Chapter 2
Print ISBN: 978-81-970867-9-3, eBook ISBN: 978-81-970867-5-5

Play the Analog Game in a Digital World! Long-Term Gamification for Raising Information Security Awareness

Margit Scholl [a*]

DOI: 10.9734/bpi/cpstr/v6/8543A

Peer-Review History:
This chapter was reviewed by following the Advanced Open Peer Review policy. This chapter was thoroughly checked to prevent plagiarism. As per editorial policy, a minimum of two peer-reviewers reviewed the manuscript. After review and revision of the manuscript, the Book Editor approved the manuscript for final publication. Peer review comments, comments of the editor(s), etc. are available here: https://peerreviewarchive.com/review-history/8543A

ABSTRACT

Modernization in our society and a more dynamic way of working is inconceivable without the use of the latest digital information communication technology (ICT) systems. Government digital agendas and business activities worldwide want to promote digital transformation in businesses and public administrations while acknowledging the digital changes taking place in society and the need to integrate information security (IS). Although information communication technology (ICT) shapes our lives, we tend to have an insufficient knowledge of the risks involved, of IS, and of the General Data Protection Regulation (GDPR); this is compounded by carelessness in handling data and insufficient IS awareness (ISA). Backed by a clear conceptual approach, information security awareness training (ISAT) is also essential for everyone. However, classical training—merely knowledge-based—is currently failing to produce long-term results. Psychologically based research shows that a systemic approach might be helpful. This is where analog game-based learning (GBL) comes into play. This updated article documents a variety of learning materials for different target groups and associated training experiences from the last decade.

Keywords: Digitization; ICT; IS; GDPR; ISA; ISAT; GBL; security awareness-raising.

1. INTRODUCTION

Modernization in our society and a more dynamic way of working is inconceivable without the use of the latest digital information communication

[a] *Department Business, Computing, Law Technical University of Applied Sciences (TH) Wildau, 15745 Wildau, Brandenburg, Germany.*
**Corresponding author: E-mail: mscholl@th-wildau.de;*

technology (ICT) systems. ICT can provide powerful strategic and tactical tools for organizations which, if properly applied and used, could bring significant advantages in promoting and strengthening their competitiveness [1]. An ICT system is an ensemble of hardware, software, networks, and all the design and qualification processes involved in work and organization [1a:9]. However, ICT and digitization increasingly permeate all aspects of today's society. Business organizations can make more efficient, competitive, and innovative decisions through the use of ICT [1b]. The societal impacts of modern ICT include the digital divide, altered work structures in institutions, the rationalization and creation of new jobs, changed communication and social behavior, the emergence of virtual communities, etc. [1a:8].

The digital agendas of governments around the world want to lay the foundations for digital transformation (DT) and ensure added value for their countries. The European Digital Agenda [2] sought to keep abreast of digital networking and the digital changes in society; as the German Informatics Society (GI) pointed out in article 7 of its Ethical Guidelines in 2015, the design and implementation of ICT systems, including any control and monitoring techniques, should be combined with user involvement [1a:6]. Since then, however, very little consideration has been given to the integration of users in technology and platform development. For Germany, recent studies of digital services show this very clearly (see [3,4]). According to a study by McKinsey from 2018 [5], citizens' satisfaction with the authorities is lower than with private-sector actors.

Moreover, we are constantly confronted with global threats—phenomena that can be described in general terms and exist independently of specific areas of attack in the economy, state, and society. However, if, for example, a cyber threat such as a malware encounters a vulnerability, a concrete threat arises [6]. Weak points include software programming errors, technical deficiencies, and organizational deficits. Such vulnerabilities are exploited by attackers in cyberspace. This also includes the people operating the systems, who are often referred to in international security investigations as the actual weak point in the security chain (see, for example, [7]).

Ignorance of or non-observance of information security and corresponding operational guidelines pose significant risks for all institutions. The term information security (IS) refers to the protection of information of all types and origins [8:9]. Dangers result from human error, organizational deficiencies, intentional actions, technical failure, or unforeseeable circumstances. 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. The principle must be: "Digitization only with information security. Information security only with awareness."

The next section briefly summarizes the main scientific knowledge about the human side of IS and information security awareness training (ISATs) as well as some of the ethical responsibilities of informatics. Because Serious Games have great potential in the field of ISAT, section 3 discusses several examples of analog game-based learning scenarios for practice, which were also tested with different institutions in the USA. Section 4 provides a summary of the further development of serious games for different target groups. Section 5 presents some conclusions generated by previous findings.

2. THE HUMAN SIDE OF INFORMATION SECURITY AND ETHICS

According to the Federal Office for Information Security (BSI), information security awareness (ISA) should address the following threats and vulnerabilities [9]: insufficient knowledge of regulations, insufficient ISA, and carelessness in handling information. Tsohou et al. conclude from recent global security surveys that ISATs are not currently working [10]. 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 [11]. 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” [12], a third reason is that training aimed at addressing security awareness gaps is not sufficient to ensure compliance with a security culture [13].

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 [14-16]). Scholl et al. point out that 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 [17]. This is because IS and IT are about more than technology [18]. ICT systems involve human actors, and users do not always behave the way they are supposed to [19]. 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, [20,21]).

Politics and informatics have ethical responsibilities with regard to DT. For example, members of the GI are expected to expand their expertise to understand the rights and interests of the various stakeholders [1a:4]. This also includes the readiness to take part in interdisciplinary discussions [1a:4]. According to article 8, members of the GI who teach computer science should also instruct learners about their individual and shared responsibilities, while at the same time serving as role models [1a:6]. Acting together needs both individual and group reflection [1a:14].

Research activities in the last few years have concluded that humans are increasingly becoming the key to increasing information security. The research team at TH Wildau has also shown in various projects and studies with different project partners that the psychological background of security behavior must be given particular consideration when raising awareness of information security and data protection. This means that a lively and practical communication of threats and corresponding security measures is necessary in order to emotionally involve the participants, achieve active sensitization to promote motivation and create more lasting information security awareness [22].

3. PRIMARY ANALOG GAMIFICATION FOR A DIGITALLY BASED LIFE

In this context, “Security Awareness” means raising awareness to promote more active mindfulness. ISA learning methods should clarify threats, vulnerabilities, attacks, and possible damage as well as the main values of IS and data protection. The three basic values are confidentiality, integrity, and availability. Additional values include authentication, commitment, and reliability [9]. In many organizations, ISA and the training of relevant competences are often limited to knowledge-transfer measures. Based on psychologically based research (see [14,23,24]) on creating lasting sensitization and promoting security-related behaviors (see [25,23,15]), the game-based learning (GBL) methodology is becoming more important for ISA. Accordingly, the so-called “3.0 Systemic Approaches” of [17] were implemented and tested at TH Wildau in different projects, starting with the projects “IT-Sicherheit@KMU” (2013–2014) [26] and “SecAware4job” (2015–2017) [27]. Major campaigns for large companies like T-Systems, Alliance, BMW, and HP were also completed using the analog “Security Parcour” of our project partner, the firm known_sense [28]. This can be individually organized and branded specifically for a company, as was done by Deutsche Post [29]: this was discussed in 2018 at the event Take Aware in Berlin [30].

