Chapter 3

Information Security Awareness in Public Administrations

Margit Scholl

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.74572

Abstract

Government digital agendas worldwide go hand in hand with the digital transformation in businesses and public administrations as well as the digital changes taking place in society. Information security (IS) and awareness (ISA) must be an integrated part of these agendas. The goal of IS is to protect information of all types and origins. Here, the employees play a necessary and significant role in the success of IS, and the entire staff of an institution need to know about their specific roles and be aware of the information security management system (ISMS). As there are still fundamental strategic deficiencies in the institutions themselves, humans should not be called "the weakest link" in the security chain. Rather, sustainable awareness-raising and training for people should be established in the institutions using interactive, authentic, and game-based learning methods. Psychological studies show the great importance of emotionalization when communicating IS knowledge and the reliable exchange of experience about IS. However, in many institutions, a change in culture is becoming necessary. IS must be integrated into all (business) processes and projects, and viable safeguards must be included. This chapter summarizes the most important scientific findings and transfers them to the practice of public administrations in Germany. Moreover, it shows examples of learning methods and provides practical assistance for IS sensitization and training.

Keywords: digitalization, threats and vulnerabilities, information security (IS), data protection, IT security, cybersecurity (CS), cyberattacks, sensitization, information security awareness (ISA), security culture, knowledge—attitude—behavior, information security awareness training (ISAT) design, lifelong learning (LLL), learning and teaching methods, authentic learning (AL), game-based learning (GBL), problem-based learning (PBL), success factors, information security management system (ISMS), risk management and safeguards

1. Introduction: A talk about security

Public administrations have always been information-processing organizations, and nowadays government digital agendas around the world (see, for example, the Federal Government of Germany or—at the European level—the European Digital Agenda [1]) are seeking to keep abreast of digital networking and the digital changes in society based on information technology (IT). However, ever-increasing digitalization is leading to fundamental changes in business processes in public administrations as they try to offer customer-friendly services to citizens and businesses. In light of this, new safeguards must be implemented in the form of continuous information security (IS) and legally compliant data protection. "No one in industry, commerce and administration would any longer dispute the need for adequate protection of their IT environment. IT security incidents can have far-reaching repercussions that harm business or interfere with the performance of tasks and thus result in high costs being incurred" [20:5]. Digitization affects almost all areas of life in an increasingly rapid way, and the underlying information communication technology (ICT) transmits, electronically processes, and stores large amounts of data and a wide variety of information [2]. In his guest contribution to a special publication of the *Handelsblatt* (November 27, 2017) on the topic of cybersecurity and privacy, the president of the German Federal Office for the Protection of the Constitution, Dr. Hans-Georg Maaßen, explains, "It is a commonplace platitude: the more we network with the outside world, the more we connect not only with opportunities and potentials but also with risks and dangers" [3]. One should be aware of the distinction between the terms "safety" and "security" in English-speaking countries. "The term 'safety' refers to the functional safety of the machine or plant and thus addresses the protection of the environment against abnormal operation. The term 'security' describes the protection of IT-supported systems against deliberate or undesired errors. Safety systems must also be protected against attacks" [76:10].

As the president of the Federal Office for Information Security (BSI) pointed out at the 14th German IT Security Conference [4], the potential for digitization offers a highly developed form of industrialization of the kind that Germany cannot do without—but at the same time cybersecurity is creating new challenges. The term IS, as used in (inter)national standards, consists of more than just IT security. The goal of IS is to protect information of all types and origins, regardless of whether they are stored on paper, in computers, or in the employees' minds [2]. In contrast, IT security is specifically oriented toward the protection of information processed and stored electronically. Nowadays, the term cybersecurity (CS) is often used. CS deals with all aspects of security in information and communication technology. The field of action of classic IT security will be extended to the entire cyberspace. This includes all information technology connected to the Internet and comparable networks and involves communication, applications, processes, and processed data or information based thereon [5]. In this chapter, the term IS is used as the general term including IT security as well as CS.

One of the relevant standards for IS is 27001 "Information Security Management Systems" (ISMS) of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) [6]. An ISMS includes four components: management principles, resources, the IS process, and the people (personnel) [20:14]. The IS process itself includes an IS policy, in which the IS objectives and strategies for their implementation are

documented, an IS concept, and the developed IS organization of the institution. When an ISMS is implemented, it is crucially important that the information and data protection are properly handled and the employees are fully aware of the consequences of misusing sensitive data [7]. In Germany, ISO/IEC 27001 IS protection certificates have been available since 2006 combined with the IT-Grundschutz as best practices [8]. The responsible public administration is thus the BSI as the national CS authority that "shapes information security in digitization through prevention, detection, and reaction for government, business, and society" [9]. The employees of an institution are a necessary and significant factor in successfully and efficiently realizing IS within an institution [10]. Therefore, all employees of the institution need to know about their specific roles and be aware of the information security management (ISM). According to the BSI [10], all employees need to know the security objectives of the institution and understand the security measures, as well as being willing to support these effectively. In particular, they must know what is expected from them in terms of IS and how they should respond in security-critical situations [10].

According to the IT-Grundschutz glossary of the BSI, IT security is "a state in which the risks posed by the use of IT due to the threats presented are limited to an acceptable level through adequate safeguards" [2]. Technical solutions for IS are necessary to address certain vulnerabilities such as viruses, denial of service attacks, etc. Nevertheless, IS as well as IT and CS are about more than technology [11], because information systems involve human beings, and users do not always act the way they are supposed to [12]. This is why human beings are often characterized as the "critical factor" within the reports and literature on IS processes. However, nowadays, there is a rethinking of this characterization of people [13], because there are fundamental strategic deficits in institutions themselves, as shown by several reports and studies:

- Less than 50% of organizations have an IT security and training program for employees [14]—meaning that at the time of the study, more than 50% did not train and educate their employees in IS.
- 46% of all companies believe that they have a critical shortage in terms of their cybersecurity skills [15].
- Only 63% of respondents in Germany take measures to raise awareness of information security and 40.5% of these organizations do not measure the effectiveness of their training [16].
- Not even half of the (surveyed) companies in Germany are sufficiently prepared for a cyberattack. Moreover, only four out of 10 companies have emergency/continuity management (43%) [17].
- 74% of security incidents remain undetected for more than 6 months [18].
- Managers prefer to pay ransom than invest in new protection features—a big risk, because ransom payments are usually six-figure amounts [19].

Technology solutions alone are not sufficient to ensure IS countermeasures. These address the challenges of IS management (ISM) in institutions, because management and behavioral aspects are pivotal to building an ISMS in organizations [20, 21]. To protect the organizational assets, including user information and systems, the human side of security should also be

managed [22–24], as is particularly evident in social engineering (SE) attacks [24]. The human element plays a significant role in the successful delivery of IS in today's organizations, and security behavior is greatly influenced by employees' personal perceptions of risk. However, these perceptions can be changed [25] through awareness-raising and IS trainings. Therefore, the tasks and duties of the management of an institution play an important role [20:18]. First of all, the topmost management level has overall responsibility for the correct functioning of the institution and for IS too. IS must be integrated into all the institutional processes—"and for that the management has the responsibility. The management level must actively initiate, manage and supervise the security process"—as an important point, sufficient resources must be made available [20:18]. Moreover, as studies confirm [26], the management has the function of a role model, must set achievable goals within the institution's IS, and should set up/initiate efficient communication and effective documentation. "One of the most difficult tasks is weighing up the costs of IS against the benefits and risks"—however, "experience shows that the most effective measures are not always the most expensive" [20:19].

The aim of this chapter is to summarize current science-based findings in the area of ISA and to merge them with the requirements of the IS standards to derive practical benefits for awareness-raising and trainings in public administrations. The structure of the chapter is as follows: section two summarizes the current scientific findings concerning ISA (sub-Section 2.1), learning methods (sub-Section 2.2), and organizational culture (sub-Section 2.3). In Section 3, these ideas are transferred into the practice of public administrations. This means a focus on information security (awareness) trainings (ISAT) in general (sub-Section 3.1), as they relate to the IT-Grundschutz (sub-Section 3.2), and with regard to cultural aspects (sub-Section 3.3). Section 4 provides a summary and outlook. This is followed by the acknowledgments and references at the end.

2. Current findings from scientific literature review and research

2.1. Information security awareness (ISA)

A constant analysis of threats that companies face is essential to understanding how the strategies of attackers evolve and to building more reliable defenses. The summary of all the reports investigated reveals that cyberattacks target people not technologies [13]. The question is "why?" One main finding, by Solms, is that Internet- and web-based systems have been introduced for millions of customers without adequate IS [27]. One direct result of this has been that criminals have shifted their attention to the end user under their new motto: "Do not try to hack into the company's IT systems; it may be very difficult—go for the naïve end user!" [27].

