "on-site attacks." And of course, the comprehensive digitization of business processes requires *analog* sensitization material. Our modern game-based analog awareness-raising measures to create long-term information security and data protection are characterized by:

- active participation
- a haptic approach
- interactivity
- discursive settings
- stories/narratives to enhance memory
- the ability to contribute personal experience
- flexible timing (from 15-minute sessions during breaks to hour-long intensives)

It has been scientifically recognized for decades that a mix of methods is necessary for different target groups, different types of learners, and abstract topics [20]. In addition to the analog serious games,

our project has therefore also focused on the development of supplementary digital serious games [13] [21] [22], which can be accessed for individual play via the project website [23]. When using the digital serious games for business purposes, it is important that there is a debriefing within the team in order to support the discursive nature of the training. In addition, suitable "on-site attacks" (simulations, on-site inspections) were carried out; their findings are reflected in instructions for action and low-threshold security concepts for SMEs [13] [23]. In addition, the topics we deal with to raise awareness are of lasting interest to employees, since they all relate to and are important in private life—this is repeatedly emphasized in both the empirical (e.g., [24]) and the scientific literature (e.g., [25] [26]).

The finding from the interviews in Study 1 [14] was that gamification with playful and experience-oriented learning scenarios clearly addresses employees and stimulates their imagination on abstract topics, but at the same time it must not take place without strategic preparation and regular content-related support. This means that measures in German SMEs that involve humor and fun must be accompanied by a strategic, respectful approach, and the playful aspect should be kept in the background so as not to jeopardize acceptance [14]. In addition, a clear plan is required for the narratives that fit the topic: they should be formulated in an appealing way that is suitable for SMEs and encourages active exchange. Here, there is another clear recommendation to facilitate implementation in German SMEs: the role and function of a moderator should be established within the SME as a strategic element in the development of the security culture and as a practical aid for raising awareness of current security issues on an ongoing basis. Whether this can be combined with other roles/functions, such as that of an information security officer [10], must be decided by the top management of the SME.

Awareness-raising and training measures targeted to specific groups of employees are considered crucial in both the BSI standards [8] and ISO/IEC standard family 2700X [9] and in the scientific literature. In addition, the conceptual idea of the "ALARM Information Security" project in the application assumed that the areas in which information security in SMEs can be improved should be specified according to employees' operational activity profiles. The first study [14], however, revealed that such a detailed breakdown for German SMEs is evidently not appropriate at present, owing to the typically low level of ISA maturity. Rather, the heterogeneity observed in SMEs and the clear need to enhance the level of awareness maturity speak against such short-term diversification, because no psychological relevance could be determined for the envisaged activity, security, or competence profiles [14]. This made it clear that at this time, awareness raising for information security should take place more intensively for all employees in SMEs. The profiling aspect was made a separate part of the project, examined by an online survey, and published as Report 1 [16]; seven overarching areas of activity profiles were defined here, for which further specified learning materials could be developed with an increased level of awareness. For further explanation, see also [27].

The second series of in-depth psychological interviews (Study 2) [28] aimed to conclusively evaluate the analog learning scenarios (serious games) that had already been developed, tested, and improved, and to use these findings to create the final versions. At this point in time, six of the seven analog serious games developed have been evaluated [28] (see also [13] [29]):

- Live and work securely at home (topics: "Home office," "Smart home," and private security in general in your own house or apartment)
- The five phases of CEO fraud (topic: "Boss fraud"—see also [22])
- Manage customer data securely in the cloud and elsewhere (topic cluster: "Password," "Customer data," and "Cloud security")
- Mobile communication, apps, etc. (topic: "Risks and how to avert them when using mobile apps")

- Cyber Pairs (topic cluster: “Attack vectors in industrial espionage,” “Cybercrime,” “Social engineering etc.”)
- Information classification (topics: “Classification” and “Purpose of documents, data, information”)

According to the interim conclusion of Study 2 [28], no two SMEs are the same despite all the similarities between them. This is particularly true when it comes to the security communication that is required in each case. Among other things, there are major cultural differences with regard to the industry, services and products, ownership, history, composition of the workforce, web presence, and communication, which affect not only the organization itself but also its security culture [28]. It has been shown too that the security cultures in the German SMEs surveyed were much more differentiated than in large companies. Some preliminary reflections on an “SME safety culture model” are provided [29] and discussed in detail in Report 2, which is currently being prepared and will be available for download from September 2023 on the project website [23].