Serious Games have great potential to make valuable contributions to socially relevant areas such as education, health, and society (see [31,32]). For this reason, GBL is receiving increasing recognition as an effective teaching and learning method that improves motivation and triggers behavioral changes [33]. Emotionalizing must address people’s specific concerns. Psychological studies [24] show that people need to “understand”—through emotional engagement—that they are themselves affected. Analog GBL is especially effective as a means of stimulating motivation and should be explicitly used for ISAT because learners can directly see the consequences of their actions and get a sense of their knowledge level in dialogue.

The implementation of German-language GBL material for the “Security Arena” in training at TH Wildau was part of the project “IT-Sicherheit@KMU” [26]. Recent research suggests that emotional design is important for both analog and digital awareness-raising materials [34,22]. Adapted, analog GBL scenarios in the English-language “Security Arena” are part of the final results of the project “SecAware4job” [27,35]. Such serious games can be purchased through the firm known sense. The themes of the learning scenarios are listed below and complemented with learning tasks and goals (see Table 1).

Table 1. Analog GBL scenarios of the "Security Arena" from the TH Wildau project "SecAware4job" [25,20]

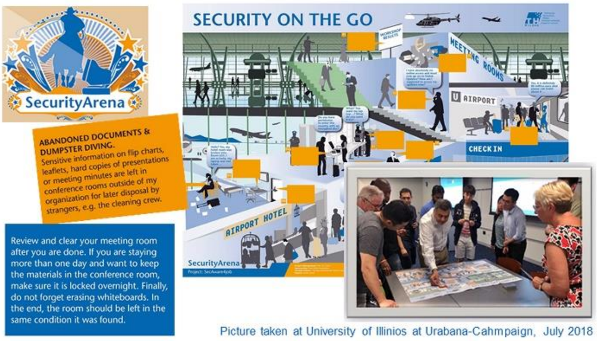
Learning scenario	Learning task	Learning goals
Clear Desk	Identify which items and information on the desk should be securely locked	Create awareness of a tidy workspace and the importance of safeguarding sensitive information
Data Security	Assemble phrases from two parts	Repeat and deepen knowledge
Internet Services	Assess the sample services and apps to determine eight risks	Know and discuss the risks of common Internet and app services
Phishing	Recognize phishing emails	Explain the criteria for detecting phishing emails
Security on the Go	Identify typical hazard scenarios in public spaces and assign appropriate protective measures	Create awareness of IS dangers and safeguards in public spaces and while travelling
Social Media	Recognize critical published images and information on social networks	Create awareness of safe behavior on social networks
Password Hacking	Guess passwords for a fictitious Facebook profile	Generate sensitivity to secure passwords and knowledge about hash values
Network Domino	Use game elements to lay out network architectures that meet the given requirements for security and functionality	Deepen knowledge of the operation of network components and sensible secure organization (infrastructure)
Incident Management	Cluster information security, privacy, and compliance incidents and assign to hotlines	Get to know sample IS, privacy, and compliance incidents and relevant reporting points
Social Engineering	Recognize the exploitation of human traits (social barriers) such as helpfulness and curiosity	Create awareness of the techniques of social engineering and social gateways

The research project SecAware4job sets out to develop and examine as many creative learning and teaching methods as possible to enable students, employees, and guests to more easily understand the complex of information security with all its facets (regulatory framework, norms and standards, protective measures, concepts, etc.) and make this issue more visual. The applied methodological framework is a learning station format ("Stationenlernen") that is derived from circuit training in sports. It is enhanced by elements of other learning methodologies such as GBL, blended learning, and authentic learning [27].

Each learning station is presented in a playful manner and consists of a five-minute introduction to a special topic (for example, “security on the go” in public spaces) that also integrates a dialogue between participants. There follows a phase of authentic learning in which the participants work as a team to solve real problems from everyday (professional) life. The teams of about ten people each receive points and discuss the solution, enabling immediate learning within a maximum of five minutes. All in all, one learning station needs approximately fifteen minutes. Playing four stations in parallel as a competition, it takes only one hour to sensitize about forty people. The completion of the learning stations is the prelude to addressing a topic in greater depth, involving as many interactive methods as possible. By way of repetition, these analog learning stations can be complemented by digital learning games in blended learning formats.

In the following, three examples of games are described in more detail. The first is *Security on the Go* (see Fig. 1). The game consists of an infographic map as a playing field. It is played in two rounds. The first round includes fourteen risk cards in orange, which describe the various security risk scenarios shown on the map; the players have to correctly match the cards to the situation shown. In the second round, fourteen defense cards in blue must be correctly matched to the orange card. Below are some potential questions that can be used to integrate people in team discussions and activities to foster interactive play:

- How do I perceive the behavior of my fellow travelers with regard to cell phone use?
- How can I obtain products for encrypting information?
- What does the term “shoulder surfing” mean?



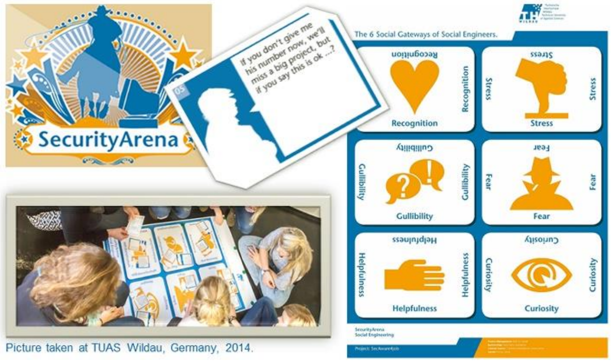
ABANDONED DOCUMENTS & DUMPSTER DIVING.
Sensitive information on flip charts, leaflets, hard copies of presentations or meeting minutes are left in or meeting rooms outside of my conference rooms outside of my organization for later disposal by strangers, e.g. the cleaning crew.

Review and clear your meeting room after you are done. If you are staying more than one day and want to keep the materials in the conference room, make sure it is locked overnight. Finally, do not forget erasing whiteboards. In the end, the room should be left in the same condition it was found.

