Sustainable Information Security Sensitization in SMEs: Designing Measures with Long-Term Effect

Margit Scholl
Technische Hochschule Wildau
margit.scholl@th-wildau.de

Abstract

This paper outlines an overall scenario for ongoing personnel development measures designed to increase information security awareness in small and medium-sized enterprises (SMEs) in Germany and to help small businesses improve their security levels and defenses. The three-year project combines different actors and a multitude of methods, with a focus on conducting interviews and online surveys with companies, developing customized game-based awareness trainings, tests, and on-site attacks, and creating measurements and evaluations as well as maturity statements, guidelines, and low-threshold security concepts. A mix of analog/digital serious games and operational trainings with reviews is of key importance here. Compared with the findings from the applied scientific literature on behavioral research and design, the ultimate goal at project's end is to extrapolate statements on the success and efficacy of the measures and their long-term effect.

Keywords: Awareness raising in SMEs, security trainings, narrative design, user experience, measurements.

1. Introduction

The 11th Allianz Risk Barometer 2022 shows cyber perils, business interruption, and natural disasters as the current top three business risks globally (AGCS, 2022a). German companies fear an interruption of their business (1st place, with 55% of the relevant responses) even more than a cyberattack (2nd place, with 50%) (AGCS, 2022b). Survey respondents (57%) see the increase in ransomware attacks as the top cyber threat over the coming year, with worrying trends such as "dual blackmail tactics" (AGCS, 2022b). Cyber or information security (ISec) is also gaining importance in the area of ecological and social corporate governance as a way to obviate increasing difficulties with regulatory authorities, investors, and other stakeholders (AGCS, 2022b). This confirms earlier assessments that the continuous implementation of information security awareness (ISA) measures not only reduces the business risk for companies but also increases their attractiveness (known_sense, 2016). The promise of awareness-raising measures being implemented and communicated to customers represents a competitive advantage because of the positive external effects generated and increased trust in the company (known_sense, 2016).

According to a recent study in Germany (DIHK, 2022), the cyberattacks of the past year have shown that any company can be targeted by hackers. Back in 2007, it was assumed that the various ISec measures of the previous years had had a positive influence on the corporate cultures of numerous German organizations and the security-related behavior of employees (Zerr, 2007), but the effects of these measures were not sustained. 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 ISec—including awareness raising and training for managers and employees—and only a third of the companies surveyed have an action plan for emergencies (DIHK, 2022). This contradiction shows a paradox at work in German companies, with an evident lack of sustained implementation of awareness-raising measures, especially in small and medium-sized enterprises (SMEs).

The research question of this paper is, How can on-the-job trainings and further educational measures for people in SMEs be designed and implemented in order to establish long-term awareness and training as part of a company security culture? This paper emphasizes a holistic approach, which is important in developing the necessary competences and actively involving people in specific ISec situations. The overall scenario of an ongoing project to increase ISA in German SMEs is outlined, including the development and testing of analog/digital serious games and operational reviews. Section 2 summarizes the applied behavioral research findings, which are important in building up the overall project scenario. Section 3 explains the project, the choice of topics, and the methods used in the holistic approach. Preliminary project results are summarized in section 4, with a look ahead to the next phases of the project.

2. Applied research findings

URI: https://hdl.handle.net/10125/103369
978-0-9981331-6-4

ISA should be seen as part of security communication in companies and is a prerequisite for successful information security management (ISM) and the development of an operational Information Security Management System (ISMS) as well as a Business Continuity Management (BCM) system. The international standard ISO/IEC 27001 (ISO/IEC 27001:2017) defines specific requirements for an ISMS:

- continuous ISec improvements
- anchoring of ISec in day-to-day business
- tailoring of ISec to meet external requirements
- building of trust with business partners and the public.

ISO/IEC 27001 also explicitly requires the training of employees and defines the details of such training. Various aspects of education and training or ISA are described under the headings Resources, Competence, Awareness, and Communication. Legislatures, customers, and the public are also seen as drivers for ISA (ISO/IEC 27001:2017). The need for regular awareness-raising and training measures is therefore clear in theory but is either not implemented in practice in SMEs or, where implementation approaches exist, does not lead to the desired sustainability. A number of studies conclude that most ISec training measures and the many operational guidelines, as well as threats of sanctions and phishing simulations, have no apparent long-term effect (Bada et al., 2016; ENISA, 2019; ISF, 2014; Volkamer et al., 2020). The German IT-Grundschutz (baseline protection) of the Federal Office for Information Security (BSI) describes the ISec risk situation as per the ORP.3 module "Awareness and Training" (BSI, 2020):

- Insufficient knowledge of regulations
- Inadequate ISA
- Ineffective activities in training design
- Inadequate training of security functions
- Undetected security incidents
- Non-observance of safety measures
- Carelessness in handling information
- Lack of acceptance of ISec requirements
- Social engineering

Back in 2009, David Lacey wrote, "You can blame individuals for making mistakes. But many will be due either to a failure by management to provide adequate resources, training and oversight, or to a flaw in the design of systems and processes" (Lacey, 2009, p. 52). Risk management or risk perception is of particular importance in SMEs. "But it takes time to coach managers to identify, assess and manage risks. Complex frameworks are off-putting. It's better to start simple and progressively increase the level of sophistication" (Lacey, 2009, p. 132).