The idea of considering the user as the "weakest link" in IS can be found in the large volume of studies that try to explain employee adherence to or noncompliance with IS. Companies' information security efforts are often threatened by employee negligence and insider breaches [29]. The lack of ISA, ignorance, negligence, apathy, mischief, and resistance are at the root of user mistakes [30]. Herath and Rao found that employees in their sample underestimate the probability of security breaches [31]. Pattinson et al. (2016)

found a strong ISA correlation for the measure relating to the three behaviors "Internet use," "mobile computing," and "email use," while the other four behaviors investigated were not significantly correlated ("password management," "social networking," "information handling," "incident reporting") [32]. Moreover, how "dangerous" an employee is for his company is also determined by his age [18]. According to the study, 51- to 69-year-old people are particularly easy to fool—they are most likely to fall for phishing attacks and social engineering, but otherwise stick to the guidelines [18]. The middle group, on the other hand, is more arrogant: the group of 35- to 50-year-olds is most likely to ignore well-known rules [18]. However, in the study, the millennials age group (18–35) is—with 64%—the riskiest group: while they are less prone to fraud and arrogance, they use all sorts of technologies, such as unauthorized third-party apps and third-party mobile devices at work, and this results in a loss of control for the central IT [18]. However, it is important to bear in mind that if a single user action can compromise an entire security program, the problem is the security program itself [33].

According to the Federal Office for Information Security in Germany (BSI), the risk situation in the area of ISA is characterized by the following specific threats and vulnerabilities [10]:

- Insufficient knowledge of regulations

  Just setting information security regulations does not guarantee that they will be respected. All employees must also be aware of the applicable regulations. Vulnerabilities due to insufficient knowledge of the regulations can compromise the confidentiality, availability, and integrity of information [10:2].

- Insufficient awareness of information security (ISA)

  Experience shows that it is not enough just to implement certain security measures. Without an understanding of the reasons for the measures and their purpose, they are often ineffective or ignored. The security culture, the security goals, and the security strategy of the institution must be understood in the real world of work, otherwise this leads to a lack of acceptance of IS measures [10:2].

- Carelessness in handling information

  It is frequently observed that despite a variety of organizational and technical security procedures, an institution's security requirements often go unheeded. When employees deal carelessly with information, established processes of information security become ineffective. Economic espionage can also take place [10:3].

But what is ISA actually? Our comprehensive review of leading academic journals shows that there is no uniform and binding definition of ISA [13]. Many theories build on the background of the scientific literature. A number of articles in the international scientific literature are based on the KAB model—knowledge, attitude, and behavior—and show that user knowledge of, or education about, IS is a basis for reflecting on their own attitudes. The overall goal of scientific literature in this research field is to get a better understanding of people's behavior and to develop it in the proper way [13]. Therefore, a large spectrum of theories has been consulted in this context to gain knowledge of actual security behavior and the factors that

influence it. The theories that are most applied as a means to explain IS behavior are the Theory of Planned Behavior (TPB), the General Deterrence Theory (GDT), the Compliance Theory (CT), the Protection Motivation Theory (PMT), the Technology Acceptance Model (TAM), the Theory of Reasoned Action (TRA), the Social Bond Theory (SBT), and, as a final example, the Involvement Theory (InvT) (see also tables in [34]. For example, Briggs et al. (2017) provide a historical overview of Protection Motivation Theory (PMT) and apply it to cybersecurity [35]).

Applying the Fogg Behavior Model (FBM) [36], we can identify a wide range of factors that can affect motivation and the ability to adopt secure behaviors. The FBM [37] asserts that for a person to perform a target behavior, he or she must (a) be sufficiently motivated, (b) have the ability to perform the behavior, and (c) be triggered to perform the behavior. Fogg further introduced the notion of *kairos*—the idea that the trigger needs to be present at an opportune moment to succeed. Fogg defines that moment as "any time motivation and ability put people above the behavior activation threshold" [37]. The investigations in [36]—based on the FBM and in-store interviews with 85 customers across 4 branches of a major UK retailer—showed that low motivation and ability among the customers questioned are, for example, combined with the attitude that because risky activities are avoided, no security is required. In contrast, high motivation and high ability among customers are not only coupled with technical affinity and the implementation of security advice but also with the desire to keep children safe and protect work files [36]. This suggests that those customers have a sense of responsibility and take social considerations into account.

One increasing threat is the human social engineering (SE) attack as a first step for further cyberattacks on institutions. SE has increasingly become a standard tool for criminals—the prospects of success are high and the awareness rate is low [38]. In SE, one is—to different degrees, depending on the perspective—perpetrator and victim at the same time: perpetrator, because one may have made a mistake and violated the security policy of one's own organization (e.g., as a result of disclosing confidential information to the attacker), and victim, because such a disclosure is always achieved as a result of deception or manipulation [38]. From the point of view of communication and psychology, a person directly affected by SE is, in any case, always a victim—the fact that someone, possibly because of "reckless" behavior, has "fallen for" an SE attack does not make him or her a culprit and, from the perspective of the social sciences, only to some extent an accomplice. And even the security experts should not view "social weaknesses" as connivance but should treat the victims as victims and therefore see them as important witnesses who contribute to the investigation of white-collar crime. However, such an attitude is not found in many organizations, and, where this is lacking, companies rarely have full access to the valuable feedback they could receive [38].

All in all, there are gaps between human knowledge and human attitudes as well as between human attitudes and *real* human behavior. Psychological factors, subjective norms, and the sociocultural, gender, and age background in nonlinear and complex interactions have a major influence on human ISA and IS behavior [13]. A main problem for human beings seems to be the application of IS knowledge in *real-world* situations [39]. But this—the concrete application of IS knowledge and situation-appropriate behavior—is necessary in real time for each employee in an organization. Employees themselves must decide how to implement IS in their own specific work contexts, and this needs higher-level ISA skills and intention as a motivational factor.

2.2. Learning methods for ISA

Learning methods for ISA should clarify threats, vulnerabilities, attacks, and possible damage as well as the main values of IS and data protection. The three basic values of IS used by the BSI in the IT-Grundschutz as well as in the international standard family ISO/IEC 2700x are confidentiality, integrity, and availability. Confidentiality requires protection against the unauthorized access to and disclosure of information. Confidential information should only be accessible to authorized persons and those using the permitted access methods. A situation in which unauthorized persons have access to data is referred to as a loss of confidentiality [2:22]. Integrity refers, on the one hand, to ensuring the correctness (uncorruptedness) of data and, on the other, to the correct operation of systems. A violation of the integrity of information takes place when the data itself—as well as other specifications relating to this data (metadata)—are changed without permission or are incomplete. Falsified data can lead to poor decisions and incorrect evaluations and can have serious consequences [2:22]. Availability means that services, the functions of an IT system, IT applications, IT networks, or even information are available and can be utilized as intended by the users at any time [2:22].

Additional values include authentication, commitment, and reliability. Authentication refers to the function that guarantees that a person, an IT component, or an application is actually the person or object it is presenting itself to be. Authenticating information is a means of ensuring that it was generated by the specific source [2:22]. Commitment combines the value of authenticity with one additional value, non-repudiation. When transmitting information, this means that the sender has provided verification of its identity and that the recipient is unable to deny having received the message [2:22]. Organizational commitment can be defined as follows: "In organizational behavior and industrial and organizational psychology, organizational commitment is the individual's psychological attachment to the organization" [40]. The reliability (also called dependability) of IT components is determined by their quality in terms of correctness, robustness, and fail-proofness so that their typical functions can be executed with the necessary precision and during the normal period of use [2:22].