Picture taken at University of Illinios at Urabana-Cahmpaign, July 2018

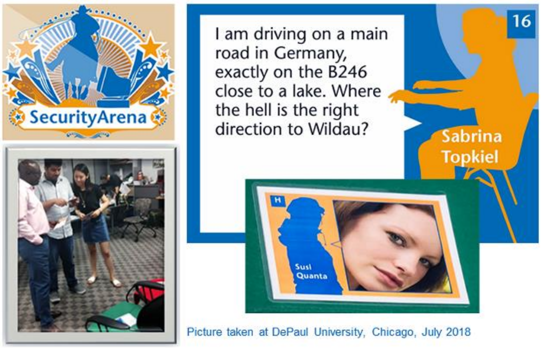
Fig. 1. Security Arena Game “Security on the Go,” developed by known_sense, adapted for TH Wildau, played with students (university and school), employees, and guests. The picture shows the game situation in the Science Lab Studio at the University of Illinois at Urbana-Champaign, USA, 2018. © TH Wildau & known_sense

The second game is *Social Engineering* (see Fig. 2), an attack focusing on human beings, which is often not well known. Research shows that social engineers used tricks to manipulate the so-called six social gateways of humans and bluff people in order to get access to information. The participants of the game have to place quote cards describing real situations onto the playing field with the six gateways. Some of the cards fit into multiple gateways and map fields—what is important here is the interactive discussion and exchange of experiences between all players.


SecurityArena
05
if you don't give me his number now, we'll miss a big project, but if you say this is ok ...?
The 6 Social Gateways of Social Engineers.
Recognition
Stress
Gullibility
Fear
Helpfulness
Curiosity

Picture taken at TUAS Wildau, Germany, 2014.

Fig. 2. Security Arena Game "Social Engineering," developed by known_sense, adapted for TH Wildau, played with students (university and school), employees, and guests at the TH Wildau, 2014. © TH Wildau & known_sense


SecurityArena
16
I am driving on a main road in Germany, exactly on the B246 close to a lake. Where the hell is the right direction to Wildau?
Sabrina Topkiel
H
Susi Quanta

Picture taken at DePaul University, Chicago, July 2018

Fig. 3. Security Arena Game "Social Media," developed by known_sense, adapted for TH Wildau, played with students (university and school), employees, and guests. The picture shows the game situation at the DePaul University, Chicago, USA, 2018. © TH Wildau & known_sense

The third game is *Social Media* (see Fig. 3). Here the background is that the Internet does not forget, and the questions are: Should I post this picture or not?

Should I post this text or not? In the discussion, the people have to demonstrate their knowledge of social media and of the relevant laws and regulations.

4. ADDITIONAL DEVELOPMENTS FOR DIFFERENT TARGET GROUPS

4.1 The Project “Security”

The project “Gender-Sensitive Study and Vocational Orientation for the Occupation Security Specialist” (“Security,” 2015–2017) [36] aims to arouse the interest of girls in the innovative and future-oriented occupation of security specialist. In the process, study courses and vocational training within the field of computer sciences should become more attractive for young women and the proportion of women in the field should increase. Based on an appealing and gender-sensitive presentation of the occupation of security specialist, portraits of female role models who are working in the field of information security, and an interactive and experience-oriented pilot event, female students will learn that these study courses and vocational training are not only technical but also very wide-ranging.

Female role models have existed in the field of computer sciences since its inception. Talking to women who have successfully shaped the information security field to cater to their professional and private lives and discussing their decision to engage in information security and their experiences as security specialists—their satisfaction, challenges, etc.—gave rise to a series of portraits, which are shown in a book, in posters, and in videos [36]. This should make female role models in the field of information security more visible for young women and society as a whole.

To get a clear impression of the job of security specialist, female students within the vocational orientation phase are invited to experience awareness-raising measures focused on information security in the form of analog and digital game-based learning scenarios. Here, they become acquainted with important aspects of information security—initiating, designing, choosing, supporting, and conducting awareness-raising and training measures to promote information security. We will design these game-based learning scenarios using a participative approach so that the scenarios take into account the day-to-day digital activities that are typical for girls of their age as well as their preferences, needs, and life situations. All in all, six analog GBL serious games with reduced complexity were developed in German together with known_sense and in cooperation with four schools in Berlin and Brandenburg. Their themes are [37]:

- *Apps and their risks*
- *Phishing*
- *Password hacking*
- *Encryption*
- *Secure on a school trip*
- *Image rights*.

4.2 The Project “SecAware4school”

In the project “Security awareness for schools” (“SecAware4school,” 2018–2020) [38], students (female, male, diverse) and their attachment figures (teachers and parents) were informed about the subject of information security and given a heightened awareness of its importance. It was essential that they acquire the habit of carefully handling personal data when using Internet services and social networks.

In order to communicate the abstract topic of information security and make it concrete and easily understandable for pupils, a variety of creative teaching and learning methods were used. This allows the basic knowledge of information security at the technical and organizational level to intersect with experience-oriented learning scenarios and coaching and mentoring concepts. The creative methods that are used include analog and digital simulations.

Pupils, teachers, and parents from five pilot program schools are taking part in the project. In each pilot school, two classes from grades 6, 9, and 11 took part with twenty students each. These were trained in line with their individual level and could then pass on the digital skills they have learned to younger grades. To achieve this, ten experience-oriented learning scenarios per grade with three different levels of difficulty have been developed, played, and/or modified. All those involved were given workshop training to expand their skills. The teachers were prepared in such a way that they could train, guide, and raise the awareness of new young safety advisors at the end of the project. The main focuses were [38]:

- Information Security: Why?
- Secure Operation of Smartphones
- Legal Framework for Information Security
- Security-Relevant Behavior
- Encryption and Digital Signatures.

In order to achieve the aims of the project, we have developed specific training and awareness-raising concepts suited to the target audience (students, parents, and teachers). In addition, we designed, tested, and evaluated the learning materials (e.g., experience-oriented learning scenarios). GBL and accelerated learning (AccL) approaches are transferred to experience-oriented learning scenarios in the field of information security. Previous studies have shown that it is particularly important to foster motivation and create an emotional connection in IS learning processes.

The project SecAware4school makes it possible to better assess the IS risks through selected methods that affect ordinary users. These methods

- promote communication skills, social interaction, and teamwork;
- explore real (problem) situations from everyday work life;
- make complex and abstract learning content concrete and tangible;

- provide direct feedback on students' learning progress;
- enable learning through a process of trial and error and repetition;
- are geared to the learners, their levels of knowledge, and their needs (learner-centered learning); and
- support the transfer and exchange of knowledge [38].

Taking into account the research findings from GBL and AccL, the project SecAware4school is dedicated to analog and digital learning scenarios. In combination, these can lead to a better assessment of the possibilities and dangers associated with information security. In light of this, the following learning scenarios have been developed at three levels of complexity in German (in sum thirty-three serious games) [39-41]. *Information Security*: This learning scenario is about practicing the use of technical terms in the area of information security. With the increasing amount of information and services available online, it is important to familiarize yourself with the relevant technical terms. *Digital Social*: This learning scenario focuses on individual behavior on social platforms online and on how you use your smartphone in your environment. The learning scenario is intended to stimulate discussion about your behavior toward other people and to raise critical awareness of the "new" media and its uses. *Security Surfer*: In the learning scenario "Security Surfer: Recognizing Dangers and Protective Measures," the Internet is looked at in global terms and its inner workings are examined in more detail. Surf through the ocean of the Internet, recognize the dangers, and find the right protective measures.