2.1 Information Security Awareness

ISA means conscious perception and is not even three decades old as a research field, making it a young discipline that requires interdisciplinary input: different perspectives, methods, content, and other components of awareness are emerging as the risks facing ISec and its response requirements grow. There are numerous definitions of ISA, some of which have very different nuances. In psychology, ISA is related to a person's current situational awareness of their environment and the resulting implications for action. Achieving sustainable ISA is a recurring challenge, since ISec includes a wide range of mostly abstract and complex topics. As humans, we are social beings and cannot see, taste, smell, or touch the bits and bytes. In addition, the core focus of the SMEs is usually on something else, and the stress of everyday work can push ISec into the background.

The international literature on the subject often explains this in terms of the KAB model (Kruger & Kearney, 2006): Knowledge, Attitude, Behavior. This model has been adopted and modified by many researchers. The core thesis is that ISA emerges from what employees or users know about ISec, its vulnerabilities and risks, what they think or what they think about it and how they actually behave in this context. A large spectrum of theories has been consulted in this research field to obtain knowledge about the real security behavior and influencing factors. The theories most applied to explain ISec behavior are the Theory of Planned Behavior, General Deterrence Theory, Compliance Theory, Protection Motivation Theory, the Technology Acceptance Model and the Theory of Reasoned Action, Social Bond Theory, and Involvement Theory (Scholl et al., 2018). Furthermore, people often ignore or underestimate the extent to which their actions in a situation are determined by the actions of others, and they often ignore or underestimate the persuasive effect that social norms can have on their choices (Cialdini, 2007), which is why role models are important. In addition, the key message that changing the behavior of employees cannot be achieved simply by imparting knowledge but must be accompanied by further measures has not yet got through to management, CISOs, and other C-level executives (Sasse et al., 2022). The study by Slusky & Partow-Navid (2012) revealed that the major problem with ISA is not a lack of security knowledge but the way that knowledge is applied in real-world situations. According to Cialdini (2007), those involved should be honestly informed about the damage caused by even a modicum of undesirable behavior.

In German-speaking countries, the following model has been established in operational ISA (Helisch & Pokoyski, 2009): Knowledge, Volition, Capacity. This

means that the key elements in security awareness intersect with operational training management and human resource development, with general security communication, and with change management, defining security awareness's three methodological levels. This has the following implications for awareness-raising measures (Helisch & Pokoyski, 2009; Pokoyski et al., 2021):

- Knowledge, "being informed" (elements drawn from learning theory, cognitive factors) as Layer 1—classical information processing is the (old-school) basis of security awareness. This involves the imparting of knowledge pertaining to security rules, guidelines (policies), security risks, and the possible consequences of security breaches.
- Volition, "being willing" (elements drawn from marketing, emotional factors) as Layer 2—merely communicating information is not enough to have a sustained and, more importantly, motivating effect on the processes of awareness: for this reason, emotional factors must also be addressed for all target groups.
- Capacity, "being able" (elements of change management and systemic communication) as Layer 3—security culture is invariably influenced by interactions with staff as well as with customers and partners. Security thus also involves systemic factors, the interactions within an organization (and its external relationships) viewed in the context of its corporate culture. Specific elements of systemic communication are "empowerment" and dialogue-based constellations (e.g., team formats).

2.2 Information Security Culture

For Lacey (2009), establishing an understanding of security culture in organizations is a must for security professionals. But it is not static or easily definable (Lacey, 2009, p. 208). Security culture can be fear based or inspirational. But trust and empowerment are more effective and go much further (Lacey, 2009, p. 208). When designing an organizational structure, it is important to understand that both the requirements and the solutions can vary greatly both between and within companies (Lacey, 2009, p. 208).

ISA is an aspect of both security marketing and security communication for the "Security Awareness Framework" of the firm known_sense (2016), and these areas, in turn, are ancillary to the concept of security culture. This implies that security culture can be viewed as all the beliefs and values cherished by individuals and organizations where there is agreement about the kind of events that pose risks, and how these risks should be countered (known_sense, 2016). Security culture is underpinned by a complex process of learning and experience, in which common goals, interests, norms, values, and behavioral patterns are established: it can thus be regarded as a part of the corporate culture, which is a visible manifestation of employees' habitual approaches to dealing with security challenges. It also delineates how security is organized in the workplace and thus reflects employees' security-related attitudes, beliefs, perceptions, and values (known_sense, 2016). The term "security culture" refers to a dynamic phenomenon that is transformed by every significant event that takes place in the organization (known_sense, 2016). This process of evolution should be considered when security awareness measures are being implemented. The above definition suggests that ISA is part of the security culture and has a significant effect on it.

