Target Groups in German SMEs for Information Security Training: The Use and Limits of Job Profiles in Designing Training Units

Hubertus von Tippelskirch, Margit Scholl
Technical University of Applied Sciences Wildau (TH Wildau), Germany

Abstract

As digitization becomes increasingly ubiquitous, the importance of information security for every institution is growing more evident year by year. According to recent studies, the cyberattacks of the past year have shown that any company can be targeted by hackers. Without proper information security, a company's survival is at risk. German companies have recognized the dangers of a wide range of cyberattacks and taken technical precautions. There has, however, been no significant increase in organizational measures for information security—including awareness raising and training for managers and employees. The question remains, however, how should awareness-raising measures be tailored to target groups? Profile groups tailored to the everyday working life and usage behavior of employees facilitate authentic learning based on a constructivist concept. Information security training is needed for every job profile in German SMEs. To verify this, an online survey was conducted and analyzed descriptively. Questions include the use of technical infrastructure and external interactions, the work environment, security measures, and the frequency and need for information security training. Correlations between job profiles, scatter plots with usage characteristics, and a comparison of usage behavior largely confirm the urgent need for awareness and the expected job profiles. SMEs are becoming more digital, more mobile, and more in need of training. The result is a "profile arc" that can be found in every company and used to guide authentic learning approaches. Constraints in the SME environment, such as short time frames with limited resources, and the impact of the pandemic need to be discussed.

Keywords: Information security (ISec), information security awareness (ISA), small and medium-sized enterprises (SMEs), constructivist concept, authentic learning, ISA training, sustainability

1. Introduction

Successful digitization requires a strategy to be implemented by the management of the company, guarantees an appropriate level of security, needs sufficiently qualified staff, demands a cultural change in the organization (the establishment of a security culture), and requires continuous further training targeted to specific groups as well as further education for all employees. The in-house training of employees to promote information security (ISec) in companies is increasingly driven by the challenge of rapidly increasing digitization [1–3]. In many studies, security gaps are considered particularly critical when they are the product of organizational deficiencies combined with human errors. The Verizon 2022 Data Breach Investigations Report emphasizes that 82 percent of the breaches that occurred were made possible by the decisions and/or active unconscious behavior of humans, involving phishing, the theft of credentials, misuse, and error [4]. However, Menges et al. [5] point out that using negative language and blaming employees are indicators of dysfunctional relationships. Information security awareness (ISA) among employees is important but should not be seen as a panacea [5]. It cannot resolve organizational and technical deficiencies, implement security protocols that go beyond staff capabilities, or manage conflicts with the productivity goals that companies expect of their employees.

In the corporate context, ISec must therefore be a concern at the top management level and should be understood holistically if a corresponding company-wide ISec culture is to be built. Small and medium-sized enterprises (SMEs) account for 99.6 percent of all German companies [3] and thus represent a major target for cyberattacks. It is a devastating indictment that, at the same time, they are considered to lack the competence to assess IT security threats [6]. Close cooperation with German SMEs taking part in a pilot program is therefore essential to developing a systematic approach that can expose and tackle areas of weakness in key business processes [3] and extrapolate specific activity profiles. This is of key importance for digitization in SMEs, as shown by the Digital Office Index [1]. The information and experience gathered in our current project with pilot companies should enable the management to combine with security officers to initiate training and further education measures tailored to the needs of the specific working groups. To this end, a survey was conducted and evaluated, allowing profiles to be developed in our project. This article presents important findings from our survey and gives an outlook on how to proceed in future. The survey and its results are a module in the project designed to build

 | DOI: 10.20533/jitst.2046.3723.2022.0097

an innovative overall scenario for ISec in SMEs and are supplemented by a number of other measures. Ultimately, the results should lead to awareness-raising measures targeted to specific groups. This should allow SMEs to use them independently.

The results are used to examine our first hypothesis (H1) that tailoring profile groups to employees' everyday work and user behavior is possible to enable authentic learning. Our second hypothesis (H2) is that ISec training is needed for every job profile in SMEs. The paper therefore deals with the research background relating to terms such as "behavior change" and "simulated authentic learning" as well as the current situation in German SMEs. After a presentation of how profile groups are created, their benefits and limitations are discussed in connection with further scientific literature in order to be able to answer the two hypotheses in a sound manner.

2. Research Background

The basis for the survey that was conducted was the modernized IT-Grundschutz [7] and its standards for protection, as established by the German Federal Office for Information Security (BSI) [8]. Further insights were also used, such as the Bitkom Digital Office Index [1] and previous surveys [2; 3].

Communicating knowledge about cyberattacks and specific ISec topics is necessary but not sufficient. Several studies conclude that most traditional ISec training measures, the many operational guidelines, and even sanctions have no apparent long-term effect (see, for example, [9]) Rather, creating awareness is important in order to achieve greater awareness and thus improve the operational level of ISec. Ultimately, the aim of the ISec training is to achieve long-term safety-related behavior among employees. The key question, however, is which awareness-raising measures can be used to achieve this and in what form. One aspect that is mentioned in the BSI standards is of central importance for the survey carried out in our project: target-group orientation. For Bada et al. [9], understanding people's perception of risk is the key to creating effective awareness-raising campaigns. One of the conclusions arising from their study of international literature and the question of why security awareness campaigns often fail is that while knowledge and awareness are prerequisites for behavioral change, they are not necessarily sufficient in and of themselves [9].

According to the literature review by Ertan et al. [10], further research is also necessary to create a better understanding of how we can promote behavioral change in the area of cybersecurity on a day-to-day basis. In particular, research needs to be conducted to determine behavioral variances between different types of employees and within different corporate environments, as these variances may also be reflected in different behaviors in relation to cybersecurity issues [10]. To identify types of employees, a survey can be used and evaluated to determine differences and similarities. "The most successful programs are those that users feel are relevant to the subject matter and issues presented" [11], which is in line with the results of the US NIST proposals [12]. The context for discussion and training is people's private, working, and social lives [13]. Serious games as a learning method mimic these real-world problems in an open, safe learning environment [14]. They must reflect reality to serve their purpose, be it in learning, training, or provoking behavioral change [15]. So, in our case, we have to meet employees at the level of their daily work life and gear the training toward their real usage of information and technology as well as their daily work routines.

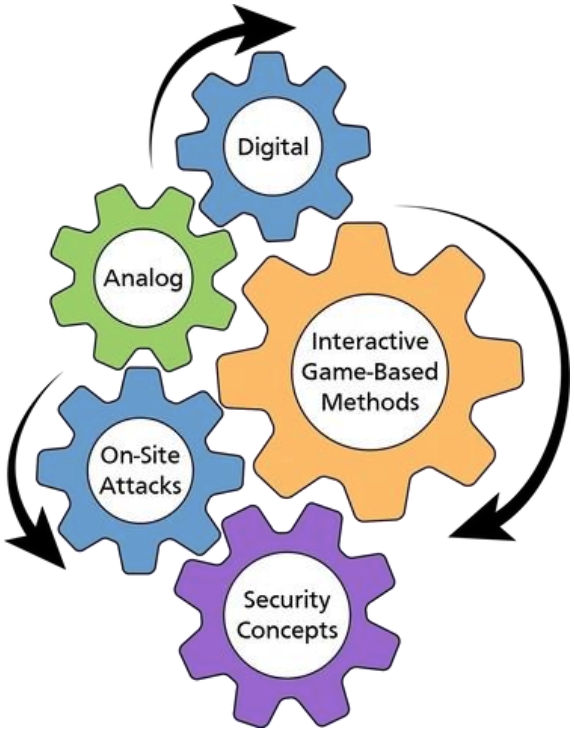

Figure 1. The project`s combined training methods

Our aim in the project is to stay close to the real task through "simulated authentic learning" [16] and thus to explore profile groups with similar needs, because this should also make it easier for employees to participate in training courses guided by a practical understanding of the content. Real-world relevance is one of the essentials of authentic learning [17]. This also supports the use of constructivist theory with its belief in the active involvement of learners, which is achieved by processing meaning and knowledge as part of an effort to encourage participative construction [18]. With the simulations based on the research data of the survey, employees can apply a process of trial and error in the protected space of a

 | DOI: 10.20533/jitst.2046.3723.2022.0097

sandbox environment [19]. Other aspects used in constructivist theory, such as "active learning," "collaborative learning," and "interactive teaching" [20] are part of our project's approach and its ongoing development of seven analog and digital serious learning scenarios along with on-site attacks in the employees' everyday environments and deriving security concepts, backed up by studies (see Figure 1). Therefore, in the context of the H1 hypothesis and given the focus on the project's German pilot companies and the provision of data for "simulated authentic learning," deriving criteria on how to form learning groups and characteristics to identify common needs can be seen as the intended results of this paper.

