The Current State of “Information Security Awareness” in German SMEs

Margit Scholl¹, Regina Schuktomow²

^{1,2}*Technische Hochschule (TH) Wildau, Hochschulring 1, 15745 Wildau, Germany*

Abstract—The role of information security in German SMEs is becoming increasingly important. External input plays a key role here, but some of it tends to overwhelm SMEs rather than providing systematic assistance that can be readily implemented. In a project funded by the German Federal Ministry for Economic Affairs and Energy, an overall scenario for new ways to achieve more sustainable information security (IS) in German SMEs is being developed, one that puts people at the heart of the measure. In addition to a current literature search on the situation in companies, the current state of information security and IS awareness is recorded in the project through a combination of different methods: in-depth psychological interviews, an online survey in four pilot companies and security-related competence profiles derived from the German IT-Grundschutz. This article presents some preliminary results published.

Keywords—Information security, awareness, human factor, German SMEs, in-depth interviews, survey, competence profiles, security topics, training methods.

I. OUTLINE

Section 2 of this paper clarifies the progress that has been made in IS as well as its current status and needs going forward. Security measures should be focused on people in order to achieve the necessary understanding of IS through an effective program of awareness-raising and ongoing practical training and further education. The background to this is briefly summarized in section 3. The goals of our German project—which is funded by a three-year grant from the Federal Ministry of Economics (BMWi) and aims to increase IS in SMEs in new ways—are outlined in section 4. Developing the overall scenario for sustainable awareness-raising, as planned in the project, relies on a concrete stocktaking of the current state of IS awareness (ISA) in German SMEs. The research questions (RQ) are presented in section 5. A combined methodology is used to answer these questions: this consists of in-depth interviews, online surveys and the derivation of security-relevant competence profiles based on the IT-Grundschutz [27]. This is also covered in section 5.

Some preliminary results from the evaluation of the current state of affairs and the answers to the RQ are presented in section 6. A summary of our current findings is shown in section 7, followed by an outlook for the ongoing process in section 8.

II. INTRODUCTION

The German economy is increasingly falling victim to cybercrime. In 2019, at least 75 per cent of all companies were affected by data theft, industrial espionage, or sabotage [1]. The majority (58%) of successful cyberattacks are carried out by e-mail, as malicious attachments or links are often opened by employees, a phenomenon that also operates in the private sphere [2]. Thus, six out of ten Internet users are victims of cybercrime [1]. The current 10th Allianz survey shows that, worldwide, operational interruptions, the pandemic outbreak and cyber incidents were the top three business risks in 2020—all of which are strongly interlinked [3]. Small and medium-sized enterprises (SMEs) are particularly affected—with their size and lack of resources worsening the situation [4] [1].

In Germany, theft—of devices and sensitive data—and social engineering (SE) are currently the most common crimes [1]. SE can occur via various channels, be it on-site contacts or calls, SMSes, or targeted phishing e-mails, the number of which is increasing dramatically [1] [5]. In the case of CEO fraud, an increasingly lucrative area, the attackers can obtain most of the information they need about a Chief Executive Officer (CEO) or Chief Finance Officer (CFO) from public sources [6] [7]. New types of attacks—such as Ransomware 2.0, which not only encrypts data but also steals it [8]—are often based on Advanced Persistent Threats (APTs), which are carried out via multiple attack sources and routes, combining different types of cyberattacks [9].

The risks and threats are often underestimated in the use of Information Technology (IT). Many SMEs are under the illusion that only large companies are the victims of attacks and as a result their valuable data tends to be poorly protected [10].

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 11, Issue 12, December 2021)

Even in research, the focus is generally not on SMEs, so the authors modelled an easy-to-use Cyber Security Canvas to remedy this deficit and to give SMEs a pragmatic way into the topic of security [10]. Given that existing approaches to IT governance, risk and compliance management are still insufficiently geared to SMEs, a competence-oriented approach to perceiving, measuring and controlling risk in SMEs is offered. [11].

In the knowledge that cybersecurity is an existential problem that is often not given proper consideration by SMEs, an increasing number of customers demand audit certificates from their suppliers as proof of a basic level of security [12]. Comparing international information security (IS) standards for certification and frameworks in combination with a corresponding literature review, it is shown that effective operational IS management is a systematic means of addressing the threats and risks to information system security, where technology is not enough [13]. Many recommended organizational factors must be integrated into technology in order to develop a broader approach to IS management, including people and business processes [13].

In addition, it became clear that while budgeting for IS is obviously important, many researchers have not looked at this aspect [13]. The representative survey by techconsult in Germany shows that—as an average across all companies—IT security tasks only account for 10 per cent of the IT spending and therefore a maximum of only around 3 per cent of annual sales [14]. The study by Hillebrandt et al. shows that many German companies are only willing to spend money on IT security when actual damage has occurred, and losses have already been suffered [15:79]. However, from a worldwide perspective, the current study by Gartner looking at trends in IT budgeting growth over time shows that after peaking in 2018 with a positive change of 3 per cent, growth levels fell back to 2 per cent in 2021 [16].

In addition, comprehensive certification can overwhelm SMEs. For this reason, Valdevit et al. presented a tailored adoption program with guidelines for SMEs back in 2009 [17]. Nevertheless, as discussed by Antunes et al. the results obtained in their project with SMEs in Portugal show a clear benefit to the SMEs in which IS audits were carried out and interventions took place, mainly attested to by the increase in their IS management (ISM) robustness and their collaborators' cyber awareness [18].

Based on an analysis of 440 findings from IS audits performed in Czech and Slovak companies during the years 2015–2019, Douchek et al. identified the following problematic areas for SMEs [19]: operations security, compliance and planning, including action to address risks and opportunities. Moreover, they found that in medium-sized enterprises other areas were relevant [19]: asset management, including manager's responsibilities, and performance evaluation, with a focus on deficits in monitoring, measurement, analysis and evaluation.

The EU Agency for Cybersecurity and the National Cyber Security Alliance (ENISA) identified four main cybersecurity challenges faced by SMEs across the European Union and United States of America in the pandemic year 2020 [20]:

- Low cyber awareness, even though cybersecurity should be integrated into the culture in SMEs.
- Lack of remote IT security, because with home offices more data and communications are being transmitted across insecure channels.
- High cost of cybersecurity solutions overall—money that many businesses simply do not have.
- Increased attacks such as phishing to trick online users.