This already makes it clear that there is no simple definition for the term "security culture" either. On the contrary: a survey of 1,200 security experts by Forrester Consulting on behalf of KnowBe4 enterprise in December 2019 produced 749 unique definitions (Collard, 2022), which can be summarized in five categories: Compliance with security policies (29%); Awareness and understanding of security issues (24%); Security as everyone's responsibility (22%); Security advocacy and support (14%); Security embedded in the organization (11%). In terms of content, the following seven dimensions are important for operational safety culture (Collard, 2022): Attitudes, Behaviors, Cognitive Factors, Communication, Compliance, (Social) Norms, and Responsibilities. Here, the following three attitudes to safety culture need to be considered in designing awareness and training measures (Collard, 2022):

- Just because I'm aware, it doesn't mean I care.
- If you try to work against human nature, you'll fail.
- What people do is way more important than what they know.

2.3 Information Security Awareness Training

According to Collard (2022), information security awareness training (ISAT) is about finding effective behavioral measures to close possible gaps between awareness as knowledge, existing intentions, and concrete behavior. Hallsworth et al. (2016) apply a modern understanding of human behavior to healthcare to show that in practice this can lead to better health outcomes at lower costs and that improvements are contingent on such an understanding. The authors transferred the Easy, Attractive, Social, and Timely (EAST) framework of the Behavioral Insights Team from 2014 to their focus of investigation: healthcare (Hallsworth et al., 2016):

- Easy means minimizing the effort for those involved. Barriers—even minor ones—should be reduced to make "good" behavior more likely.
- Attractive means capturing people's limited attention through visual or spatial design with new features and simple and clear messages.
- Social means that people as social beings are strongly influenced by what others do ("social norms") (see also Cialdini, 2007). Making good behavior more visible can make it appear more common and easier to copy.
- Timely means recognizing the moments of effective intervention and then implementing measures in good time. The effect of behavioral interventions should be evaluated.

For our own scenarios described in section 3 it becomes obvious that the EAST framework can and should also be applied to ISec. This is where B. J. Fogg's (n.d.) "Behavior Design" comes into play. He wants to help people to be successful and calls for barriers to be broken down so that people can behave accordingly. "The Fogg model of behavior shows that three elements must converge simultaneously for a behavior to occur: motivation, ability, and a prompt. If a behavior does not occur, at least one of these three elements is missing" (Fogg, n.d.). His behavioral model highlights three main motivators, Sensation, Anticipation, and Belonging, each of which has two sides: Pleasure/Pain, Hope/Fear, Acceptance/Rejection (Fogg, n.d.). These core motivators apply to everyone and are central to human experience—hence his advice (Fogg, n.d.): Focus on small steps to promote long-term change. His model also shows that ability and motivation have a "compensatory relationship" when it comes to performing behaviors (Fogg, n.d.). According to Fogg, there are three ways to increase skills: the worst way is to train people. Another possibility is to give the human a tool or resource that facilitates his behavior. Fogg advocates the third way: scaling back the intended target behavior so that it is easier for people to achieve, with debriefings showing a positive learning effect (Lacruz & Américo, 2018). In terms of behavior design, this means focusing on the simplicity of the target behavior, thereby enhancing personal capability. As a consequence, if the conception and design of awareness-raising and training measures are to increase ISec, one must first be clear about the desired behavioral chains that are ultimately to be achieved with the measures.

The design of these measures must pay close attention to the methods of communication, especially when efficacy and long-term effects are required. As comprehensive digitization has been carried out over the years, digital teaching methods have become increasingly important, and their effect should be assessed in comparison to analog ISec training methods. Sixteen years ago, Burke et al. (2006) attempted to determine the relative effectiveness of different methods of occupational safety and health training aimed at improving safety knowledge and performance and reducing adverse outcomes such as accidents, illness, and injuries. The most engaging training methods involve active employee participation and, as a result, lead to greater knowledge acquisition and reduced accidents, illness, and injury (Burke et al., 2006). These training methods include *practical exercises* and *dialogue*. They are more effective than other safety and health training methods. It was concluded at the time that these results challenge the emphasis on more passive computer-based and remote training methods for public health personnel (Burke et al., 2006).

In order to develop an appropriate training concept in line with international and national standards such as the ISO/IEC family of standards 2700X (ISO/IEC 27000:2018(E)), or the BSI standards 200-1 to 200-4 (BSI, 2017), the risk and threat situation must be made clear, the target groups determined, and training content specified. Furthermore, in order to determine their efficacy, the measures must also be carried out, their success defined, and their effectiveness checked. In terms of continuous improvement, the existing ISA must also be regularly adapted to current circumstances and increasing risks. Section 3 outlines the relevant steps and makes it clear that great care should be taken over the methods, design, and wording used in the measures as per the literature summarized here in section 2.

3. The project and its overall scenario

The project "Awareness Lab SME (ALARM) Information Security" is funded by the German Federal Ministry for Economic Affairs and Climate Action (BMWK) and runs from October 1, 2020, to September 30, 2023. The project is part of a group of support initiatives. SMEs benefit from a focus on concrete practical examples as well as competence and IT security programs that are provider-neutral and tailored to the SME's particular needs. The BMWK allows the final project results to be used free of charge.