In the *Awareness Lab SME (ALARM) Information Security* project, the results of our initial study [21] and the outcomes of this—Report 1 [22]—are the basis for developing new awareness-raising measures tailored to SMEs and personal engagement with the issues (see figure 1). The goal here—and thus the value added for SMEs—is to provide integrative interlocking measures that contribute to systematic awareness raising and help, in actual terms, to develop a security culture. The project departs in this respect from unsuccessful forms of classical training. The surveys and summaries of the current situation are intended to generate recommendations for the introduction of modular awareness-raising measures and low-threshold security concepts in German SMEs.

3. Methodology

Our survey was designed as an online survey, created with "QUAMP Survey Sociolutions," and should engage participants for a maximum of 15 minutes. In the first question, participants were asked to assign themselves to one of fifteen job profiles that most closely matched their activities. The second question focused on their position in the hierarchy (apprentice/trainee/intern, employee, middle management, executive/top management), hereinafter referred to as hierarchy groups. This was followed by seventy-three questions from the five question categories: "technical infrastructure," "risks from external interaction," "working environment," "security measures," and "awareness raising." The questions are along the lines of "How often do you have to deal with the following in or for your job?"

A four-point Likert scale for frequency was chosen with an ordinal scale level and response options of "always," "often," "rarely," and "never." The scale was intended to "force" a clear decision from the participants, as there is a tendency to choose the middle when the scale is odd [23]. There followed questions about training needs with the response options "not at all," "low," "medium," and "high." The survey finished with an open question about the most important ISec term.

Four pilot companies from Brandenburg and Baden-Württemberg took part in the online survey, as did other partner companies from the Chambers of Industry and Commerce (IHK) and the project sponsor; total N=108 people. The sample design was stratified disproportionately according to company size, industry, and region. It was not weighted, because the focus was on a status analysis and not on the representativeness of the population of SMEs in Germany. Of the fifteen job descriptions surveyed, twelve were represented among the respondents. These were:

- Sales / Field sales
- Purchasing / Procurement
- Personnel matters / Human resource management / HR
- IT / Administration
- Materials management / Logistics / Warehousing
- Customer management/service
- Manufacturing / Production
- Finance / Bookkeeping / Accounting
- Research / Development
- Marketing / Communication
- Secretary's office / Reception / Doorman / Mailroom
- Process management / Quality assurance / Controlling

The respondents did not feature anyone from facility management, the legal department, or public relations. Data analysis made use of descriptive statistics and the graphical representation of the response distributions in the individual job profiles through bar charts, pie charts, and radar charts. In order to describe direct relationships between either a pair of job profiles or the hierarchy groups, the Pearson correlation coefficients were determined and presented in a correlation matrix. This provided initial conclusions as to which combinations had a lot in common and could later be grouped together.

Special scatter diagrams were developed to characterize a job profile. A scatter diagram provides information about the membership in a hierarchical group (per median) and the mean values of the answers to the seventy-three usage and assessment questions. The values of the entire framework of all twelve fields of activity were entered in the background of the graph and served as a referencing point cloud. The displayed field of activity and particularly strong and weak correlation pairs were highlighted by means of special coloring and dot shapes. A special feature here was that the question items were sorted according to the mean values of the associated job profile, making it possible to do a step-by-step reading of use frequency and estimated need. These scatter diagrams were used to identify the

 | DOI: 10.20533/jitst.2046.3723.2022.0097

peculiarities of one job profile as compared to the others and where commonalities existed. Based on the correlations, the comparative analysis through the scatter diagrams and the addition of the IT-Grundschutz [7], job profiles were put together into profile groups. In the first qualitative study of the project on the impact analysis of security awareness in SMEs based on in-depth psychological interviews [21], the necessary training content had previously been developed, which could now be assigned to suitable profile groups on the basis of qualitative considerations.