We must therefore assume that there is a very clear range of security cultures in German SMEs. This goes hand in hand with a significantly different level of awareness maturity in the companies. Against this background, a patented solution awareness in the sense of “one-size-fits-all” for all forms of security culture in the entire spectrum of German SMEs seems impossible on a practical level [28], and this is confirmed by the international scientific literature [30]. However, the analog serious games developed in the “ALARM Information Security” project have a major advantage: their modular approach, designed for differentiation, with the possibility of individual customization, supports the SMEs in using this wide range for themselves in the serious games’ material with their own practical examples to be supplemented and thus adapted in a practice-oriented manner [28].

The conclusion of the evaluation (Study 2 [28]) was that the analog experience-oriented learning scenarios (serious games) in the “ALARM Information Security” project with the associated simulations represent sophisticated, empowering awareness tools for SMEs. These analog serious games for SMEs manage to reduce to an appropriate level the sense of overwhelm experienced by employees when faced with the often abstract topic of information security and take away their fear of the risks that are posed and possible failure. Employees can open up without fear, share their experiences, and ask questions, giving them a more balanced sense of the “disturbing” topic of information security and enabling them to get a read on it for their specific workplace. This is the intention behind awareness/sensitization measures: for staff to be careful and remain attentive. This is why it is so important to have a format like our analog serious games, which can be as short as 15 minutes or as long as an hour.

The stations “Secure home living & working,” “Cyber pairs,” and “Mobile communication, apps, etc.” were evaluated as excellent communication accelerators, involving participants in a worthwhile discourse on information security [28]. The other analog serious games also work in a similar way, but according to the second study [28], they are not equally effective in every environment. In particular, the learning scenario “Information classification” was changed significantly as a result of this evaluation, especially since classification is not (yet) established as a standard process in most German SMEs [28]. Our finding was that no analog learning scenario works equally well everywhere, and defining an exact fit for the particular serious game is made more difficult by the great cultural heterogeneity in the German SME environment. The current recommendation is that the learning scenarios should be geared differentially to particular target groups, since the level of awareness in German SMEs still needs to be increased. The learning scenarios and materials developed in the “ALARM Information

Security" project should be used to generate a basic level of awareness relating to information security in SMEs, and this should backed up on an ongoing basis. Specializations are reserved for further participatory information security projects.

The second study, however, revealed that "security awareness" is viewed by those taking part in the survey as an important component of information security and that gamified development generally has an extremely energizing effect. Not only were all the participants from SMEs motivated and cheerful while playing, they were also serious and concentrated in their attitude [28]. During the group discussions, all the participants contributed to the productive feedback at the follow-up sessions, which we particularly advocated. We were therefore able to conclude that the idea of using gamification to raise awareness to a level that creates integration and clearly exceeds the sensitization performance of theoretical learning approaches worked well [28]. The majority of people gave a positive rating to the exchange of ideas during the game, especially when small groups or pairs were formed by the participants, who engaged in intense personal discussions in synchrony with one another [28]. In this case, however, the moderators need to keep an eye on the time available. There were repeated positive evaluations for the fact that the games stimulated conversations about "real-life situations" [28]. This shows that our serious games represent a kind of simulation of real work and everyday scenarios. The reference to information security in people's own private lives was evidently put across with some clarity.

The successful evaluation of the analog Serious Games for Security Awareness in SMEs developed in the "ALARM Information Security" project is thus a given—they create a social space, while also providing users with a dramatic framework that supports a concrete sensitization process. Nevertheless, Study 2 [28] pointed to the fact that the awareness measures remain ineffective unless the analog/digital autonomy of staff is promoted and integrated as an internal "living firewall." Employees who are not trusted to behave responsibly feel disenfranchised [28]. Security that relies on preventing this kind of freedom in decision making can lead to reactance, which can in turn lead to new security incidents in the company. What we need, though, is resilience. "Resilience is the ability to absorb and adapt to changes in the environment (ISO/IEC standard 22300), with risk management playing a central role (ISO/IEC standard 31010)" [31]. The great importance of risk assessment for all employees and risk management as a central aspect for managers has already been shown in previous projects. We had already developed an analog serious game for this as part of another project [7]. Security awareness and sensitization count as "social work" in SMEs [28], and the entire management needs to model this.