A university research team and subcontractors of the project as well as SMEs and associated partners are developing and testing ISA tools with the aim of promoting the nationwide improvement of security awareness in German SMEs and thus a general increase in ISA. To this end, an innovative process scenario for ISec is being developed iteratively in three phases using an agile, participatory approach—this involves experience-oriented scenarios, both analog and digital, as well as

"on-site attacks" and further checks. The overall scenario is intended to raise awareness among managers and employees with a focus on targeted personnel development in SMEs, which is not available as yet on this scale. Here, ISec is made concrete and tangible in the context of work processes that have become increasingly digital. At the same time, people are actively involved at an emotional level in the development of measures. This should result in a company-wide ISec culture being established with long-term effect.

3.1 Methodology for defining the ISec topics that are currently important in SMEs

The first step was to define the ISec topics that are important for the target groups (employees of the four pilot SMEs). A preliminary study (Pokoyski et al., 2021)—conducted by one of the project subcontractors and based on anonymized in-depth interviews—was carried out between January and March 2021. A summary of the results was produced (in German) in April/May 2021. The BMWK approved their publication in August 2021.

Fifteen two-hour face-to-face interviews were initially planned, and the constraints imposed by the pandemic meant that these were all carried out online (Pokoyski et al., 2021). The study sample included a total of sixteen people from the pilot SMEs who were surveyed in 90-minute online interviews by a three-person team of project subcontractors. Most of the interviews were carried out from home offices. The interviews were conducted in secure WebEx rooms set up by the University as project leader, although in four instances the interviewees were at their place of work. Four of them had management roles, nine were management and executive assistants (including 3 IT specialists), two were staff without managerial function or staff responsibility, and one was a trainee. One participant was aged between 18 and 25, six were between 26 and 35, four were between 36 and 45, three were between 46 and 55, and two were over 56. The methodology uses morphological market and media research, supplemented by secondary research, including comparative descriptions and key performance indicators (KPI) (Pokoyski et al., 2021). It takes into account internal security awareness campaign evaluations carried out by the subcontractor between 2009 and 2020, focused on six large German companies operating in different industries (Pokoyski et al., 2021).

Parallel to the study, an online survey was started by the university research team that dealt specifically with the fields of activity in the four SMEs: the results are published in German as the first of a total of three planned reports (von Tippelskirch et al., 2022).

3.2 Summary and discussion of the findings from the interviews and survey

The results of the initial online questionnaire (Report 1, 2022) indicate that ISec is not currently viewed holistically in SMEs. From the in-depth interviews (Pokoyski et al., 2021) it was found that the issue of ISec is directly related to the unique quality of SMEs, which confidently present themselves in a dynamic zone involving family-style, trust-based cooperation, and flexibility in response to the needs of the market. It is clear from all the interviews that the participants identify strongly with their company and feel close ties with it. The managing directors and other executives emphasize the sense of belonging and loyalty felt by their employees and the high degree of confidence they have in them. An understanding of each other's difficulties and foibles is evident, and the picture that is painted is of relaxed, generally harmonious cooperation. The size of the companies also facilitates direct contact with staff. A feature of SMEs is their high degree of flexibility, the possibility of finding individual solutions, and the ability to respond quickly to the needs of the market. This agility has showed its value during the pandemic, when working in a home office has not only been sanctioned but actively supported by the prompt provision of equipment (laptops, headsets, cameras, etc.) (Pokoyski et al., 2021).

The interviews confirm that trainings and other awareness-raising measures are being implemented in all the pilot SMEs taking part. However, without support, the issue of ISec is soon conflated with "data protection," and when a holistic view is taken of security, it is linked with "compliance," "occupational safety," and "fire protection" (Pokoyski et al., 2021). When applied to data protection, the idea of "awareness raising" is key, covering the sensitive data that, according to the interviewees, needs to be secured: personal data and sensitive topics, including salary, contracts and contract details, and company secrets. The SMEs taking part in the study have as yet made little use of holistic security awareness concepts, of the kind envisaged in the project, or an awareness framework with a documented strategy. The same is true of ISA measurements and other evaluations related to the raising of employee awareness. There is a general lack of any systematic process of awareness raising, which would help develop a functioning security culture. The results of the study on ISec topics for SMEs, weighted according to supposed relevance and importance, produced the following ranking (Pokoyski et al., 2021):

1. Passwords
2. Phishing, CEO Fraud, etc.
3. Social engineering, Manipulation, etc.
4. Apps, software, etc.

5. Security in the home office
6. Data protection in the cloud and in the context of customers and suppliers
7. Messenger services, secure transmission, storage, encryption, etc.
8. Information classification (only for SMEs where it is an implemented process).

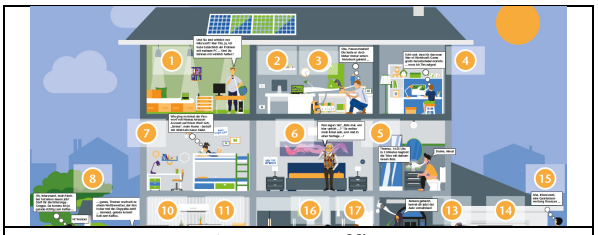
The topics “Mobile security” and “Safety on the go” were accorded low priority, which can be attributed to the COVID-19 situation (Pokoyski et al., 2021).