Hard disk encryption, for example, is rarely implemented in German SMEs, and there are hardly any written rules on IT security and very little emergency planning [15]. This also increasingly affects the use of mobile devices. Purely technical solutions such as virus protection, spam protection and firewalls are often used but are operated in isolation [15]. Holistic information security management systems (ISMS), as per the ISO family 2700x [22] [23] or the German BSI standards 200-1 to 200-3 [24] [25] [26], and knowledge of the German IT-Grundschutz Compendium [27] are rare. "Holistic" means that security concepts must take into account the entire company organization [22] [23]. However, there is a lack of SME-focused ISMS. As a result, Wagner et al. strongly recommend explicitly considering the specific role of SMEs and creating dedicated and auditable standards [12]. Their study shows that most domain-specific security standards are applicable to large enterprises. In contrast, SMEs seek the support of security experts, who, for their part, often struggle with a lack of experience in operational technology [12].

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 11, Issue 12, December 2021)

According to the 10th Allianz survey, companies look to de-risk supply chains and boost business continuity management (BCM) for extreme events [3]. However, emergency management systems or a dedicated BCM—based, for example, on BSI standards 100-4 or 200-4 [28] [29]—are rarely found in German SMEs [30]. The German craft association *Das Handwerk* even lacks IT security analyses, comprehensive IT security concepts and employees with IT security knowledge [15]. Many critical success factors relating to the implementation of BCM in SMEs must be taken into account [31].

III. FOCUSING ON PEOPLE

The most common way of attacking sensitive data and provoking system failure is by tricking and manipulating people [32]. Cybersecurity should therefore have a primary focus on people and not just on protecting data and systems [32:3]. The IT Security Study 2020 by eco [33], an Internet industry association, also sees security awareness as increasingly important, so that companies are more and more reliant on employee training. While only 41 per cent of those surveyed in 2019 stated that they regularly train employees to be aware of cybercrime, in 2020 this figure had risen to 52 per cent [33] [32:5].

According to the Command Control Cybersecurity Index 2020, cybersecurity decision makers in Germany acknowledge their own omissions [32:6]:

- One third of companies do not keep their workforce sufficiently informed about current cyber risks.
- 42 per cent also refrain from systematically raising awareness about digital dangers on business trips.
- 31 per cent even say that employees have so far played no role at all in their company's security strategy.

This last finding is noteworthy, as SE attacks are on the increase in various forms [34] [1] [5] [35]. Wang et al. make clear how important it is to understand which attack scenarios are combined with which attack methods, and how these combinations lead to the success of an SE attack [35]. In addition to focusing on organized crime, foreign intelligence services, hobby hackers and competing companies and suppliers, analysis of perpetrators is particularly concerned with former employees, who may act intentionally or unintentionally [1] [5].

There is still too little focus on employees—it is crucial that the issue of IS is made a top priority by management and that it is institutionalized in the company by staff with special responsibility in this area [1].

In SMEs, training for *all* employees still needs to be implemented [34], and this failing means that when comparing the situation today with that in 2011, no real positive change is evident. This means that new efforts are necessary [36]. Continuously raising awareness of IS and risks remains of existential importance for SMEs. When further training is carried out in German SMEs, classic, non-digital (analogue) measures are still favoured by external trainers aiming to provide quality individual support for participants [38].

The COVID-19 pandemic in particular has shown how flexible attackers are: cyberattackers are part of a criminal industry that carries out attacks for financial reasons, under the rubric of “Cybercrime as a Service”, and the attackers have become more professional [8] [3] [5]. Because of the time lag between an attack and its consequences [40], a holistic management strategy for setting up ISMS and a long-term way of thinking about the deployment of measures tailored to specific requirements are key factors in reducing these security deficiencies. According to Li et al., the long-term orientation comprises the three dimensions of continuity, future viability and perseverance, which must be established in companies in the realm of information security [39]. Attackers use human vulnerability with specific methods from applied social science and with the help of fictitious, carefully crafted emails and websites: employees are spied on, analysed and then manipulated so that their access data is ultimately used to penetrate the company networks [41:4]. A company must raise its employees' awareness of security risks over the long term. This also requires the extensive involvement of all interested parties—particularly in training programmes that are aimed at sustainability, it is essential for the works and staff councils to be fully involved [41]. KnowBe4 sees deficits in security awareness training in the following three aspects [41:7]:

- passivity of learning methods
- inflexibility of the learning content
- over-compression of the apprenticeship period

The above examples of vulnerabilities make it clear that the security measures must by no means only be of a technical nature. People need to be at the centre of what is happening. The motto has to be: “Digitization only with IS and IS only with awareness.” IS must become a meaningful addition to everyday work, because attentive employees are necessary for the future of SMEs.

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 11, Issue 12, December 2021)

IV. OUR PROJECT

Although SMEs have an increased perception of risk, they are still relatively unwilling to carry out an IT security analysis and take suitable measures [15]. Many studies argue that compared to large companies, SMEs—and craft businesses, in particular—have extremely limited financial and human resources available for IS (see [4] [10] [11] [12] [15]). As a result, there is often a lack of coordinated IS strategies and practical, low-threshold instructions for building an operational IT security culture in SMEs. It is also crucial that the management understands their own overall responsibility for IS [22] [23] [24], so that executives actively fulfil their function as role models.

This is where our project comes in: it is building a practice laboratory for SMEs to cover these areas of deficit. The process of developing an awareness of IS issues is to be researched in a participatory manner and promoted in a practical setting for the needs of SMEs. A diverse overall scenario for raising awareness with appropriate staff development—i.e. building up appropriate IS competency—is intended to sustainably strengthen “operational security awareness” in everyday professional life. This goes beyond purely cognitive learning and also includes haptic understanding, the forging of emotional connections and the exchange of experience. Incidents are also demonstrated and low-threshold solutions practised. In addition to the process of developing measures, it is important for any such measures to be tested and evaluated to allow conclusions to be drawn about sustainability.

Awareness raising is “only the first step”, but it is the key to motivating people to improve their behaviour in the field of IS over the long term [43]. The relevant analogue and digital learning scenarios, which are developed in our project as a means to raise awareness and enhance personal competence, are therefore carefully thought out and designed to provide an entertaining but intense experience. They should clarify the common attack scenarios and their long-term consequences. In addition, suitable “on-site attacks” are deployed to focus attention in SMEs: the results of these attacks are also communicated to executives and employees in discursive exchanges. Moreover, each trial phase is accompanied by “awareness measurements”, while a train-the-trainer concept supports the operational implementation of the measures in four pilot SMEs.

The overall scenario of our project is thus a practical exercise laboratory with prototypes, materials and instructions for human resource development in IS: these are made available to all SMEs in German and can be downloaded free of charge from the project website at the end of the project. This provides the basis for ongoing preventive training for employees, which in the best-case scenario ensures that SMEs are spared damage, while the alertness of attentive staff significantly reduces the risk these companies run of suffering such damage.