In many organizations, ISA and the training of corresponding competences (ISAT) are limited to knowledge-transfer measures. For example, trainings with appropriate presentations supported by flyers, posters, brochures, or web-based trainings (WBT) are often used as an awareness campaign, which the employees can or must complete at a particular place and at a time of their choosing. Notwithstanding the benefits of WBT, studies show that approaches that focus only on knowledge transfer do not generate any lasting safety/security awareness among employees [41–44]. We call these ways of raising ISA "1.0 Learning Theoretical Approaches" (see **Figure 1**) [45]. Based on these empirical findings and in addition to knowledge transfer, some awareness-raising activities include marketing elements, which capture the attention of the addressees and emotionalize them on the subject of IS—"2.0 Advertising Approaches," according to our classification (see **Figure 1**) [45]. However, psychologically based research [38, 39, 42, 46, 47] shows that in addition to the theoretical approach to knowledge transfer and the marketing-oriented approach of emotionalizing, a more comprehensive systemic approach with emotions and social participation in the team as well as personal communication and interaction in actionable scenarios is needed to create lasting sensitization to IS and promote security-related behaviors [41, 46, 48]. This is why the learning methodology for ISA should be

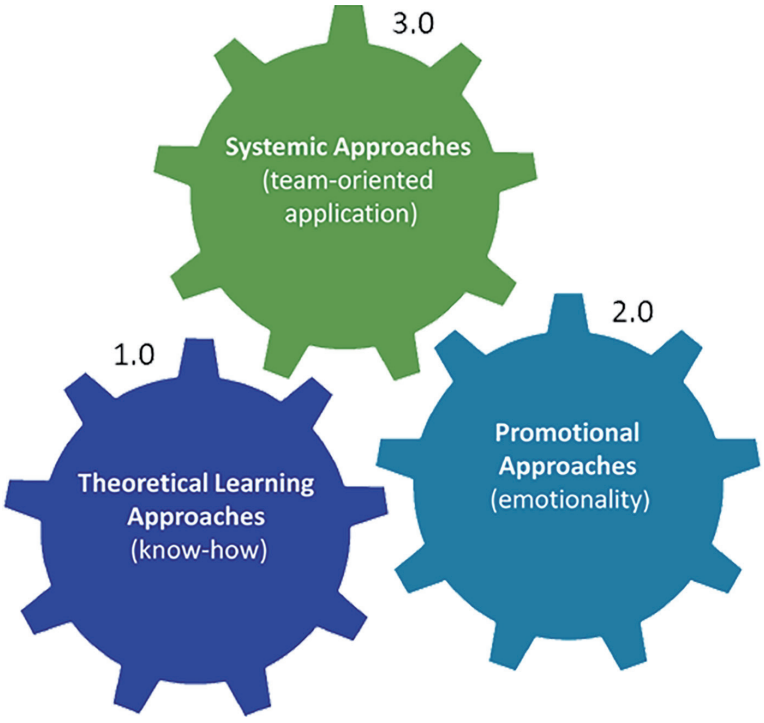

Figure 1. IAS needs learning 3.0, meaning a systemic approach that includes not only knowledge transfer and emotionalization but also interactivity with team-oriented exchange.

"3.0 Systemic Approaches" (see **Figure 1**) [45], which were implemented at the Technical University of Applied Sciences (TUAS) Wildau [49–51]. Here, at a research university with a strong practical emphasis, a consistent combination of research and teaching not only serves to meet future challenges but is also crucial for starting a career. The education of students as future employees should therefore be based on the current state of science and on practical requirements in companies, administrations, and institutions. This includes building knowledge to engender a holistic understanding of technology and develop sensitivity to IS issues. This applies, above all, to less technology-related courses such as business and administrative studies because awareness of and competence in IS cannot be delegated only to IT professionals. Instead, every employee must contribute to IS and is responsible for it in his or her specific environment.

The project "Information Security Awareness for Job Beginners" (SecAware4job) at the TUAS Wildau, which was funded by the Horst Görtz Foundation in the period from September 1, 2015, to August 31, 2017 [50], set out to sensitize students as future employees (especially those doing nontechnical courses) to the day-to-day challenges involved in creating IS and protecting digital infrastructure. With SecAware4job, a job-oriented additional qualification for students has been created in the past 2 years in the form of an innovative training with certification to increase ISA and competencies in IS. Specifically, the additional qualification should

- develop the competencies in IS required for starting a career,
- encourage and support changes in consciousness and behavior,
- facilitate risk assessment and decision making, and
- provide traceable, certified qualifications for entry into the profession [50].

In order to convey the abstract and complex topic of IS with all its facets (legal framework, standards, protective measures, security concepts, etc.) to the students in an easily comprehensible and tangible way, a methodical approach to the additional qualification was chosen that includes as many creative and interactive teaching and learning methods as possible. Based on current research findings on the effectiveness of awareness-raising measures, analog and digital game-based learning (GBL) scenarios were developed and tested according to the GBL approach [49]. Ten stations in the "Security Arena," which had been procured via the former third-party project "IT-Security@SME" in the period 2013/14 and adapted with the project partner known_sense, are now focused on the new target group (students) and also translated into English (see **Figure 2**) [50]. In addition, five analog GBL scenarios have been redesigned and implemented, including a new board game "Keep your data private. Every day." (see **Figure 3**) and a social engineering role-playing game, which are two very comprehensive game developments in the research project SecAware4job [50]. To supplement and complete the analog learning scenarios, eight digital GBL scenarios were conceived and programmed: these can be retrieved via the SecAware4job website [52] and used free of charge [50].

The additional qualification that had been developed was tested in three rounds as a (compulsory) module "Sensitization for IS". The accompanying scientific research on the effectiveness of the additional qualification and the learning scenarios developed show that the students are very satisfied with the methodological approach. In terms of an authentic learning (AL) approach, adaptations of GBL scenarios to the specific target group and their real references are of great importance for learning success. Further teaching and learning methods have already been compiled in the former European project "Community of Integrated Blended Learning in Europe" (COMBLE) [53] as Methopedia [54]. Moreover, by discussing current public security incidents, the problem-based learning (PBL) method has been introduced into the classroom too. So, the challenge of the general learning approach for ISA is to combine AL with GBL and PBL in a smart way. In addition to the specification of content, cultural and linguistic aspects must be taken into account. In the project SecAware4job, English-language learning stations were designed and tested and will now be available in international degree courses like European Management. Moreover, in this winter semester (WS 2017/18), the master's degree course European Management (EMM17) developed new ideas for GBL scenarios relating to the European Union's new General Data Protection Regulation (GDPR) as pilot games. The student project teams presented three analog games and one digital App game in January 2018 (see **Figure 4**), which will be tested in the coming months with other target groups.

Overall, the application of materials and methods to ISA in many other events and with other target groups like employees and guests at the TUAS always leads to very positive feedback. The challenges in developing the IS learning scenarios lie in a good didactical structure as well as in simplifying complexity and limiting the content to the essentials. The strength

Figure 2. Adapted, analog game-based learning scenarios in the English-speaking "Security Arena" as final results of the project "SecAware4job" [50]. The games can be purchased through our project and cooperation partner, the Cologne-based company known_sense.

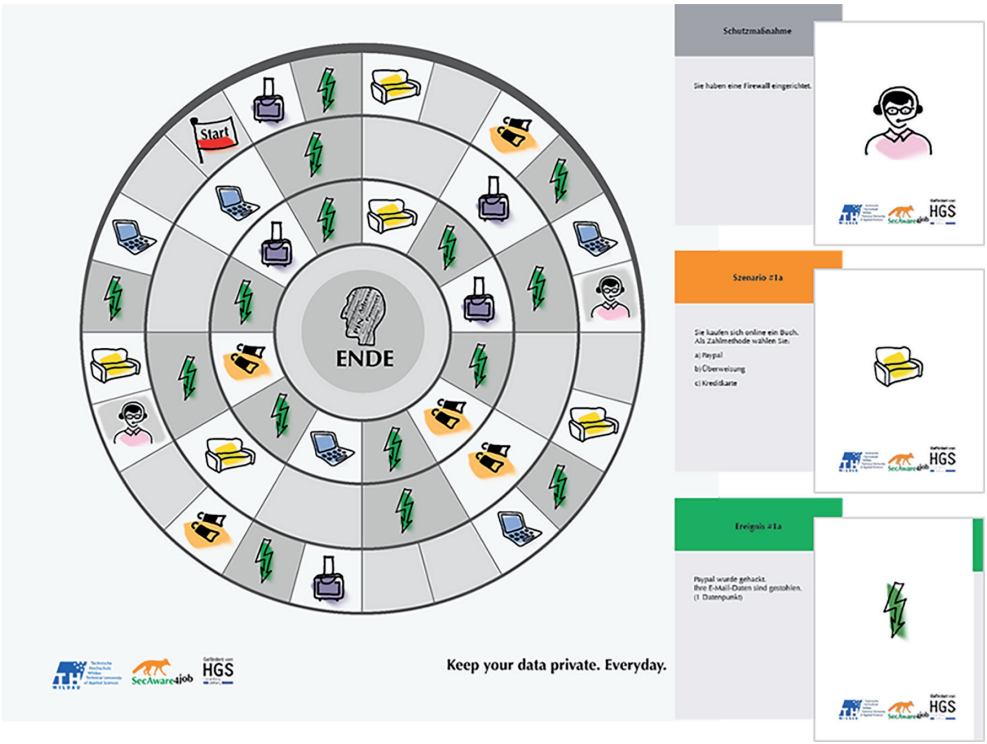

Figure 3. Newly developed analog game-based learning scenarios (in German) relating to Internet services and data protection as a final result of the project "SecAware4job" [50]. The game can be purchased through our project and cooperation partner, the Cologne-based company known_sense.

of the analog games is in the necessary systemic approach with emotionalization and the exchange of peoples' experiences. As part of the "Security Arena," most games are designed to be completed and discussed in less than 15 minutes. They can also be used very well as team circuit training, which can also be set up as a competition. The goal of the digital learning scenarios, which can be completed alone and irrespective of time and place, is to expand, deepen, and sustainably anchor individual knowledge. However, this alone would not help to raise ISA. We need a smart combination (**Figure 5**).