Corroborating the psychology-based Study 1 (Pokoyski et al., 2021) that was conducted, the online questionnaire carried out for report 1 (von Tippelskirch et al., 2022) also revealed that the respondents view many ISec topics as “old” and in such general terms that it is hard to limit them to just one activity profile. As a result, the profiles defined in this report are lumped together into the following profile groups (von Tippelskirch et al., 2022): general basic competences; production, development, sales; data processing and IT infrastructure; maintenance and communication; organizational and PA work, administration and HR; strategic planning and management.

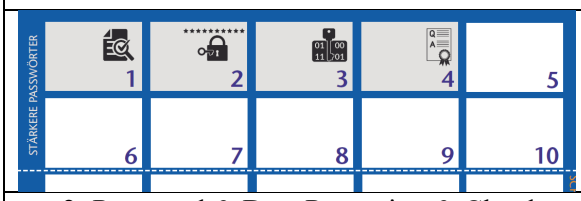
ISATs should be specific to an activity profile and its specific tasks. According to the results of both the study and the report, this requires a higher level of ISec maturity on the part of the SMEs. Suitable training material is required if ISATs are to be organized efficiently in everyday work life. In addition, a tightly woven ISec network in the form of an optimally established “human firewall” involves people switching roles for training purposes and discussing and internalizing the lessons so learned (von Tippelskirch et al., 2022). The approach chosen in the project is to develop awareness-raising measures as easily adaptable learning scenarios that can ultimately be used and specified by the SMEs themselves. In the project, the results of the initial Study 1 and the outcomes of Report 1 are the basis for developing new awareness-raising material tailored to the concerns of the SME in question and employees’ personal engagement with the issues. 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.

3.3 Gamification and embedded narratives

There are various methods for promoting ISA that can be used to create and model awareness: their content, implementation, and success depend, among other things, on the business model, the corporate and security culture, and the ISec maturity. From section 2 of this paper it is important to point out that ISA is a multidisci-



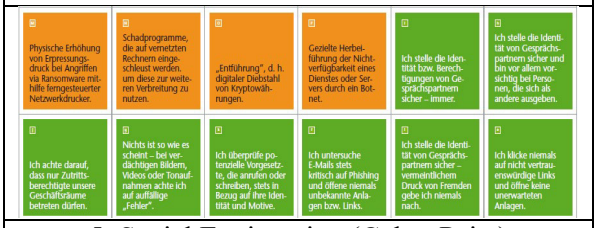
1: Home Office



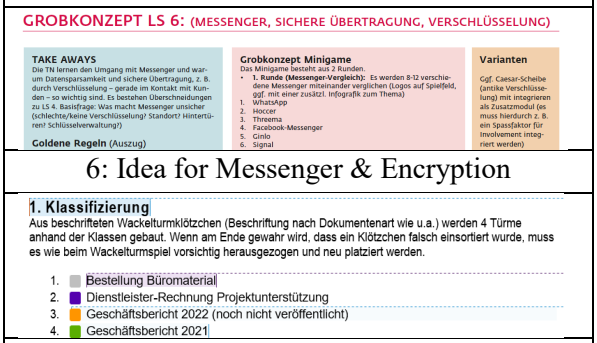
2: Password & Data Protection & Cloud

3: CEO Fraud

4: Software & Apps



5: Social Engineering (Cyber Pairs)



6: Idea for Messenger & Encryption

7: Idea for Information Classification

Figure 1. Analog learning scenarios (aLS) under development as part of the project for SMEs (pre-final for aLS 1–5, and initial ideas for aLS 6–7)

plinary area involving cognitive, emotional, and systemic factors.

Although gamification or serious games as learning support are not new, in recent years they have gained in popularity in ISec research. However, we know from the Study 1 that German SMEs still have reservations: playing should not be the main focus. Other studies also illustrate that there is a danger that the commonly used motivational goal of winning the game causes learning experiences designed to promote understanding and the ability to cope with challenges (e.g., emergency responses) to fall by the wayside (Lacruz & Américo, 2018). These results from Lacruz & Américo (2018) make it clear that debriefings positively influence the experiential learning cycle. In addition, Schell (2020) emphasizes that the success of a game depends to a large extent on the player's willingness to regard it as meaningful. Naul & Liu (2020) recommend using narratives that stimulate the imagination and include characters with whom learners can empathize. In principle, the primary purposes of "serious" games can be diverse and used in many areas, such as education, healthcare, advertising, and politics, for teaching or training (Arriaga et al., 2013). The handbook (Bernardes et al., 2022) contains recent research showing the broad spectrum of gamification for economic and social development.

3.3.1 Analog learning scenarios. For ISec, we need moderation tools for discursive team settings, intensive training specific to the target group with simulations and other discursive, gamified, or interactive elements to involve people emotionally, motivate them, and make ISec "understandable." These instruments must contain didactic and emotional components from learning theory as well as marketing components.