V. METHODS OF RECORDING THE STATUS QUO AND RESEARCH QUESTIONS

In order to achieve optimal results in developing tailor-made measures for establishing sustained awareness of security issues, the project combines several different methods: psychology-based in-depth interviews, an online survey and security and competence profiles that were derived for global fields of activity in SMEs. Given the results of the combined status recording, seven analogue and digital learning environments will be defined for future personnel development. Each learning environment will be based on a practice-relevant “story”, which will be developed together with the project subcontractors as an experience-oriented, interactive learning scenario and tested with the pilot SMEs and other actors.

Depth psychology touches on the unconscious mental processes that explain human behaviour and experience [45]. Therefore, based on the interviews with managers and employees in SMEs, this paper’s first research question (RQ1) focuses on determining

- a) how the safety culture is perceived in the company, and
- b) the extent to which the participants are aware of IS.

The second research question (RQ2) relates to the online survey and has two aspects:

- a) What is the current level of understanding of IS-relevant topics in everyday business and how present are they?
- b) To what extent can the relevant competencies actually be quantitatively derived from the fields of activity identified by the survey?

For the theoretical-based definition of IS competence profiles, the IS standards and GDPR are used in combination with practical descriptions. The third research question (RQ3) thus examines the following issues:

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 11, Issue 12, December 2021)

- a) For what business areas should IS-specific or general learning scenarios be developed?
- b) In what depth should awareness-raising measures address IS topics?

4.1. In-Depth Interviews

Depth psychology interviews reveal unconscious psychological effects and influencing factors. These factors determine the behaviour of people affected by security [45]. The interviews are usually conducted as one-to-one conversations, observing confidentiality and anonymization. However, owing to the COVID-19 pandemic, the interviews had to be conducted online. WebEx from Cisco was used as a communication tool: this runs on its own servers and complies with the relevant data protection regulations.

In the project, 90- to 120-minute interviews were carried out by psychologists with sixteen managers and employees from the four pilot companies. Such security impact analyses pay attention to the connections between what is said, facial expressions, body language, etc. The participants embark on a mental journey and explore the deep connections themselves during the interview. This often opens up new perspectives, which are systematically pursued in terms of their behavioural relevance. Surprising aspects can be taken into account during subsequent explorations. These small but meaningful samples make it possible to produce intensive, scientifically sound, psychological analyses. The voluntary disclosure of hidden security motives can, after analysis in a psychological context, feed into the drafting of urgent recommendations designed to improve the security culture in every company [45].

4.2. The Online Survey

The online survey with targeted questions served two functions in the project: on the one hand, it was less time-consuming and allowed the actual situation pertaining to larger groups of participants to be recorded independently of time and place; on the other, it was used as a basis for recognizing security-relevant activities across all SMEs that require security and competence profiles to be derived.

The online questionnaire was preceded by a data protection declaration, which provided information about the project, the actors involved and the aim of the survey. In addition, the handling of personal data in accordance with data protection law was explained and consent requested for its collection, processing, storage and transfer within the research project.

The survey was abandoned by a total of eighteen people immediately after it was called up and by two other people immediately after the data protection declaration.

The survey itself was designed as an online questionnaire and created using Quamp Survey Solutions. Participant completion time was not intended to exceed 15 minutes. It comprised a total of seventeen closed questions with single or multiple answers and finished with an open question on the most important IS topic. The four possible answer options are “never”, “rarely”, “more often” and “never”. Overall, the online survey covered the following aspects:

- field of activity/job
- group of people
- workplace, including hardware and software
- Internet access and activities
- networks and activities
- encryption and digital signature
- occupational security through entry, admission and access protection
- (tele)communication
- personal activities relating to online banking, bookings and orders
- internal and external contacts
- personal and confidential information
- travel activities
- training courses and training needs

The survey with the four pilot companies took place from 15 February to 1 March 2021. Contrary to our intention that as many employees as possible should receive the link to the questionnaire, the relevant information was not forwarded to everyone. A total of ninety-nine people from the pilot companies (trainees, employees and managers) called up the questionnaire, and eighty-three people completed it, so the dropout rate was 16 per cent.

In the period from 24 February to 21 March 2021, the survey was carried out with two control groups. The first control group related to the promoter’s environment. Here twenty-two people went to the survey page, but 36 per cent dropped out, so that in the end fourteen people filled out the questionnaire. The second control group involved four associated transfer partners. Here seven people called up the questionnaire, but only five people completed it, so the dropout rate was 29 per cent. In light of this high dropout rate in the two control groups, the four pilot companies were obviously more motivated to fill out the questionnaire.

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 11, Issue 12, December 2021)

The evaluation of the overall data is currently still in progress. In the next chapter of this paper, the first partial results are presented.

4.3 Job, Security and Competence Profiles

The starting point for the outputs of our project are the specific business processes in SMEs—i.e. the everyday operational scenarios and the job activities associated with them—combined with different responsibilities. Following security and data protection standards, these are used to define theory-based security and competence profiles with regard to IS and data protection. This constitutes the third pillar of our current-status monitoring of SMEs.

Each of the job activities has its own requirements and rules that must be observed. The topic of IS itself plays a general role [1] [5] [47]. Tailored training concepts should be applied to the job activities and tasks of the employees [22] [23] [24]. Therefore, our project also deals with job profiles [48] and is based on a search through descriptions of the job advertisements on various job platforms [49] [50] [51] [52] [53] [54]. The goal is to define the main job profiles and task areas common to all SMEs, including the generally used applications and systems.

Our discussion within the project team covering several phases of results is not yet complete. However, so far it has led to seven accumulated, overarching areas of job activities, whose security relevance is compared with the help of the requirements set out by the BSI IT Grundschrift Compendium [27]. In other words, the defined job profiles lead to security profiles and create competence profiles. The security profiles represent an assessment of whether, for example, a certain activity represents a high security risk and key point of attack for the company and in what way. For example, a job profile “general office administration”—e.g. an administrative office with or without permission to manage resources—has a high security risk because of the large amount of internal information available and its close work with customers. So, it represents the central point for information management. In addition to general office management, the office has administrative and organizational tasks, such as appointment coordination or database maintenance. Taking into account the specific blocks with IS requirements in the IT-Grundschrift Compendium [27], specific security requirements can be converted into skill enhancement for employees and formulated, for example, into specific goals for training and further education.

This feeds into the resulting competence profiles. However, this remains part of an ongoing research process.