2.3. Information security awareness culture in an organization

As the BSI points out in all standard documents, IS concerns all personnel without exception. By acting responsibly and with quality awareness, every individual can avoid causing damage and contribute to success. Increasing ISA and providing appropriate training for staff members and all management personnel are therefore fundamental prerequisites

Figure 4. Newly developed ideas for game-based learning scenarios (A, B, C analog; D digital) focused on the General Data Protection Regulation (EU), generated by the student group EMM17 in WS 17/18.

for IS. In order to be able to implement security measures as planned, personnel must have the necessary basic skills to do so [20:24]. Here, the top management has responsibility as a role model. The management must play a proactive role in shaping employee compliance with IS behavior [26]. Advice should be seen as an enabler that supports the organization's goals [25]. In addition to knowledge about how security mechanisms must be operated, this also involves an understanding of the spirit and purpose of security measures. The work atmosphere, common ideals, and the commitment of personnel are all factors that decisively influence IS. If new personnel are taken on or existing ones are given new tasks, they must be provided with thorough training so that they can adjust to the new situation. This must also involve teaching them about the security-related aspects of their job. If personnel leave the institution or their responsibilities change, this process must be accompanied by appropriate security safeguards (e.g., the withdrawal of authorization or the returning of keys and identity cards) [20:24].

Employees must be made aware of relevant hazards and know how they can affect their institution. The better the employees know the risk situation, the sooner the corresponding security measures will be accepted. Employees must have the necessary knowledge to be able to understand and apply measures correctly. For this, there must be an awareness of security and a safety culture can be set up and designed [10]. Although there are many sanctions available in dealing with disregard of the rules, employees will not be rewarded if they comply with the IS security policy [55]. While many organizations are aware that this "comply or die"

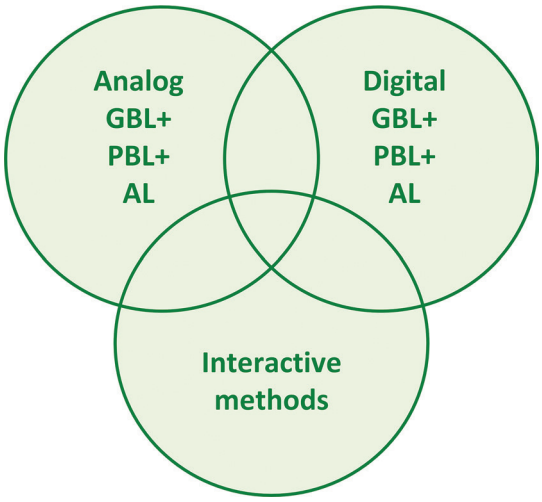

Figure 5. Integrative usage of analog and digital game-based learning (GBL), combined with problem-based learning (PBL) and authentic learning (AL) for sensitization and to mimic real situations in the workplace and private life as well as interactive learning methods with emotionalization through user experience, team exchange, and storytelling as a means to raise information security awareness (ISA).

approach does not work for modern enterprises where employees collaborate, share, and show initiative, they do not have an alternative approach to fostering secure behavior [56]. "Countermeasure awareness was shown to be a significant indicator of the perceived need for digital IS. This implies that increasing users' security awareness level through education and training may be an effective way to encourage the adoption of security tools that leads to safer technology use" [57]. It seems that attitudes toward compliance with IS organizational policies also have a significant effect on behavioral intention with regard to IS compliance, whereby the policies must be livable. Tsohou et al. argue that ISA processes are associated with interrelated changes that occur at the organizational, technological, and individual level [58]. As a result of this, an organization needs to roll out a series of ISA programs oriented toward perception, comprehension, and projection [23].

As summarized in [13], for organizations it is important to realize that

- creating an effective ISA program requires targeted communication and training that caters to specific employee groups;
- for proper commitment to security, the optimal IS culture must be carefully defined in each case; and
- the top management must be a role model and give advice—they should be seen as an enabler supporting the organization's goals.

In light of the gaps between IS knowledge, attitudes, and real behavior and the fact that acting in real-life situations is very important for an appropriate security level in institutions,

trainings for ISA should be a continuous IS factor. Moreover, the emotional level should be explicitly addressed, because social participation in a communicative team process is a key component in awareness-raising activities based on psychological theories [45, 51]. Learners must directly see/feel the consequences of their actions and should get a sense of their knowledge level in dialog. Therefore, sensitization for ISA and trainings of IS should use the smart combination of GBL plus PBL plus AL based on real-life situations.

3. Transference to practice and public administrations

The improvement of perception and comprehension vis-à-vis IS can advance a person's ability to project real-life situations if there is an overall exchange in the institution. Moreover, it seems that the constructs of organizational impact and attacker assessment have a stronger influence on the ISA than technical knowledge. Management and employees need to understand the pivotal role they play for the IS of an organization [13]. The learning process in organizations must be based on the user-centered approach, which pays attention to target groups, gender, and culture, based on individual knowledge and skills as well as on concrete workplace needs and contexts. The user-centered approach should also allow staff exchanges regarding IS along the business process chain. The integration of formal and informal mechanisms—initiated by the management—can enhance the important exchange and interaction between employees and could be a stabilizing factor in raising ISA in the institution. Frequent interaction is the basis for the formation of interpersonal relationships and psychological attachment to the organization. Since threat analysis, self-efficacy, and response effectiveness have a significant impact on the intention to comply with IS guidelines, such aspects of emotionalization and motivation should be incorporated into the sensitization to and training of ISA [13].

In Germany, with its federal structure, public administrations are very differently positioned in respect of IS. Large federal agencies are often at the forefront of many current topics, such as legislation (IT security law, e-government law, and the digital agenda) or application content like big data analysis or IS. For example, almost two-thirds of the administrations currently surveyed continue to see issues of data security and privacy as a key challenge in using big data analytics [59]. Only one-third believe that a company's own staff has the skills and knowledge to continually drive the administration through data analytics [59]. However, only 37% invest sufficiently in appropriate education and training [59].

If we take a closer look at IS, my experience as a BAköV qualification center [60] is that it is very difficult for small and medium-sized enterprises (SME) and small municipalities to build up a corresponding IS know-how and general training program in their organization. Instead, the training program for the "IT Security Officer in Public Administration" (ITSO) has been established in the federal administration for a decade and is increasingly being used by medium-sized and large state administrations during an annual three-week summer academy in Brühl (Germany). Since 2007, the modular training course for ITSO has been developed and offered by the BaköV in coordination with the BSI acting internally for the federal agencies. Besides knowledge transfer in 5–15 days, it includes an IS-relevant written project

submission and a two-hour exam on a personal computer (PC) program. A form with 120 questions must be filled out with a score higher than 75%—successful students are awarded a certificate valid for 5 years. A total of approximately 600 certificates have been awarded so far [62]. In addition, there are other certified training courses at federal level—e.g., for the data protection and emergency officer. Moreover, there are a wide range of e-learning courses for the employees of the federal authorities. Nevertheless, the development of procedures and models for measuring and assessing the level of IS in federal agencies remains a challenge.

The literature review reveals a general lack of trainings, which is cited as a top reason why contingency and response plans are not effective [22]. In particular, it seems that over the past 15 years institutions have not put their main focus on developing ISA and ISAT-responsible information users [61]. In Germany, after the establishment of the federal project "Security wins!" in 2010, about 80,000 employees from 143 federal authorities were sensitized to IS in the workplace prior to 2017 [62]. The insight from this federal ISA campaign with interactive methods and GBL scenarios is, on the one hand, that raising awareness is an issue that needs to be revisited again and again. On the other hand, the central control system of the federal agencies has proven itself with framework agreements and decentralized implementations and adjustments. For the federal administrations, very valuable materials have been compiled as a so-called "toolbox": flyers and posters, moderation cards, and a CD about live hacking, which is very popular. Hacker's live shows in particular demonstrate how well emotionalization can lead to concern and attention. Moreover, they also show the importance of awareness in thinking about or pointing out the role of the aggressor—a possibility which should be incorporated into awareness-raising and trainings that include psychological aspects [38, 39, 42, 46, 47]. Nevertheless, this campaign is just a drop in the ocean when we consider the entire group of employees. It should be noted that it is the Länder and Kommunen that represent the main proportion of employees in Germany's public administration; the proportion constituted by the federal government is only about one-eighth of the total number of employees. Moreover, public administrations are also responsible to their citizens, and the question arises as to whether information campaigns on IS in public places should not also be part of urban and regional planning [34].