- *Social Networks*: In this learning station, the aim is to find solutions and contact persons in different situations and to be aware of proper and considerate interaction in social networks.
- *Storytelling*: This learning scenario helps to introduce students to a topic or provide more in-depth knowledge of it. In SecAware4school, the focus is on all aspects of information security.
- *Fake or Real*: In this scenario, you get to know various cases, terms, tools, and strategies that can be used to "falsify" current news and learn to optimize your own behavior.
- *Security Duel*: The learning scenario "Security Duel: Information Security in the Company" gives students the chance to determine potential points of attack in a company and identify suitable protective measures.
- *Data Espionage & Secure Space*: This learning scenario is ideal for raising awareness of possible safety-relevant objects in the workplace that require special storage.
- *Image Rights* (Digital): This learning scenario helps clarify the issue of image rights.
- *Hacker Terminal*: This learning scenario is good for delving into and repeating basic concepts of information security. In the role of the retro hacker, the goal is to use clues to guess "encrypted" passwords in order to locate possible access points and find a way into the system. Technical terms are learned, and the chain of association is reinforced.

- *Secure Passwords*: How do we handle passwords? This learning scenario shows some everyday examples of how to handle passwords. The goal here is to find the right approach to dealing with passwords in order to ensure maximum password security.

4.3 The Project “DIZ”

Two complex analog game scenarios were developed and tested as part of the project “Mittelstand 4.0 Kompetenzzentrum Stuttgart” (SME 4.0 Competence Center Stuttgart), in short, “Digitization Center” (“DIZ,” 2020–2021) [42]. These game scenarios were then tested by the IT security working group. The aim is to sensitize the employees of small and medium-sized companies to the topic of information security in a playful way. To help implement these measures, the project’s cooperation partners and the working group itself were to be provided with the two-game scenarios for their own events.

The project was focused on devising and developing two complex analog game-based learning scenarios for small and medium-sized companies with minor digital additions. For the target group in the manufacturing sector, the learning scenarios are focused on social engineering, while the emphasis shifts to security risk management for the group comprising middle management in production. The final results are summarized in [43,44].

GBL was used to allow learners to actively engage with content instead of being exposed to information passively (via lectures, videos, or reading). It offers the possibility of experimentation and allows mistakes to be made in the process. Learning games are motivating and support behavioral change [45:1]. The specific focus tailored to the particular target group is important for the design and conception of the project and for adjusting the material to the day-to-day experience of the target groups. This connection to real situations and challenges improves learning success [46:2].

Moreover, training must be distinguished from awareness raising. Sensitization measures should create awareness of information security and enable individual participants to recognize the importance of the topic, reflect on their own behavior and react accordingly [47:6]. Training, on the other hand, aims to build deeper knowledge and skills. The development of learning scenarios is primarily concerned with raising awareness. This should emotionalize the topics and motivate participants to engage with them, thus laying the foundation for continuous training.

The two developed complex serious games were [42-44]:

- *Social Engineering*: The BSI understands social engineering as a method that exploits human characteristics such as helpfulness, trust, fear, and respect for authority to gain unauthorized access to information or IT systems [48:7]. According to the study “Bluff Me If U Can,” the term social engineering often has positive associations [49:8]. However, this type of interpersonal manipulation is one of the most frequent types of attacks directed at companies in Germany for the purposes of data theft, industrial espionage, and sabotage [50:9]. Depending on the type of attack, a distinction can be made between technology-based and human-based social engineering attacks [51:10]. Technology-based attacks include phishing and the use of malware, while human-based attacks include identity change, identity theft, and shoulder surfing. The game-based learning scenario to be developed will take up the various aspects and facets of social engineering, taking into account psychological principles, and will incorporate the needs and specific characteristics of the manufacturing industry.

- *Security Risk Management***:** In general terms, risk management is defined in ISO Guide 73 as “coordinated activities for the management and control of an organization, taking into account risks” [52:11]. Security risk management takes information security risks into account. An introduction to risk management is provided by BSI Standard 200-3, which, among other things, provides guidance on threat identification, risk classification, and risk management so that the results can be integrated into the existing security concept [53:12]. The management of information security risks is also covered in ISO/IEC 27005 [54:13].

These learning scenarios are intended to sensitize the management of small and medium-sized enterprises (SMEs) to the fundamental importance of risk management and alert them to potential risks. The overall aim is to enable them to apply risk management, to detect weaknesses and thus to avoid and reduce risks, and, if necessary, to accept the residual risk. Risk management also includes communication with the security areas and the risk manager. The implicit intention of the scenario is therefore also to act as a kind of communication accelerator in mediating between management and security protagonists or risk managers.

4.4 The Project “ALARM Information Security”

SMEs collect, process, and use large amounts of sensitive data with the help of digital IT solutions. The problem is that these companies tend to underestimate the risks and dangers posed by ever more ingenious attackers. A lack of concern for or ignorance of information security, the violation of company guidelines on information security, or the absence of any such guidelines are all risks confronting businesses of all shapes and sizes. The numerous attack points in an enterprise represent defects in the security system. These can have delayed consequences for SMEs. This is where the multidisciplinary research project “Awareness Lab SME (ALARM) Information Security” (2020–2023/2024) [55] comes into play.

This project aims, over the space of three years, to create a complete scenario that ranges from raising awareness in SMEs and supporting them in the area of information security to creating tools to enable them to support themselves. Each project year is split into three consecutive phases, each manifesting as an agile and participative process. The phases are geared toward the development of innovative analog and digital learning scenarios, "on-site attacks," and scientific testing, including awareness measurements, quizzes, and tests. This whole scenario is intended to perform the vital task of raising awareness among executives and employees and thus lead to targeted staff development in SMEs and very small businesses (VSBs), which at present is not standard in these companies. The idea is to make IT security tangible and comprehensible by connecting it with digital processes, which are increasingly prevalent in the workplace. Participants will also be emotionally engaged and actively involved in the development of measures. This should create a durable culture of information security across the organization.

Working in cooperation with pilot SMEs and handicraft businesses, the project will systematically infer deficiencies and shortcomings within key business processes using defined activity protocols. Security and competence profiles will also be derived from the data. Measures will be developed in both analog and digital form with a view to activating ongoing and far-reaching awareness of security concerns. These measures will be thoroughly tested and evaluated in a real-world setting. Best-practice guidelines accompanied by success stories from the participating companies will be promulgated at the national level via associated transfer partners in a bid to appeal to other business concerns. Innovative measures to enhance in-house awareness in SMEs and VSBs are the prelude to a maturity assessment. The impact analyses are complemented by quality and outcome assurance combined with risk management and an accompanying evaluation. The networking of all participants will be promoted nationwide.