VI. RESULTS AND DISCUSSION

5.1. In-Depth Interviews

On the basis of the depth psychology interviews, it was possible to determine the needs for IS. Some topics for the measures in the project were identified according to their presence and importance. Without further inquiry being made, the following three topics were prioritized:

- passwords
- phishing (and related areas)
- data protection etc.

This confirms the previous result from Thiel and Thiel, which suggests that simple basic measures such as password protection have not been properly implemented for many years [30]—obviously this problem has still not been resolved. In addition to this, over a decade ago, more than one in five companies surveyed (22%) was affected by SE in an analogue manner and almost one in seven (15%) digitally [30]—with phishing currently second in the above list, there seems to be an awareness of these relationships. In answering RQ1, it can be argued that old common problems in IS apparently continue to be of great importance for SMEs. The third topic is likely to have come more into focus due to the widespread use of the GDPR.

The following topics were only added to the list on request:

- CEO fraud etc.
- Social Engineering, manipulation, etc.
- apps, software, etc.
- security in the home office
- data protection in the cloud as well as in the context of customers and suppliers
- messenger services, secure transmission, storage, encryption, etc.
- information classification—only where introduced as a process

From the interviews, it was assumed that the topic of mobile security would be high in the ranking, but it is currently of little relevance due to the pandemic situation and travel restrictions [45]. It should also be noted that the subject of IS in SMEs is associated by the test subjects with the particularities of SMEs. The participants presented the pilot companies as familiar, trusting and flexible.

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 11, Issue 12, December 2021)

A target group-specific diversification of topics, with an in-depth exploration of topic details for specific awareness-raising and training measures were not classified as significant in the evaluation of the interviews. This means that the SMEs involved are only at the beginning of a maturity model designed for permanent awareness-raising with regard to IS. SMEs obviously need to understand even more that regular input with basic awareness is required for all target groups, even if training courses or other awareness-raising measures are already being carried out in all the pilot SMEs involved. In a further answer to RQ1, it should be noted that generally applicable risks or safety issues, which are identified across all areas and target groups, play an essential role in everyday work for everyone—whether management or trainees.

Due to the overly positive presentation of safety communication, an attractive but interestingly inconsistent error culture is experienced and defended in the participating SMEs. In addition, CEO fraud attempts are presented as failed attempts, since contact with management or the IT administrator is made by the potential victims without hesitation and fraud becomes quickly apparent. This is a far more positive result than in other studies (see, for example, [4] [15] [39]). Nevertheless, it is possible that precisely in the context of our pilot SMEs, the dangers are overlooked or taken lightly.

In the final answer to RQ1, relating to the perceived safety culture in SMEs, figure 1 shows the perspectives as an overall result: the respondents' own SME is perceived internally as consistent in its security culture. It offers family ties, but at the same time established security structures can be ignored without any noticeable consequences. To the outside world, the companies respond to the needs of the market in a flexible, tried-and-tested manner and rely on mutual commitment. This already provides a partial answer to the second research question (RQ2), which deals with the understanding and presence of topics relevant to information security in everyday business. For this purpose, the first results of the online survey are presented in the next section.

5.2. Results of the Online Survey

Not all fields of activity that could be selected in the online survey were ticked. This suggests that the link to the online survey was selectively passed on to employees, and this was also confirmed by a managing director.

Nevertheless, it was possible to form pairs using a correlation matrix and visualize their correspondence within a topic ranking using scatter diagrams. Even if confirmation by further quantitative analyses regarding possible clusters is still pending, seven job profiles can be derived with the addition of qualitative considerations, which are explained in the next section. In this respect, the second research question (RQ2), focusing on the fields of activity to be determined, is answered. In order to establish a sustainable and firmly anchored safety culture in SMEs, targeted measures must be taken that are adapted to the people, the fields of activity, the existing knowledge and the circumstances of the company. This includes awareness-raising concepts such as training or education in a tangible and understandable form such as experiential and interactive analogue and digital learning scenarios. In order to reach individual target groups of the activity profiles and increase their competencies for information security, integrated measures are required in companies. The report supports the need for adapted measures, but after adding quantitative analysis techniques and observations in the scatter diagrams, it also shows the limits of tailoring to individual fields of activity.

Figure 1. The “feeling of security awareness” in SMEs

The following further results of the online survey should be mentioned:

- E-mail as the central means of communication is available to all groups of people involved with a prevalence of 100 per cent. Many people have contact with customers or business partners (the categories “often” and “always” feature in 70–80 per cent of cases).

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 11, Issue 12, December 2021)

Contacts with colleagues are most prevalent with a total of 99 per cent stating constant or frequent contact. In this respect, the presence of e-mail as a relevant area in information security is a given in everyday operational life (RQ2), and this is confirmed by the fact that phishing is ranked second on the basis of the interviews.

- The software package most used in the workplace is Microsoft Office (with 89 per cent citing frequent or constant use)—if you also consider its infrequent use (in 11 per cent of cases), the software product is ubiquitous. With regard to the answer to RQ2 in connection with RQ1, it should be noted that the problem area “prompt installation of patches” is not explicitly mentioned as security relevant.
- ERP software is only used “often” and “always” by around half of the employees in SMEs.
- The work device that is used “often” (18%) to “always” (60%) is the laptop—however, this does not necessarily mean mobile working. Mobile work is not usually available for the majority of people in German SMEs, and it is rarely the main aspect of a person’s job. It is important to remember that the pandemic travel restrictions were in operation at the time of the survey. A permanent job workspace is available for approx. 95 per cent of respondents. Co-working spaces, which are used “rarely” or “never” (95%), are completely underrepresented.

Figure 2. Security risks in pandemic times. From top to bottom: Co-working spaces, permanent workspace, home office, mobile working and varying workspaces

- Fax services, although still legally relevant in Germany, are on the verge of extinction—frequent use stands at a maximum of 32 per cent and almost exclusive use is relatively uncommon at 25 per cent.