3.1. Information security (awareness) trainings (ISAT)

Although scientific research indicates a general need for (cyberthreat) education, trainings, and awareness [22, 63, 64], our review of the scientific literature [13, 65] shows that the design of the ISA trainings has not been the subject of significant research. Only a few studies from the literary field of knowledge, attitude, and behavior give (general) recommendations on the design of training measures (see [66, 67]). As mentioned above, it should be a user-centered approach and "awareness campaigns should be tailored to employees' needs" [25]. The BSI training describes in general how to set up and maintain an (effective) awareness-raising and training program for IS [10]. The aim of such programs is for employees to perceive safety-critical situations and mitigate their impact, while also providing the necessary knowledge and skills for safety-conscious behavior [10]. In particular, the module "ORP.3 Sensitization and Training" describes the procedural, technical, methodological, and organizational requirements for awareness-raising and IS training [10]:

- *Few successful awareness-raising and training activities*

  The activities carried out for ISAT are not always as successful as desired. The causes for this can be lack of management support, unclear goals, bad planning, lack of success control, lack of continuity, or too few financial and human resources. If no appropriate measures are taken to ensure the success of the activities carried out, the goal of the respective training activity can often not be achieved. If the institution has insufficient activities to raise awareness and train employees, IS can be at risk, which leads directly to restrictions on task performance [10:2].

- *Inadequate training of staff on security functionalities*

  Employees often do not apply newly introduced security programs and features, because they do not know how to operate them, and because they are considered time-consuming in their day-to-day work. In addition, the lack of ISAT after the introduction of new software can lead to unintentional operating errors or incorrect configurations and to errors in the operation and delays in work processes. Therefore, the procurement and installation of (security) software is not enough. In critical IT systems and applications, misuse can threaten the very existence of the business [10:3].

- *Risk that security incidents will not be identified*

  The daily operation of IT and ITC components can cause many failures and errors. There is a risk that security incidents will not be identified as such by staff and that cybersecurity attacks or attempted attacks go undetected. Security incidents and technical errors are sometimes not easy to distinguish. If users and administrators are not specifically trained and sensitized, vulnerabilities can go undetected and may be exploited. If security incidents are not detected in time or are completely missed, full countermeasures cannot be taken in time. Small security loopholes in the institution may be exacerbated and become critical threats to integrity, confidentiality, and availability. This can hinder business processes, cause financial damage, or lead to regulatory and legal sanctions [10:3].

- *Understanding and accepting safeguards*

  Technical security safeguards often lead to less user-friendly IT. Users will only accept such safeguards when they understand why the restrictions—for example, for surfing, for sending and receiving e-mails, or for password usage—are necessary [2:204]. Employees are only able to actually follow the security policies that have been decided upon when they know how to handle the IT securely and confidently [10:3]. Insufficient acceptance of IS must be corrected.

Neither the BSI training description [10] nor the BAköV manual [2] describes specific learning and teaching methods in detail but only refers to the possible content of training courses and potential confounding factors. Tsohou et al. conclude from recent global security surveys that ISAT are not currently working [68] and the question is, why have mainstream ISA techniques failed for so long? The following aspects are likely to play a role:

- One aspect might be a "technocratic" view of risk communication, meaning the tendency for technical experts to tell people what they think and ought to know [69]. This is fundamentally flawed and has been strongly criticized by experts in safety risk communications as ineffective and inefficient [69]. However, providing simple advice directly to nonexperts is no trivial matter, and even experts can disagree about what is important [70]. Moreover, it might disregard the daily mix and overlap between work and home, and therefore ignore an insight from practice—as stated by Ian Kilpatrick, chairman of the Wick Hill Group—"If you don't change home security behavior, it is hugely more difficult to effect change in the office" [71].
- A second aspect might be in 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" [56]. Maybe there is also a "proxy agency effect" [36], where a person defers to experts to ensure that they themselves can still do the things they want to do [28]. Forget et al. [72] consider that users may "disengage" from security if they have already transferred the responsibility to somebody else. Moreover, employees may look for routines to prevent life from "tipping into chaos" and to give them "the confidence to go about their daily activities" [73].
- A third aspect relating to IS campaigns is that a training aimed at addressing security awareness gaps cannot be sufficient to ensure compliance with a security culture [74]. The necessary cultural change in institutions must go hand in hand with a mutual learning process between the top-down requirements of the management and the bottom-up activities of the employees—described as a "spiral of transformative interaction" [13, 34].

In the design of ISAT, emotionalization—as mentioned above—is extremely important for the motivation of employees. Emotionalization must address people's specific concerns, be it at work or at home—including aggressor thinking—to create PBL and AL scenarios for ISAT. Psychological studies [38, 39] show that people have to "understand"—through emotional engagement—that they are themselves affected. GBL is increasingly viewed as an effective method for teaching and learning in education. It is especially effective as a means to stimulate motivation and change behavior and should be explicitly used for ISAT. With the learning approach 3.0 (see Section 2.2), learners can directly see the consequences of their actions and get a sense of their knowledge level in dialog. The integrated AL/PBL scenario development and usage of interactive analog/digital GBL also support IS abilities, which we increasingly need in daily life and in the workplace—for example, communication, cooperation, social interaction, and creativity [49–51]. The emotional level should be explicitly addressed, because social participation in a communicative team process is a key component in this third stage of awareness-raising activities based on psychological theories [45]. Integrated analog and digital game-based ISAT with interactive elements lead to the further involvement of human actors.

3.2. Content of ISAT and institutional programs

The "IT-Grundschutz catalogs" published by the BSI [8] provide a summary of the elementary hazards that are important for ISA and ISAT. Institutions and employees should be aware of

cyber espionage, which can cause considerable damage. In addition, the disclosure of information that is meant to be protected, identity theft, abuse of personal data, abuse of permissions, and social engineering in general are growing threats. If aggressors are able to infiltrate the institution, it is possible that equipment or data carriers may be destroyed or that unauthorized persons use or get administrator access to devices and systems. Lower levels of knowledge and awareness among employees could lead to the incorrect use or administration of devices and systems, data loss, and the loss of integrity of sensitive information. As stipulated in the EU's new GDPR, the violation of laws or regulations can result in huge damage claims. Moreover, without a good work atmosphere, employees may deny having made a mistake, and there is also the potential for insider threats to arise. All these elementary hazards must be addressed in any case in an ISAT oriented to the target group.

The following are specific requirements for ISAT set out by the BSI. The ITSO—nowadays also called Information Security Officer (ISB in German)—is responsible for meeting these requirements. Deviations should be mentioned separately in an institution's requirement guidelines. The ITSO/ISB of an institution should always be involved in all processes and also in strategic decisions. Besides that, the ITSO/ISB is responsible for ensuring that all requirements are met in accordance with the security policy that has been defined and then checked [10]. The BSI differentiates between basic requirements for ISAT, which must be met by institutions in any case, and standard requirements, which should be met in principle [10]. In addition, exemplary proposals are made for requirements that should be taken into account when there is increased need for an institution to be protected. Here, the concrete determination takes place within the framework of a separate risk analysis [10]. It should be clear which basic values are given priority by the requirement.

The basic requirements are as follows [10]:

- The institution's top management MUST actively support security campaigns and trainings for its employees. Therefore, before the start of ISAT and the IS program, the support of the management must be ensured. The management must be sufficiently sensitized to security issues. All supervisors must support IS by setting a good example. Managers must enforce security standards and alert their employees to compliance [10:4].
- There MUST be contact persons (ITSO/ISB) for security issues who can answer both seemingly simple and complex or technical questions. The contact persons MUST be known to all employees of the institution. This information must be easily accessible and available to everyone in the institution [10:4].
- All employees and external users who use the ICT and IoT components MUST be trained and sensitized, inasmuch as this is relevant for their work. To this end, the organization must have binding, understandable, current, and available guidelines specifying the use of the respective components. If ICT or IoT systems or services are used in a way that is in the interests of a competitor institution, this must be communicated [10:5].

