Awareness in Information Security

Margit SCHOLL
Department Business, Computing, Law, Technical University of Applied Sciences (TUAS) Wildau
Wildau, Brandenburg 15745, Germany

ABSTRACT

The digital transformation taking place in society is changing social behavior. Technical developments must be understood and designed in an acceptable user-friendly way. In line with the General Data Protection Regulation (GDPR) of the European Union (EU), information security (IS) must be in place for the use of mobile devices and services, in particular IS by design and IS by default. Nevertheless, the significant and associated hazards of abuse and organized crime must be prevented. Information security awareness (ISA) is a necessary response to the challenges ahead. IS and ISA must be an integrated part of these agendas. The goal of IS is to protect information of all types and origins. Psychologically based research shows that a systemic approach might be helpful in raising awareness. This is where game-based learning (GBL) comes into play. Psychological studies show the great importance of emotionalizing when communicating IS knowledge and the reliable exchange of experience about IS. A new integration of analog serious games and different learning methods, called awareness training 3.0, is needed as a means to incorporate *knowledge* transfer, *emotionality*, and *team-based* applications. This paper summarizes important scientific findings, transfers them to the practice of IS trainings, and discusses examples.

Keywords: Information security (IS), data protection, information security awareness (ISA), IS compliance, information security awareness trainings (ISAT), game-based learning (GBL)

1. INTRODUCTION

Government digital agendas worldwide go hand in hand with the digital transformation of processes in businesses and public administrations as well as the digital changes taking place in society.

Digit(al)ization affects almost all areas of life in an increasingly rapid way, and the underlying information communication technology (ICT) electronically collects, stores, processes, and transfers large amounts of data and diverse information. Through the cross-sectoral nature of information and communication technologies (ICT), digitalization affects almost all areas of life. Under the slogan "Digitalization for All," adequate and affordable Internet access has been proposed by the B20 taskforce and the G20 to develop solutions for the challenges of a digital world economy.[i] The G20 wants to shape digitalization to create an interconnected world and is seeking to connect everyone to the Internet by 2025. As part of the G20 Digital Economy Ministerial Declaration, an international working program was agreed as "A Roadmap for Digitalization" in Annex 1, while Annex 2 addresses the development of digital skills in lifelong learning. The G20 Priorities on Digital Trade in Annex 3 are a contribution to open markets and a fair trading system.

Information security (IS) and awareness must be an integrated part of these agendas. The motto should be: digitization with integrated information security, and information security with integrated awareness-raising. 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. In contrast, IT security is specifically oriented toward the protection of information processed and stored electronically. Moreover, the term cybersecurity (CS) includes all information technology connected to the Internet and comparable networks.

A current example in Germany is the renewed hacker attack on the federal government network that took place around the turn of the year 2017/18. This is a technical network that is considered particularly secure.[ii] Generally speaking, attackers' ability to compromise victims' systems and networks has been greatly enhanced in terms of penetration speed, and the rate of these cyberattacks continues to escalate, which increases the danger to organizations' brand reputation and revenue [30]. Damage to the reputation of an organization or injury to people could be even more critical and permanent than a one-time financial expense. Moreover, the reliance on technology-based solutions is associated with a limited understanding of complicated information system security (ISS) characteristics intertwined with technical, institutional, sociocultural, and organizational aspects [11]. "Consequently, it is natural that the focus of ISS has shifted from technical approaches to approaches pertaining to socio-organizational and individual behavior" [33]. Public administrations, companies, and other organizations are required to protect the information they manage and to guarantee IS and the protection of sensitive data. They can only accomplish this when those responsible know which information in which business processes and which IT are endangered by which threats.

The following second section of the article briefly explains the important basic terms of IS. In Section Three, the results of a continuing literature research on information security awareness trainings (ISA), IS complaints, and information security awareness trainings (ISAT) are collected and discussed. The fourth section summarizes the essentials and gives an outlook for the future. In addition to the references, there is an annex with previously unpublished tables of the original literature research from 2016, which served as a starting point for the following essay.

2. BASIC VALUES OF INFORMATION SECURITY

According to the IGI Global dictionary (2017)[iii] there are two different views—and therefore definitions—of digitalization. From a societal point of view, it means the integration of digital technologies into everyday life, including the process of making digital everything that can be digitized and the process of converting information into digital format. From a more technical point of view, it refers to the technology of digitizing information into the binary digits that can be processed by computers: the computer then decodes the digits and generates information that can be read by humans. However, in either case users face a complex scenario with many abstract elements that are not easy to understand. Successful digit(al)ization in democratic societies must therefore ensure an adequate level of IS, security and privacy standards, and data protection. The new General Data Protection Regulation (GDPR)[iv] of the EU, which has been in force since 2016, has been applied since 25 May 2018 and is having a major impact on the provision of digital services. It highlights the importance of another, human aspect of technology development: the training of software developers must take safety aspects into account right from the start. This has been attempted for the first time in the field of data protection: in article 25 of the GDPR it explicitly provides data protection by design and by default. Thus, the users of new secure technology do not need to know every detail but only how these systems can be used securely.

Questions of IS and IT security are part and parcel of daily life. According to the German IT-Grundschutz of the Federal Office for Information Security (BSI), the following scenarios are risky because they can cause potentially serious damage to an organization and to individuals [05, 10]:

- Physical injury
- Negative internal or external effects
- Violation of laws, regulations, or contracts
- Impairment of the right to informational self-determination
- Impaired ability to perform tasks
- Financial effects.

One does not do security on the side. Security is not a feature. It is a process. Security must be planned from the beginning and integrated into all the processes, the IT landscape, and the entire organizational structure, in collaboration *with* the people concerned to create an internal, corporate safety and security culture. However, security must be easy for people—otherwise it will not be used or will be simplified by users themselves. The general goals of IS are as follows [05]:

- Confidentiality—this requires protection against the unauthorized access to and disclosure of information. Confidential information must only be accessible to those authorized and using the permitted access methods.
- Integrity—this refers, on the one hand, to ensuring the correctness (uncorruptedness) of data and, on the other, to the correct operation of systems. Falsified data can lead to poor decisions and incorrect evaluations, and can have serious consequences.
- Availability—this means that services, the functions of an IT system, IT applications, IT networks, or even data and information are available to be used as intended by users at any time.
- