

Résumé of the Gamified Increase in Security Awareness in German Small and Medium-Sized Businesses after Three Years' Practice of "ALARM Information Security"

Margit C. Scholl

**University of Applied Sciences Wildau (TH Wildau)
Wildau Institute for Innovative Teaching, Lifelong Learning, and Design Evaluation
(WILLE)**

The latest cybersecurity reports for 2023 again show a critical situation in IT security in Germany—in fact, the threat in cyberspace is higher than ever before. There can be no doubt that small and medium-sized enterprises (SMEs) need to build their cyber resilience around their staff. Humans are becoming the key to increasing information security. Within just three years and under the difficult conditions of the COVID-19 pandemic, the "Awareness Lab SME (ALARM) Information Security" project has developed a practice-oriented mix of methods in analog and digital form (serious games). All the tested materials have now been made available free of charge. The aim of the overall scenario was to promote the urgently needed operational awareness raising of executives and employees in SMEs. This article summarizes the key findings.

Keywords: information security, awareness raising, serious games, awareness training, on-site attack simulations, low-threshold security concepts

INTRODUCTION TO THE INFORMATION SECURITY SITUATION IN GERMANY

Ignorance or non-observance of information security and the corresponding operational guidelines poses significant risks for all companies [1][2]. The term information security refers to the protection of information of all types and origins [3] and goes beyond the terms IT security, cybersecurity, and data protection, which—despite their differences—are often used synonymously. Dangers exist in the form of human error, organizational deficiencies, intentional actions, technical failure, or force majeure. Managers and employees of companies should therefore be attentive to technical and organizational measures (TOM) that can be used to adequately address the risks. This requires active personnel development in companies for information security and extensive risk management with regard to operational processes.

Owing to the time lag between, for example, a cyberattack and its operational impact, there can also be prolonged consequences for a company, so a long-term mindset plays a crucial role in reducing security risks. According to Li et al. (2018), this long-term orientation includes three dimensions that must be established in companies in the area of information security: continuity, future viability, and endurance [4]. This approach was also pursued as part of the "Awareness Lab SME (ALARM) Information Security" project presented here with the focus on "helping small and medium-sized enterprises (SMEs) to help

themselves.” The results of this practice-oriented research project make a sound contribution to active personnel development and sustained awareness raising. The project and its results are of particular importance as a means to increase the level of security in German SMEs, as investigations into the situation repeatedly show that despite advancing digitization, awareness of IT security in Germany is still inadequate (see, for example, [5]). Even if risk perception has increased, there is a lack of comprehensive implementation of various information security measures, which cannot only be of a technical nature. The current study by the German Chamber of Industry and Commerce [6] highlights that although SMEs are now taking technical precautions to reduce risks, there has been no significant increase in organizational measures for information security—including awareness raising and staff training—and only a third of the companies surveyed have an emergency plan.

According to the Federal Office for Information Security (BSI), information security awareness (ISA) should address the following threats and vulnerabilities [7]: insufficient knowledge of regulations, insufficient ISA, and carelessness in handling information. Tsohou et al. (2012) concludes from recent global security surveys that ISA trainings (ISATs) are not currently working [8]. One reason might be a “technocratic” view of risk communication, meaning the tendency for technical experts to tell people what they think and ought to know [9]. A second reason might be policies “ending up as long lists of dos and don’ts located on web pages most employees only access when they have to complete their mandatory annual ‘security training’ and which has little to no effect on their security behavior” [10]; a third reason is that training aimed at addressing security awareness gaps is not sufficient to ensure compliance with a security culture [11].

Psychological research shows that in addition to the classical theoretical approach to knowledge transfer and the marketing-oriented approach of emotionalization, a systemic approach to team-based communication is needed (see [12–14]). ISAT needs a “methodology 3.0”: social participation in a communicative team process is a key component in this third stage of emotionally based awareness-raising activities [15]. This is because IS and IT are about more than technology [16]. ICT systems involve human actors, and users do not always behave the way they are supposed to [17]. The adverse characterization of people in the field of IS has now been rethought, because there are fundamental strategic IS deficits in institutions themselves (see, for example, [18, 19]). Alotaibi et al. (2023) argues that the significant evidence of unsecure employee behavior, which is a major threat and can undermine cybersecurity in companies, should not lead to staff being sanctioned [20]. Rather, there are often a large number of technical and organizational obstacles and stressful situations in the core business of everyday working life, that interfere with employees’ ability to make safety-related decisions and behave in the approved way [20].

Within just three years and under the difficult conditions of the COVID-19 pandemic, the “Awareness Lab SME (ALARM) Information Security” project [21] has developed a practice-oriented mix of methods in analog and digital form as a concrete response to this general situation. Our participatory research design involved SMEs as pilots for material testing in specified operational situations. All the materials have now been made available free of charge and serve to raise awareness among managers and employees; they have been developed, tested, improved, and finalized with the pilot SMEs. There is no doubt that SMEs also need to build their cyber resilience at the human level.

The complexity of the practice-oriented “ALARM Information Security” project was clear from the start: the intention was to develop an overall scenario to raise awareness and support SMEs in the area of information security, fostering their capacity to help themselves within the space of just three years. The underlying research design mainly contained new developments—within the purview of a central project management control—which were carried out iteratively in three agile and participatory phases, involving an innovative process scenario for information security with analog and digital experience-oriented scenarios as well as “on-site attacks” and other checks, such as awareness measurements, quizzes, and tests. The aim of the overall scenario was to address the urgent need for operational awareness raising among executives and employees and personnel development in SMEs, which has not yet been widely effective. To this end, IT security in connection with increasingly digital work processes should be made concrete; at the same time, people should be emotionally touched, motivated, and given an active role in developing

awareness-raising measures. The aim is to strengthen a sustainable, company-wide information security culture and increase the level of security in German SMEs.

The “ALARM Information Security” project is funded by the Federal Ministry for Economic Affairs and Climate Protection (BMWK) until March 31, 2024. The project documentation in German [22] refers to the results achieved in the period from October 1, 2020, to the original project end on September 30, 2023. The cost-neutral extension (CNE) of the project until March 31, 2024, is intended to make the high-quality materials that were obtained as a mix of methods more widely known at other SME events. In addition, the CNE enables the publication of the project documentation in book form, along with further articles about the results in English.

This article summarizes the key phases and findings and reflects on the results in the light of the international literature on the subject. The overall manager of the “ALARM Information Security” project also presents her own summary of the complex project that was carried out. The article is structured as follows: chapter 2 outlines the background for the gamified analog and digital developments in the project; chapter 3 sets out the methods of testing and the final results, which are further discussed and reflected on in chapter 4; chapter 5 presents the conclusions drawn from the project.

BACKGROUND TO THE “ALARM INFORMATION SECURITY” PROJECT

Over the last decade, the University of Applied Sciences Wildau (TH Wildau) and its corporate partners have developed a range of modern materials to increase information security awareness in various projects for different target groups. This was motivated, on the one hand, by the increasing prevalence of cyberthreats in Germany and worldwide (see, for example, [23] [24]) and, on the other, by the realization that traditional learning methods have evidently not yet led, as had been hoped, to increased mindfulness in increasingly digitized work processes (see, for example, [25]). Current studies also point to the ongoing critical situation. Tanriverdiyev (2022) notes that the reliance on information and communications technologies (ICT) has led to an increase in cyberattacks against individuals, companies, and governments worldwide, and that these attacks are no longer limited to data theft or financial losses but have broader implications for national security and economic stability [26]. Sharma and Zamfiroiu (2023) emphasizes the increasing complexity and frequency of cyberattacks, which require innovative and proactive cybersecurity measures. The previous reactive approach to cybersecurity is no longer sufficient; a proactive, adaptive strategy is required [27] to maintain an adequate level of security in the institutions. But technology alone is not enough. The critical role of human factors in shaping cybersecurity outcomes and practices continues to be explored [28]. Whether malicious or not, employees’ actions can have significant and detrimental outcomes for their organizations [29]. In any case, there is a long-standing requirement that traditionally *knowledge-based* training methods must change [30]. Moreover, security training must be implemented as continuous training and as further education in institutions/companies [28].

Several studies emphasize the critical role of public perception and awareness in cybersecurity for the better protection of organizations and individuals [28]. Abrahams et al. (2024) argues that effective cybersecurity strategies must include educational components that cater to different audiences, from college students to working professionals [28]. The findings of Epstein & Zankich (2022) suggest that a third of Internet users disclose more personal information than they would if they were more effectively warned about the risks involved [31]. The results of Posey & Shoss (2023) support the idea that targeted (whether malicious or not) security breaches can be viewed as events that occur in the complex interface between organizational behavior and security, and that stressors are related to employee security breaches [29]. Information security policies (ISPs) play a key role in organizational information security [32]. Clear organizational rules, even for emergencies, are necessary in all institutions, but they are by no means present everywhere; they are especially hard to access in stressful situations and certainly not written in a way that can be easily understood [32, 33]. The approach cannot therefore be to denigrate employees as the weakest link in the security chain [20, 25]. Likewise, involving organizational members in ISP development offers a number of benefits, providing detailed knowledge of the context, forming a common language, and promoting an information-security mindset [32]. However, the involvement of organizational members

requires special skills on the part of the project manager, because he/she has to clarify the goals of the contributions to a policy and make it clear what is expected of the participants; different methods also need to be used to achieve the goals of the group work [32].

The serious games we developed, which are presented in chapter 3, can also be useful for such a task. The basis for this was the “3.0 Systemic Approaches” of the so-called Security Arena [15], which were implemented and tested at TH Wildau in different projects, starting with “IT-Sicherheit@KMU” (2013–2014) [34] and “SecAware4job” (2015–2017) [35] [36] (Figs. 1 and 2). Ten analog scenarios were developed and tested with students and employees in German and English: Clear Desk, Data Security, Internet Services, Incident Management, Password Hacking, Phishing, Security on the Go, Social Engineering, Social Media, and Network Dominos. These learning scenarios (analog serious games) are still in use. They can be used individually as an awareness measure focused on this issue or for groups operating in competition (as is frequently practiced out by students). But they can also be used in classic teaching formats to provide didactic variety and a motivational boost. So far, it has always been possible to motivate people to actively participate.

FIGURE 1
THE “SECURITY ARENA”
WAS DEVELOPED AND IMPLEMENTED AT THE TH WILDAU TOGETHER WITH THE
PROJECT PARTNER KNOWN_SENSE, STARTING WITH THE PROJECTS “IT-
SICHERHEIT@KMU” (2013–2014) [34] AND “SECAWARE4JOB” (2015–2017) [35] [36].



Figure 2 shows pictures of the Security Arena's analog learning scenario "Social Engineering," which was used, for example, in Orlando in 2018. The English-language learning scenarios were tested in 2018/19, with international partners at DePaul University in Chicago and the University of Illinois at Urbana-Champaign, as well as in a hospital in Chicago, the Illinois Department of Children & Family Services (DCFS). These analog interactive serious games to increase information security awareness enable the inclusion of all participants and an intensive exchange of experiences on the specific topic, thus representing a good basis for awareness raising and training.

FIGURE 2
THE SECURITY ARENA'S ENGLISH-LANGUAGE LEARNING SCENARIOS
WERE ALSO USED IN WORKSHOPS AT CONFERENCES



The holistic approach of the current "ALARM Information Security" project is aimed at promoting awareness of information security in SMEs, in light of the specific requirements and needs of these companies. The following aspects were of central importance:

1. **Concept development:** At the beginning of the project, a comprehensive concept was developed for integrative awareness raising in the area of information security. By recording the current situation using in-depth psychological interviews and online surveys, this concept considers the specific requirements and needs of SMEs.
2. **Practical tests:** The individual awareness-raising methods and training measures developed were tested intensively in practice. Real everyday scenarios in the companies were simulated in order to check the effectiveness of the awareness-raising content.
3. **Awareness measurements and maturity statements:** Based on the practical tests, awareness measurements and maturity statements should be explored for future purposes. Such complex instruments are intended to provide information about the extent to which awareness-raising methods and security measures are ready for use and effective.