This third study of the "ALARM Information Security" project, which is now available, supplements the first two studies with very specific answers to many of the questions that we hear again and again when conducting awareness events. It is intended to support the moderators and multipliers of security awareness measures—as well as executives (top management) and IT and security specialists—in establishing appropriate communication in the company to make it possible to successfully plan, implement, and evaluate awareness-raising and training on information security and data protection issues. The following factors are dealt with in Study 3, which includes the moderation briefings and numerous hints and tips on the analog learning scenarios:

- Awareness, degree of maturity, and security culture as background influences
- The material of the analog serious games
- The preparation for the individual analog serious games
- The relevant goal and the didactic intention of the individual games
- The stories and game dynamics of the individual learning scenarios
- Tips for moderation

- Golden rules for the participants
- Possible questions
- Solutions for the individual analog learning scenarios

Although security awareness is now one of the formal components of the business processes and compliance definitions in companies, it is not necessarily embraced by all those involved. However, the successful raising of staff awareness to enhance information security is undeniably a success factor for SMEs. Study 3 is thus seen as a guide for SMEs—i.e., a practical self-help guide.

There is also a summary of the success factors that have been seen to have a lasting effect on security awareness. The security culture needs to be expanded in SMEs; the managers need to be convinced to support the process and should expand systemic communication with regard to information security. Managers must learn to understand their function as role models, recognize and use multipliers for information security and awareness, and make time resources available to employees for awareness-raising measures. Targeted methods with a high synergy factor are to be used, to convey the personal advantages for all target groups and to choose a clear, authentic, and above all non-technical approach. With increasing maturity, numerous different communication channels can be used to target specific groups.

The necessary mix across multiple channels is also confirmed internationally: delivering the same message in different ways has changed staff attitudes toward the importance of security measures more effectively than just delivering it once [32]. It can also be seen internationally that overburdening employees with too much technical information can have a negative effect [32]. It is particularly important to make the training appealing and interesting because it promotes willingness to participate, encourages employees to engage in more self-development activities, allows the (learned) knowledge to be disseminated more quickly through peer-to-peer interaction, and reduces the "security fatigue" that is now occurring. Education, training, and raising awareness of information security remain the key approaches to changing security behavior worldwide [33]. But security behavior is a very complex, multidimensional, nonlinear construct that requires further research. Attempts are currently being made to develop this construct with a number of models (see, for example, [34] [35] [30]). The three studies in our project indicated that pure knowledge transfer is now considered to have failed (see also [12] [6] [36]), which is why new paths have been taken in the "ALARM Information Security" project and experience-oriented learning scenarios and serious games have been developed.

5.2 Our findings from the three studies for German SMEs

The "ALARM information security" project has comprehensively achieved its goals and provides excellent materials that have been tried and tested in practice and can be used to raise awareness among employees in SMEs and enhance information security (see [23]). These materials are available free of charge via the website The analog and digital serious games and other materials such as suitable low-threshold security concepts also contain instructions and information for the specific internal implementation of this didactically prepared mix of awareness-raising measures in German SMEs.

Irrespective of the successful completion of the project with all the final results in September 2023, further activities are still required: targeted, broad publicity is called for, as is the use of the existing high-quality, didactically refined materials for raising employee awareness to ensure effective transfer to SMEs. In addition, we should devote more attention to the topic of "security culture" in German SMEs: secure digital transformation can only happen through continuous improvement of the security culture based on increased competence in the area of cybersecurity. This also affects the executives

and management, because information security is not just a matter for the boss—a better level of security awareness than the current average for SMEs is a prerequisite for the success of the current process of digitization.