Contrary to the findings from the research, the BSI sees the gearing of ISAT and the program to the respective target groups only as a SHOULD in the standard requirements [10]. An audience analysis should be carried out so that action is based on specific requirements. The program can then be created in response to different background needs. It should be regularly

reviewed and updated. However, it should be noted that, according to the research findings, a target group and needs analysis should be mandatory to ensure the success of the action. Moreover, according to BSI [10:5], the training of all employees with regard to their responsibilities for information security issues is also only a SHOULD. Sensitization and training programs SHOULD be regularly checked to ensure that they are up-to-date and adjusted and further developed as necessary [10:5]. Security officers SHOULD be familiar with the IT-Grundschutz methodology and for that, an appropriate IT-Grundschutz training course should be planned on the basis of practical examples [10:5]. The learning success in the field of information security SHOULD be measured and evaluated according to the target group to determine to what extent the objectives described in the awareness-raising and training programs are reached. The measurements should include both quantitative and qualitative aspects and the results should be used to enhance sensitization and improve the appropriate training courses [10:5]. Further requirements may be necessary to increase the protection of any exposed institutions or organizational areas. Particularly exposed persons such as managers and security workers SHOULD undertake in-depth training with regard to possible hazards and appropriate behaviors and precautions [10:6].

Since 2007, the BaköV training course for the ITSO of federal agencies [2] has recommended that security officers initiate and establish the sensitization and training of employees in a modular manner. The course content is grouped into the following 13 training areas, which are in turn assigned to six defined target groups (see **Table 1**). Of course, not all target groups need all the training modules, so some can be used optionally or are not needed at all.

BAköV training modules [2]	**Target group/function**						
	A	**B**	**C**	**D**	**E**	**F**	**…**
1. Basic concepts of information security (IS)	x	x	x	x	x	x	
2. IS in the workspace	x	x	x	x	x	x	
3. Laws and regulations	x	x	x	x			
4. The organization's security concept	x	x	x	x		x	
5. Risk management		x		x		x	
6. (Information) security management		x		o			
7. IT systems		x				x	
8. Operational area		x				x	
9. Technical implementation of security safeguards		x				x	
10. Emergency management		x		x		x	
11. New developments in the IT sector	o	x	x			x	
12. The business management side of IS	x	x	o				
13. Infrastructure security		x		x		o	

Recommendation of training modules and target groups from the BAköV [2: 207] (x: the module is recommended, o: the module is optional). Six examples of defined target groups (A: supervisor, B: security management, C: data protection officer, D: infrastructure security officer, E: users, F: administrators). In order to clarify that this assignment is only meant to serve as an example and must be adapted concretely to the particular institution, undefined target groups are listed here as… .

Table 1. BAköV matrix.

3.3. Measurements of ISA and compliance for information security

To support organizations in discovering the evaluation methods and metrics that meet their individual needs, an overview of current measures for assessing effectiveness was given in [65]. The advantages, disadvantages, and appropriate application of methods like monitoring security procedures, surveys, and security benchmarks are discussed [65]. While the number of firms that apply such measures is increasing, surveys of corporations show that it is unusual for these measures to be accompanied by specific in-depth evaluations of their effectiveness. The literature review reveals that only a few organizations use different metrics for deeper and continuous measurement of their awareness program [65]. However, ISAT should be ongoing as the organization changes and employees move into and across roles, with a focus on what is necessary for their jobs [75]. Therefore, ISAT should not overwhelm employees with information or take up excessive paid work time [76]. As a consequence, security officers should specifically adapt the above BAköV matrix (Section 3.2) to their institution, to their content, and to their target groups. Rather than relying on generalized computer-based packages, IS training should be geared to the specific work environment. IS officers should carefully analyze the concrete situation in the institution: for example, if factors such as noncompliance with security measures, poor acceptance, or social engineering are present, as described in the BSI training [10]. In addition, they should determine which IS core values are particularly at risk in which processes, at which locations, and at which times. Since these awareness-raising measures demand resources such as time, money, and the willingness of employees, every institution should have an interest in assessing their effectiveness [65].

The developed spiral of transformative interaction between an organization and its staff with regard to (IS) learning processes [13] shows the interaction between top-down specifications and individual bottom-up influences on the establishment of a modern, future-oriented organizational security culture. We seek to implement and test our conceptual project design on the transformative interaction between human-based and organizational (IS) learning processes and to promote in-depth ISA measurement in game-based learning environments. Situational and specific ISAT combined with IS awareness-raising measures and evaluation should be an indispensable part of today's organizations with livable IS and policies [34].

4. Summary and outlook

In a general way, ISA programs and ISATs may generate a false sense of security, as taking part in ISA programs reduces perceptions of vulnerability, while the intentions for compliant security behavior are not affected [77]. Information and IT security awareness-raising measures and the evaluation of these measures are an indispensable part of today's information and knowledge society [65]. This assumes that—according to the BSI concept [8, 10, 20, 78]—the relevant IS issues must be regularly trained in accordance with institutional requirements and the necessary sensitization created [10]. Moreover, it gives practical hints for the efficient design of ISAT as a planned, cyclical, and organizational approach. In addition, the

BaköV training program [2] gives suggestions for target-group-oriented themes, particularly for the federal administration, which can be adjusted for the federal state and local public administrations.

A lack of understanding of security issues coupled with the pervasive use of computers often makes employees the "critical factor" in the IS equation. However, as Dark points out [79], knowledgeable human beings are better at preventing IS breaches that occur due to negligence or accident as well as those that stem from malicious activity and the anomalous behavior of systems. They can efficiently and effectively respond to incidents by reporting them promptly, quarantining problems, and diagnosing and treating these problems correctly [79]. We see an increase in social engineering (SE), which is an attack on, and manipulation of, people to get hold of sensitive information and protected data from the institution in preparation for attacks that will not be carried out at once but rather later—e.g., advanced persistence threats (APT). Attacks via SE are often multilevel. By the aggressor pretending to have insider knowledge and at the same time appealing to people's desire to help, he can expand his knowledge in a series of further steps [10:4]. If employees are not adequately sensitized to attacks of this kind, there is a risk that they can be manipulated through skillful communication so that they act inappropriately. This can lead to internal information being passed on via malicious software or even money transferred to alleged business partners. The subsequent worldwide damages can run into the billions [10:4]. Regulations can be more easily complied with, the more informed the employees are about the facts and the better they understand the reasons. ISA is necessary for successful digitization: this requires an organizational strategy, the guarantee of an appropriate IT security level, sufficiently qualified personnel, and a cultural change in the organization, with ongoing, target-group-oriented training for all employees.

However, there is no simple linear cause-and-effect relationship between institutional safeguards and knowledge, attitudes, and real behavior. Despite the increasing interest of researchers in the topic, awareness remains a critical issue in IS [36]. To protect the organizational assets, including user information and systems, the human side of security should also be managed [22, 24], and this plays a significant role in the successful delivery of IS in today's organizations [25]. 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 [56]. Learning in IS should be developed by integrating target-oriented, interactive analog/digital GBL scenarios and team-oriented methods as an ongoing process. Depth psychological studies [38, 47] show that emotionalization and motivation should be important factors in creating short-term scenarios in real-life situations using AL and 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.

We know from our research, experience, and trainings that

- technical security alone is not enough;
- there is still a lack of sensitivity in the business processes of companies and administrations;
- security behavior is necessary for all employees, and not only in the workplace; and

- predefined regulations have to be lived, and this requires a cultural change in the organizations.

Moreover, the author can enrich the current report results of [80] with her own experience and findings for future activities in public administrations as well as in companies:

1. Strategically anchor digitization

Note: No digitization without IS; no IS without continuously increasing ISA and user-centered ISAT.

2. Create organizational units

Introduce ISMS for the institution. Create a position for the IS and introduce security officers.

3. Define responsibilities

Big institutions may consider whether a Chief Digital Officer makes sense nowadays. Undoubtedly, all institutions today need IS officers plus a data protection officer and an emergency officer—and they should think carefully about an awareness officer too.

4. Build up digital literacy

The knowledge assets of an institution and the value of IS are crucial factors in the success of the digital transformation. The use of digital technologies requires new skills from the employees and creates new job profiles. Such new job profiles should include awareness, particularly ISA.

5. Distinguish business processes and models

Businesses should clearly distinguish between the digital strategy for business processes and business models, because the transformation processes have different results to the goal and require different approaches. Public administrations should think about new processes too, combined, however, with IS and ISA.

According to [81], the six major digital trends (mobility, big data, social media, cloud computing, artificial intelligence, and robotics) primarily affect six areas in companies (business models, products and services, customer segments, channels, business processes, and workplaces). The IS challenges will not diminish; attacks will become more diverse. Institutions must make efforts to educate all employees not only in the work environment but also as a means to safeguard their private lives and thus society. Game-based learning (GBL) is especially effective as a means to stimulate motivation and change behavior and should be explicitly used for raising awareness. ISATs should combine GBL plus PBL plus AL in line with real-life situations [51]. Because of complex nonlinear relations between knowledge of IS, attitudes, and the secure behavior of human beings in day-to-day organizational work and in their private lives, further scientific explorations of ISA and ISAT are needed in future. This further research work can be carried out very well at the TUAS Wildau in a research and teaching unit with practical relevance, since here studies for nontechnical public administration have been offered for years, and in winter semester 2018/19 the degree program in administrative computer science will be launched.