To implement the project's goals, specific training concepts, awareness-raising concepts, and learning materials, adjusted to the needs of SMEs, were developed, tested, and evaluated. GBL and AccL underpin the experience-oriented learning scenarios, which focus on the area of information security. All the materials that are developed will be free for all companies to use at the end of the project as downloads or via online platforms. This will promote a heightened awareness of IT security and raise security levels all across Germany. The themes of the training material are [55,56]:

- Analog serious games:
  - *Home office* (see also [57])
  - *Multi-factor authentication*
  - *Five phases of CEO fraud* (see also [58])
  - *Mobile communication*
  - *Cyber pairs*
  - *Data and information protection*
  - *Information class roulette*

- Digital serious games:
  - *The first day*
  - *The hacker's attack*

- ○ *The search for clues* (see also [58])
- ○ *AI* (artificial intelligence) *in the home office* (see also [57])
- ○ *Everything just cloud*
- ○ *Doing classifications*
- ○ *The ransomware attack*

- In situ simulations and security concepts:
- ○ *CEO fraud*
- ○ *E-mail check*
- ○ *Hacking*
- ○ *Phishing*
- ○ *Smishing*
- ○ *Tailgating*
- ○ *Incident reporting*

- Additional material:
- ○ Digital *self-test*
- ○ Digital *password hacking*
- ○ Flyers and brochures
- ○ Events and press reports
- ○ Scientific publications
- ○ Networking and partners.

5. CONCLUSION

Our various information security awareness projects over the last decade show that the awareness-raising topics used for different target groups are very similar. However, when gamified awareness-raising methods are being developed, the needs of the specific target group and their actual everyday environment must be taken into account. The complexity of the topics must be reduced in varying degrees: so that immersive stories can be used to talk about information security, the target group can be affected emotionally, and people can be motivated to live their increasingly digitalized lives more mindfully.

5.1 The Primary Experiences with Analog Serious Games

The aim of this paper is to explain concepts for analog GBL scenarios. Designing ISAT with analog scenarios, emotionalizing, and team-based exchange—as mentioned above—is extremely important for the motivation and successful sensitization of human actors in the field of IS. In-depth psychological studies show that emotionalizing and motivation are important factors in creating short-term scenarios in real-life situations using authentic learning (AL) and problem-based learning (PBL). Our own extensive experience with such learning materials and methods in projects and events suggests that ISA and the knowledge associated with it could be improved in almost all participants, and behavioral changes triggered.

For repetition and monitoring individual progress, simple digital GBL scenarios are also useful—e.g., a quiz app that was developed with twelve questions based on three main topics from the EU's GDPR chapter 3, art. 12–23. This will be used to explain data protection to students between the 7th and 13th grades using smartphones or tablets. The European Management Master (EMM) project team has used a free app called "Kahoot" to create the digital GBL scenario—i.e., the quiz. Using the result slide, the presenter will have the chance to explain the answers in more detail if many students had the wrong answer. However, digital GBL scenarios were not the focus of the primary paper.

Analog and digital serious games should be used in combination to raise ISA. As part of our ongoing research projects, we will perform a systematic evaluation with both GBL methodologies to get more durable results. Nevertheless, there is no simple linear cause-and-effect relationship between institutional safeguards and knowledge, attitudes, and real behavior. ISA remains a critical issue. Therefore, ISAT and programs must be developed as a user-centered approach. Moreover, a clear set of IS principles needs to be identified and communicated [12]. Learning in IS should be developed by integrating target-oriented, interactive analog/digital GBL scenarios and team-oriented methods as an ongoing process.

5.2 Findings from the Current Analog and Digital Developments

Previous studies and research work carried out in the projects described above have indicated that learning processes in the area of information security must involve learners' emotions (see, for example, [20,22,23,24,34]), so that they get to be engaged, generating a sense of personal motivation in relation to the abstract themes of information security. The findings from the overall scenario and the three studies in the project "ALARM Information Security" are given in [59].

The human factor has an increasingly important role to play in information security. User behavior is now widely recognized as a critical component of cybersecurity, and training is the method most frequently recommended as a means to ensure secure behaviors [60:17]. However, there is typically no input on methods and didactics, which would certainly be relevant. Since the digital age requires interaction with digital services (online services), ISA is becoming more important than ever for everyone. Yet, because ISA is now defined as a set of factors, it is not enough to simply increase knowledge [61:18]. This makes ensuring the efficiency of awareness-raising and training measures for information security extremely difficult. Given the significant role that individuals play in the security well-being of organizations, end users of IT systems are encouraged to see themselves as part of the information security solution and are expected to perform certain security functions (as a kind of "backend human firewall," for example). However, there is often a gap between the organization's expectations of the end users' part in information security and their functional role [62,19]. Actual security-relevant behavior does not simply follow in a linear manner from knowledge [59].

For example, social engineering continues to be a significant problem for organizations of all sizes today. Cybercriminals continue to develop new and sophisticated methods to trick individuals into disclosing confidential information or granting unauthorized access to infrastructure systems [63]. In addition to employees, management is increasingly becoming the focus of investigations. According to [63], managers can mitigate SE attack risks through a layered approach that combines training, reminders, testing, fostering a culture of security, and balancing technological measures with human vigilance. This was precisely the motivation behind the complex “ALARM Information Security” project, the targeted results of which are available to German SMEs free of charge for internal awareness-raising measures via the project website [55]. If these results attract international interest, a new project is to be financed with TH Wildau [26] and the firm known_sense [28].

Managers who monitor cybersecurity policies often rely on management encouragement (e.g., rewards) and employee characteristics (e.g., attitude) to foster compliant behavior [64]. The results of [64] demonstrate that cybersecurity legitimacy has an important impact on employee compliance with cybersecurity initiatives. This is important because it highlights to managers that they cannot simply expect compliant employee behavior when implementing cybersecurity initiatives, but rather that employees must be convinced that the initiatives are fair and reasonable [64]. According to the experience gained in the “ALARM Information Security” [55] project, the first step in convincing people is for continuous awareness-raising measures to be implemented that actually incorporate the experiences of employees in the dialogue.

Despite their limited resources, SMEs are considered the backbone of the European economy [2]. In such circumstances, SMEs could potentially benefit from the free and low-cost Cybersecurity Awareness (CSA) resources created and distributed by various public and private European entities [65] so that SMEs can use them to enhance the knowledge and skills of their employees and improve and change their cybersecurity attitudes and behaviors. As a result of this awareness-raising process, security-conscious employees can serve as the company’s first line of defense against cyberattacks and cybercrime [65]. The research of Chaudhary et al. shows, however, that although the European organizations’ materials benefit European SMEs, they require some adaptation to better suit the needs and situations of SMEs. Furthermore, the awareness resources aimed exclusively at SMEs and the different business areas of SMEs are inadequate [65]. For German SMEs, the “ALARM Information Security” project [55] provides a coordinated and integrated set of awareness-raising measures free of charge for internal use that has been tested several times in German companies.