A recurring factor—be it in our training courses, the relevant norms [9] and standards [8], or the international scientific literature—is the importance of top management and of the executive board and directors, who should play a supporting role and act as role models. This means that increasing the level of IT and cybersecurity in SMEs through a gradual increase in security awareness among decision makers and management with the top-down transfer of awareness skills to employees is far more crucial than was previously thought. However, developing managers as role models in the area of security requires a methodical understanding of security awareness and the ability to communicate cybersecurity and awareness in ways that are vivid, straightforward, and comprehensible. In SMEs, skilled trade businesses, and start-ups, knowledge about the dangers of the digital world in general is not sufficient to ensure sustainable security awareness, because knowledge must be supplemented with emotional and systemic skills in order to achieve a sufficient level of security awareness. This requires a much better understanding than we currently have, which is why further research is needed here as well.

According to our application-oriented and practical experience with the "ALARM Information Security" project, a better understanding of information security awareness must be created in German SMEs, especially with regard to marketing tools. Management should therefore be familiar with memorable stories (narratives, storytelling), imagination, and metaphors to reduce the complexity of the topic and simplify the task of security communication. We advocate systemic communication based on "discursive didactics." This means increasing the principle of "talking security" in SME business processes and building further mechanisms to prevent cyberattacks, by improving people's ability to freely discuss cybersecurity, the risks it poses, and ways of defending against it.

At the same time, this means that the knowledge in SMEs, skilled trade businesses, and startups about possible courses of action in all sub-areas of cybersecurity—be it prevention, detection, or reaction—must be increased. Since German SMEs are struggling with resources for information security, it should be made clear that managers and executives require systemic guidance supported by effective tools. By "effective tools," we mean simple gamified materials that have an elaborated graphic design and a haptic component to aid comprehension: these materials should be specifically designed for the management to ensure that their risk assessment in the SME situation, their prioritization of measures, and their embodiment of a security model are bolstered, transparently deployed, and accepted.

The aim must be to increase the competence to act in all sub-areas of cybersecurity in SMEs, skilled trade businesses, and start-ups by demonstrating and transforming security communication methods. Top management and executives must be able to pass on their well-founded assessment of the operational security situation to their employees in an appropriate, intelligible way. Perhaps "ambassador concepts" of awareness and security communication can also be implemented in such a way that employees can mature into "awareness ambassadors."

We conclude that there are three necessary steps in the process:

1. the establishment of moderators within a SME. They would have the task of using practical, vivid, narrative methods and formats to illustrate abstract topics and thus remove significant barriers to information security within the SME.
2. the establishment of recognized training for moderators, whether they are recruited internally in the company or from consulting firms (multipliers). The training should enable the moderators

and multipliers to decouple cyber security topics from the IT context in such a way that they are understandable for everyone and security communication is comprehensible.

3. the establishment of recognized certification for moderators and multipliers is important in order to achieve long-term efficacy.

5.3 Outlook for further applied research and practical implementation in SMEs

The use of secure digital processes, secure digital technologies, and secure digital business models—which will secure and increase the competitiveness and innovative ability of German SMEs—is a MUST for the country, for the prosperity of its citizens, for the further development of companies, and for the authorities providing the funding for new grants. Our experience in various security projects with a focus on "the human factor" and with a wide variety of target groups and actors suggests that this is possible by using visual, narrative-based materials, reducing complexity, and developing an understanding of complex conditions and relationships. This would presumably also bring people closer to the technologies of the future, involving a participative approach to information sharing, the integration of discussion and understanding, the ability to take positive action, and involvement on an equal footing.

It is possible that not every SME will be able to do this on its own. Therefore, transfer structures must also be established with other players in IT and cyber security, in which the gamified methods being developed for employees and newly developed consulting tools for top management can be further refined with certified multipliers from specialized consulting companies or handed over to these multipliers for practical deployment within established customer relationships with SMEs. Technological, organizational, and work-design skills in IT and cybersecurity should be increased, and it should be possible to evaluate the security of and trust in (provider/user) information and communication systems. To achieve this, the connections between IT and cybersecurity and data protection must be addressed and translated into intelligible stories and images. In general, in the course of digitization, it should be noted that the people who commission, offer, and operate platforms as well as the developers of digital solutions (online services) should focus on the users of the systems, be they employees, consumers, or citizens in general (see also [37]).