We must be able to enter into an intensive exchange about ISec: talk about security! The analog learning scenarios are developed jointly by the subcontractor known_sense and the university research team (see fig. 1). They are designed as assignment games for the topics defined by the pilot SMEs in Study 1 (see above), so that a moderator can easily get into conversation with the participants, and the participants with each other, giving them a chance to contribute their experience. Analog assignment games—as per the "Home Office" scenario (fig. 1), for example, which is played on a board representing a large family house—involve information cards being read out loud by the participants, after which they are discussed and assigned to a suitable part of the family house. Here, players start with risk cards, which are used to identify the critical spots in the house. After that, possible improvements are focused on with the defense cards.

The tests to be carried out with attending participants in three iterations per game are used both to simplify the complexity of the topics while maintaining the attractiveness of the game and to optimize the emotional game design. The response has been very positive so far not only from tests with the pilot companies but also at public events. Improving the detailed preparation of the feedback is an ongoing process in the project. The final versions will be made available in German for download, free of charge, from the project website.

3.3.2 Digital learning scenarios. Parallel to the seven analog serious games, the seven digital games are being developed together with another subcontractor, Gamebook Studio, who uses the popular *Visual Novel format* to integrate a player as an active participant in his/her own story in a *simple* manner. All decisions that the player has to make influence the further course of the game (see fig. 2).

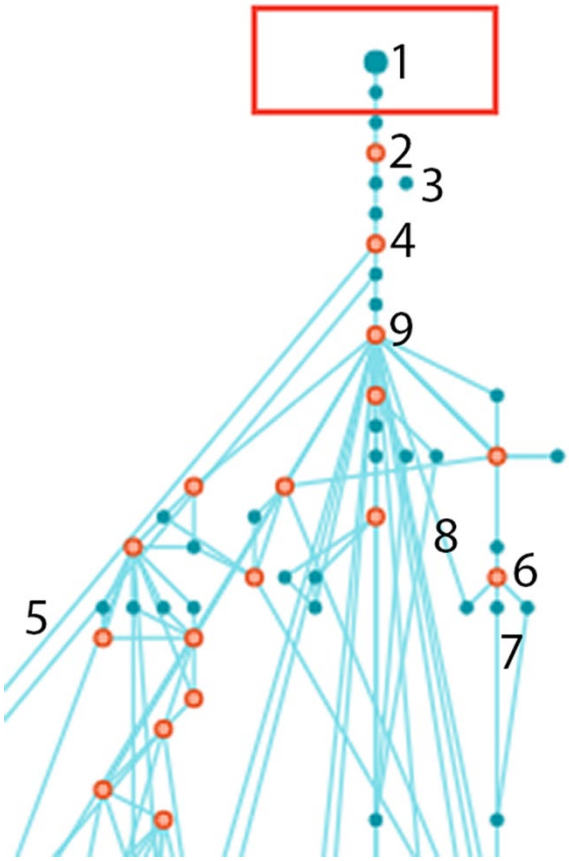


Figure 2. Digital learning scenarios under development: one decision tree in a preliminary version.

Fig. 2 shows an excerpt from the digital scenario "The Hacker Attack," in which the player runs through the game in the role of a social engineer: Number 1 indicates the start of the digital game, which is being developed using Gamebook Technology. Green nodes in the schedule are "story modules" that provide information to the player (text, instructions, feedback, music,

etc.). Number 2 refers to a red node where the player has to make decisions, including whether they want to be addressed as a woman or a man, which is determined at the beginning. Number 3 shows a story module that is not connected by a line—the designer has already set out an alternative, but it is not integrated into the current game story. At decision point 4, the player can interrupt the game and look at the stored glossary (5) to get more input. Decision point 6 is a "time choice": the player has to decide between possibilities and then proceeds accordingly to number 7. Should the player need too much time, then the game will send her/him back (8). However, all the information the player has already accumulated is retained and will lead to other options for the next step at decision point 9. This explanation shows how important the designer's empathy with the topic and the target group is in building the story.

Figure 3. Examples of avatar emotions in the project's serious digital games (pre-final version).

The player of the digital serious games slips into a different role in each of the seven games and experiences the concrete company situation of the ISec topic from a different perspective—e.g., that of a forensic scientist, a hacker, a security officer, or the artificial intelligence of the game company.

The digital learning scenarios can therefore be played from very different perspectives, which provide deeper insight into the various topic areas as well as the risks and dangers peculiar to them. At the same time, the player becomes more familiar with the company's situation and employees: the boss, the dispatcher, the workshop manager, and the trainee. The avatars can show some emotions (see fig. 3) and sounds can also be heard; although the figures do not speak, the situation and decision options are presented with texts, so that the player has time to think about the question.

The digital games are thus not a copy of their analog counterpart. Rather, they have their own content on the topics selected for SMEs and thus represent interesting learning supplements that employees can complete independently, regardless of time and place. The variety of different perspectives also has two positive effects: On the one hand, it ensures that playing does not become boring and that the motivation to learn is sustained. On the other, it conveys the relevance of the various actors and their methods within ISec. The Visual Novel format with Gamebook Technology is therefore suitable as a simple but effective tool for conveying very different content in a separate, personalized learning experience. Every game decision not only has consequences for the further course of the personalized story but also differentiates the topic in more depth and thus offers different learning paths and levels of difficulty—depending on your previous knowledge, personal strengths and weaknesses, and learning preferences. This means that every type of learner and every level of knowledge is addressed with decisions, and the format is therefore suitable for use in a particularly broad target group.