4. **Instructions for action:** Specific, comprehensive instructions for action have been developed that help SMEs to successfully implement the awareness-raising measures and integrate them into their everyday operations.
5. **Possible certifications for awareness moderators:** As part of the project, an initial moderator training course for analog serious games was developed and tested. The future certification of individuals as moderators of innovative learning methods could promote awareness-raising measures within SMEs and stabilize their use in the long term. In addition, an “awareness certification” of selected employees could serve the SME as a quality criterion and proof of the implementation of the requirement for awareness-raising measures according to ISO/IEC 27001 and the BSI standard 200-2 (see BSI 2021).
6. **Security strategy:** Within the three-year project period, a holistic strategy for information security awareness in SMEs was developed, which can be integrated into the overall corporate strategy. The awareness-raising content was included as an important component of the company’s information security strategy.
7. **Sustainability aspects:** Ideas for greater sustainability were included in the development process of the learning scenarios / serious games and all materials to ensure that the awareness-raising measures for appropriate personnel development are effective in the long term and can be continuously improved.
8. **Building a company-wide information security culture:** By virtue of their integrative interlinking and the extensive, practice-oriented assistance provided, all the project results serve to increase awareness of information security in all areas of the SME and the practical integration of security practices into everyday operational life. This promotes the development of the company’s information security culture and increases the SME security level.

METHODS AND RESULTS

The starting point for developing all the materials in “ALARM Information Security” was the in-depth psychological interviews that were carried out in the project by the subcontractor known_sense [37] and whose results are published in the form of three studies on the project website (called Study 1, Study 2, and Study 3; see [21]). At the same time, online surveys were designed, and international literature research was carried out by the TH Wildau team to ascertain the current situation in SMEs. Based on the analog serious games that were subsequently developed and their successive practical tests, the feedback from different target groups of pilot SMEs, and the improvements made to the learning scenarios and development of materials, this research project has a considerable wealth of empirical findings about information security and awareness in SMEs. Effective cybersecurity strategies require a balanced approach that combines technological advances with an understanding of the human factors involved and compliance with international standards, incorporating a holistic view [28]. As part of this research project “Awareness Lab SME (ALARM) Information Security,” the research team at TH Wildau ran numerous scientific workshops and other events with great enthusiasm. The primary goal was to promote a strong information security awareness in SMEs by increasing the reach and awareness of the developed learning scenarios and using other materials and low-threshold concepts to raise awareness among SME employees.

Didactic Background of the Developed Analog Serious Games

The seven developed analog serious games can be used as part of a company’s holistic awareness concept, based on the “station learning” methodology (see, for example, [38]). They can be used in combination with other serious games of this type as awareness training with or without competition between the target group teams. They can also be used as an introduction or as a teaser for more in-depth training on the topic of information security. The typical time frame for an awareness-raising measure should be about 15 minutes only; this requires good time management on the part of the moderator. The moderation steps are as follows [21, 37]:

- Step 1: Introduction (approx. 4–6 min.)

- Step 2: Game (if necessary two phases: $2 \times 2.5\text{--}3.5 \text{ min.} = 5\text{--}7 \text{ min.}$)
- Step 3: Debriefing (approx. 2–5 min.).

Figure 3 shows the seven developed analog serious games that are available for download in German on the project website [21]. An overview is given in [39]:

- **“Home Office” (Live & Work Securely at Home)** provides an overview of the most important operational and private information security and data protection risks in your own apartment or house as well as associated preventive measures to minimize the risks.
- **“Multi-Factor Authentication” (MFA)** combines aspects of password protection and MFA and demonstrates that the protection of information depends to a large extent on secure authentication. It shows how a “strong”—i.e., secure—password is created and demonstrates that one (!) factor is not sufficient to protect very sensitive information.
- **“The Five Phases of CEO Fraud”** provides an overview of the overall process of CEO fraud attacks and corresponding prevention measures. Of particular interest is an area that is often overlooked: the “prelude” involving the preparations for an attack.
- **“Mobile Communication, Apps & Co.”** raises awareness of the risks and of the preventive measures that reduce the potential dangers of mobile communication or app usage.
- **“Cyber Pairs” (Social Engineering)** breaks down possible barriers and leads to more security when dealing with the terminology and names of common or new cybercrime attacks by helping to understand them in detail and fostering the ability to distinguish between possible preventive measures. The clarification of terms is always linked to the question of what each of us can do to minimize risks.
- **“Data and Information Protection”** refers to the protection of information and data from customers, employees, and business partners as an aspect of every company’s business process. It helps clarify how data and information protection can be ensured by recapitulating and practicing the use of the most important protection strategies.
- **“Information Class Roulette”** illustrates the purpose of information classification in every organization. The “right” classes for protecting valuable information depend on the potential impact on availability, damage, or loss of information. It provides an understanding of information classification and the need for it, even if the organization has not yet adopted classification as a routine.

The specific didactic aspects of the seven developed analog serious games are described in brief below. Each analog learning scenario comes with four downloads: a moderation guide, a construction guide, a handout on the serious game, and the print templates. As a result of funding from the BMWK, all materials are available in German free of charge for internal, noncommercial use (see [21]).

FIGURE 3
SEVEN NEW ANALOG SERIOUS GAMES
FROM THE PROJECT “ALARM INFORMATION SECURITY,”
DEVELOPED TO RAISE INFORMATION SECURITY AWARENESS IN SMEs.
THE FUNDING APPLIED ONLY TO THE DEVELOPMENT OF THE GERMAN VERSION.



Didactic Intention of Analog Serious Game 1: Home Office

For this serious game, one can download, for internal, noncommercial use, the German moderation guide [40], the construction guide [41], the handout [42], and the print templates [43]. In recent years, more and more employees have been working from home. The topic of “home office” has become even more popular, especially as a result of the COVID-19 pandemic. Since you are usually on the same home network for work as you are for private purposes, the same or similar rules must be observed when it comes to information security as are applied at work. There are also risks from the “Smart Home” area. This serious game is intended to provide an overview of the most important operational and private information security and data protection risks in your own apartment or house as well as the associated prevention measures that can be used to minimize risks. A detailed description of the home office scenario is given in [44]. At the end of the debriefing phase, the moderator can explain the “golden rules” provided. The game for the home office addresses a variety of issues [40]:

- Security risks for the employer arise in the home office primarily through the shared use of the in-house network or devices for work AND private purposes.
- The same safety requirements apply in the home office as in the workplace.
- In addition, the employer’s guidelines for working from home must be observed.
- Work at home only with the tools provided or approved by the company; always separate professional and private matters and transfer data via an encrypted VPN (virtual private network) connection.

Didactic Intention of Analog Serious Game 2: Multi-Factor Authentication

To download the material for the second analog game in German, see the moderation guide [45], the construction guide [46], the handout [47], and the templates [48]. Protecting sensitive information and specific assets is one of the most important information security tasks in companies/institutions/public administrations. The loss of customer data can lead to the loss of customers, complex legal disputes,

reporting obligations, fines, and reputational damage with high collateral costs. When backups of customer data are stored in the cloud, the topic becomes even more explosive, because with cloud services the company is no longer solely responsible for the data stored there without outside help. The biggest risks in this regard include negligence in authentication, such as weak passwords and poorly managed access rights, security gaps in the cloud service, and inadequate preparation for the worst-case scenario of a possible incident. This serious game combines aspects of password protection and multi-factor authentication (MFA) and is intended to demonstrate that the protection of information depends to a large extent on secure authentication. Below are some examples of “golden rules” that apply in this case [45]:

- Your password should not
 - be known to anyone but you;
 - be accessible to anyone but you;
 - be stored unencrypted on your computer;
 - contain any character strings that can be associated with you, such as user IDs, vehicle license plates, dates of birth or telephone numbers, or terms that can be found in dictionaries.
- In order to significantly increase your security standard and better protect your company against phishing or brute force attacks, it is recommended that password protection be supplemented with a second barrier (MFA).

Didactic Intention of Analog Serious Game 3: The Five Phases of CEO Fraud

To download the material for the third analog game material in German, see the moderation guide [49], the construction guide [50], the handout [51], and the templates [52]. CEO Fraud (sometimes also called “boss scam” or “fake president scam” or “BEC” = business email compromise) is the name of a social engineering scam that is “popular” in cybercrime circles and involves identity fraud. Employees can be made to believe that high-ranking superiors have requested that large sums of money be transferred to foreign accounts. However, CEO Fraud does not start with the actual financial fraud but is characterized by an intensive preparation phase during which the fraudsters collect information about their targets and combine various attack vectors. This serious game is intended to provide an overview of the overall process of CEO Fraud and point out preventive measures—especially for the “prelude,” which is often overlooked. A detailed description of the CEO situation is given in [53]. Below are some examples of “golden rules” to protect yourself against CEO Fraud [49]:

- Use data and information, both your own and that of your company, sparingly on social networks and other websites.
- Pay particular attention to fake emails (phishing) that appear to come from the company management and in which—often accompanied by pressure and a request for absolute confidentiality—a request is made to transfer large amounts of money to a foreign bank account.
- Also pay attention to the content details of the emails: legitimacy checks for payment requests, deviations from standard emails from superiors in terms of sender address, address, greeting, structure, or overall design.
- Verify suspicious payment requests by calling back or asking the person who placed the order in writing.
- Remain critical of attempts at intensive, intrusive contact by people you do not know.

Didactic Intention of Analog Serious Game 4: Mobile Communication, Apps & Co.

To download the material for the fourth analog game in German, see the moderation guide [54], the construction guide [55], the handout [56], and the templates [57]. In recent years, mobile communication has shifted from notebooks to smartphones and tablets, which have practical apps. A separation between work and private life no longer seems possible for most users, especially if there is no clear demarcation between work and private hardware. This mix, along with increasingly unsecure apps and the lax handling of access rights, poses a high risk for companies. This serious game is intended to raise awareness of risks and

preventive measures that reduce the potential dangers of mobile communication or the use of apps. Some examples of “golden rules” for mobile communication are as follows [54]:

- Smartphones and tablets are practical tools, but some apps do more with your devices than you think and want.
- Apps can be gateways for malware and cybercriminals and promote identity theft and manipulation.
- You generally take responsibility for any apps you install on your mobile devices—i.e., you must inform yourself about possible risks.
- Install apps from trustworthy sources: if in doubt, only use official stores. Otherwise, there is a risk of malware or keyloggers.
- Remove apps you no longer use, as every additional app is a security vulnerability.

Didactic Intention of Analog Serious Game 5: Cyber Pairs (Social Engineering)

To download the material for the fifth analog game in German, see the moderation guide [58], the construction guide [59], the handout [60], and the templates [61]. The aspect of white-collar crime is becoming an increasingly crucial competitive factor for companies. As a result of digitization and the associated activities of cybercriminals, numerous attack methods or vectors to which organizations feel exposed have been successfully adapted by malicious actors. This means that new security gaps and attack methods are emerging in ever shorter cycles, sometimes with terminology that requires explanation—such as English terms or Anglicisms—in which technically based vectors are often combined with human-social factors to form complex structures. This serious game is intended to break down possible barriers and lead to greater security when dealing with the terms and names of common or new cybercrime attacks, helping people to understand them in detail and enabling them to differentiate between possible prevention measures—this always goes hand in hand with the question of what each of us can do to minimize risks. Social engineering, a form of manipulation in which unauthorized persons attempt to gain access to information or IT systems under false pretenses, is the most effective form of deception [58]. Some “golden rules” are listed below [58]:

- Ensure the identity of the person you are speaking to and do not open any email attachments or links from unknown senders.
- In the analog and digital world, pay attention not only to your personal data but also to data entrusted to you by your company and its customers: cybercriminals are attacking our information infrastructures more and more frequently and with ever better tools.
- Networking is one of the basic principles of your business, and trust in the security of the information entrusted to you by customers is the basis of your company’s business.
- Cybersecurity aspects such as firewalls, password security, virus and spam protection, and network monitoring are highly relevant not only for all employees but also for customers and for business dealings with them.
- In the end, defending against potential perpetrators is not just about outstanding technology; above all, it is a matter of your personal awareness and healthy security consciousness.

Didactic Intention of Analog Serious Game 6: Data and Information Protection

To download the material for the sixth analog game in German, see the moderation guide [62], the construction guide [63], the handout [64], and the templates [65]. Protecting information and data from customers, employees, and other parties is part of every company’s business. This serious game is intended to help ensure data and information protection by recapitulating and practicing how to use the most important protection strategies. Information is the “crown jewel” of your company, and it is therefore particularly important to protect it. Below are some examples of “golden rules” for this topic [62]:

- Everyone is personally responsible for the security of all the information in their own work environment.
- Adhere to the “need-to-know” principle—i.e., you only pass on information to the extent absolutely necessary and to authorized persons.
- You are also clear about what customer data is stored where.

- Only store or process necessary customer data.
- Moreover, if customer data is personal,
 - it must be collected, processed, and used lawfully;
 - it may only be collected, processed, and used for a specific purpose within the scope of legal permissions;
 - it must be appropriate and relevant and should not be collected and processed in a way disproportionate to the intended use.