Despite the undoubted success of the "ALARM Information Security" project for all those involved, we definitely see some residual weaknesses. According to the findings of the project, these relate to three areas in German SMEs:

- The provision of high-quality and didactic awareness-raising materials for employees in SMEs is not sufficient for SMEs to actually use them internally. Rather, SMEs need to be "taken by the hand" to ensure that the transfer to sustainable use is successful.
- This means, for one thing, that moderators for awareness-raising measures within the SMEs should be trained ("awareness ambassadors/consultants"). These moderators can be recruited internally in the SME or externally via consulting firms. The quality of the moderation, in turn, depends on effective training, which should be ensured through certification.
- A further decisive factor in successful security communication is the top management (executive directors) and managers within the SME. Consulting firms can play a key role here. Advice/coaching, however, requires different materials for managers than the previously developed awareness-raising measures for employees.

This relies on the approval of further application-oriented research projects in the field of information security/cybersecurity focused on the top management in German SMEs.

Prof. Margit C. Scholl, PhD
Technical University of Applied Scienes Wildau
August 2023

Literature

[1] Scholl, M., & Schuktomow, R. (2021). The Current State of "Information Security Awareness" in German SMEs. *International Journal of Emerging Technology and Advanced Engineering (IJETAE)*, [online] 11(12), pp.151–163. Available at: https://ijetae.com/files/Volume11Issue12/IJETAE_1221_16.pdf.

[2] Dang-Pham, D., Kautz, K., Hoang, A. P., & Pittayachawan, S. (2022). Identifying information security opinion leaders in organizations: Insights from the theory of social power bases and social network analysis. Computers & Security, 112, 102505.

[3] BSI—Bundesamt für Sicherheit in der Informationstechnik (2022). Die Lage der IT-Sicherheit in Deutschland. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=5. Accessed: July 19, 2023.

[4] DIHK—Deutscher Industrie- und Handelskammertag e. V. (Ed.) (2022). *Zeit für den digitalen Aufbruch: Die IHKUmfrage zur Digitalisierung/Time for the digital awakening. The IHK survey on digitization.*

[5] Zerr, K. (2007). Security-Awareness-Monitoring. DuD Datenschutz und Datensicherheit 31. Wiesbaden: Springer Gabler.

[6] Bada, M., Sasse, A.M., & Nurse, J.R. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? ArXiv, abs/1901.02672.

[7] Scholl, M., Gube, S. and Koppatz, P., 2021. Development of Game-Based Learning Scenarios for Social Engineering and Security Risk Management for SMEs in the Manufacturing Industry. *Journal of Systemics, Cybernetics and Informatics*, [online] 19(2), pp. 51–59.
Available at: http://www.iiisci.org/journal/sci/FullText.asp?var=&id=ZA516ND21.

[8] a) BSI—Bundesamt für Sicherheit in der Informationstechnik (2017). *BSI-Standards 200-1 bis 200-4*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html. Accessed: August 09, 2023.

b) BSI—Bundesamt für Sicherheit in der Informationstechnik (2020). *BSI-Kompendium*, *Baustein ORP.3*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/02_ORP_Organisation_und_Personal/ORP_3_Sensibilisierung_und_Schulung_Editon_2022.pdf?__blob=publicationFile&v=3. Accessed: August 09, 2023.

[9] a) ISO/IEC 27000:2018(E), Information technology — Security techniques — Information security management systems— Overview and vocabulary. INTERNATIONAL STANDARD ISO/IEC 27000, fifth edition 2018-02.

b) ISO/IEC 27001:2017. Berlin: Beuth, 2017.

[10] a) Scholl, M., & Ehrlich, E.-P. (2020). *Informationssicherheitsbeauftragte: Aufgaben, notwendige Qualifizierung und Sensibilisierung praxisnah erklärt*. Frankfurt am Main: Buchwelten-Verlag.

b) Scholl, M., & Ehrlich, E.-P. (2020). *Information Security Officer: Job profile, necessary qualifications, and awareness raising explained in a practical way*. Frankfurt am Main: Buchwelten-Verlag.