Acknowledgements

I would like to thank my interdisciplinary research and development team for their reliable and creative cooperation in the field of information security awareness. I thank Frauke Fuhrmann, Denis Edich, Ernst-Peter Ehrlich, Kai-Benjamin Leiner, Lars Robin Scholl, and Peter Koppatz for the successful completion of our "SecAware4job" project funded by the Horst Görtz Foundation (HGS). I would like to thank Dr. Horst Görtz and the HGS for financial support of the "SecAware4job" project and for publication of this book chapter. Moreover, I thank our project partner Dietmar Pokoyski and his company known_sense in Cologne for their cooperation—he is also the sole distribution partner for all of our game-based learning scenarios.

Author details

Margit Scholl

Address all correspondence to: margit.scholl@th-wildau.de

Department Business, Computing, Law, Technical University of Applied Sciences (TUAS) Wildau, Wildau, Brandenburg, Germany

References

[1] Bundesministerium für Wirtschaft und Energie (BMWi)/Federal Ministry of Economics and Energy. International Dimension: EU – Digital Agenda. Bonn; 2014. Available from: http://www.bmwi.de/Redaktion/EN/Dossier/digitisation.html [Accessed: 2017-05-29]

[2] Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern (BAköV)/Federal Academy of Public Administration in the Federal Ministry of Interior. Manual of IT Security Officer in the Public Administration, version 3.0. Brühl; 2009

[3] Available from: https://www.verfassungsschutz.de/de/aktuelles/zur-sache/zs-2017-004-gastbeitrag-handelsblatt-20171127 [Accessed: 2017-12-28]

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI)/Federal Office for Information Security. 14. Deutscher IT Sicherheitskongress. Knowing risks, accepting challenges, designing solutions. In: Conference Proceedings for the 14th German IT Security Conference, Preface. Bonn, Bad Godesberg; 2015. Available from: https://www.bsi.bund.de/DE/Service/Aktuell/Veranstaltungen/IT-Sicherheitskongress/14_ITSicherheitskongress/14_ITSiKongress.html [Accessed: 2018-01-20]

[5] Available from: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html [Accessed: 2017-10-28]

[6] International Organization for Standardization (ISO) Survey, The ISO Survey of Management System Standard Certifications (2006-2015): ISO/IEC 27001—Information Technology—Information Security Management Systems—Requirements, ISO/IEC 27001: 2013/Cor 2:2015. 2015

[7] PCI Security Standards Council. Security Awareness Program. Special Interest Group, PCI Data Security Standard (PCI DSS), Version 1.0; 2014

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI)/Federal Office for Information Security. Self-Declaration and IT-Grundschutz Certificate. Bonn; 2016. Available from: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCertification/OrganisationofCertification/organisationofcertification_node.html [Accessed: 2016-12-01]

[9] Available from: https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html;jsessionid=70E868EBB5E530CDA1AF059A22A5D485.1_cid341 [Accessed: 2018-01-10]

[10] Bundesamt für Sicherheit in der Informationstechnik (BSI)/Federal Office for Information Security. ORP.3: Sensibilisierung und Schulung/Sensitization and training. Bonn; 2016. Available from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html [Accessed: 2018-01-17]

[11] Kruger H, Drevin L, Steyn T. Email security awareness: A practical assessment of employee behaviour. In: Futcher L, Dodge R, editors. Fifth World Conference on Information Security Education. IFIP – International Federation for Information Processing. Vol. 237. Boston, MA: Springer; 2007:33-40

[12] 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

[13] 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. pp. 2235-2244. Available from: http://hdl.handle.net/10125/50168 [Accessed: 2018-01-20]

[14] Verton D. The Hacker Diaries. New York: McGraw-Hill, Inc.; 2002

[15] Enterprise Strategy Group (ESG). Brief: Cybersecurity Skills Shortage: A State of Emergency. Research Report, IT Spending Intentions Survey; 2016. Available from: http://www.esg-global.com [Accessed: 2018-01-20]

[16] Allianz für Cyber-Sicherheit/Alliance for Cyber Security. Awareness-Umfrage. 2015. Available from: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/awareness-umfrage-2015.pdf?__blob=publicationFile&v=5 [Accessed: 2016-12-02]

[17] Digitalverbund Bitkom 9/2017. Quoted and available from: https://manucarus.wordpress.com [Accessed: 2018-01-17]

[18] Ponemon Institute Report 2017. Quoted and available from: https://manucarus.wordpress.com [Accessed: 2018-01-20]

[19] Verizon's Data Breach Investigations Report 2017. Available from: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ [Accessed: 2017-05-30]

[20] Bundesamt für Sicherheit in der Informationstechnik (BSI)/Federal Office for Information Security. BSI-Standard 100-1. Information Security Management System. Version 1.5. Bonn; 2008. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.html [Accessed: 2018-01-20]

[21] Singh AN, Picot A, Kranz J, Cupta MP, Ojha A. Information security management (ism) practices: Lessons from select cases from India and Germany. Global Journal of Flexible Systems Management. 2013;**14**:225-239

[22] Kim EB. Recommendations for information security awareness training for college students. Information Management & Computer Security. 2014;**22**:115-126

[23] Shaw RS, Chen CC, Harris AL. The impact of information richness on information security awareness training effectiveness. Computers & Education. 2009;**52**:92-100

[24] Workman M. Gaining access with social engineering: An empirical study of the threat. Information Systems Security. 2007;**16**:315-331

[25] 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. Business white paper: Hewlett Packard; 2016

[26] Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences. 2012;**43**:615-660

[27] Von Solms SH. The 5 Waves of Information Security: From Kristian Beckman to the Present. In: Rannenberg K, Varadharajan V, Weber C, editors. SEC 2010, IFIP International Federation for Information Processing AICT 330. 2010;1-8

[28] Bandura A. Social cognitive theory: An Agentic perspective. Annual Review of Psychology. 2001;**52**:1-26

[29] Chen CC, Medlin BD, Shaw RS. A cross-cultural investigation of situational information security awareness programs. Information Management & Computer Security. 2008;**16**:360-376

[30] Safa N S, von Solms R, Furnell S. Information security policy compliance model in organizations. Computers & Security, 2016;**56**:70-82

[31] Herath T, Rao HR. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems. 2009;**47**:154-165

[32] Pattinson M, Parsons K, Butavicius M, McCormac A, Calic D. Assessing information security attitudes: A comparison of two studies. Information & Computer Security. 2016;**24**:228-240

[33] Winkler I. The Human Exploitation Kill Chain (Video), RSA Conference (2017), USA. 2017. Available from: https://www.rsaconference.com/events/us17/agenda/sessions/6682-The-Human-Exploitation-Kill-Chain%20RSA [Accessed: 2017-05-30]

[34] Scholl M. Raising Information Security Awareness in the Field of Urban and Regional Planning. Submitted to the International Journal of E-Planning Research (IJEPR). 2018 (forthcoming)

[35] Briggs P, Jeske D, Coventry L. Behaviour Change Interventions for Cybersecurity. Behavior Change Research and Theory. London: AP; 2017:115-136. DOI: 10.1016/B978-0-12-802690-8.00004-9

[36] Zz Z et al. (review process). Security Kairos: The Art and Science of Raising Awareness and Offering Consumer Advice at Point-of-Sale. 2018 (forthcoming)

[37] Fogg BJ. A behavior model for persuasive design. 2009. In Proceedings of the 4th International Conference on Persuasive Technology (Persuasive 2009). Article No. 40. DOI: 10.1145/1541948.1541999

[38] Haucke A, Pokoyski D. Mea culpa - Schuld, Scham und Opferrolle bei Social Engineering. kes. 2018;**1**:6-8

[39] Pokoyski D. Security Awareness: Von der Oldschool in die Next Generation – eine Einführung. In: Helisch M, Pokoyski D, editors. Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Wiesbaden: Vieweg+Teubner; 2009. pp. 1-8

[40] Available from: https://en.wikipedia.org/wiki/Organizational_commitment [Accessed: 2017-06-10]

[41] Albrechtsen E. A qualitative study of users' view on information security. Computers & Security. 2007;**26**:276-289