Didactic Intention of Analog Serious Game 7: Information Class Roulette

To download the material for the seventh analog game in German, see the moderation guide [66], the construction guide [67], the handout [68], and the templates [69]. The purpose of information classification is to protect the valuable data of any organization. The “right” classes depend on the potential impact on availability, corruption, and loss of information. This serious game helps you understand information classification and the need for it. Because information classification is not the same for all small businesses, in this serious game the “golden rules” provide more insight [66]. In most organizations, an average of four classes of information appear in this context:

- Secret / Very Highly Confidential / Strictly Confidential: Information that is only accessible to a very limited group of named people and would have a major impact on the company or its stakeholders if it became public—e.g., strategic or organizational information and restructuring documents, business plans, trade secrets, medical data, and documents containing sensitive personal information. Therefore, great care must be taken when managing and transmitting it.
- Confidential/Highly Confidential: Information that is only accessible to a limited group of designated persons and would have a moderate impact on the company and its stakeholders for business use if it were made public—e.g., incident and test reports, backup data carriers, technical documentation and diagrams, source codes, contracts, customer data, project plans, and project documentation.
- Internal/Normal: Information for business use with a low level of impact on the company and its stakeholders if it becomes public—e.g., internal communications/publications, travel plans, standards, internal guidelines, project documentation, personal data such as customer data, including names, address books, email addresses, and telephone numbers.
- Public/Open: Information that is neither privileged nor needs to be protected. Disclosure would have no impact on the company and its stakeholders—e.g., PR information for newspapers, websites, and published marketing materials such as brochures or flyers.

Digital Addition to the Analog Serious Game 7: A Roulette Game

If the institution is unwilling to buy a small roulette wheel for the seventh serious game “Information Class Roulette” in the “ALARM Information Security” project, it can be played digitally. The digital roulette was used in an earlier project called “Development of game-based learning scenarios for social engineering and security risk management in the manufacturing industry” [70]; it can also be used in other projects or trainings [71]. In the original project, the two game-based learning scenarios on social engineering and security risk management in the manufacturing industry were developed for the project “SME 4.0 Competence Center Stuttgart” [70].

Didactic Background of the Developed Digital Serious Games

The aim of the “ALARM Information Security” digital serious games is to enable employees to independently explore the topics of the analog serious games and experience them with other focuses [72]. However, the digital serious games—as part of a holistic awareness concept—can also be played independently of the analog games and in any order. We strongly recommend a personal debriefing. The seven digital serious games represent everyday situations drawn from SMEs [72].

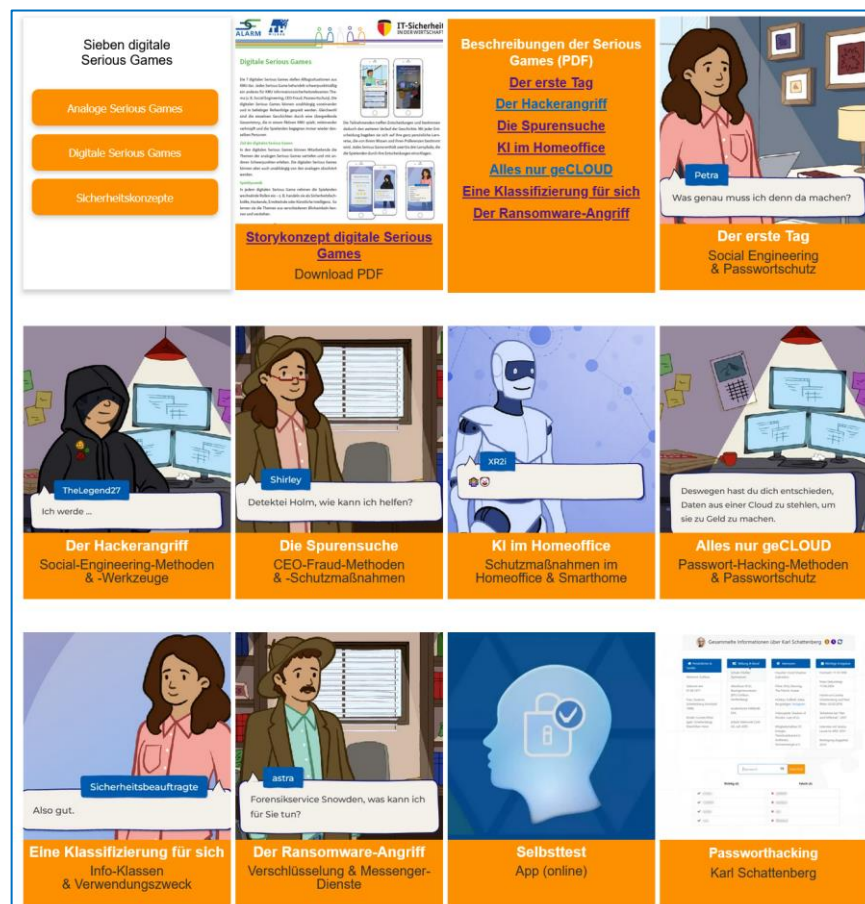
Each game focuses on a different topic relevant to information security for SMEs; they correspond to the analog games but do not duplicate them. The individual stories of the digital games are linked together by an

overarching story that takes place in a fictional SME; the players meet the same people again and again and get to know the company better with each serious game they play. Figure 4 shows the website area for the digital serious games in the “ALARM Information Security” project [21]. At the beginning of Fig. 4, there is a general story concept available as a PDF download [72], along with a specific description for each digital game. This is followed by the seven digital games, which can be played directly from the project website. At the end, there are two digital add-ons: a personal self-test, which has been recently redeveloped, and an adapted hacking game, the original idea for which comes from the previous Security Arena [36] [37]. The seven new digital serious games are described in brief below (see Figs. 4 and 5).

The time frame for each digital serious game is 15–20 min. (one game played through). On the left-hand side of Fig. 5 you can see the number and the titles of the serious game translated into English. On the right, three key images from the game are shown, which were used in the German game descriptions made available for download from the project website [21].

The digital serious games were developed by the subcontractor Gamebook GmbH in coordination with the TH Wildau research team. In terms of implementation, all the digital games are played individually. Our recommendation is that a joint debriefing and exchange with the other participants in the company should take place online or in person. The funding of the BMWK applied only to the development of the German version.

FIGURE 4
SEVEN NEW DIGITAL SERIOUS GAMES FROM THE “ALARM INFORMATION SECURITY” PROJECT DESIGNED TO RAISE INFORMATION SECURITY AWARENESS IN SMEs AND TWO ADDITIONS (A SELF-TEST AND A PASSWORD-HACKING GAME). THE FUNDING APPLIED ONLY TO THE DEVELOPMENT OF THE GERMAN VERSION



Digital Serious Game 1: The First Day

In the first digital game, it's your first day in the imaginary company Grüsselig. Because they "know so much about computers"—or so the boss thinks—the players are directly tasked with IT security, a task that they first have to familiarize themselves with. And which is accompanied by some pitfalls and challenges. But first, it's time to get to know your new colleagues. The target group consists of first-time players and those who have previously had little or no contact with the topic of information security. It is primarily intended as an introduction to this and a first step in awareness training, in combination with other serious games in this format. The game can also be used as an introduction or to loosen up an analog training course on the subject of social engineering and password protection. As with all our digital serious games, the players have to select their decisions from a list of suggestions, and at the end the actions they have taken are evaluated (Fig. 5-1.).

Digital Serious Game 2: The Hacker's Attack

In this serious game, the players take on the perspective of the attackers. As hackers, the players try to launch a social engineering attack at Grüsselig and break into the company network. There are different approaches to choose from, but only one leads to success. The focus is on players who want to specifically engage with social engineering methods and test various tools. It is intended as an introduction, to loosen up or intensify a training course on the topic of social engineering (Fig. 5-2.).

Digital Serious Game 3: The Search for Clues

As a forensic scientist, the players receive information via an anonymous call that the Grüsselig company has fallen victim to CEO Fraud. If the player finds out quickly enough which scam was used and who skimmed the money, they might be able to get it back. The focus is on players who would like to specifically deal with CEO Fraud methods and test various protective measures (Fig. 5-3.).

Digital Serious Game 4: AI in the Home Office

The players take on the role of an artificial intelligence (AI) that monitors the computers of the Grüsselig employees for security issues and helps them. As AI, the players visit the home offices of three company employees from different business areas. From an AI perspective, they experience how the same mistakes are always made in the home office. The target group consists of people who would like to specifically deal with security in the home office and would like to test various protective measures. The idea is to provide intensive training on the topic of security in the home office and smart home (Fig. 5-4.).

Digital Serious Game 5: Everything Just CLOUD

The aim of the game is to examine the topics of data storage in the cloud and password security from different perspectives: from the point of view of the attacker and the trainer. The focus is on different aspects of the threat and on facilitating a holistic experience of the topic. Efficiency and care are assessed (Fig. 5-5.).

Digital Serious Game 6: Information Classification

The players deal with the topic of information and data classifications separately. What exactly is information classification in a business context? What part does it play in everyday life, and how is it used sensibly in the company? To do this, the players take on the role of the AI. The AI in the gaming context is now ready for the market and has been established as an assistance system at the Grüsselig company. The target group consists of people who want to delve deeper into information classification (Fig. 5-6.).

Digital Serious Game 7: Ransomware

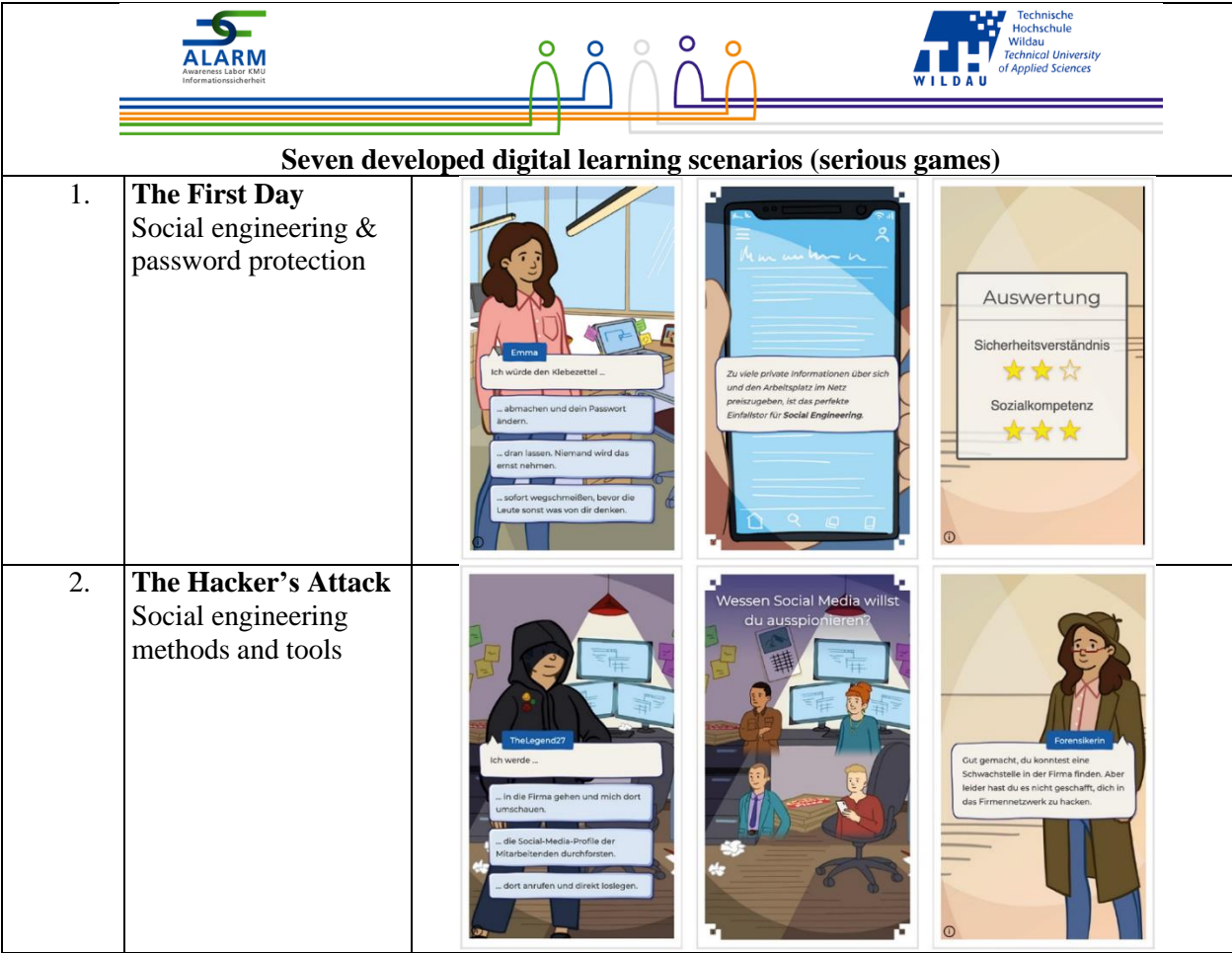
The Grüsselig company was hacked. Owing to a ransomware attack, all of the company's data has been encrypted, and only one person has the code to unlock everything again. The players take on the role of the forensic scientist to uncover the case and limit the damage. The only clue is that it happened via a messenger





service. The target group consists of people who want to delve deeper into encryption and messenger services (Fig. 5-7.).