4. Results

Detailed results can be found in the complete German report on security-related job descriptions [22]. Here we give just one example of the four hierarchic groups: senior managers in SMEs typically have foreign-language skills and use social (career) networks; they need to rely on online bookings and make use of data encryption, digital signatures, freeware, and backup software. Their activities are characterized by mobile working and traveling, coupled with frequent usage of USB sticks, external hard drives, credit cards, and databases. There is thus a significant risk facing the top management group in SMEs and they need specific awareness-raising coaching. The middle-management group, for example, also makes frequent use of databases as well as Enterprise Resource Planning (ERP) programs. The employees hardly ever use social media, tablets, smartphones, or payware and are also not entrusted with confidential data, email encryption, data deletion, or data encryption. This group needs general awareness raising on the topic of information security. Trainees do not go on business trips or get visited by externals at their workplace. They get less involved in crucial areas, but in many cases they have a company key and are tasked with shredding documents and answering calls. However, except for (top) management, the hierarchic groups were primarily used as a way of identifying basic skills.

The job profiles were more critical in defining the training profiles. The analysis of the responses by job profile confirms basic assumptions about typical usage behavior in many cases, such as the heavy use of sensitive personal data by the HR group, while also revealing some anomalies. Marketing is the only job profile in the median of the respondents to be assigned to the senior management/top management. The highest correlation occurs between the purchasing and sales job profiles.

The first three profile groups form the core of each SME and the top of the information security profile arc (see Figure 2). The other groups represent the four gatekeepers who can shield the core operation as far as possible. Their roles are not staffed in every SME but must nevertheless be assigned and consciously performed. The profile arc thus provides guidance on which learning content is important at which point.

At the top of the profile arc (Figure 2) are the general requirements and basic competences for acquiring a position in a medium-sized company. The corresponding basic security requirements apply to all job descriptions. The focus here is on providing elementary protection and fundamental knowledge. This area must therefore be developed in a particularly broad way, but at a level that can be taught to all job profiles. A general training should be offered as part of activating learning scenarios.

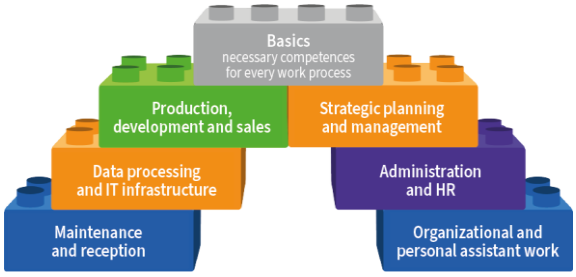

Figure 2. Using the "profile arc" to identify target group characteristics

"Production, development, and sales," which are core activities—in other words, activities directly related to the manufacture of the product or the creation of the service—were characterized by certain common features. These were, for example, a low level of encryption measures, infrequent access to sensitive personal data, and minimal access to sensitive areas, with no use made of credit cards or online banking. Similarly, work is done primarily at fixed workstations and desktop computers. These respondents often rated the need for training for themselves and the company as low. Also included is the sales subgroup, which operates very close to the core activities but has a more agile profile based on travel, stronger external contacts with customers, and procedural data processing. In a special position within this group is the job profile of research and development, which has a higher demand for security measures. In addition to repeating basic knowledge, training could be offered here for development- and process-heavy tasks in the area of encryption and industrial espionage and for the more mobile subgroup in the area of travel security.

The "Strategic planning and management" is where decisions are made and guidelines set. It is one of the two navigators managing risks. This group has partial or total access to all areas of the company, including sensitive data, safes, and security-related mechanisms. It is also highly mobile and extremely exposed due to its constant contact with all stakeholders. It must be the first to be kept up to date and secured across all security domains. This group can be trained in, for example, the topic of travel

 | DOI: 10.20533/jitst.2046.3723.2022.0097

security and, most importantly, risk management.

The "Data processing and IT infrastructure" is crucial for the establishment and maintenance of the technical infrastructure. It is the digital gatekeeper of the four groups at the bottom of the arc and controls technical access. It also develops the technical guidelines and controls the related security training, which is why it also puts the most emphasis on the training requirements. It is therefore the second navigator managing protection. It is tied to a fixed workplace, but at the same time it needs to be deployed everywhere in the company and is competent in all technical devices and networks. In addition to a special focus on teaching the latest guidelines and training concepts, this group could, for example, be offered training in ransomware as a means to protect and maintain data availability and confidentiality.