- Surfing the Internet is a ubiquitous work activity in German SMEs: the categories “often” and “always” together make up 94 per cent of responses, while 5 per cent seldom surf the Internet. The use of cloud services stands at 67 per cent, albeit with a tendency towards infrequent use. The definitive non-usage of cloud services stands at 33 per cent. With regard to the answer to RQ2 in connection with RQ1, it should be noted that the associated security-relevant risks were only mentioned by the interview participants when prompted.
- The professional benefit of social and career networks as well as messenger services is not very pronounced in SMEs: the categories “rarely” and “never” together constitute between 66 and 83 per cent.
- In most of the pilot SMEs, encryption and digital signatures are not yet used. The security elements used most often are passwords (the categories “often” and “always” figured in 84 per cent of -responses). Here the answer to RQ2 confirms the result from RQ1, suggesting that the most conspicuous security problem in SMEs is still passwords.
- Workplace security through access protection does not seem to be relevant between colleagues in SMEs: 98 per cent know their colleagues’ workplaces. The answer to RQ2 also confirms the emphatic family ties established in RQ1.
- 35 per cent of the respondents regularly deal with online orders, but the proportion of regular online banking and regular online bookings as well as professional credit card use is down to 11–16 per cent and is therefore concentrated on a clearly defined set of people. In this respect, this answer in RQ2 explains why CEO fraud was only mentioned in the interviews (RQ1) when the interviewees were prompted. However, such an attack could well become security relevant for particular people and thus for the SME.
- In addition, the participants made a specific connection between “information security” and data protection (34%), data security (21%), awareness (11%), passwords (10%) and confidentiality (9%).

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 11, Issue 12, December 2021)

Figure 3. Priority list of information security keywords: data protection, data security, awareness, passwords and confidentiality.

Our survey shows a very heterogeneous picture with regard to the frequency of training courses attended on the subject of information security. Production employees stated that they had never or rarely attended such an event. By contrast, employees from the areas of marketing and accounting are more likely to benefit from such measures (66%). A relatively small proportion of employees regularly take part in training courses for IS. Even if our survey is not representative, this point coincides with the WIK study [15] and BSI information [25] [40]. In our survey, 57 per cent of employees see a “frequent” need for training in information security for themselves. Added to this is the proportion who see a high need for training—the “always” category here stands at around 15 per cent. If the training needs for the entire company are considered, the assessment of the proportion seeing the need for “frequent” training stands at 52 per cent of respondents, with 33 per cent citing a “high” need for training. Thus, there is a marked need for IS awareness and training in German SMEs.

5.3. Results of the Profile Definition

In response to RQ3 relating to the IS topics for which specific learning scenarios should be developed, the following cross-SME job profiles were defined based on the standards, online survey, research and qualitative considerations:

- general profile (applies as a prerequisite and for acquiring a job)
- production, development and sales
- information processing and IT infrastructure
- maintenance and placement
- organizational and auxiliary activities
- administration and staff
- strategy and leadership

For example, a person who works in the broad area of administration must have the following IS-relevant skills or be trained in them in line with the specific job requirements and the modules of the IT-Grundschutz Compendium [27]:

- very good social skills: correct behaviour when receiving/looking after third parties to protect information (module measure ORP.1.M3)
- correct supervision of public traffic to protect company and employee information (INF.10.M2): visitor identification required and entered in a logbook
- management of resources and correct inventory to guarantee company functionality (ORP.1.M8)
- correct archiving procedure when entering data into the database, adding metadata and digitizing materials (OPS.1.2.2.M4 and POS.1.2.2.M21)
- safe handling of documents and devices: announcing the sending of confidential content, e.g. via fax (NET.4.3.M14 and NET.4.3.M15).

Other aspects are the secure use of IT, be it mobile devices, operating systems or applications. Based on the competence profile presented, specific training and awareness-raising measures can be created for the individual job areas, giving employees the necessary know-how. The definition of the profiles therefore constitutes an important role for IS in individual companies. It is to be seen as a self-help tool for SMEs.

However, in response to RQ3, relating to the profundity of specific awareness-raising measures, and with an eye to the results of RQ1 and RQ2, it must be stated that German SMEs still need to strive for a higher level of IS maturity. At the moment, the main priority is to institute continuous measures for “basic awareness”.

VII. OUTCOME OF THE FINDINGS TO DATE

German SMEs are only at the beginning in terms of continuous operational awareness and still require generally applicable awareness-raising measures. Only at a later stage of maturity do very specific awareness-raising measures actually appear to be of practical importance for the individual target groups.

The researched job profiles are largely confirmed by the online survey carried out in pilot companies as part of the project. However, the survey was not forwarded to all employees, so that the anonymized participants probably do not represent the entire spectrum of employees, and therefore some fields of activity were not covered.

However, both the online survey and the depth-psychology interviews confirmed that the processing of data and the use of digital communication are essential in all pilot SMEs.

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 11, Issue 12, December 2021)

Moreover, the sudden increase in home offices has made the protection of information resources a new problem for SMEs in our study. It confirms Alharthi and Regan's literature review in 2021, which suggests that the application of security guidelines is important but not a direct means of reducing the risk of SE attacks [55].

Based on the individual statements made by the interviewees and thanks to lean hierarchies with direct contacts to the managing director and the IT department, our four pilot companies see themselves as more positively equipped than might be suggested by the results of other studies. For example, the results of Aldawood and Skinner show that despite facing the most modern cybersecurity precautions and trained personnel, hackers can continue to successfully steal information that is of vital importance to companies [56]. Our further investigations will take into account the results of these authors who identified a plethora of circumstances that affect users' ability to detect and counter threats: these include business, environmental, social, political, constitutional, organizational, economic and personal factors [56].

In addition, current studies within our literature search show again that despite increasing digitization, there is still a lack of comprehensive awareness of IS in SMEs and, even if the risk perception has increased, there is a lack of holistic implementation of diverse security measures, including ongoing awareness campaigns. The extensive literature search by Chowdhury and Gkioulos on training methods shows that solutions that provide hands-on experience, team-skills development and high levels of real-life fidelity are often preferred to other options, with simulation-based solutions showing the highest amount of research and development [57]. Nonetheless, there is still a gap in the research on how to improve current cybersecurity training offerings to demonstrate whether integrating advantageous attributes from different delivery methods can produce more comprehensive and effective solutions [57]. Our project will help to fill this gap in the next two years.

The limitations of our study need to be addressed: only sixteen in-depth interviews could be held and only eighty-seven fully completed online questionnaires were evaluated. Some findings from other studies were confirmed. Overall, however, the assessment of the situation by the participants of our German pilot SMEs was more positive than average in comparison to other studies. Further scientific research must follow.

VIII. OUTLOOK ON HOW TO PROCEED

To cater to the security-relevant topics identified in our previous study in the first project year and with the help of the defined competence profiles, stimulating analogue learning scenarios and digital simulations will be designed in the next project year and tested in a participatory manner with the pilot SMEs. Further SMEs will be integrated in the evaluation phase in the second project year. "Stimulating scenarios" refers, in particular, to interactive, entertaining, team-based scenarios from everyday operational work life that engage participants' emotions and raise awareness of IS. In addition, suitable, so-called "on-site attacks" with awareness measurements and maturity statements are being developed: these will be instrumental in establishing an IS strategy in SMEs and identifying low-threshold security concepts.