Our insight is that employees must be involved in the development of security measures on an equal footing. This is currently also highlighted by the study of [66] with regard to the critical role played by information security guidelines in organizational IS: the researchers have found in case studies that the participation of organizational members represents added value for both the process and for ISP development since the direct feedback helps to identify the problems and represents a significant improvement [66]. However, it is clear that further research in the field of human-centred cybersecurity and organizational information security is necessary.

As pointed out in [59], the use of secure digital processes, technologies, and business models—which will ensure and increase the competitiveness and innovative ability of German SMEs—is a MUST for the country, for the prosperity of its citizens, for the further development of companies, and for the authorities providing the funding for new grants. Our experience in various security projects with a focus on “the human factor” and with a wide variety of target groups and actors suggests that this can be achieved by using visual, narrative-based materials, reducing complexity, and developing an understanding of complex conditions and relationships [59].

Technological, organizational, and work-design skills in IT and cybersecurity should be increased, and it should be possible to evaluate the security of and trust in (provider/user) information and communication systems [59]. To achieve this, the connections between IT, cybersecurity, and data protection must be addressed and translated into intelligible stories and images [59].

Despite the undoubted success of the “ALARM Information Security” project for all those involved, we definitely see some residual weaknesses. According to the findings of the project, these relate to three areas in German SMEs [59]:

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

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

ACKNOWLEDGEMENTS

As project manager and initiator of all Wildau University's awareness projects described in this paper, I would like to thank all the different funders. Moreover, 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 each project is documented on the project websites. 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.

COMPETING INTERESTS

The author has declared that no competing interests exist.

REFERENCES

1. Aziz ND, Nawawi AH, Ariff NR. ICT evolution in facilities management (FM): Building information modelling (BIM) as the latest technology. Procedia-social and behavioral sciences. 2016 Oct 31;234:363-71.

1a. Gesellschaft für Informatik e.V. (GI) / The society for computer science. Unsere Etischen Leitlinien. Berlin; 2015.
Version 07/2015.

1b. AlBar AM, Hoque MR. Factors affecting the adoption of information and communication technology in small and medium enterprises: A perspective from rural Saudi Arabia. Information Technology for Development. 2019 Oct 2;25(4):715-38.

2. Bundesministerium für Wirtschaft und Energie (BMWi)/Federal Ministry of Economics and Energy. International Dimension: EU – Digital Agenda. Bonn; 2014.
Available:http://www.bmwi.de/Redaktion/EN/Dossier/digitisation.html
Last access: May 29, 2017.

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

4. Ruiz Ben E, Scholl M. Usable privacy and security in Online Public Services. Cham: Springer International Publishing; 2023b.

5. McKinsey, Campany. Der Bürger im Mittelpunkt: Mehr Vertrauen in Behörden durch ein besseres Bürgererlebnis / The citizen is the focus: More trust in authorities a better citizen experience (in German); 2018.
Available:https://www.mckinsey.de/~/media/McKinsey/Locations/Europe%20and%20Middle%20East/Deutschland/Publikationen/Der%20Buerger%20im%20Mittelpunkt/der%20burger%20im%20mittelpunkt.pdf. Last access: January 4, 2024.

6. BSI—Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.) / Federal Office for Information Security (Ed.) (Oktober 2023). Die Lage der IT-Sicherheit in Deutschland / The situation of IT security in Germany 2023 (in German); 2023.
   Available:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410
   Last access: November 7, 2023.
7. Quader F, Janeja VP. Insights into organizational security readiness: Lessons learned from cyber-attack case studies. Journal of Cybersecurity and Privacy. 2021;1(4):638-659.
8. Scholl M, Ehrlich EP. Information Security Officer: Job profile, necessary qualifications, awareness raising explained in a practical way. Frankfurt am Main: Buchwelten-Verlag; 2020.
9. BSI—Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.) / Federal Office for Information Security (Ed.). ORP.3: Sensibilisierung und Schulung/Sensitization and training. Bonn; 2016.
   Available:https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html
   Last access: January 17, 2018.
10. Tsohou A, Karyda M, Kokalakis S, Kiountouzi E. Analyzing trajectories of information security awareness, Information Technology & People. 2012;25:327-335.
11. Stewart G, Lacey D. Death by a thousand facts: Criticising the technocratic approach to information security awareness. Information Management & Computer Security. 2012;20:29-38.
12. Kirlappos I, Beautement A, Sasse MA. ’Comply or die’ is dead: Long live security-aware principal agents. In Adams, A.A, Brenner, M, Smith, M. (Ed.), Financial Cryptography and Data Security, Lecture Notes in Computer Science. Heidelberg: Springer. 2013;7862:70-82.
13. Fagade T, Tryfonas T. Security by compliance? A study of insider threat implications for Nigerian banks. In Tryfonas, T. (Ed.), Human Aspects of Information Security, Privacy, Trust, HAS 2016, Lecture Notes in Computer Science, Cham: Springer. 2016;9750:128-139.
14. Pokoyski D. Security Awareness: Von der Oldschool in die Next Generation – eine Einführung. In Helisch, M, Pokoyski, D. (Ed.), Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, Wiesbaden: Vieweg+Teubner. 2009;1–8.
15. Khan B, Alghathbar KS, Nabi SI, Khan MK. Effectiveness of information security awareness methods based on psychological theories, African Journal of Business Management. 2011;5(26):10862–10868.
16. Beyer M, Ahmed S, Doerlemann K, Arnell S, Parkin S, Sasse A, Passingham N. Awareness is only the first step: A framework for progressive engagement of staff in cyber security, Hewlett Packard, Business White Paper; 2016.
17. Scholl M, Fuhrmann F, Pokoyski D. Information security awareness 3.0 for job beginners. In Varajão, J.E, Cruz-Cunha, M.M, Martinho, R, Rijo, R, Bjørn-Andersen, N, Turner, R, Alves, D. (Ed.), Proceedings of the

Conference on ENTERprise Information Systems (CENTERIS). 2016;433-436.