The "Administration and HR" deals with very sensitive areas relating to financial and personnel administration. In this context, access rights are narrowly restricted but go very deep. The group is the financial and personnel "gatekeeper," controlling financial flows and personnel access. General company keys, access to the safe, access to even the most sensitive personal data, on-duty smartphones, and responsibility for document destruction and data deletion are of crucial importance here. Staff in this area have many contacts both internally and externally. This profile group could, for example, be specially trained in the topic of data protection.

The "Maintenance and reception" staff did not figure among the respondents (unfortunately, such staff may not have been considered for the survey, or their tasks were taken over by other staff or outsourced personnel). However, they are responsible for setting up and maintaining the building's technical infrastructure and control spatial, postal, and, as a general point of contact, telephone access. They are therefore the physical gatekeepers and although they are at a lower level in the hierarchy, they are critical when it comes to implementing security measures. Training on the subject of disinformation and social engineering, for example, would be a good idea.

Organizational and personal assistant work occupies a hybrid role, positioned between its intermediary, organizational, or administrative activity and the respective job profile with authority over it. In other words, it is the communicative "gatekeeper" controlling all information flows—for example, to the company management or a department. It also has access to financial areas such as online bookings, online orders, and credit cards. This profile group likewise needs to be focused on topics such as disinformation and social engineering but can also always go deeper into other areas based on specific tasks they might have. With regard to our second hypothesis (H2), it is worth emphasizing that the above training examples are also of value for most other profiles. In security practice, the profile groups can only be broadly (rather than precisely) differentiated on a small scale, and all areas can be affected by different attack vectors. The thematic assignments should thus be seen as "lighthouse topics" of the profile and radiate out from there to the entire company to be multiplied and disseminated independently.

In response to the question "Name the information security term that is most important to you," terms relating to privacy protection were accorded the greatest importance (34%). This was followed by terms related to data security (21%), awareness (11%), passwords (10%), and confidentiality (9%), as illustrated in Figure 3. However, this again shows that information security training is not characterized by isolated, individual topics but by regulations that have been put in place—as with the General Data Protection Regulation (GDPR)—or by a holistic, basic understanding of the issues involved.

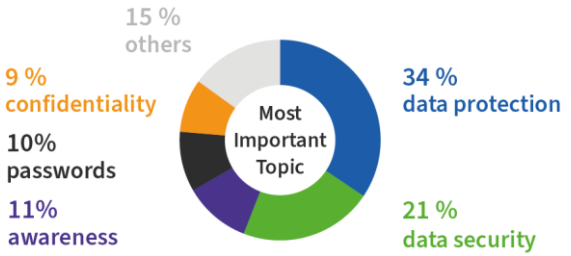

Figure 3. Most important information security topic

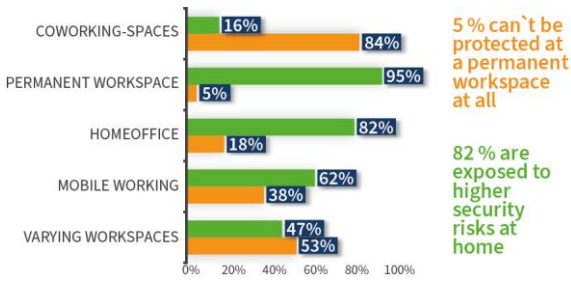

Figure 4. Workspaces and work environments in February 2021. How often used: never (orange), rarely, more often or regularly (green)

Another factor that was accelerated by the pandemic is the increase in time spent working at home. Compared to the period before the Covid-19 pandemic, the number of employees who carry out their work at home has roughly doubled. In addition, a correlation has been demonstrated between increased use of an office at home and individuals with higher educational attainment. It is also reasonable to assume that to a large extent this will lead to permanent change and shape new security postures [24]. During the survey period (February 2021), 82 percent of the employees were exposed to

 | DOI: 10.20533/jitst.2046.3723.2022.0097

higher security risks while working at home and 5 percent could not be protected at a permanent workspace at all (see Figure 4).