However, successful learning is generally based on solid data collection and personalization of the learning experience adapted to this data. The digital learning scenarios thus use in-game messages providing feedback on participants' decisions—showing points as stars—without disturbing their immersion in the story. KPI-based live tracking to assess user behavior and a supplementary user survey for self-assessment of the level of knowledge on the subject before and after playing the learning scenario also help in the optimization process. The feedback so far has been positive. Detailed analysis of the feedback must be left to a separate research paper.

3.3.3 On-site attacks. In addition to the seven analog and digital learning scenarios, the project also includes seven on-site attacks for which another subcontractor is responsible. Ethical questions and the agreements with the managing directors of the SMEs also play a key role. Additional practice-oriented instructions and tips for low-threshold security concepts for SMEs should emerge from the relevant findings. These will also be available on the project website at its completion. The overall feedback from these gamified processes, which will not be complete until 2023, must also be left to a separate research paper.

So far, one phishing attack has been carried out in the project. Another three "on-site attacks" are planned for 2022, with three more to be coordinated in 2023.

Conducting on-site attacks is tricky and must be done with extreme caution. Some scientists have grave concerns about them (see Volkamer et al., 2020). However, the aim of our project is to enhance employee awareness: the procedure should thus not be perceived by employees as an "attack" on their personal work processes or lead to personal exposure. Every on-site attack must be designed in such a way that it does not have a negative impact on the working atmosphere and the culture of trust in the company. It is important to ensure that employees feel safe/secure in their work environment and see the on-site attacks as a supporting tool to raise awareness. The attacks are always discussed with the responsible persons in the company and all employees receive all the relevant information and results before and/or after the attacks, so that these attacks do not damage the company's culture of trust and error.

3.4 Security Awareness Measurements

Security is not so much a state as a process. All measures must be checked for their effectiveness in operational work, including security and awareness measures, because otherwise processes cannot be managed and improved. The "Return on Security Investment" (ROSI), for example, is not compatible with a holistic view of ISA. Different approaches are therefore required to verify the effectiveness of ISA measures.

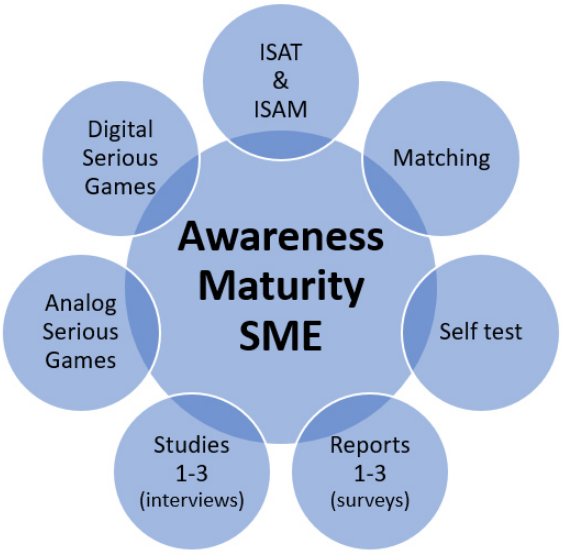


Figure 4. The overall scenario of ongoing personnel development to increase ISA in SMEs

Moreover, it is evident that ISA measurement (ISAM) is an interdisciplinary challenge and an open research question in scientific terms. We know that risk perception is an important indicator. But WHAT do we actually measure, and HOW? How can we infer consciousness from a person's understanding or attitude? How can we infer actual behavior from this? Do questionnaires and tests with knowledge surveys reflect reality? Probably not. We would need to observe people in their everyday lives, making them "transparent" in terms of their personal data, which is not desirable in an open, democratic society. While being fully aware of this problem, we still want to try to implement ISAM in the project in two different ways. The first approach uses the analog and digital learning scenarios with test and control groups, and pre- and post-tests. In the second approach, the mathematical partial order methodology is examined for a possible ranking; however, it is still not clear which indicators are actually suitable for this purpose. The ultimate goal of these efforts is a maturity model for awareness, incorporating all the elements, results, experiences, expectations, and knowledge (see fig. 4).

4. Limitations, current conclusions, summary, and outlook

The results of the interviews (Study 1: Pokoyski et al., 2021) and the survey (Report 1: von Tippelskirch et al., 2022) cannot be regarded as representative, because of the small size of the samples (four pilot SMEs). Nevertheless, they give a concrete and up-to-date insight into how ISec and ISA are faring in German SMEs. In the project, the results and the further participation of the SMEs form a valuable basis for personal examination of the ISec topics. Narratives with references to daily life and the working world seem to be suitable communication tools. Their design must actively involve people in dialogue about ISec, touch them emotionally, and include their own experiences. The added value of the project lies in the systematic and integrative interlocking of a wide variety of measures that contribute to systemically oriented awareness-raising and specifically to the development of a security culture.