In the second project year, we are increasingly focusing our research on the "security culture" of SMEs and studying the importance of ethical issues. The importance of the security culture in SMEs was highlighted in 2013 in the research project by Sanchez et al. [58]. However, the evaluation of the developed learning scenarios will be published in a second result study and report in 2022.

Our overall scenario of the project "Awareness lab SMEs (ALARM) information security" is intended to ensure that the employees of the SMEs gain motivation and self-confidence for lifelong learning and develop their potential for personal responsibility in the field of IS. In this sense, the experience-oriented learning scenarios will support learners to take an active part in the process, as recommended by Larsen-Freeman et al. [59].

In the third project year we will have to analyse the degree to which the following hypotheses are fulfilled:

- Our reality-related everyday scenarios are designed to help increase the individual awareness of individual employees in SMEs.
- The targeted interactivity with discursive exchange is intended to raise awareness throughout the company and noticeably increase the security level of SMEs.
- In addition to the continuous evaluations, in-depth interviews and an online survey will take place in every subsequent project year.

There is a growing body of literature in the information systems, computer science and HCI disciplines studying phishing and training (e.g. [60] [61] [62] [63] [64]).

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 11, Issue 12, December 2021)

In further papers we will explain how our work will draw on these prior works, build on their findings and make new contributions. However, more research on effective trainings and awareness measurements concerning the human factor in information security and awareness is necessary.

Acknowledgements

We would like to thank our project subcontractor known_sense for carrying out the in-depth interviews and preparing the results in an upcoming study.

We would also like to thank Stefanie Gube and Hubertus von Tippelskirch from our research team for the online survey: Stefanie supported the design of the survey and carried it out; Hubertus is intensively involved in its evaluation. We would like to thank the entire research team for their commitment to discussing and determining the proper profile definitions.

We are very grateful to Simon Cowper for professionally correcting this article.

REFERENCES

- [1] bitkom 2000. Spionage, Sabotage und Datendiebstahl–Wirtschaftsschutz in der vernetzten Welt: Studienbericht 2020/ Espionage, sabotage and data theft - economic protection in the networked world: Study report 2020, Berlin, Germany, retrieved from https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf. Accessed: 17 May 2021.
- [2] Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) 2020. Cyberrisiken im Mittelstand 2020/ Cyber risks in medium-sized businesses 2020, Report, Berlin, Germany, Brussels, Belgium, retrieved from <https://www.gdv.de/resource/blob/61466/0456901217b39a5893bc6829b8d7d156/report-cyberrisiken-im-mittelstand-2020-data.pdf>. Accessed: 17 May 2021.
- [3] Dobie, G., Hubmann, C., Keg, D., Larumbe, A., Polke, H., and Whitehead, J. 2020. Allianz Global Corporate & Specialty SE, Munich, Germany, retrieved from <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020-Appendix.pdf>. Accessed: 17 May 2021.
- [4] Eggers, F. 2020. Masters of disasters? Challenges and opportunities for SMEs in times of crisis. Journal of Business Research, 116, 2020, pp. 199–208.
- [5] European Union Agency for Cybersecurity (ENISA) 2020 <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape>. Accessed: April 23, 2021.
- [6] European Union Agency for Cybersecurity (ENISA), February 10, 2016 <https://www.enisa.europa.eu/publications/info-notes/how-to-avoid-losing-a-lot-of-money-to-ceo-fraud>. Accessed: 23 April 2021.
- [7] KnowBe4 (ed.) undated. CEO Fraud – Schützen Sie Ihr Unternehmen gezielt gegen Social Engineering/ CEO Fraud—Protect your company against social engineering in a targeted manner, Whitepaper, retrieved from <https://www.knowbe4.de/wissen/whitepaper/ceo-fraud>. Accessed: 24 May 2021.
- [8] Schonschek, O. 2021. Wie sich Cyberangriffe weiterentwickelt haben/ How cyberattacks have developed (pp. 3–5), Die nächste Stufe der Cyberangriffe/ The next level of cyberattacks (pp. 6–8), Wie es zu einer Evolution der Cyberangriffe kommt/ How Cyber Attacks Evolve (pp. 9–12). In e-book Cyberattacken der nächsten Generation/ Next generation cyber attacks, Security Insider, Vogel IT-Medien GmbH (March 2021), pp. 3-12, retrieved from www.security-insider.de. Accessed: 15 March 2021.
- [9] Bundesamt für Sicherheit in der Informationstechnik (BSI)/ Federal Office for Information Security (ed.) undated. Advanced Persistent Threat, undated, retrieved from <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahren/APT/apt.html>. Accessed: 23 April 2021.
- [10] Teufel, S., Teufel, S., Aldabbas, M. and Nguyen, M. 2020. Cyber Security Canvas for SMEs. International Information Security Conference, Springer, Cham (August 2020), pp. 20–33.
- [11] Johannsen, A. and Kant, D. 2020. IT-Governance, Risiko- und Compliance-Management (IT-GRC) für KMU–Literaturanalyse und Ansatzbildung/ IT Governance, Risk and Compliance management (IT-GRC) for SMEs–Literature Analysis and Approach Formation, 2020, retrieved from https://www.researchgate.net/profile/Andreas-Johannsen/publication/343305523_IT-Governance_Risiko-und_Compliance-Management_IT-GRC_fur_KMU_-_Literaturanalyse_und_Ansatzbildung/links/5fa179d6a6fdccfd7b97b10/IT-Governance-Risiko-und-Compliance-Management-IT-GRC-fuer-KMU-Literaturanalyse-und-Ansatzbildung.pdf. Accessed: 20 April 2021.
- [12] Wagner, P., Hansch, G., Konrad, C., John, K.H., Bauer, J. and Franke, J. 2020. Applicability of Security Standards for Operational Technology by SMEs and Large Enterprises. 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), IEEE, Vol. 1 (September 2020), pp. 1544–1551.
- [13] Al-sofi, T.A.B., Al-Shaibany, N.A., Al-Khulaidi, A.A. and Almekhlafi, Y.M. 2021. Analysis of Information Security Management Systems Frameworks in Organizations. International Research Journal of Modernization in Engineering Technology and Science, Vol. 03, Issue 02 (February 2021), e-ISSN: 2582-5208.
- [14] techconsult 2017. IT-Sicherheit – 5 Schritte für den Mittelstand/ IT Security—5 Steps for Medium-Sized Companies, [online], retrieved from <https://docplayer.org/79934925-Studienbericht-zur-security-bilanz-deutschland-2017.html>. Accessed: 13 February 2021.
- [15] Hillebrand, A. Niederprüm, A., Schäfer, S., Thiele S. and Henseler-Unger I. 2017. Aktuelle Lage der IT-Sicherheit in KMU/ Current Situation of IT Security in SMEs. Report. Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (WIK), Bad Honnef, Germany (December 2017), retrieved from https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/PDF-Anlagen/Studien/aktuelle-lage-der-it-sicherheit-in-kmu-langfassung.pdf?__blob=publicationFile&v=3. Accessed: 17 May 2021.
- [16] Gartner, Inc. and its affiliates 2021. Top Priorities for IT: Leadership Vision for 2021, CM_GTS_11134162020.