18. Kruger H, Drevin L, Steyn T. Email security awareness: A practical assessment of employee behavior. In Futcher, L, Dodge, R. (Ed.), Fifth World Conference on Information Security Education, IFIP – International Federation for Information Processing. Boston, MA: Springer. 2007;237: 33-40.
19. Aytes K, Terry C. Computer security and risky computing practices: A rational choice perspective, Journal of Organizational and End User Computing. 2004;16:22-40.
20. Scholl M. Information Security Awareness in Public Administrations. In Comite, U, Public Management and Administration, Open Access: INTECH d.d.o. Rijeka (InTechOpen); 2018.
Available:https://www.intechopen.com/chapters/59667
Last access: January 6, 2024.
21. Scholl M, Fuhrmann F, Scholl LR. 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.
Available:http://hdl.handle.net/10125/50168
Last access: January 20, 2018.
22. Scholl M. Sustainable Information Security Sensitization in SMEs: Designing Measures with Long-Term Effect. (University of Hawai’i at Manoa), Proceedings of the 56th Hawaii International Conference on System Sciences. Honolulu, HI: University of Hawai’i at Manoa, Hamilton Library. Handle. 2023;10125/103369.
23. Helisch M, Pokoyski D. (Ed.). Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, Wiesbaden: Vieweg+Teubner; 2009.
24. Haucke A, Pokoyski D. Mea culpa - Schuld, Scham und Opferrolle bei Social Engineering. Kes. 2018;1:6-8.
25. Albrechtsen E. A qualitative study of users’ view on information security, Computers & Security. 2007;26:276-289.
26. Summary of projects https://wildau.biz/. Project “IT-Sicherheit@KMU” / IT Security@SMEs was funded by the Land Brandenburg with ESF.
27. Fuhrmann F, Scholl MC, Edich D, Koppatz P, Scholl LR, Leiner KB, Ehrlich EP. Informationssicherheitsbewusstsein für den Berufseinstieg. Final report of the Project“SecAware4job. Aachen: Shaker; 2017.
DOI: 10.2370/9783844054668.
28. known_sense (Homepage). Compliance parcourses.
Available:https://www.known-sense.de/compliance-parcours
Last access: January 4, 2024.
29. known_sense (Homepage). Security brand management, https://www.known-sense.de/kopie-systemische-kommunikation.
Last access: January 4, 2024.
30. TAKE AWARE 2018 in Berlin.
Available:https://www.youtube.com/watch?v=j_Vdu5CdWG4.

Update of the event for 2024 in Munic: https://www.take-aware-events.com/events/take-aware-2024-muenchen
Last access: January 4, 2024.

31. Göbel S. Autorenumgebung für Serious Games-StoryTec: Eine Autorenumgebung und narrative Objekte für personalisierte Serious Games. TU Darmstadt, Dissertation; 2017.
32. Institute of Play. Q Design Pack School; 2015.
Available:http://www.instituteofplay.org/wp-content/uploads/2013/09/IOP_QDesignPack_School_1.0.pdf
Last access: March 3, 2016.
33. Bösche W, Kattner F. Fear of (serious) digital games and game-based learning? Causes, Consequences and a possible countermeasure, International Journal of Game-Based Learning. 2011;1(3):1–15.
34. Prott F, Scholl M. Raising Information Security Awareness Using Digital Serious Games with Emotional Design. IADIS International Journal on WWW/Internet. 2022;20(2):18–34.
35. Project SecAware4job (website).
Available:https://secaware4job.wildau.biz/
The project was financed by the Horst Görtz Foundation (HGS).
36. Project Security (website).
Available:https://security.wildau.biz/en.html
The project was funded by the Federal Ministry of Education and Research (BMBF).
37. Project Security (website learning scenarios)
Available:https://security.wildau.biz/files/Projekt_Security_Lernszenarien.pdf
38. Project “SecAware4school (website).
Available:https://secaware4school.wildau.biz/en.html
The project was financed by the Horst Görtz Foundation (HGS).
39. Scholl M, Schuktomow R. Information Security at Schools: A Practical Game-Based Application with Sustained Impact. Journal of Systemics, Cybernetics and Informatics. 2020;18(5):74–85.
Available:http://www.iiisci.org/journal/sci/FullText.asp?var=&id=SA989TJ20
40. Schuktomow R, Scholl M, Gube S, Koppatz P, Edich D, Gerlach J. Projektdokumentation Informationssicherheitsbewusstsein für den Schulalltag (SecAware4school) Frankfurt am Main: Buchwelten-Verlag; 2020.
41. Schuktomow R, Gube S, Scholl M, Koppatz P, Edich D. Lernszenarien - Anleitungen. Wildau: Technische Hochschule Wildau; 2020. Available:[38].
42. Project “Digitization Center (DIZ)” (website)
Available:https://diz.wildau.biz/index-en.html
Project was funded by the Research Center Informatics (FZI) Karlsruhe, Germany, for the SME 4.0 Competence Center Stuttgart.
43. Gube S, Scholl M, Walch MC, Koppatz P, Pokoyski D. Projektdokumentation Serious Games für KMU im produzierenden

Gewerbe: Social Engineering und Security Risk Management. Wildau: Technische Hochschule Wildau; 2021. Available:[42].

44. Gube S, Scholl M, Koppatz P, Walch MC, Pokoyski D. Moderationsanleitung zu Social Engineering Theater und Security Risk Roulette Wildau: Technische Hochschule Wildau; 2021. Available:[42].
45. Buffum PS, Boyer KE, Wiebe EN, Mott BW, Lester JC. Mind the Gap: Improving Gender Equity in Game-Based Learning Environments with Learning Companions. In C. Conati, N. Heffernan, A. Mitrovic, & M. F. Verdejo (Hrsg.), Artificial Intelligence in Education: 17th International Conference, AIED 2015, Madrid, Spain, June 22-26, 2015 (S. 64–73). Schweiz: Springer International Publishing; 2015. Doi:10.1007/978-3-319-19773-9_7
46. Lombardi M. Authentic Learning for the 21st Century: An Overview. (D.G. Oblinger, Ed.); January 2007. Available:https://www.researchgate.net/publication/220040581_Authentic_Learning_for_the_21st_Century_An_Overview. Last access: April 30, 2020.
47. de Zafra D, Pitcher S, Tressler J, Ippolito J. Information Technology Security Training Requirements: A Role and Performance-Based Model. (National Institut of Standards and Technology, Hrsg.) Gaithersburg; 1998. Available:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf. Last access: June 3, 2020.
48. BSI—Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.) / Federal Office for Information Security (Ed.). IT-Grundschutz-Kompendium. Köln, Bonn: Reguvis Bundesanzeiger Verlag, Bundesanzeiger Verlag. 2020;42. Available:IT-Grundschutz-Kompendium Last access: April 30, 2020.
49. known_sense. Studie: Bluff me if U can - Gefährliche Freundschaften am Arbeitsplatz, Tiefenpsychologische Wirkungsanalyse Social Engineering und seine Abwehr. (known_sense, Ed.) Köln. 2015;36. Available:http://www.known-sense.de/BluffMeIfUCanAuszug.pdf.
50. Berg A, Niemeier M. Wirtschaftsschutz in der digitalen Welt. (bitkom, Ed.). 2019;3. Available:https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf Last access: April 30, 2020.
51. Albladi SM, Weir GR. User characteristics that influence judgment of social engineering attacks in social networkes. (University Strathclyde: Human Centric Computing and Information Science, Hrsg.) Glasgow: Springer Open. 2018;3. Available:https://doi.org/10.1186/s13673-018-0128-7
52. Klipper S. Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010 (2. Ausg.). Wiesbaden: Springer Fachmedien. 2015;44. DOI: 10.1007/978-3-658-08774-6