The project deviates significantly from previous unsuccessful forms of classic ISA training. The final versions of the gamified training materials, the results of the awareness measurements, the instructions and low-threshold security concepts, and well-founded statements on the degree of maturity can only be expected at the end of the project in fall 2023.

5. Acknowledgements

As the initiator of "Awareness Lab SME (ALARM) Information Security" and project manager, I would like to thank the Federal Ministry for Economic Affairs and Climate Action for funding this project. I am grateful to our long-standing security awareness partner, the company known_sense, and the other subcontractors, Game-

book Studio, Thinking Objects, and sudile, whose special input into the project can be found on the project website https://alarm.wildau.biz/en. My special thanks to the pilot companies for their active involvement and to my research team—also featured on the project website—who have moved the project forward in different constellations. Finally, I would 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.

6. References

AGCS—Allianz Global Corporate & Specialty SE (Ed.) (2022a). *Allianz risk barometer 2022.* (English version: worldwide results).

AGCS—Allianz Global Corporate & Specialty SE (Ed.) (2022b). *Allianz Risk Barometer 2022* (German version: results of Germany)

Arriaga, P., Esteves, F., & Fernandes, S. (2013). Playing for better or for worse? Health and social outcomes with electronic gaming. In M. M. Cruz-Cunha, I. M. Miranda & P. Gonçalves (Eds.), *Handbook of research on ICTs for human-centered healthcare and social care services* (pp. 48–69). IGI Global.

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

Bernardes, O., Amorim, V., & Moreira, A. C. (2022) (Eds.). *Handbook of Research on Cross-Disciplinary Uses of Gamification in Organizations*. IGI Global.

Burke, M. J., Sarpy, S. A., Smith-Crowe, K., Chan-Serafin, S., Salvador, R. O., & Islam, G. (2006). Relative effectiveness of worker safety and health training methods. American journal of public health, 96(2), 315-324.

Cialdini, R. B. (2007). Descriptive social norms as underappreciated sources of social control. Psychometrika, 72(2), 263-268.

Collard, A. (2022). „Verhaltensdesign in Security Awareness Programmen, Webinar of KnowBe4, May 20, 2022)"/ "Behavioral Design in Security Awareness Programs".

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

ENISA—European Union Agency for Network and Information Security (2019). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*.

BSI —Federal Office for Information Security (Ed.) (2020). *BSI-Kompendium*, *Baustein ORP.3*.

BSI—Federal Office for Information Security (Ed.) (2017). *BSI-Standards*.

Fogg, B. J. (n.d.). *Fogg Behavior Model*. Retrieved May 26, 2022, from https://behaviormodel.org/

Hallsworth, M., Snijders, V., Burd, H., Prestt, J., Judah, G., Huf, S., & Halpern, D. (2016). Applying behavioral insights: simple ways to improve health outcomes. World Innovation Summit for Health, Doha, Qatar, 29–30 November.

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

ISF (2014). *From Promoting Awareness to Embedding Behaviors, Secure by choice not by chance*.

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

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.

known_sense (ed.) (2016). *Security Awareness Framework*. Cologne.

Kruger, H. A., & Kearney W. D. (2006). A prototype for assessing information security awareness, Computers & Security, Vol. 25, No. 4, pp. 289–296.

Lacey, D. (2009). *Managing the Human Factor in Information Security: How to win over staff and influence business managers*. John Wiley & Sons.

Lacruz, A. J., & Américo, B. L. (2018). Debriefing's Influence on Learning in Business Game: An Experimental Design. *BBR. Brazilian Business Review*, *15*, 192-208.

Naul, E., & Liu, M. (2020). Why Story Matters: A Review of Narrative in Serious Games. Journal of Educational Computing Research, Vol. 58, No. 3, pp. 687-707.

Pokoyski, D., Matas, I., Haucke, A., & Scholl, M. (2021). *Qualitative Wirkungsanalyse Security Awareness in KMU* (Projekt "ALARM Informationssicherheit") (p. 72). Wildau: Technische Hochschule Wildau.

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

Schell, J. (2020). *Die Kunst des Game Designs: bessere Games konzipieren und entwickeln*. BoD–Books on Demand. 2. Edition, 2016.

Scholl, M. C., Fuhrmann, F., & Scholl, L. R. (2018). Scientific knowledge of the human side of information security as a basis for sustainable trainings in organizational practices, Proceedings of the 51st Hawaii International Conference on System Sciences.

Slusky, L., & Partow-Navid, P. (2012). Students Information Security Practices and Awareness, Journal of Information Privacy and Security, Vol. 8, No. 4, 2012, pp. 3–26.

Volkamer, M., Sasse, M. A., & Boehm, F. (2020). Analysing Simulated Phishing Campaigns for Staff. *European Symposium on Research in Computer Security* (pp. 312-328). Cham: Springer.

von Tippelskirch, H., Schuktomow, R., Scholl, M., & Walch, M. C. (2022). *Report zur Informationssicherheit in KMU – Sicherheitsrelevante Tätigkeitsprofile (Report 1)* (p. 111). Wildau: TH Wildau.

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