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 11, Issue 12, December 2021)

- [17] Valdevit, T., Mayer N. and Barafort, B. 2009. Tailoring ISO/IEC 27001 for SMEs: A guide to implement an information security management system in small settings. European Conference on Software Process Improvement, Springer, Berlin/Heidelberg (September 2009), pp. 201–212.
- [18] Antunes, M., Maximiano, M., Gomes R. and Pinto, D. 2021. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, 1(2), 2021, 219–238.
- [19] Doucek, P., Nedomova, L., Luc L. and Novak L. 2020. Information Security: The Glory and Penury of SMEs in the Czech and Slovak Republics. *International Conference on Engineering Management of Communication and Technology (EMCTECH)*, IEEE (October 2020), pp. 1–7.
- [20] European Union Agency for Cybersecurity (ENISA) and the National Cyber Security Alliance (NCSA) (ed.), 2020. Stay Secure Online—2020, Transatlantic Cybersecurity Checklist for Small Businesses, retrieved from <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/smes-cybersecurity/transatlantic-cybersecurity-checklist>. Accessed: 25 April 2021
- [21] 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, see: <https://www.iso.org/standard/73906.html>. Accessed: 14 May 2020.
- [22] Bundesamt für Sicherheit in der Informationstechnik (BSI)/ Federal Office for Information Security (ed.) 2017. IT-Grundschutz Arbeitshandbuch/ IT Grundschutz Work Manual: DIN ISO/IEC 27001 und DIN ISO/IEC 27002, BSI-Standards 200-1/2/3, 2nd revised edition, 459 pages, Bundesanzeiger Verlag, Cologne (October 2017).
- [23] Bundesamt für Sicherheit in der Informationstechnik (BSI)/ Federal Office for Information Security (ed.) 2017. BSI Standard 200-1 Information Security Management Systems (ISMS), (October 2017, in English), retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2001_en_pdf.html. Accessed: 20 June 2020.
- [24] Bundesamt für Sicherheit in der Informationstechnik (BSI)/ Federal Office for Information Security (ed.) 2017. BSI Standard 200-2 IT-Grundschutz Methodology, (October 2017, in English), retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html. Accessed: 29 June 2020.
- [25] Bundesamt für Sicherheit in der Informationstechnik (BSI)/ Federal Office for Information Security (ed.) 2017. BSI Standard 200-3 Risk Analysis Based on IT-Grundschutz, (October 2017, in English), retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf?__blob=publicationFile&v=2. Accessed: 2 July 2020.
- [26] Bundesamt für Sicherheit in der Informationstechnik (BSI)/ Federal Office for Information Security (ed.) 2021. IT-Grundschutz-Kompodium/ IT Grundschutz Compendium. Reguvis Fachmedien GmbH, Cologne, BSI, Bonn, Germany, retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium/IT_Grundschutz_Kompodium_Edition2021.pdf?__blob=publicationFile&v=6. Accessed: 17 May 2021.
- [27] Bundesamt für Sicherheit in der Informationstechnik (BSI)/ Federal Office for Information Security (ed.) 2009. BSI Standard 100-4 Business Continuity Management, retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2. Accessed: 14 May 2020.
- [28] Bundesamt für Sicherheit in der Informationstechnik (BSI)/ Federal Office for Information Security (ed.), BSI Standard 200-4 Business Continuity Management, Community Draft, January 2021, retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI-Standards/standard_200_4_CD.pdf?__blob=publicationFile&v=3. Accessed: 24 May 2021.
- [29] Thiel C. and Thiel C. 2010. Business Continuity Management für KMU/"Business Continuity Management for SMEs. *Datenschutz und Datensicherheit-DuD*, 34(6), 2010, pp. 404–407.
- [30] Nasiren, M.A., Abdullah M.N. and Asmoni M. 2016. Critical Success Factors on the BCM Implementation in SMEs. *Journal of Advanced Research in Business and Management Studies*, 3(1), 2016, 105–122.
- [31] [a] Schonschek O. 2021. Der Mensch ist das Angriffsziel Nummer 1/ Human is the number 1 target (pp. 3-5), Security Awareness als Teil des Risikomanagements/ Security Awareness as Part of Risk Management (pp. 6-8), CBT: Wie sich Mitarbeiter sensibilisieren lassen Wie es zu einer Evolution der Cyberangriffe kommt/ CBT: How to Raise Employee Awareness How Cyber Attacks Evolve (pp. 9–11);
[b] Kipke C. 2021. Moderne Sicherheitskultur gegen Hacker-Angriffe/ Modern security culture against hacker attacks. KnowBe4 DACH (pp. 12–13). In e-book Cyberattacken der nächsten Generation/ Next generation cyber attacks. Security Insider, Vogel IT-Medien GmbH (March 2021), pp. 3–13, retrieved from <https://www.security-insider.de/security-awareness-d-42985/>. Accessed: 27 April 2021.
- [32] Verband der Internetwirtschaft e.V. (eco)/ German Insurance Association 2020. IT-Sicherheitsstudie 2020/ IT security study 2020, Cologne, Germany, retrieved from <https://www.eco.de/presse/eco-it-sicherheitsstudie-2020-unternehmen-ruesten-sich-fuer-den-ernstfall/>. Accessed: 17 May 2021.
- [33] Bundesamt für Sicherheit in der Informationstechnik (BSI)/ Federal Office for Information Security (ed.) 2018. Die Lage der IT-Sicherheit in Deutschland 2018, Bonn, Germany, retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=5. Accessed: 17 May 2021.
- [34] Wang, Z., Zhu H. and Sun, L. 2021. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE*, Access, 9, 2021, pp. 11895–11910.