The survey shows that people in different areas of activity have taken part in training or awareness-raising measures on the subject of ISec with varying frequency. However, the findings from manufacturing/production were particularly striking, with over 30 percent stating that they had *never* attended any training on ISec. It is interesting to note that around 80 percent of management or trainees rate the need for training for themselves as medium, and over 30 percent of middle management and employees see a high need for training for themselves somewhat more often. In general, all respondents see a need for training, even if this is estimated to be higher for the company than for themselves (see Figure 5). This fully confirms our second hypothesis (H2), that ISec training is required in every job profile in SMEs.

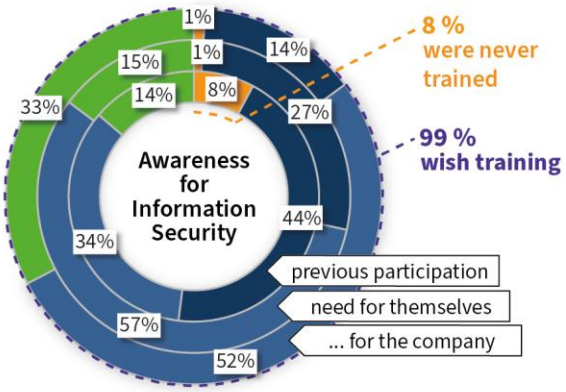

Figure 5. Awareness-raising activities on information security. Participation / need: never / not at all (orange), rarely / low (dark blue), more often / medium (light blue), and regularly / high (green)

5. Discussion

The survey's database and its seven profile groups offer an interesting option for determining international research questions for German SMEs, focused mainly on the idea of tailored information security training. In order to establish a sustainable and firmly rooted security culture in companies, measures must be targeted and specifically adapted to the staff, the job profiles, the existing knowledge, and the circumstances of the company. The survey provided the necessary data to enable job profiles to be grouped on the basis of their daily work. "Simulated Authentic Learning" can be based on the derived criteria represented by the profile arc developed for this purpose and its group modules, so that hypothesis H1 was also confirmed. Our results give guidance on how to form learning groups and identify characteristics for shared needs.

Awareness-raising concepts such as training or education in a comprehensible and tangible form, such as in the experiential and interactive analog and digital learning scenarios of our project, should be adapted and developed accordingly. The survey shows that in order to reach individual target groups represented by the profile groups and to increase their competencies for information security, integrated measures are required in companies. The results presented here therefore support the need for actions tailored to everyone in the SMEs and confirm hypothesis H2. However, at the same time, the results show the limits of an isolated focus on individual job profiles.

"One size fits all" for security awareness measures does not constitute sustainable practical advice for chief security officers (see also [25]). However, for the isolated implementation of individual profile groups in SMEs, even in the accompanying study [21], no direct psychological relevance could be determined, because the level of awareness raising in German SMEs is too low. Despite the heterogeneity, there are, in general, valid risks and safety issues that should first be identified across all areas and target groups; these play a significant role in the everyday working life of all the groups of people surveyed [21].

This aspect of the profiles must be examined more closely in further or subsequent evaluations. The limitations inherent in a small sample of this kind must be considered. It should not be regarded as representative. It is also possible that there was some distortion in the selection process when test subjects were being chosen for the survey within the SMEs. Further research, such as cluster analysis or partial orders [26], has not been undertaken so far.

In addition, the special pandemic situation certainly had an impact on issues relating to workplaces, company parties, business trips, and external contacts, for example. Security in the home office will also be an ongoing issue and requires future attention. With regard to an authentic learning approach, there is also the challenge of how to adapt training methods to individual safety environments and contact persons, such as children in the family. It is already difficult to engage and train employees in the company setting, but the home environment is much more difficult to reach and protect.

One avenue for further research is to develop practices like "train-the-trainer" programs to apply the findings of the survey in the SMEs on a lasting, self-perpetuating basis. Train-the-trainer can be an effective dissemination and multiplier strategy to equip a company with the necessary knowledge and training material to integrate the content that is provided in their existing in-house training [27]. It also creates a strong incentive to adopt the particular program at their home company [28]. However, this still relies on managers who are willing to fund

 | DOI: 10.20533/jitst.2046.3723.2022.0097

resources and allocate working time in the interests of long-term viability. Constructivist strategies and authentic learning show some limitations: in the SME environment, these include short time frames with limited resources and businesses that do not support a learner-centered culture with facilities, technology, motivated instructors, and tradition [29]. Where the expectation is that all of the material is provided (along with the answers), coupled with close supervision and content-driven learning tested by an exam, more structured methods may be required [29] or greater motivation generated first. There is another way to create a better understanding of how we can promote behavioral change in the area of cybersecurity on a day-to-day basis [10]. Ertan et al. [10] identify four behavioral patterns that have a major impact on how people practice cybersecurity: compliance with security guidelines, coordination and communication between groups, phishing/email behavior, and password behavior. In addition, the concept of a security culture is an important overarching theme straddling the four behaviors, which overlap within the frame it provides [10].