Digital Addition to the Digital Serious Games: A Digital Self-Test

The self-test is a low-threshold awareness-raising measure that generates data, determines the level of knowledge of the participants, allows comparison with other self-test users and expands or refreshes the level of knowledge of the participants with an immediate evaluation. This became necessary because defining areas of activity and the awareness measurements based on them would only produce results that can be evaluated at a later point in time. A parallel development began with the self-test in order to be able to supply basic questions for automated recommendations. The collected data thus forms the basis for scientific considerations. The main goal was to identify indicators and the learning paths calculated from them and develop recommendations for targeted awareness-raising measures in response to the knowledge gaps identified by the self-test (see Fig. 4).

FIGURE 5
SEVEN DEVELOPED DIGITAL LEARNING SCENARIOS (SERIOUS GAMES) TO INCREASE INFORMATION SECURITY AWARENESS IN SMEs (FINAL VERSIONS)



3.	The Search for Clues CEO Fraud methods & protection measures	
4.	AI in the Home Office Protective measures in the home office & smart home	
5.	Everything Just CLOUD Password hacking methods & password protection	
6.	A Classification in Itself Info classes and intended use	

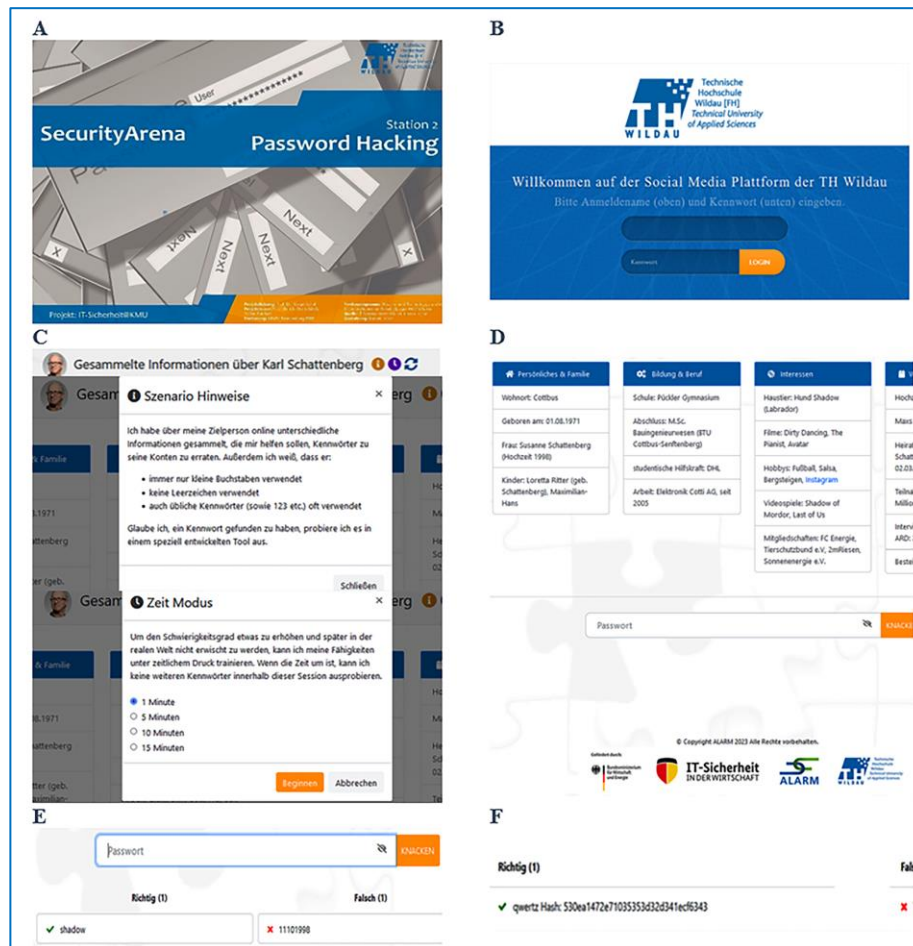
7.	The Ransomware Attack Encryption and messenger services	
----	---	--

Digital Addition to the Digital Serious Games: A Password Attack Scenario

The idea for the second additional digital game, Password Hacking, has been in use for several years in the Security Arena of the project partner known_sense [37] and was first used at the TH Wildau in the “IT Security@KMU” project [34] for students and employees. This project was financed from 2013 to 2014 as a technical investment in a mobile awareness-raising initiative by the Ministry of Science, Research, and Culture (MWFK) of the state of Brandenburg with funds from the European Regional Development Fund (ERDF). Figure 6 shows the poster (A) of the old digital learning station “Password Hacking” in the Security Arena (see Fig. 1). In the initial screen for exercise (Fig. 6-B), the log-in name and passwords must be guessed and entered using an imaginary user profile of a person on a social media platform.

The new version, which has now been adapted in the “ALARM Information Security” project, can be seen under C to E. The information collected about the imaginary person Karl Schattenberg (C) is put together (D), and the game provides information about the scenario and the possible time mode (C). Here too, simple passwords should be derived from the information and entered (E). If the assumed password is correct, it will be displayed with a green tick on the left; if it is wrong, it will be visible on the right with a red cross (E). In the old version, for correctly guessed passwords, we not only listed the password with a green tick but also showed its hash value (F). Depending on the target group, we were able to provide further training on the meaning and purpose of the passwords saved as hash values. However, this required a personal discussion, which is not a problem in the analog setting but requires a digitally initiated debriefing in the digital setting. To reduce complexity, this was omitted from the “ALARM Information Security” project.

FIGURE 6
DIGITAL ADD-ONS TO THE “ALARM INFORMATION SECURITY” PROJECT



Didactic Background to the Low-Threshold Security Concepts That Were Developed from the Seven On-Site Attack Simulations

In addition to the seven analog and digital learning scenarios, the “ALARM Information Security” project also includes the results of seven on-site attacks for which another subcontractor, Thinking Objects, was primarily responsible. Ethical questions and the agreements with the managing directors of the pilot SMEs also play a key role. Additional practice-oriented instructions and tips for low-threshold security concepts for SMEs emerge from the findings. These are now available for download. Conducting on-site attacks is tricky and must be done with extreme caution. 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, nor should it lead to personal exposure. Specific didactic aspects of the seven developed on-site attack simulations are briefly described below. Each simulation comes with two downloads: an information sheet and a low-threshold security concept. Again, as a result of funding from the BMWK, all materials are available in German free of charge for internal, noncommercial use (see [21]).

FIGURE 7
SEVEN NEW INFORMATION SHEETS AND LOW-THRESHOLD SECURITY CONCEPTS
DERIVED FROM SEVEN ON-SITE SIMULATION ATTACKS IN THE PROJECT “ALARM
INFORMATION SECURITY” [21] DESIGNED TO RAISE INFORMATION SECURITY
AWARENESS IN SMEs (IN GERMAN)



On-Site Attack Simulation 1: CEO Fraud

The information sheet [73] points out that everyone makes an important contribution to ensuring that the employer, the company, and you personally do not fall victim to a cyberattack. It then briefly explains what CEO Fraud is and why SMEs should be familiar with this attack method, because it involves a significant amount of money. The attacker sends a fake email to someone in the company, usually someone in the finance or accounting department [73]. The email looks like it comes from a CEO or other executive and asks the person to complete a financial transaction [73]. The reason for the transaction is often presented as urgent or secret in order to put the employee under pressure [73]. The fake emails are often very convincing and can be made to look official by including an imitation of the company logo and being written in the kind of language and style used by actual executives [73]. The information sheet advises end users to [73]

- check emails;
- use authentication methods;
- respect confidentiality;
- verify the requested transaction internally; and
- verify the contact(s).

The low-threshold security concept on the topic of CEO Fraud for management and IT managers [74] deals with technical measures such as email filters and organizational protective measures. It is emphasized that with this type of attack, the number of technical protective measures in the area of CEO Fraud is limited, which is why organizational measures are significantly more effective [74]. Passwords also play a role here,

because if the criminals have gained access to a management mailbox, technical protection measures will actually not work at all, and the attacker can write even more authentic emails or copy and use real emails with old payment orders [74]. The most important organizational measures are regular information and clear regulations. There must be straightforward, procedures for reviewing requests and approving payments or transactions [74]. Possible exceptional situations should also be discussed in advance to determine whether special procedures will be established for this, such as telephone reassurance [74].

On-Site Attack Simulation 2: Email Check

We are responsible for our own information security, which is why we must also handle our own identity data carefully. Email checking and password security are therefore also important in the second simulation. The information sheet [75] shows that identity theft is a relevant topic in the area of IT security. Illegally copied collections of identity data leaks circulate in criminal circles via various media, and those affected often only find out about the existence of such leaks when their own identity is used illegally and damage occurs [75]. Online tools are presented that allow end users to check whether their email address is part of known large data leaks [75]. The usual protective measures are recommended [75].

It is also pointed out that no reputable company will ask for your password and that it is important to be regularly informed about the current recommendations on password criteria [75]. The topic of passwords is discussed in more detail in the low-threshold security concept for management and IT managers [76]. It should be noted that, in addition to regular changes, a password must always be changed if there is a suspicion or certainty that it has fallen into someone else's hands [76]. In addition, two-factor log-in and password-less log-in are briefly discussed [76].

On-Site Attack Simulation 3: Hacking

Raising awareness of the security of one's own identity files also plays a major role when it comes to hacking. The corresponding information sheet lists the following protective measures for end users [77]:

- Use strong passwords and two-factor authentication.
- Keep software and operating systems current with patches and updates.
- Be careful and attentive when opening emails and attachments.
- Use firewall and antivirus software.
- Be careful and alert when using public Wi-Fi.
- Carry out regular data backups.
- Have healthy skepticism about unexpected requests.
- Keep personal information private.

The low-threshold security concept on the topic of best-practice protective measures for management and IT managers [78] goes into these aspects in detail and also deals with the topics of risk assessment and redundancy in the systems.

On-Site Attack Simulation 4: Phishing

The information sheet on the subject of phishing makes it clear that phishing emails are one of the main gateways for cyberattacks and can cause major economic and operational damage [79]. End users are therefore also called upon to make an important contribution by paying greater attention to protecting the company from this form of attack. The attackers target all the access data to the company network and try to trick people in front of their screens into clicking on links or entering personal access data on fake websites [79]. If access to the company network is successful, hackers can surreptitiously paralyze systems or steal important data [79]. The following information is given to end users [79]:

- Pay attention to discrepancies between the supposed sender and the email address used.
- Cybercriminals often rely on the urgency factor and try to put pressure on the recipient group to act.
- Pay attention to the date and time.
- Often no personal salutation is used. In official emails you will generally be addressed by your name.

- Incorrect spelling and grammar are often an indication of fake emails.
- Pay attention to the signature. Often this does not correspond to the company's signature requirements.

With regard to error culture, it is recommended that, in case of an attack, IT support be informed immediately, and the compromised device disconnected from the (work or private) network and Internet. In addition, reference is made to a public checklist with concrete action steps [80]. In the low-threshold security concept [81], the topic is treated more intensively and primarily with regard to technical measures. Information is compiled in a generally comprehensible form for management and IT managers: email filters, antivirus and endpoint protection, web filters, passwords, multi-factor authentication, patch management, backups, hard drive Encryption, smartphones, the cloud, and tricks. However, organizational regulations also play an important role, especially with respect to the last point. The need for employees to react appropriately if they are tricked is spelled out, along with the importance of having a company reporting channel that is clearly defined and communicated [81]. The helpdesk should be a central contact point and have suitable measures available, based on a checklist on how to proceed [81]. In the event of an attack, accusations and blame quickly lead to users no longer asking for help or reporting an incident the next time it occurs [81]. Here too, a positive error culture in the company is very valuable.