[11] Alotaibi, S., Furnell, S., & He, Y. (2023). Towards a Framework for the Personalization of Cybersecurity Awareness. In: Furnell, S., Clarke, N. (Eds.) Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol 674. Springer, Cham. https://doi.org/10.1007/978-3-031-38530-8_12.

[12] Helisch, M., & Pokoyski, D. (Eds.) (2009). *Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung / Security Awareness - New ways to successfully raise employee awareness.* Wiesbaden: Springer Vieweg.

[13] Scholl, M. (2023). Sustainable Information Security Sensitization in SMEs: Designing Measures with Long-Term Effect. Proceedings of the 56th Hawaii International Conference on System Sciences 2023. URI: https://hdl.handle.net/10125/103369. ISBN: 978-0-9981331-6-4 (CC BY-NC-ND 4.0), pages 6058-6067.

[14] Pokoyski, D., Matas, I., Haucke, A., & Scholl, M. (2021). *Qualitative Wirkungsanalyse Security Awareness in KMU*. Projekt "ALARM Informationssicherheit". In: Scholl, M. (Hrsg.) [online] Wildau: Technische Hochschule Wildau, p.72. Available at: https://alarm.wildau.biz/.

[15] Scholl, M. (2021). *Foreword with an Introduction to and Summary of the Study "Added Value for SMEs" (Translation)*. Vorwort zur Qualitative Wirkungsanalyse Security Awareness in KMU Tiefenpsychologische Grundlagenstudie im Projekt »Awareness Labor KMU (ALARM) Informationssicherheit«.
DOI: 10.13140/RG.2.2.21236.88961

[16] von Tippelskirch, H., Schuktomow, R., Scholl, M., & Walch, M. C. (2022). *Report zur Informationssicherheit in KMU– Sicherheitsrelevante Tätigkeitsprofile (Report 1)* (p. 111). Wildau: TH Wildau.
Available at: https://alarm.wildau.biz/static/20b6d15448c0ba23729e0f45daa20650/alarm-informationssicherheit-report-1.pdf.

[17] Kävrestad, J., Fallatah, W., & Furnell, S. (2023). Cybersecurity Training Acceptance: A Literature Review. In: Furnell, S., Clarke, N. (eds) Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol 674. Springer, Cham, pp. 53-63. https://doi.org/10.1007/978-3-031-38530-8_5 .

[18] Fertig, T., Schütz, A., & Weber, K. (2022). Automated Measuring of Information Security Related Habits. Proceedings of the 55th Hawaii International Conference on System Sciences | 2022. URI: https://hdl.handle.net/10125/80267. ISBN: 978-0-9981331-5-7 (CC BY-NC-ND 4.0), pages 7702-7711.

[19] Ogbanufe, O. (2020). "Information Security Is Not Really My Job": Exploring Information Security Role Identity in End-Users. Proceedings of the 53rd Hawaii International Conference on System Sciences 2020. URI: https://hdl.handle.net/10125/64263. ISBN: 978-0-9981331-3-3 (CC BY-NC-ND 4.0), pages 4256-4263.

[20] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behav. Inf. Technol.*, vol. 33, no. 3, pp. 237_248.

[21] Prott, F. and Scholl, M. (2022). Raising Information Security Awareness Using Digital Serious Games with Emotional Design. *IADIS International Journal on WWW/Internet*, 20(2), pp.18–34.

[22] Scholl, M. (2023). Raising Awareness of CEO Fraud in Germany: Emotionally Engaging Narratives Are a MUST for Long-Term Efficacy. Álvaro Rocha, C. Ferrás, & W. Ibarra (eds.), *Information Technology and Systems*. Cham: Springer International Publishing. Doi: 10.1007/978-3-031-33258-6_40.

[23] https://alarm.wildau.biz/. Accessed: August 09, 2023.

[24] sosafe: Human Risk - Review 2023. Die europäische Cyber-Bedrohungslage: Experteneinblicke und Strategien, https://sosafe-awareness.com/de/ressourcen/reports/human-risk-review/. Accessed: July 13, 2023.

[25] Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations. Proceedings of the 51st Hawaii International Conferenceon System Sciences 2018. URI: http://hdl.handle.net/10125/50524. ISBN: 978-0-9981331-1-9 (CC BY-NC-ND4.0), pages 5085-5094.