However, managerial implications can be identified, learning content assigned, and action recommended. Managers should determine the actual situation in their own company, assess risks, and create an awareness that all employees of a company play an important role. Further, a common security structure underpinned by basic knowledge needs to be established and enhanced to create a "human firewall" [21] by using the proposed, more defined target group modules. In the area of "Strategic planning and leadership," this discrete target group should be trained so that they can ensure the creation, communication (internal and external), and review of general security policies and guidelines and can lead by example in terms of training and behavior. As with all the profiles, the training for "Production, development and sales" should focus on creating awareness in dealing with the internet, information security in general, and the application of access controls. In the area of "Data Processing and IT infrastructure," access, entry and access control concepts must be implemented and stressed. The development, communication, and testing of IT security policies as well as apps and software are also part of the training. The same applies to the establishment of "reminders," the updating and maintenance of IT infrastructure and security mechanisms. "Administration and HR" must receive training tailored to their specific authority to ensure personnel and financial flows. "Maintenance and reception" staff must be enabled to monitor access and have work safety and evacuation plans ready. Particular awareness must be built up here to protect against on-site attacks by social engineers and disinformation. In "Organizational and personal assistant work" communications must be monitored and legitimized, and special training provided depending on the department in question and the special authority granted. Social engineering and manipulation should also be a focus here. If the results presented here are compared with other surveys [2; 3] and a longer period of time, a number of things become very clear: SMEs are becoming more digital, more mobile, and more in need of training. The second hypothesis H2, which specifies the ISec needs, is confirmed for every job profile but has to be thought of in terms of intertwined modules rather than isolated elements. Usage behavior is vulnerable, information security is important, and the need for effective training is omnipresent.

The identified profile groups in German SMEs confirm the hypothesis H1 so far, as they support authentic learning based on recognizable everyday work and user behavior. However, it should be understood as a framework at most for a tailored ISec training. Further research is needed to show whether this can successfully reduce vulnerabilities in people's real work life. Meanwhile, the importance of information security training in German SMEs is growing. However, there are several pitfalls involved in raising awareness, such as a shaky understanding of security awareness and its unique position, an overreliance on compliance programs, failure to assess the programs properly, and, finally, a lack of access to engaging and appropriate materials [9]. Using the profile groups should help to reduce these risks, especially in creating customized learning scenarios. But even if all this helps, these improved measures still compete with the economic challenges, such as productivity losses, time constraints, training costs, and opportunity costs. Furthermore, as seen, for instance, in simulated attacks, thought needs to be given to legal compliance and the impact on self-efficacy and trust [30]. A long-term change management approach [31] should be established to critically monitor and assess the long-term efficacy of the security training.

6. Outlook

The statements made in Report 1 [22] should not be regarded as representative, and any assessment of them must take into account the limitations inherent in a small sample of this kind. It is also possible that there was some distortion in the selection process when test subjects were being chosen for the survey within the SMEs. Nevertheless, the report provides a more concretized, up-to-date insight into how SMEs are actually faring in the conditions imposed by the pandemic. In addition, the concept of a security culture is an important overarching theme. Furthermore, the report's database [22] with its seven profile groups offers an interesting option for determining international research questions for German SMEs too.

 | DOI: 10.20533/jitst.2046.3723.2022.0097

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 Verwaltung spro zessen 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-in-der-wirtschaft.de/ITS/Redaktion/DE/PDF-Anlagen/Studien/aktuelle-lage-der-it-sicherheit-in-kmu-langfassung.pdf (Ac-cess 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. Lambrinoudakis, 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=publicationFileandv=3 (Ac-cess Date: 17 December 2021).

[7] Bundesamt für Sicherheit in der Informationstechnik (Ed.). (2021, January 26). IT Grundschutz.https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_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-Grundschutz/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. Governement 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-thetrainer_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).