On-Site Attack Simulation 5: Smishing

Smishing is a portmanteau combining SMS (short messages) and phishing (theft of access data via fake messages or emails) [82]. A smishing attack is therefore a phishing attack via SMS, which is why the corresponding information sheet has very similar content to the phishing information sheet [4a]. Since 2021, the BSI has been continuously providing public information about smishing attacks and their increasing importance for cybercriminals [82]. The following tips are compiled for end users in the "Error Culture" section of the information sheet [83]:

- If your work cell phone is affected,
 - activate airplane mode to unplug the device; and
 - inform your IT department.
- If your private cell phone is affected,
 - activate airplane mode to unplug the device;
 - inform your mobile phone provider;
 - file a criminal complaint with the local police station, being sure to take your smartphone with you; and
 - back up all your important data such as photos and documents locally—for example, via a USB connection. After you have filed a report, reset your smartphone to factory settings. With a factory reset, all your saved and installed data will be lost. However, this step is necessary to completely remove the Android malware distributed via the current SMS spam messages.

The low-threshold security concept also briefly explains alternatives whereby a company smartphone does not need to be used directly in the internal company network as an access point for attacks [84].

On-Site Attack Simulation 6: Tailgating

Tailgating is a physical security attack in which an unauthorized person attempts to gain access to a building or a specific area within the building. This is often achieved by the person walking through a secured door directly behind an authorized employee [85]. The corresponding information sheet makes it clear that tailgating is one of the classic social engineering attacks [85]. A social engineer is a psychologically well-trained person who often exploits employees' human traits, such as helpfulness, respect for authority/uniforms, and trust, in order to gain unauthorized access to a site or building. Through raising their own awareness, employees can recognize the dangers and help prevent unauthorized persons from gaining access to protected areas by [85]

- remaining vigilant at all times and ensuring that no unauthorized person follows them in;
- using the company's access systems and not sharing access cards or keys with others;

- politely but firmly asking unauthorized persons to move away from a secured area;
- remaining calm and controlled and not provoking an attacker;
- notifying the security services; and
- reporting incidents to company management.

The low-threshold security concept for SMEs [86] covers the aspects of access control, visit management, and clean-desk and clear-screen policy as well as the locking of rooms and of sensitive data and devices. In addition, renewed emphasis is put on the importance of having a clear reporting channel for such a safety-relevant event, which must be known to the employees [86].

On-Site Attack Simulation 7: Incident Response

An incident is an unexpected event that affects the IT security or operations of a company, such as a cyberattack, data leak, physical damage to IT systems, or the failure of critical applications and services [87]. If employees suspect an incident, they should immediately report it to their manager or the IT department, as a quick report is important to minimize the damage and facilitate the restoration of normal operations [87].

For management and IT managers, the low-threshold security concept [88] primarily addresses the special importance of emergency management in the area of IT security. It briefly describes how to deal with emergencies that can threaten the existence of the company [88]. Relevant questions are posed so that managers can see whether they are able to answer them on behalf of their company and are therefore prepared for emergencies.

DISCUSSIONS AND REFLECTION

Story and Game Dynamics of the Seven Analog Games

With 15 minutes per serious analog game, a circuit training with four learning stations can be set up so that participants cover four topics in one hour. However, the time frame can also be intensified and last up to an hour with discussions between interested participants. These analog scenarios are based on one person as a moderator for each serious game (learning station), who has spent from 10 to 60 minutes familiarizing themselves with the game descriptions. Moderators can also be chosen from the target group itself. The group size per station should be a minimum of four people and a maximum of twenty people. From our experience, the optimal group size for an intensive exchange is eight to twelve people per station.

Story and Game Dynamics of Analog Serious Game 1: Home Office

- As part of this serious game, we see the house on the playing area where the friendly couple Yvonne and Thomas work; they live together with Thomas's father and Anke and Marco, their children.
- Seventeen scenarios are assigned to your work, each containing an information security or data protection risk. The risks are described on seventeen orange risk cards, with the corresponding protective measures on seventeen green protection cards.
- The orange risk cards should first be placed on the corresponding scenarios, and in a second round the green protection cards should be placed on the appropriate risks.
- Start the clock as soon as the team begins placing the risk cards corresponding to the appropriate scenarios on the playing area.
- Stop the time after 2½ minutes. Put the risk cards that were misplaced in the correct position and count the points.
- Start the timer again once the team begins matching the protection cards next to the relevant risk cards. Stop the time after another 2½ minutes (a total of 5 minutes).
- Scoring: There is one point for each correctly sorted card (with two pre-sorted example cards, there is a possible maximum of 32 points).

Story and Game Dynamics of Analog Serious Game 2: Multi-Factor Authentication

- This serious game consists of several parts and follows the logic of escape games.
- First, the twenty password cards should be ranked according to their strength by distributing them on the twenty boxes in the playing area in the correct order from 1 to 20.
- The numerical codes of the top three cards, in the correct order of their “Strength” ranking, give the appropriate numerical code for the large box—i.e., the combination lock can be opened with this three-digit code.
- In the large box, there is a small box with a lock, to which the corresponding key should be found (document bag!) and used.
- Once the small box is opened, the serious game is over.
- Scoring: A maximum of 30 points can be scored, 20 for the correct order of the passwords (one point for each correctly positioned password), and 5 points each for opening the two boxes.

Story and Game Dynamics of Analog Serious Game 3: The Five Phases of CEO Fraud

- As part of this serious game, we see a kind of infographic on the playing area that depicts the five main phases typically found in CEO Fraud (research, testing, maintaining contacts, attack, damage) as a process.
- Each of the five main phases is divided into further detailed process steps (twenty-one in total), each represented on the playing cards with a suitable icon and the associated plain-text label.
- These twenty-one playing cards should be sorted on the playing field in the correct processing order. The three “wrong” cards that do not fit into this process are sorted out by the participants.
- It can be helpful to instruct the participants to first sort all of the cards into categories according to the five main phases and then start with the detailed assignment.
- Optionally, in a second part of the exercise, the four cards that use phishing to initiate CEO Fraud or a support scam should be selected from the six email cards and placed in the center of the playing area. The two non-critical cards are placed next to the playing area.
- Start the clock as soon as the team begins placing the cards on the appropriate spaces on the playing area.
- After 6 minutes, stop the time, rearrange the cards that were incorrectly placed, and count the points.
- Scoring: There is one point for each correctly sorted card (maximum: 24 points; optionally including email cards: 30 points).

Story and Game Dynamics of Analog Serious Game 4: Mobile Communication, Apps & Co.

- On the playing area of this serious game, we see a section through three floors of a subway station and a house in the background as the central key visual. This learning card with a hidden object picture shows twelve scenarios for smartphone or app use as well as focused smartphones with screenshots belonging to the scenarios on the edges.
- Twelve information security and data protection risks are assigned to the twelve numbered scenarios and twelve numbered smartphones that match the scenarios in the subway station or house. The risks are described on twelve orange risk cards, and the corresponding protective measures, on twelve green protection cards.
- First, the orange risk cards should be placed on the corresponding scenarios; in a second round, the green protection cards should be placed on the appropriate risks.
- Start the clock as soon as the team begins placing the risk cards corresponding to the appropriate scenarios on the field.
- Stop the time after 2½ minutes. Put the risk cards that were misplaced in the correct position and count the points.
- Start the stopwatch again once the team begins matching the protection cards to the relevant risk cards. Stop the time after another 2½ minutes (for a total of 5 minutes).
- Scoring: There is one point for each correctly sorted card (maximum: 24 points).

Story and Game Dynamics of Analog Serious Game 5: Cyber Pairs (Social Engineering)

- First, the thirty-two blue cyber memo cards should be arranged so that sixteen correct cybersecurity terms are created—next to each other in two columns, each with space for two more cards to the right of the two blue ones.
- In the second round, the sixteen orange cyber risk cards with the definitions should be assigned to the sixteen terms and placed next to the blue cyber memo card on the right.
- In the third round, the sixteen green cyber protection cards with prevention measures should be placed next to the orange cyber risk cards.
- Scoring: One point is awarded for each correctly sorted term from two blue cyber memo cards (maximum 16 points in the first round). For each additional cyber risk card (orange, second round) and each additional matching cyber protection card (green, third round), there is one additional point for each correct assignment (a maximum of 16 additional points per round). A total of up to 48 points can be achieved in three rounds.

Story and Game Dynamics of Analog Serious Game 6: Data and Information Protection

- As part of this serious game, we see five typical scenarios from the administration building of a model company in which customer rights play a role (first row from top) and eleven scenarios, each of which is on the playing area in the style of a hidden object picture, containing information security or data protection risks (in the second and third rows).
- First, all sixteen blue and green playing cards on the playing area should be arranged in one go so that they match the scenarios shown.
- Optionally, in a second part of the game, the “picture frame” cards can be brought into play to simulate the distinction between personal and non-personal data.
- For this purpose, those cards that do NOT contain any personal information are placed on the walls of the offices on the playing field wherever there is space. The personal cards are not placed and are therefore sorted out.
- Scoring: For each correctly sorted card there is one point (16 for part one, and 6 for part two—i.e., only for those placed on the playing area: a maximum of 22 points).

Story and Game Dynamics of Analog Serious Game 7: Information Class Roulette

- The moderator or a participant spins the roulette wheel and inserts a ball.
- The number received decides which category a card should be drawn from—for example, the “Five,” the top card from the classification category “General Classification” is drawn and discussed.
- If the roulette wheel puts the ball on the “zero,” a category can be selected.
- The participants take turns reading the contents of the card they have drawn out loud.
- The statement given there must be judged as “true” or “false” by assigning the allocated chips in the playing area to “TRUE” or “FALSE.”
- The teams are free to decide on the number of chips or their amount; however, you must bet a minimum of 5 chip points per card drawn.
- After the chips have been placed, the moderator reveals the correct answer and explains the background, although discussions will need to be reduced as the game progresses.
- Teams with a correct answer receive their amount plus half of their “stake” back, and an additional amount of at least 5 chip points. The chips of the teams with the wrong answer go to the “bank”—i.e., they are confiscated by the moderator.
- The ball is then thrown into the roulette wheel again, as allowed by the playing time, after which a new playing card is drawn.
- Scoring: At the end of the game, the team with the most points wins.
- Note: This moderation guide refers to teams. The game can also be played by individual people against each other.

The Goals of the Seven Digital Games

The game dynamics of the digital games is that in every digital serious game, the players take on changing roles [72]—e.g., they act as security specialists, hackers, investigators, or artificial intelligence. In this way, they get to know and understand the topics from different perspectives. The participants make decisions and thereby determine the further course of the story. With every decision, they embark on their own personal learning journey, which is determined by their knowledge and preferences. Every serious game contains two to three learning paths that the players take through their decisions. At the end of a game, participants receive feedback on the points they achieved. This includes suggestions and requests to the players as well as a short summary of the lessons learned in the specific game. Over the course of the game, messages are displayed that draw attention to advantageous or disadvantageous decisions and behaviors. In addition, a lexicon module offers participants the opportunity to read important information security terms before and after the game.

The goals of the digital serious games are as follows:

- The aim of serious game 1 (The First Day) is to introduce players to the topic of information security using classic situations involving social engineering and password protection, which all players can readily identify with. Participants' understanding of safety and social skills are assessed.
- The aim of serious game 2 (The Hacker's Attack) is to familiarize players with the common strategies used by hackers in a real situation, looked at from the hacker's perspective, and to experience in a playful way how even the smallest security gaps are enough to allow hackers access. Efficiency and the variability of attack routes that the players try out are evaluated.
- The aim of serious game 3 (The Search for Clues) is for players to uncover common CEO Fraud practices and take effective protective measures. Time plays a special role here: only if the players resolve the attack in time can they prevent greater damage. Efficiency, discovered learning content, and social skills are assessed.
- The aim of serious game 4 (AI in the Home Office) is for players to identify the most common mistakes that people make in the home office carrying out smaller tasks. Practical and funny examples are used to draw attention to the pitfalls of working from home. Security awareness and machine learning are assessed.
- The aim of serious game 5 (Everything Just CLOUD) is for players to uncover common CEO Fraud practices and take effective protective measures. Time plays a special role here: only if the players resolve the attack in time can they prevent more serious damage. Efficiency, discovered learning content, and social skills are assessed.
- The aim of serious game 6 (Information Classification) is for players to uncover common CEO Fraud practices and take effective protective measures. Time plays a key role here: only if the players resolve the attack in time can they prevent greater damage. Efficiency, discovered learning content, and social skills are assessed.
- The aim of serious game 7 (Ransomware) is for players to uncover common CEO Fraud practices and take effective protective measures. Time plays a specific role here, too: only if the players resolve the attack in time can they prevent multiple damage. Efficiency, discovered learning content, and social skills are assessed.