[26] Farshadkhah, S., & Stafford, T. (2019). The Role of "Eyes of Others" in Security Violation Prevention: Measures and Constructs. Proceedings of the 52nd Hawaii International Conference on System Sciences 2019. URI: https://hdl.handle.net/10125/59927. ISBN: 978-0-9981331-2-6 (CC BY-NC-ND 4.0), pages 4895-4903.

[27] von Tippelskirch, H., & Scholl, M. (2022). Target Groups in German SMEs for Information Security Training: The Use and Limits of Job Profiles in Designing Training Units. *Journal of Internet Technology and Secured*

Transactions, [online] 10(1), pp.787–795. Available at: https://infonomics-society.org/jitst/published-papers/volume-10-2022/.

[28] Pokoyski, D. und Matas, I. (2022). Enabling vs. Entmündigung - Qualitativer Konzepttest analoger Security Awareness-Lernszenarien für KMU im Projekt »ALARM Informationssicherheit«. In: Scholl, M. (Ed.), [online] Wildau: TH Wildau.
Available at: https://alarm.wildau.biz/static/c0e4d00beefe1dc5fac9b50b6087265f/studie-2-master-final.pdf.

[29] Schuktomow, R., von Tippelskirch, H. & Scholl, M. (2023). Informationssicherheit in den Arbeitsalltag nachhaltig integrieren: Informationssicherheitskultur verstehen, mit Serious Games sensibilisieren und das Informationssicherheitsbewusstsein der Mitarbeitenden erhöhen. 36. AKWI Jahrestagung 2023. Erweiterung für die INFORMATIK 2023. Im Erscheinen.

[30] Topa, I., & Karyda, M. (2023). Addressing Organisational, Individual and Technological Aspects and Challenges in Information Security Management: Applying a Framework for a Case Study. Proceedings of the 56th Hawaii International Conference on System Sciences 2023. URI: https://hdl.handle.net/10125/102687. ISBN: 978-0-9981331-6-4 (CC BY-NC-ND 4.0), pages 470-479.

[31] Homepage Jutta Heller, https://juttaheller.de/resilienz/resilienz-abc/definition-organisationale-resilienz/. Accessed: July 18, 2023.

[32] Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, *10*, 132132-132143.

[33] Nwachukwu, U., Vidgren, J., Niemimaa, M., & Järveläinen, J. (2023). Do SETA Interventions Change Security Behavior?: A Literature Review. Proceedings of the 56th Hawaii International Conference on System Sciences 2023. URI: https://hdl.handle.net/10125/103396. ISBN: 978-0-9981331-6-4 (CC BY-NC-ND 4.0), pages 6300-6309.

[34] Jaeger, L. (2018). Information security awareness: literature review and integrative framework. Proceedings of the 51st Hawaii International Conferenceon System Sciences 2018. URI: http://hdl.handle.net/10125/50482. ISBN: 978-0-9981331-1-9 (CC BY-NC-ND4.0), pages 4703-4712.

[35] Schütz, A., & Fertig, T. (2023). The Forgotten Model–Validating the Integrated Behavioral Model in Context of Information Security Awareness. Proceedings of the 56th Hawaii International Conference on System Sciences 2023. URI: https://hdl.handle.net/10125/103462. ISBN: 978-0-9981331-6-4 (CC BY-NC-ND 4.0), pages 6841-6850.

[36] Sasse, M. A., Hielscher, J., Friedauer, J., & Peiffer, M. (2022). Warum IT-Sicherheit in Organisationen einen Neustart braucht / Why IT security in organizations needs a fresh start. Federal Office for Information Security (BSI) (Hrsg.) (2022): Proceedings of the 18. Deutscher IT-Sicherheitskongress des BSI / 18th German IT Security Congress of the BSI, February 2022.

[37] Ruiz Ben, E., & Scholl, M. (2023). Challenges Posed by the Digital Transformation Paths of the Online Access Act in Germany: Implementation and the Need to Raise Awareness. In J. Liebowitz, *Pivoting Government through Digital Transformation* (pp. 147–170). Boca Raton: CRC Press [Boca Raton]. Doi: 10.1201/9781003369783-10.