53. BSI—Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.) / Federal Office for Information Security (Ed.). BSI-Standard 200-3: Risikoanalyse auf der Basis IT-Grundschutz. Bonn; 2017.
Available:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.pdf
Last access: May 5, 2020.
54. Bitkom (Ed.) (n.a.). ISO/IEC 27005.
Available:https://www.kompass-sicherheitsstandards.de/
https://www.kompass-sicherheitsstandards.de/Risikomanagement/ISO-IEC-27005
Last access: May 5, 2020.
55. Project Awareness Lab SMEs (ALARM) Information Security (website).
Available:https://alarm.wildau.biz/en
The project is funded by the Federal Ministry for Economic Affairs and Energy (BMWK).
56. Scholl M, Schuktomow R, von Tippelskirch H, Prott F, Koppatz P, Pokoyski D, et al. (forthcoming). Neue Wege für mehr Informations sicherheit in KMU: Projektdokumentation Awareness Labor KMU (ALARM) Informationssicherheit. Frankfurt/M.: Buchwelten Verlag; 2024.
57. Scholl M. 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, London: IntechOpen; 2023.
Available:https://www.intechopen.com/online-first/1171513
Last access: January 6, 2024.
58. Scholl M. Raising Awareness of CEO Fraud in Germany: Emotionally Engaging Narratives Are a MUST for Long-Term Efficacy. (Álvaro Rocha, C. Ferrás, & W. Ibarra), Information Technology and Systems. Cham: Springer International Publishing; 2023.
DOI: 10.1007/978-3-031-33258-6_40
59. Scholl M. Chapter 5 - Findings from the overall scenario and the three studies of the project Awareness Lab SMEs (ALARM) Information Security followed by a conceptual outlook. Wildau: Technische Hochschule Wildau; 2023.
DOI: 10.13140/RG.2.2.12630.22082
60. Kävrestad J, Fallatah W, Furnell S. Cybersecurity Training Acceptance: A Literature Review. In: Furnell, S, Clarke, N. (eds) Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, Springer Cham. 2023;674:53-63.
Available:https://doi.org/10.1007/978-3-031-38530-8_5.
61. Fertig T, Schütz A, Weber K. Automated Measuring of Information Security Related Habits. Proceedings of the 55th Hawaii International Conference on System Sciences. 2022;2022.
Available:https://hdl.han-dle.net/10125/80267
ISBN: 978-0-9981331-5-7 (CC BY-NC-ND 4.0):7702-7711.

62. Ogbanufe O. ‘Information Security Is Not Really My Job: Exploring Information Security Role Identity in End-Users. Proceedings of the 53rd Hawaii International Conference on System Sciences. 2020;2020.
Available:https://hdl.handle.net/10125/64263
ISBN: 978-0-9981331-3-3 (CC BY-NC-ND 4.0):4256-4263.
63. Ribeiro R, Mateus-Coelho N, Mamede H. Improving Social Engineering Resilience. In Enterprises. ARIS2-Advanced Research on Information Systems Security. 2023;3(1):34-65.
64. Cram WA, D'Arcy J. ‘What a waste of time: An examination of cybersecurity legitimacy. Information Systems Journal. 2023;33(6):1396-1422.
65. Chaudhary S, Gkioulos V, Goodman D. Cybersecurity awareness for small and medium-sized enterprises (SMEs): availability and scope of free and inexpensive awareness resources. In European Symposium on Research in Computer Security:97-115. Cham: Springer International Publishing; 2022, September.
66. Paananen H, Siponen M. Organization Members Developing Information Security Policies: A Case Study; 2023.
Available:https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/14/ Last access: January 5, 2024.

Biography of author(s)

Margit Scholl
Department Business, Computing, Law Technical University of Applied Sciences (TH) Wildau, 15745 Wildau, Brandenburg, Germany.

Research and Academic Experience: After studying physics/meteorology in Mainz and Berlin, she worked as a researcher on a number of projects for the German Research Foundation (DFG), developing numerical models. She did her doctorate in meteorology at Berlin's Freie Universität. Afterwards, she was a unit head within the Berlin Senate administration. In 1994, she was a professor at the University of Applied Administrative Sciences Bernau and at TH Wildau in 1997. From 1998 to 2001, she was head of the IT user service in the Brandenburg State Office for Data Processing and Statistics. In 2001, she returned to TH Wildau as an ambitious researcher and Professor for Business Informatics and Administrative IT in the Faculty of Business, Computing, and Law.

Research Specialization: Her objects of interest are project management, including e-government and international orientation, process management, including acceptance and quality management, risk management and change management, business applications such as enterprise resource planning systems and document management systems, multimedia, including learning technologies virtuality, and intercultural aspects, IT security, and IT baseline protection. Moreover, her research focuses are IT and didactics, infrastructures for promoting learning, individual and organizational learning, digital media in education, and PPBBL (Problem and Project-Based Blended Learning).

Number of Published papers: She has published 154 papers in several reputed journals.

Special Award: She won the university's research prize in 2011.

Any other remarkable point(s): In 2010, she founded the WILLE Institute (Wildau Institute for Innovative Teaching, Lifelong Learning, and Constructive Evaluation), which is part of the Centre of Technology Transfer and Advanced Learning (TWZ e.V.). In 2013, she did a research semester at the University of Washington's iSchool in Seattle, USA. In 2014, she converted her university professorship to a five-year research professorship. Her aim in this new position was to focus on developing and deploying a holistic understanding of technology in an area that will in the future be more strongly characterized by diversity. She retired in September 2023; however, she will continue to work on projects at TH Wildau and offer further training and certification through WILLE for employees from universities, public administrations, and SMEs with a focus on information security and management systems, data protection and security, awareness raising, and project management.

DISCLAIMER
This chapter is an extended version of the article published by the same author(s) in the following journal.
Systemics, Cybernetics and Informatics, 16(3), 2018.
Available: https://www.iiisci.org/journal/sci/FullText.asp?var=&id=IP048LL18

Peer-Review History:
This chapter was reviewed by following the Advanced Open Peer Review policy. This chapter was thoroughly checked to prevent plagiarism. As per editorial policy, a minimum of two peer-reviewers reviewed the manuscript. After review and revision of the manuscript, the Book Editor approved the manuscript for final publication. Peer review comments, comments of the editor(s), etc. are available here: https://peerreviewarchive.com/review-history/8543A