Results of the Seven On-Site Attack Simulations

Every on-site attack simulation 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 supportive tool to help raise awareness. The attacks were 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 trust and error culture.

By educating yourself, for example, about the fraud method, you can minimize risks, identify fraud attempts, and take appropriate measures to protect yourself. The information sheet advises end users on their protection [73]. The low-threshold security concept on the topic of CEO Fraud for management and IT managers [74] deals with technical measures such as email filters and organizational protective measures. The last point in the information sheet is the error culture in the company, as mistakes can happen to all of us. If a person falls for the fake email, he/she will complete the requested transaction without realizing it is a scam [73]. The money is then usually transferred to an account controlled by the fraudsters; in some cases, confidential information such as company secrets or employee data is stolen, too [73]. In such a case, action must be taken very quickly, which is why the company must be open about errors. Possible exceptional situations should also be discussed in advance and whether special procedures will be established for this, such as telephone reassurance [74].

With regard to error culture, the recommendation in the phishing example is that IT support should be immediately informed, and the compromised device disconnected from the (work or private) network and Internet. In addition, reference is made to a public checklist with concrete action steps [80]. However, organizational regulations also play an important role, especially with regard to the last aspect. It is made clear that employees must react appropriately if they are tricked, for which there must also be a reporting channel in the company that is clearly defined and communicated [81]. Be aware that accusations and finger-pointing can quickly lead to users not asking for help or reporting an incident the next time.

When it comes to tailgating, the company must have a clear reporting channel for such a security-relevant event, which must be known to the employees [86]. At the end of the security concept training, management and IT managers are reminded of the need for employee awareness to be raised. How sensitive the employees should be, or how low-threshold the reports of incidents should be must be based on the protection needs of the particular company area and communicated accordingly [86]. For management and IT managers, the low-threshold security concept [88] primarily addresses the special importance of emergency management in the area of IT security. The incident management story includes a brief description of how to deal with emergencies that can threaten the existence of the company [88]. With the help of relevant questions, managers discover whether they can answer such questions on behalf of their company and are thus prepared for emergencies. In the event of an IT security emergency, targeted communication with customers, partners, and employees is important [88]. In addition, depending on the extent of the emergency, the police, the BSI, and, if necessary, the public must also be informed at some point. Emergency management is important for all institutions and always has two sides: a proactive aspect with preventive measures that must be implemented, and a reactive aspect with coping measures that will hopefully be effective in an emergency. In addition to setting up an appropriate information security management system (ISMS), an SME also needs to take care of an effective business continuity management system. Larger and medium-sized companies can use BSI Standard 200-4 [89] as a guide; smaller and microenterprises should establish minimum measures.

CONCLUSIONS

In the future, hardly anything will work without information technology—but it will only work with it if the basic values and protection goals of information security as well as the guarantee goals of data protection are integrated, observed, and actively implemented. Using secure digital processes, digital technologies, and digital business models, and thus securing and increasing the competitiveness and innovative ability of German medium-sized businesses is a MUST for Germany, for the prosperity of its citizens, for the further development of SMEs, and for the authorities funding new programs.

We are dealing with an increasingly dynamic environment of digitization, which is characterized by a constantly changing threat situation and a variety of new and old attack vectors. Individuals, the economy, and society as a whole are all affected. A sustainable level of security can only be effectively guaranteed in all institutions through an ongoing systematic approach to adequately protecting business processes with a continuous improvement process. A correspondingly well-thought-out, appropriate ISMS with adapted, effective security process and qualified personnel must be established in the institutions [3]. The use of

technology is essential, but, without people, a security process will not work or be viable. When developing analog and digital learning scenarios (serious games / realistic simulations) for information security awareness, we discovered that the term “gamification” is largely unknown in German SMEs and needs to be explained first. Afterwards, the principle was understood and made sense to most respondents [90].

The increasingly comprehensive digitization of business processes requires analog sensitization. Our modern game-based analog awareness-raising program, which has long-term positive effects on information security and data protection includes the following features:

- Active involvement of the participants
- Use of haptics to enhance comprehension
- Interactivity
- Discursive settings
- Stories/narratives as an aide-mémoire
- Ability to contribute personal experience
- Flexible scheduling (from 15 minutes during a break to an hour for intensification)

However, repeated instances have made it clear that the game-based training of security awareness in German SMEs should not be focused on the idea of play, which causes awareness-raising measures to be met with significant resistance [90]. The managers of SMEs putatively take a customer-oriented perspective. The in-depth psychological background is that information security in SMEs is primarily aimed at customers, and therefore the devaluation of the gamified aspects of training among managers can be interpreted as a projection [90]. The supposedly pejorative perspective of the customers is taken here, so that, in the opinion of many managers, any efforts made in the context of information security would be in vain [90]. This is a consequence of the fact that information security in German SMEs has so far been determined by extrinsic factors. However, managers should also recognize intrinsic factors that make information security critical to their organization.

Based on our experiences in the “ALARM Information Security” project and in previous security projects with a focus on “the human factor” and with a wide variety of target groups and actors, this is achieved through visualization, narration, and reducing complexity, while at the same time building an understanding of complex conditions. This would probably also bring people closer to the technologies of the future: they should be informed in a participatory manner, be involved in discussions that promote understanding, be able to engage proactively, and take part on an equal footing [91].

Peter Danil (2023) from the BSI recently reiterated the following point: “Everyone is under attack. There are no exceptions!” [92]; and as Tim Berghoff (2023) puts it, “Neither criminals nor industrial spies are interested in the size of a company.” [93] What is of interest are the products, the content, the business processes, the structure, the partners, and the business relationships (as well as the private relationships that make people vulnerable to blackmail). The EU’s NIS 2 directive is intended, among other things, to strengthen security along the value and supply chains [93]). According to Berghoff (2023), it is already clear here that more companies will be directly affected by NIS 2 than many IT managers would assume [93].

Our evaluation results from the developed learning scenarios can be summarized as follows [94]:

- Gamified security awareness in the form of the serious games developed is taken seriously by the participants. They are viewed as an important element in enhancing information security and are also thought to have a revitalizing effect. This means that when playing the learning scenarios, all participants were motivated, in a good mood, and concentrated, and everyone was also on task when it came to feedback during the review.
- In our experience, we have succeeded with the help of gamification in bringing awareness-raising measures to a level that ensures the involvement of participants. The awareness-raising performance of the learning scenarios significantly exceeds that of the usual learning theory approaches and works well with all participating groups.
- The didactic concept on which the learning scenarios are based in the “ALARM Information Security” project—“Talking Security”—also works smoothly in SMEs. Above all, the discursive setting and the team-oriented interactions in the analog learning scenarios promote

conversations about “real-life situations” and confirm the project’s suitability as a simulation of real work and everyday scenarios.

Our discursive, team-oriented storytelling approach is also borne out internationally. Leitner (2023) uses dynamic surveys in the digital awareness exercises, which go beyond our customizable digital learning scenarios, in order to visualize individual decisions for all participants during the digital exercise [95]. We can summarize our essential aspects according to Leitner (2023) as follows [95]: The story must be

- captivating, inspiring participants, while getting them to concentrate;
- interactive, actively involving participants by having them make decisions;
- informative, so that participants receive immediate feedback on their decisions;
- security conscious, including one or more security incidents;
- comprehensible and close to the reality of participants; and
- involving, ensuring that participants submit their [digital] decisions, with answers typically anonymized.

It should also be noted that a training approach that only emphasizes the technical aspects not only does not work [96] but the resulting overtaxing of most employees with too much technical information can even have a negative effect through the training [97]. In addition, it has been scientifically recognized for decades that a mix of different methods is necessary for different target groups, different learning types, and abstract topics (see, for example, [98], [99]). Alshaikh et al. (2018) confirms that linking information security with the private lives of employees on the topic of information security has a motivating effect [100]. In addition, international study results suggest that informal methods for increasing employees’ security awareness are effective and cost-effective and measures to promote the exchange of advice can lead to an improved security situation [101].

Looking ahead, we assumed that an interdisciplinary team will definitely have to integrate psychological aspects and tests for ISA in future awareness projects. According to Sykosch (2022), the established quality criteria for psychological tests are objectivity, reliability, validity, scalability, normalization, economics, usefulness, reasonableness, non-falsifiability, and fairness [102]. The first [90] and second study [94] of the “ALARM Information Security” project showed that no two German SMEs are the same. This has an impact on the fit and use of the learning scenarios developed in the project, even if no fine-grained differentiation was diagnosed in the project owing to the need for basic awareness raising. SMEs must therefore think about which learning scenario—provided free of charge—can be used sensibly for which target group, at what time, and in what way. To achieve this, employees should be trained as moderators. Moderators for awareness-raising measures within an SME would have the task of using practical, pictorial, narrative methods and formats in order to illustrate relevant but abstract topics and thus eliminate significant barriers to information security within the SME.

We also recognized that the level of maturity of the German SME is obviously crucial for the sustainable use of such modern simulations. The project also made it clear that the awareness maturity level correlates with the digital autonomy of employees. If the digital autonomy of employees in SMEs is not promoted, then measures to increase security awareness will remain ineffective because employees will feel disempowered, and they will not accept the security measures. This can, in turn, lead to (unconscious) resistance and, as a result, to new security incidents. Sensitization and security awareness are therefore “internal social work” [90, 94] and require role modeling from managers, a discourse about concrete experiences with security measures and their necessity within business processes, and the active involvement of employees in the improvement processes. In combination with the idea of “giving SMEs more of a hand,” consulting companies could also have their employees trained in experience-oriented moderation to provide better support.

So, as a first step, it is to be hoped that many German SMEs will seize this opportunity to increase the necessary information security awareness (ISA) in their company and proactively implement our tools from the “Awareness Lab SME (ALARM) Information Security.” Memorable stories (narratives, storytelling) should be developed about the security situation that use imagination and metaphors to help reduce topic complexity and simplify security communication. Above all, we advocate systemic communication with,

in particular, “discursive didactics” and an increase in the principle of “talking security” in SME business processes.

ACKNOWLEDGMENTS

I am grateful to our long-standing security awareness partner, the firm known_sense, and the other subcontractors, Gamebook Studio GmbH, Thinking Objects GmbH, and sudile GbR, whose individual input on the project is documented on the project website. A special word of thanks to my university research team (in various constellations) for their great commitment to all of our projects. 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.

FUNDING

As project manager and initiator of all the security awareness projects at TH Wildau mentioned here, I would like to thank the German Federal Ministry for Economic Affairs and Climate Action (BMWK) for funding the current project, “Awareness Lab SME (ALARM) Information Security,” which runs from October 2020 to March 2024.

TRAINING COURSES AND AWARENESS-RAISING EVENTS

Training courses and awareness-raising events after the end of the project “Awareness Lab SME (ALARM) Information Security” can be booked through the Technology Transfer and Continuing Education Center at TH Wildau (TWZ e.V.) at the Wildau Institute for Innovative Teaching, Lifelong Learning, and Design Evaluation (WILLE): <https://twz-ev.org/institute/wildau-institut-fuer-innovative-lehre-lebenslanges-lernen-und-gestaltende-evaluation/#tab-id-1>.

REFERENCES

- [1.] BSI—Bundesamt für die Sicherheit in der Informationstechnik/Federal Office for Information Security (Ed.), Die Lage der IT-Sicherheit in Deutschland/The situation of IT security in Germany (in German). Retrieved November 7, 2023, from <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410>, 2023.
- [2.] F. Quader, VP. Janeja, Insights into organizational security readiness: Lessons learned from cyber-attack case studies. *Journal of Cybersecurity and Privacy*, 1/4 (2021) 638-659.
- [3.] M. Scholl, E.P. Ehrlich. Information Security Officer: Job profile, necessary qualifications, and awareness raising explained in a practical way, Buchwelten-Verlag, Frankfurt am Main, 2020.
- [4.] Y. Li, N. Zhang, M. Siponen, Keeping secure to the end: a long-term perspective to understand employees’ consequence-delayed information security violation, *Behaviour & Information Technology*, 2018. doi: 10.1080/0144929X.2018.1539519.
- [5.] I. Henseler-Unger, A. Hillebrand, Aktuelle Lage der IT-Sicherheit in KMU/ Current situation of IT security in SMEs (in German), *Datenschutz und Datensicherheit (DuD)*427(2018), 686–690. <https://doi.org/10.1007/s11623-018-1025-y>.
- [6.] DIHK—Deutscher Industrie- und Handelskammertag e. V. (Ed.). Zeit für den digitalen Aufbruch: Die IHK-Umfrage zur Digitalisierung/Time for the digital awakening: The IHK survey on digitization (in German). Retrieved November 2, 2023, from <https://www.ihk.de/blueprint/servlet/resource/blob/5488158/8d01cc3ef58c3a251d6520f2ac4653b2/ergebnisse-der-ihk-digitalisierungsumfrage-data.pdf>, 2022.