International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (E-ISSN 2250-2459, Scopus Indexed, ISO 9001:2008 Certified Journal, Volume 11, Issue 12, December 2021)

- [35] Bundesministerium für Wirtschaft und Energie (BMWi)/ Federal Ministry of Economics Affairs and Energy (ed.) 2019. Schlaglichter der Wirtschaftspolitik/ Economic policy highlights (March/April 2019), retrieved from https://www.bmwi.de/Redaktion/DE/Publikationen/Schlaglichter-der-Wirtschaftspolitik/schlaglichter-der-wirtschaftspolitik-04-2019.pdf?__blob=publicationFile&v=11. Accessed: 28 May 2021.
- [36] Bitkom (ed.) 2018. Weiterbildung für die digitale Arbeitswelt, Eine repräsentative Untersuchung von Bitkom Research im Auftrag des VdTÜV e. V. und des Bitkom e. V./ Further training for the digital world of work, a representative study by Bitkom Research, Berlin, Germany, 2018, retrieved from https://www.bitkom.org/sites/default/files/2018-12/20181221_VdTU%CC%88V_Bitkom_Weiterbildung_Studienbericht.pdf. Accessed: 17 May 2021.
- [37] Li, Y., Zhang N. and Siponen M. 2019. Keeping secure to the end: a long-term perspective to understand employees' consequence-delayed information security violation. *Behaviour & Information Technology*, Vol. 38 (5), 2019, pp. 435–453.
- [38] Bundesamt für Sicherheit in der Informationstechnik (BSI)/ Federal Office for Information Security (ed.) 2019. BSI-Veröffentlichungen zur Cyber-Sicherheit: Industrial Control System Security, Top 10 Bedrohungen und Gegenmaßnahmen 2019/ Top 10 threats and countermeasures 2019 (Version 1.30, 2019), retrieved from https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=1. Accessed: 17 May 2021.
- [39] KnowBe4 (ed.) undated. Der Mitarbeiter als "letzte Verteidigungslinie" / The employee as the "last line of defense". Whitepaper, retrieved from <https://www.knowbe4.de/>. Accessed: 28 April 2021.
- [40] Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, A. and Passingham M. 2016. Awareness Is Only the First Step: A Framework for Progressive Engagement of Staff in Cyber Security, Hewlett Packard, Business white paper.
- [41] Helisch, H. and Pokoyski, D. 2009. Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung/Security Awareness—New ways to successfully raise employee awareness, Springer Vieweg, Wiesbaden, Germany.
- [42] [a] Pokoyski, D., Matas, I., Haucke, A. and M. Scholl 2021. Qualitative Wirkungsanalyse Security Awareness in KMU. Tiefenpsychologische Grundlagenstudie im Projekt Awareness Labor KMU (ALARM) Informationssicherheit/ Qualitative impact analysis of security awareness in SMEs. In-depth psychological basic study in the Awareness Labor SME (ALARM) information security project (August 2021 in German), ISBN 978-3-949639-00-5.
- [b] Scholl, M. 2021. Foreword with an Introduction to and Summary of the Study "Added Value for SMEs" (Translation). DOI: 10.13140/RG.2.2.21236.88961, 2021.
- [43] Schmidt, H., Gondolf J. and Haufs-Brusberg, P. 2018. Studie zur Information Security Awareness in kleinen und mittleren Unternehmen (KMU)/ Study on Information Security Awareness in SMEs, Hochschule Düsseldorf, Medien, Düsseldorf, Germany. DOI: <https://doi.org/10.20385/2625-3690/2018.1>
- [44] Forrester Consulting 2020. The 2020 State of Security Operations. Thought Leadership Paper Commissioned by Palo Alto Networks.
- [45] Gittermann, A. undated. Wie erstelle ich ein Tätigkeitsprofil / How do I create a job profile, undated, retrieved from <https://engagiert-mitgestalten.de/de/materialien/fuer-koordinatorinnen>. Accessed: 17 May 2021.
- [46] StepStone, <https://www.stepstone.de/>. Accessed: 5 January 2021.
- [47] Indeed, <https://de.indeed.com>. Accessed: 5 January 2021.
- [48] Monster Worldwide Deutschland, <https://www.monster.de/>. Accessed: 5 January 2021.
- [49] GS Property Service Germany, retrieved from <https://p-sg.de/hausmeister-aufgaben/>. Accessed: 5 January 2021.
- [50] Staufenberg Institut GmbH, retrieved from <https://www.staufenberg.de/magazin/jobsuche/was-muss-ich-als-personaler-mitbringen.html>. Accessed: 5 January 2021.
- [51] IVB Neue Medien GmbH, retrieved from <https://www.steuerklassen.com/stellenbeschreibung/sekretaer/>. Accessed: 5 January 2021.
- [52] Alharthi D. and Regan, A. 2021. Social engineering InfoSec Policies (SE-IPs). In *Proceedings of 14th International Conference on Network Security & Applications (CNSA 2021)*, David C. Wyld et al. (eds): AIAP, SIGML, CNSA, NIAI – 2021, CS & IT - CSCP 2021 (January 2021), pp. 57–74.
- [53] Aldawood H. and Skinner, G. 2019. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, 11(3), 2019, pp. 1–16.
- [54] Chowdhury N. and Gkioulos, V. 2021. Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, 40, 100361, 2021, pp 1–20.
- [55] Sánchez, L.E., Santos-Olmo, A., Fernandez-Medina, E. and Piattini, M. 2013. ISMS Building for SMEs through the Reuse of Knowledge. *Small and Medium Enterprises: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2013, pp. 394–419.
- [56] Larsen-Freeman, D., Driver, P., Gao, X. and Mercer, S. 2021. Learner Agency: Maximizing Learner Potential [PDF], retrieved from www.oup.com/elt/expert/. Accessed: 25 April 2021.
- [57] Abbasi, A., Dobolyi, D., Vance A. and Zahedi, F.M. 2021. The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites. *Information Systems Research* (32:2), pp. 410–436
- [58] Burns, A.J., Johnson M.E. and Caputo D. 2019. Spear Phishing in a Barrel: Insights from a Targeted Phishing Campaign. *Journal of Organizational Computing and Electronic Commerce* (29:1), pp. 24–39.
- [59] Jensen, M.L., Dinger, M., Wright, R.T. and Thatcher, J.B. 2017. Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems* (34:2), pp. 597–626.
- [60] Nguyen, C., Jensen, M.L., Durcikova, A. and Wright, R.T. 2021. A Comparison of Features in a Crowdsourced Phishing Warning System. *Information Systems Journal* (31:3), pp. 473–513.
- [61] Schuetz, S., Lowry, P., Pienta D. and Thatcher, J. 2020. The Effectiveness of Abstract Versus Concrete Fear Appeals in Information Security. *Journal of Management Information Systems* 37(3), 723–757.