[42] DSV-Gruppe; EnBW; <kes>; known_sense; nextsolutions; Pallas; editors. Entsicherung am Arbeitsplatz – die geheime Logik der IT-Security in Unternehmen. Köln & München; 2006. Available from: http://known-sense.de/de/Produkte/Security_Studien_2/ [Accessed: 2018-03-06]

[43] SanNicolas-Rocca T, Schooley B, Spears JL. Designing effective knowledge transfer practices to improve is security awareness and compliance. 47th Hawaii International Conference on System Sciences (HICSS); 2014:3432-3441

[44] Straub DW, Welke RJ. Coping with systems risk. Security planning models for management decision making. MIS Quarterly. 1998;**22**:441-469. DOI: 10.2307/249551

[45] Scholl M, Fuhrmann F, Pokoyski D. Information security awareness 3.0 for job beginners. In: Varajão JE, Cruz-Cunha MM, Martinho R, Rijo R, Bjørn-Andersen N, Turner R, Alves D, editors. Proceedings of the Conference on ENTERprise Information Systems (CENTERIS). 2016. pp. 433-436

[46] Helisch M, Pokoyski D, editors. Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Wiesbaden: Vieweg+Teubner; 2009

[47] known_sense, Lanxess, Technische Hochschule Wildau, <kes> (editors). Bluff me if u can – Gefährliche Freundschaften am Arbeitsplatz. Tiefenpsychologische Wirkungsanalyse Social Engineering und seine Abwehr, 2015. Available from: http://www.knownsense.de/BluffMeIfUCanAuszug.pdf [Accessed: 2016-03-16]

[48] 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**:10862-10868

[49] Fuhrmann F, Scholl MC, Edich D, Ehrlich EP, Leiner KB, Scholl LR. Raising awareness for information security in a playful way. In: Proceedings of the London International Conference on Education (LICE). London: Infonomics Society; 2016:190-191

[50] Fuhrmann F, Scholl MC, Edich D, Koppatz P, Scholl LR, Leiner KB, Ehrlich EP. Info rmationssicherheitsbewusstsein für den Berufseinstieg. Abschlussbericht Projekt SecAware4job. Aachen: Shaker; 2017. DOI: 10.2370/9783844054668

[51] Scholl M, Fuhrmann F. Living in a digital world: Improving skills to meet the Challenges of digital transformation through authentic and game-based learning. Keynote at the 21st world multi-conference on Systemics, cybernetics and informatics (WMSCI 2017). Journal of Systemics, Informatics and Cybernetics. 2017;**5**:81-86. Available from: http://www.iiisci.org/journal/CV$/sci/pdfs/IP037LL17.pdf [Accessed: 2017-12-25]

[52] Available from: http://secaware4job.wildau.biz [Accessed: 2018-01-20]

[53] Available from: https://www.comble-project.eu [Accessed: 2018-01-21]

[54] Available from: https://methopedia.eu [Accessed: 2018-01-21]

[55] Chen Y, Ramamurthy K, Wen K-W. Information security policy compliance: Stick or carrot approach? Journal of Management Information Systems. 2014;**29**:157-188

[56] Kirlappos I, Beautement A, Sasse MA. "Comply or die" is dead: Long live security-aware principal agents. In: Adams AA, Brenner M, Smith M, editors. Financial Cryptography and Data Security. FC 2013, Lecture Notes in Computer Science. Vol. 7862. Heidelberg: Springer; 2013:70-82

[57] James T, Nottingham Q, Kim BC. Determining the antecedents of digital security practices in the general public dimension. Information Technology and Management. 2013;**14**:69-89

[58] Tsohou A, Karyda M, Kokalakis S, Kiountouzi E. Managing the introduction of infor-mation security awareness programmes in organisations. European Journal of Information Systems. 2015;**24**:38-58

[59] KPMG Wirtschaftsprüfungsgesellschaft AG (KPMG). Big Data, große Baustelle. Mit Daten Werte schaffen 2017 – Sonderausgabe für die öffentliche Verwaltung. Available from: https://home.kpmg.com/de/de/home/themen/2017/09/mit-daten-werte-schaffen-2017--spotlight-oeffentlicher-sektor--.html [Accessed: 2018-01-20]

[60] Available from: https://twz-ev.org/weiterbildungen/it-sicherheitsbeauftragte-i/ [Accessed: 2018-01-21]

[61] Young R. Growth perspective of information security. Journal of Information Privacy and Security. 2014;**5**:51-67

[62] Exchange of information between the qualification centers of the BAköV at the TUAS Wildau on January 27, 2017

[63] Jones BH, Chin AG, Aiken P. Risky business: Students and smartphones. Tech Trends. 2014;**58**:73-83

[64] McCrohan KF, Engel K, Harvey JW. Influence of awareness and training on cyber security. Journal of Internet Commerce. 2010;**9**:23-41

[65] Scholl M, Leiner KM, Fuhrmann F. Blind spot: Do you know the effectiveness of your information security awareness-raising program? In: Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017); 2017. pp. 58-62. Available from: http://www.iiisci.org/Journal/CV$/sci/pdfs/SA199CD17.pdf [Accessed: 2017-12-26]

[66] Scholl M, Fuhrmann F, Pokoyski D. The human factor: How can information security awareness be sustainably achieved in E-government? In: Scholl HJ, Glassey O, MFWHA J, editors. Electronic Government and Electronic Participation. Joint Proceedings of Ongoing Research, PhD Papers, Posters and Workshops of IFIP EGOV and ePart 2016. Innovation and the Public Sector, 23. Netherlands: IOS Press; 2016:403-404

[67] Slusky L, Partow-Navid P. Students information security practices and awareness. Journal of Information Privacy and Security. 2012;**8**:3-26

[68] Tsohou A, Karyda M, Kokalakis S, Kiountouzi E. Analyzing trajectories of information security awareness. Information Technology & People. 2012;**25**:327-352

[69] 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

[70] Reeder R, Ion I, Consolvo S. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. In: Proceedings of the 2017 IEEE Symposium on Security and Privacy (S&P). IEEE; 2017. DOI: 10.1109/MSP.2017.265093101

[71] Caldwell T. Making security awareness training work. Computer Fraud & Security. 2016;(6):8-14

[72] Forget A, Pearman S, Thomas J, Acquisti A, Christin N, Cranor LF, Harbach SEM, Telang R. Do or do not, there is no try: User engagement may not improve security outcomes. In: Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). USENIX Association; 2016:97-111

[73] Coles-Kemp L, Hansen RR. Walking the line: The everyday security ties that bind. In: Tryfonas T, editor. Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science. Vol. 10292. Cham: Springer; 2017:464-480. DOI: 10.1007/978-3-319-58460-7_32

[74] Fagade T, Tryfonas T. Security by compliance? A study of insider threat implications for Nigerian banks. In: Tryfonas T, editor. Human Aspects of Information Security, Privacy, and Trust, HAS 2016, Lecture Notes in Computer Science. Vol. 9750. Cham: Springer; 2016:128-139

[75] Kirlappos I, Parkin S, Sasse MA. Learning from "shadow security": Why under-standing non-compliance provides the basis for effective security. In: Proceedings of the Workshop on Usable Security (USEC); San Diego, CA, USA. 2014

[76] Van Niekerk JF, von Solms R. Information security culture: A management perspective. Computers & Security. 2010;**29**:476-486

[77] Bauer S, Bernroider EW. The effects of awareness programs on information security in banks: The roles of protection motivation and monitoring. In: Tryfonas T, Askoxylakis I, editors. Human Aspects of Information Security, Privacy, and Trust. HAS 2015. Lecture Notes in Computer Science. Vol. 9190. Cham: Springer; 2015:154-164

[78] Bundesamt für Sicherheit in der Informationstechnik (BSI)/Federal Office for Information Security. ICS Security Compendium, Version 1.23. Bonn; 2013. Available from: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html [Accessed: 2018-01-20]

[79] Dark MJ. Security education, training and awareness from a human performance technology point of view. In: Whitman ME, Mattord HJ, editors. Readings and Cases in Management of Information Security. Mason, OH: Course Technology; 2006:86-104

[80] Tata Consultancy Services (TCS), Bitkom Research. Deutschland endlich auf dem Sprung? Trendstudie. TCS_Bitkom_Research_Trendstudie_Digitalisierung_2017.pdf. 2017. Available from: https://www.bitkom-research.de [Accessed: 2018-01-20]

[81] Tata Consultancy Services (TCS). Die zwei Gesichter der Digitalisierung. Deutsche Unternehmen sind gespalten. Studie-Die-zwei-Gesichter-der-Digitalisierung.pdf. 2017. Available from: http://sites.tcs.com/2-Gesichter-der-Digitalisierung/ [Accessed: 2018-01-21]