- [7.] BSI—Bundesamt für die Sicherheit in der Informationstechnik/Federal Office for Information Security (Ed.), ORP.3: Sensibilisierung und Schulung/Sensitization and training (in German). Retrieved January 17, 2018, from https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html, 2016.
- [8.] A. Tsohou, M. Karyda, S. Kokalakis, E. Kiountouzi, Analyzing trajectories of information security awareness, *Information Technology & People*, 25 (2012), 327-335.
- [9.] G. Stewart, D. Lacey, Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, 20 (2012), 29-38.
- [10.] I. Kirlappos, A. Beaument, M.A. Sasse, 'Comply or die' is dead: Long live security-aware principal agents, in: A.A. Adams, M. Brenner, M. Smith (Eds.), *Financial Cryptography and Data Security, Lecture Notes in Computer Science*, Springer, Heidelberg, 2013, 7862, 70-82.
- [11.] T. Fagade, T. Tryfonas, Security by compliance? A study of insider threat implications for Nigerian banks, in: T. Tryfonas, (Ed.), *Human Aspects of Information Security, Privacy, Trust, HAS 2016, Lecture Notes in Computer Science*, Springer, Cham., 2016, 9750, 128-139.
- [12.] D. Pokoyski, Security Awareness: Von der Oldschool in die Next Generation – eine Einführung, in: M. Helisch, D. Pokoyski, (Eds.), *Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*, Vieweg+Teubner. Wiesbaden, 2009, 1–8.
- [13.] B. Khan, K.S. Alghathbar, S.I. Nabi, M.K. Khan, Effectiveness of information security awareness methods based on psychological theories, *African Journal of Business Management*, 5/26 (2011) 10862–10868.
- [14.] M. Beyer, S. Ahmed, K. Doerlemann, S. Arnell, S. Parkin, A. Sasse, N. Passingham, Awareness is only the first step: A framework for progressive engagement of staff in cyber security. Hewlett Packard, Business White Paper, 2016.
- [15.] M. Scholl, F. Fuhrmann, D. Pokoyski, Information security awareness 3.0 for job beginners, in: J.E. Varajão, M.M. Cruz-Cunha, R. Martinho, R. Rijo, N. Bjørn-Andersen, R. Turner, D. Alves (Eds.), *Proceedings of the Conference on ENTERprise Information Systems (CENTERIS)*, 2016, 433-436.
- [16.] H. Kruger, L. Drevin, T. Steyn, Email security awareness: A practical assessment of employee behavior, in: L. Fitcher, R. Dodge (Eds.), *Fifth World Conference on Information Security Education, IFIP – International Federation for Information Processing*, Springer, Boston/MA, 2007, 237, 33-40.
- [17.] K. Aytes, C. Terry, Computer security and risky computing practices: A rational choice perspective, *Journal of Organizational and End User Computing*, 16, 2004, 22-40.
- [18.] M. Scholl, Information Security Awareness in Public Administrations, in: U. Comite, *Public Management and Administration*, Open Access: INTECH d.d.o. Rijeka (InTechOpen). Retrieved January 6, 2024, from <https://www.intechopen.com/chapters/59667>, 2018.
- [19.] M. Scholl, F. Fuhrmann, L.R. Scholl, Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices, in: *Proceedings of the 51th Hawaii International Conference on System Sciences (HICSS)*, Big Island, Hawaii, 2018, 2235-2244. Retrieved January 20, 2018, from <http://hdl.handle.net/10125/50168>.
- [20.] S. Alotaibi, S. Furnell, Y. He, Towards a Framework for the Personalization of Cybersecurity Awareness, in: *International Symposium on Human Aspects of Information Security and Assurance*, Springer Nature Switzerland, Cham, 2023, 143-153.
- [21.] Homepage of the project “Awareness Lab SME (ALARM) Information Security”. Retrieved February 2, 2024, from, <https://alarm.wildau.biz/> (German), <https://alarm.wildau.biz/en> (English), 2023.

- [22.] M. Scholl, R. Schuktomow, H. von Tippelskirch, F. Prott, P. Koppatz, D. Pokoyski, U. Küchler, M. Vogt, Neue Wege für mehr Informationssicherheit in M. Scholl (ed.), *KMU: Projektdokumentation Awareness Labor KMU (ALARM) Informationssicherheit*, Buchwelten Verlag, Frankfurt/M, 2024, 232.
- [23.] AGCS—Allianz Global Corporate & Specialty SE (Ed.), Allianz risk barometer 2022 (English version: worldwide results). Retrieved September 12, 2022, from https://www.allianz.com/en/press/news/studies/220118_Allianz-Risk-Barometer-2022.html
- [24.] AGCS—Allianz Global Corporate & Specialty SE (Ed.), Allianz Risk Barometer 2022 (German version: results of Germany). Retrieved February 10, 2024, from <https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press-de.html>.
- [25.] M. Bada, A.M. Sasse, J.R. Nurse, Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *ArXiv*, abs/1901.02672; 2019.
- [26.] E. Tanriverdiyev, The state of the cyber environment and national cybersecurity strategy in developed countries. *Studia Bezpieczeństwa Narodowego*. 23/1 (2022) 19-26. <https://doi.org/10.37055/sbn/149510>.
- [27.] R.C. Sharma, A. Zamfiroiu, Cybersecurity Threats and Vulnerabilities in the Metaverse, in: 2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA), IEEE, 2023, 1-7. doi: 10.1109/iMETA59369.2023.10294950.
- [28.] T.O. Abrahams, S.K. Ewuga, S.O. Dawodu, A.O. Adegbite, A.O. Hassan, A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection, *Computer Science & IT Research Journal*, 5/1 (2024), 1-25.
- [29.] C. Posey, M. Shoss, Employees as a Source of Security Issues in Times of Change and Stress: A Longitudinal Examination of Employees' Security Violations during the COVID-19 Pandemic. *Journal of Business and Psychology*, (2023), 1-22.
- [30.] M. Helisch, D. Pokoyski (Eds.), *Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*, Vieweg+ Teubner, Wiesbaden, 2009.
- [31.] R. Epstein, V.R. Zankich, The surprising power of a click requirement: How click requirements and warnings affect users' willingness to disclose personal information. *PLoS ONE* 17/2 (2022): e0263097. <https://doi.org/10.1371/journal.pone.0263097>.
- [32.] H. Paananen, M. Siponen, Organization Members Developing Information Security Policies: a Case Study. Rising like a Phoenix: Emerging from the Pandemic and Reshaping Human Endeavors with Digital Technologies. *ICIS*, 2023. Retrieved from https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/14
- [33.] I. Kirlappos, M.A. Sasse, What usable security really means: Trusting and engaging users, in: *Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 2*, Springer International Publishing (2014), 69-78.
- [34.] Landing page. Summary of projects. The project "IT-Sicherheit@KMU"/IT Security@SMEs (in German) was funded by the Land Brandenburg with ESF. Retrieved February 10, 2024, from <https://wildau.biz/>.
- [35.] F. Fuhrmann, M.C. Scholl, D. Edich, P. Koppatz, L.R. Scholl, K.B. Leiner, E.P. Ehrlich, Informationssicherheitsbewusstsein für den Berufseinstieg. Final report of the Project "SecAware4job" (in German), Shaker, Aachen, 2017. doi: 10.2370/9783844054668.
- [36.] Project website "SecAware4job". The project was financed by the Horst Görtz Foundation (HGS). Retrieved February 10, 2024 from, <https://secaware4job.wildau.biz/>.
- [37.] known_sense (homepage). Compliance parcourses. Retrieved January 4, 2024, from <https://www.known-sense.de/compliance-parcours>.
- [38.] Methodpedia website. Retrieved January 4, 2024, from <https://methopedia.eu/de/posts/learning-stations/learning-stations/>.

- [39.] Project website “ALARM Information Security” (handout overview of analog learning scenarios). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/21fb54f246157ed6a1668ee840dfec0f/handout-aLS-A4-final.pdf>.
- [40.] Project website “ALARM Information Security” (moderation instructions of analog learning scenario 1). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/64c89b39ca8fd082ca46962fd7dcfcd8/moderation.pdf>.
- [41.] Project website “ALARM Information Security” (construction manual of analog learning scenario 1). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/fdb35a8e957e2b77ead449be5610b035/konstruktion.pdf>.
- [42.] Project website “ALARM Information Security” (handout of analog learning scenario 1). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/1a931bd03a1cc07d7aa195d8ca515ee3/handout.pdf>.
- [43.] Project website “ALARM Information Security” (overview and print templates as ZIP file of analog learning scenario 1). Retrieved July 31, 2024, from <https://alarm.wildau.biz/als1/>.
- [44.] M. Scholl, German SMEs & Home Office: Narrative-Driven Game-Based Awareness Raising with Long-Term Efficacy, in: S. Mistretta, Reimagining Education - The Role of E-learning, Creativity, Technology in the Post-pandemic Era, IntechOpen, London, 2023. Retrieved January 6, 2024, from <https://www.intechopen.com/online-first/1171513>.
- [45.] Project website “ALARM Information Security” (moderation instructions of analog learning scenario 2). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/4e3dd32ac8b65dffdfc6248d5a2899c1/moderation.pdf>.
- [46.] Project website “ALARM Information Security” (construction manual of analog learning scenario 1). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/4069f8d7ea17cad084dc0f8b49e452c1/konstruktion.pdf>.
- [47.] Project website “ALARM Information Security” (handout of analog learning scenario 2). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/7ef7165382627cd57d9a2b60f20caa27/handout.pdf>.
- [48.] Project website “ALARM Information Security” (overview and print templates as ZIP file of analog learning scenario 2). Retrieved July 31, 2024, from <https://alarm.wildau.biz/als2/>.
- [49.] Project website “ALARM Information Security” (moderation instructions of analog learning scenario 3). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/03a867dc24427973dfe941f4f90694de/moderation.pdf>.
- [50.] Project website “ALARM Information Security” (construction manual of analog learning scenario 3). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/0e2cda8206ac30f3381b61431da1f295/konstruktion.pdf>.
- [51.] Project website “ALARM Information Security” (handout of analog learning scenario 3). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/5fdc750bb6399eaf7c42c06aee294d9a/handout.pdf>.
- [52.] Project website “ALARM Information Security” (overview and print templates as ZIP file of analog learning scenario 3). Retrieved July 31, 2024, from <https://alarm.wildau.biz/als3/>, 2023
- [53.] M. Scholl, Raising Awareness of CEO Fraud in Germany: Emotionally Engaging Narratives Are a MUST for Long-Term Efficacy, in: Á. Rocha, C. Ferrás, W. Ibarra, Information Technology and Systems, Springer International Publishing, Cham, 2023. doi: 10.1007/978-3-031-33258-6_40.
- [54.] Project website “ALARM Information Security” (moderation instructions of analog learning scenario 4). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/1f91fc14e336446b8d14b649c47c4bcd/moderation.pdf>.
- [55.] Project website “ALARM Information Security” (construction manual of analog learning scenario 4). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/ee318d5d31472905f9beb598529ba621/konstruktion.pdf>.

- [56.] Project website “ALARM Information Security” (handout of analog learning scenario 4). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/dffcfb290b5264185532b7ce21e43580/handout.pdf>.
- [57.] Project website “ALARM Information Security” (overview and print templates as ZIP file of analog learning scenario 4). Retrieved July 31, 2024, from <https://alarm.wildau.biz/als4/>, 2023
- [58.] Project website “ALARM Information Security” (moderation instructions of analog learning scenario 5). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/a09006b5358532fffd1ef9dc8232cd9/moderation.pdf>.
- [59.] Project website “ALARM Information Security” (construction manual of analog learning scenario 5). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/49f710e6d0dc14e82c2634533fb0601f/konstruktion.pdf>.
- [60.] Project website “ALARM Information Security” (handout of analog learning scenario 5). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/0abb531a6825528d233fa0eee85d7fe/handout.pdf>.
- [61.] Project website “ALARM Information Security” (print templates of analog learning scenario 5). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/d3a36f8873ae241bf327242ae37baf6f/druckvorlagen.pdf>.
- [62.] Project website “ALARM Information Security” (moderation instructions of analog learning scenario 6). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/16cf17b914c4dcd92e8ccd8b8d193a31/moderation.pdf>.
- [63.] Project website “ALARM Information Security” (construction manual of analog learning scenario 6). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/402265cad09aa5d2722b4ac0cf3d1f27/konstruktion.pdf>.
- [64.] Project website “ALARM Information Security” (handout of analog learning scenario 6). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/c821510cf4c34138161e22057cbf0dd2/handout.pdf>.
- [65.] Project website “ALARM Information Security” (overview and print templates as ZIP file of analog learning scenario 6). Retrieved July 31, 2024, from <https://alarm.wildau.biz/als6/>.
- [66.] Project website “ALARM Information Security” (moderation instructions of analog learning scenario 7). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/a732b3d5f31a1732b0a05b0d68451943/moderation.pdf>.
- [67.] Project website “ALARM Information Security” (construction manual of analog learning scenario 7). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/e77b171bec8e36204d9e4f604fcc508d/konstruktion.pdf>.
- [68.] Project website “ALARM Information Security” (handout of analog learning scenario 7). Retrieved July 31, 2024, from <https://alarm.wildau.biz/static/a1111e0d37e4d6a93d365ace3a77b9ed/handout.pdf>.
- [69.] Project website “ALARM Information Security” (overview and print templates as ZIP file of analog learning scenario 6). Retrieved July 31, 2024, from <https://alarm.wildau.biz/als7/>.
- [70.] Project website “DIZ”. Retrieved July 31, 2024, from <https://diz.wildau.biz/index-en.html>.
- [71.] Project website “DIZ”. Digital roulette. Retrieved January 4, 2024, from <https://diz.wildau.biz/roulette/index.html#0>.
- [72.] Project website “ALARM Information Security”. Storykonzept der digitalen Serious Games (PDF)/Story concept of digital serious games (in German). Retrieved January 4, 2024, from <https://alarm.wildau.biz/static/68a7aaceafb85c9e2b8e6ee7a3f3d557/handout-dLS-A4-final.pdf>.
- [73.] Project website “ALARM Information Security”. TO (Hrsg.), INFOBLATT – Security kompakt zum Thema CEO Fraud für Endanwender:innen (Mai 2023)/TO (Ed.), INFO SHEET – Security compact on the topic of CEO fraud for end users (in German) (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/51370b1daaac6d3627f907f6dd44320d/infoblatt-ceo-fraud.pdf>.

- [74.] Project website “ALARM Information Security”. TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema CEO Fraud für Geschäftsführung und IT-Verantwortliche (in German) (Mai 2023)/TO (Ed.), Low-threshold security concept on the topic of CEO fraud for management and IT managers (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/4113fae4179e3edfd988f780eac72377/sicherheitskonzept-ceo-fraud.pdf>.
- [75.] Project website “ALARM Information Security”. TO (Hrsg.), INFOBLATT – Security kompakt zum Thema E-MAIL-CHECK für Endanwender:innen (in German) (Mai 2023)/TO (Ed.), INFO SHEET – Security compact on the topic of E-MAIL CHECK for end users (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/1339d766094b7540eb3917dfd16efd47/infoblatt-e-mail-check.pdf>.
- [76.] Project website “ALARM Information Security”. TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema Passwörter für Geschäftsführung und IT-Verantwortliche (Mai 2023)/TO (Ed.), Low-threshold security concept on the subject of passwords for management and IT managers (in German) (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/2490c04004c3fed16c4e42f8c023b6aa/sicherheitskonzept-passwoerter.pdf>.
- [77.] Project website “ALARM Information Security”. TO (Hrsg.), INFOBLATT – Security kompakt zum Thema Hacking für Endanwender:innen (Mai 2023)/TO (Ed.), INFORMATION SHEET – Security compact on the subject of hacking for end users (in German) (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/3b7be8d4e19aeb0acbdf2725aff83025/infoblatt-hacking.pdf>.
- [78.] Project website “ALARM Information Security”. TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema Schutzmaßnahmen BestPractice für Geschäftsführung und IT-Verantwortliche (August 2023)/TO (Ed.), Low-threshold security concept on the topic of best practice protective measures for management and IT managers (in German) (August 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/c01309141eb514821ae4f062018ea316/sicherheitskonzept-hacking.pdf>.
- [79.] Project website “ALARM Information Security”. TO (Hrsg.), INFOBLATT – Security kompakt zum Thema Phishing für Endanwender:innen (Mai 2023)/TO (Ed.), INFORMATION SHEET – Security compact on the subject of phishing for end users (in German) (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/2930c5b73cae1bf26d4cad18918d160b/infoblatt-phishing.pdf>.
- [80.] BSI—Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.)/Federal Office for Information Security (Ed.) (2019). Checkliste von BSI und Polizei (ProPK): Phishing vom 30.10.2019 / Checklist from BSI and police (ProPK): Phishing from October 30, 2019 (in German). Retrieved January 11, 2024, from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/BSI-ProPK-Checkliste-Phishing.pdf?__blob=publicationFile&v=1.
- [81.] Project website “ALARM Information Security”. TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema Phishing für Geschäftsführung und IT-Verantwortliche (August 2023)/TO (Ed.), Low-threshold security concept on the subject of phishing for management and IT managers (in German) (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/18bef186ff53794592b6e72b5c372472/sicherheitskonzept-phishing.pdf>.

- [82.] BSI—Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.)/Federal Office for Information Security (Ed.), “Smishing”: SMS-Phishing im Herbst 2021 mit neuen Betrugsmaschinen (2021) (in German). Retrieved January 11, 2024, from https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smishing_SMS-Phishing_141021.html.
- [83.] Project website “ALARM Information Security”. TO (Hrsg.), INFOBLATT – Security kompakt zum Thema Smishing für Endanwender:innen (Mai 2023)/TO (Ed.), INFO SHEET – Security compact on the topic of smishing for end users (in German) (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/807b021566fa7de971256a7804a06d0c/infoblatt-smishing.pdf>.
- [84.] Project website “ALARM Information Security”. TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema Smishing für Geschäftsführung und IT-Verantwortliche (Mai 2023)/TO (Ed.), Low-threshold security concept on the topic of smishing for management and IT managers (in German) (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/b092a1f2e1f8f26e3d2653b642e137e3/sicherheitskonzept-smishing.pdf>.
- [85.] Project website “ALARM Information Security”. TO (Hrsg.), INFOBLATT – Security kompakt zum Thema Tailgating für Endanwender:innen (Mai 2023)/TO (Ed.), INFORMATION SHEET – Security compact on the topic of tailgating for end users (in German) (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/c69f8ff7c21c42f7682e96d34355b164/infoblatt-tailgating.pdf>.
- [86.] Project website “ALARM Information Security”. TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema Tailgating für Geschäftsführung und IT-Verantwortliche (in German) (Mai 2023)/TO (Ed.), Low-threshold security concept on the topic of tailgating for management and IT managers (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/9b0746bca2b4de7e3cb093bbf7aa7db0/sicherheitskonzept-tailgating.pdf>.
- [87.] Project website “ALARM Information Security”. TO (Hrsg.), INFOBLATT – Security kompakt zum Thema Vorfallsmeldung für Endanwender:innen (Mai 2023)/TO (Ed.), INFORMATION SHEET – Security compact on the topic of incident response for end users (in German) (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/e1ddf24caf73b4f705d3203995171dd/infoblatt-vorfallsmeldung.pdf>.
- [88.] Project website “ALARM Information Security”. TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema Incident Response für Geschäftsführung und IT-Verantwortliche (Mai 2023)/TO (Ed.), Low-threshold security concept on the subject of incident reporting for management and IT managers (in German) (May 2023). Retrieved December 20, 2023, from <https://alarm.wildau.biz/static/c833bc1d2a42cc26040b0f2648d719bf/sicherheitskonzept-incident-response.pdf>.
- [89.] BSI—Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.)/Federal Office for Information Security (Ed.) (2023) Business Continuity Management. BSI-Standard 200-4. (pp. 310, in German), Reguvis Fachmedien GmbH, Bonn, 2023. Retrieved January 11, 2024, from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschrift/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8.
- [90.] D. Pokoyski, I. Matas, A. Haucke, Qualitative Wirkungsanalyse Security Awareness in KMU: Tiefenpsychologische Grundlagenstudie im Projekt Awareness Labor KMU (ALARM) Informationssicherheit. M. Scholl (Ed.), Technische Hochschule Wildau, Wildau, 2021. Retrieved September 5, 2023, from <https://alarm.wildau.biz/static/d6490e49f8d31adfa35259134b8d1b9d/220316-alarm-studie-final.pdf>.

- [91.] M. Scholl, Sustainable Information Security Sensitization in SMEs: Designing Measures with Long-Term Effect, in: University of Hawai'i at Manoa (Ed.), Proceedings of the 56th Hawaii International Conference on System Sciences, Honolulu, HI: University of Hawai'i at Manoa, Hamilton Library, 2023. <https://hdl.handle.net/10125/103369>, (CC BY-NC-ND 4.0), 6058-6067.
- [92.] P. Danil (BSI – Bundesamt für die Sicherheit in der Informationstechnik/Federal Office for Information Security). IT-Sicherheit für KMU/ IT security for SMEs (in German). Webinar der IHK Koblenz am 14.11.2023, 13:30-14:30 Uhr. Retrieved November 17, 2023, from <https://www.ihk.de/koblenz/unternehmensservice/digitalisierung/aktuelle-trends-5879040>.
- [93.] T. Berghoff, Mit NIS-2 wird IT-Sicherheit zur Chefsache. Security Insider vom 22.11.2023, online. Retrieved November 23, 2023, from <https://www.security-insider.de/mit-nis-2-wird-it-sicherheit-zur-chefsache-a-cc064ecceaa1e4fdcf500c3b22f847b4/>.
- [94.] D. Pokoyski, A. Haucke, A., Enabling vs. Entmündigung: Qualitativer Konzepttest analoger Security Awareness-Lernszenarien für KMU im Projekt Awareness Labor KMU (ALARM) Informationssicherheit/Enabling vs. incapacitation: Qualitative concept test of analog security awareness learning scenarios for SMEs in the Awareness Labor SME (ALARM) information security project. Scholl, M. (Hrsg.), Technische Hochschule Wildau, Wildau, 2022. <https://alarm.wildau.biz/static/c0e4d00beefe1dc5fac9b50b6087265f/studie-2-master-final.pdf>. Letzter Zugriff: 05.09.2023.
- [95.] M. Leitner, A Scenario-Driven Cyber Security Awareness Exercise Utilizing Dynamic Polling: Methodology and Lessons Learned, in: Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023), 634-642. Copyright 2023 by SCITEPRESS – Science and Technology Publications, Lda, under CC license (CC BY-NC-ND 4.0). doi: 10.5220/0011780400003405.
- [96.] S.H. von Solms, J. du Toit, E. Kritzinger, Another Look at Cybersecurity Awareness Programs, in: International Symposium on Human Aspects of Information Security and Assurance, Springer Nature Switzerland, Cham, 2023, 13-23. https://doi.org/10.1007/978-3-031-38530-8_2.
- [97.] B. Alkhazi, M. Alshaikh, S. Alkhezi, H. Labbaci, Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. IEEE Access, 10, 2022, 132132-132143.
- [98.] P. Eyerer, D. Krause, Methoden-Mix erhöht die Lehr-Lern-Effektivität und deren Effizienz/Method mix increases the teaching-learning effectiveness and its efficiency (in German), Neues Handbuch Hochschullehre/New handbook for university teaching 36, 2009.
- [99.] B. Hoffmann, U. Langefeld, Methoden-Mix. Unterrichtliche Methoden zur Vermittlung beruflicher Handlungskompetenz in kaufmännischen Fächern/Teaching methods for teaching professional skills in commercial subjects, 3, 1998.
- [100.] M. Alshaikh, S.B. Maynard, A. Ahmad, An exploratory study of current information security training and awareness practices in organizations, in: Proceedings of the 51st Hawaii International Conference on System Sciences 2018, 5085-5094. <http://hdl.handle.net/10125/50524> ISBN: 978-0-9981331-1-9 (CC BY-NC-ND4.0),
- [101.] S. Farshadkhah, M. Maasberg, T.S. Ellis, C. van Slyke, An Empirical Examination of Employee Information Security Advice Sharing, Journal of Computer Information Systems, (2023) 1-16. Retrieved August 1, 2023. <https://doi.org/10.1080/08874417.2023.2176947>.
- [102.] A. Sykosch, Zur Messbarkeit von IT-Sicherheitsbewusstsein. Dissertation, Universitäts- und Landesbibliothek Bonn, 2022. Retrieved November 19, 2023, from <https://bonndoc.ulb.uni-bonn.de/xmlui/bitstream/handle/20.500.11811/9568/6526.pdf?sequence=1&isAllowed=y>.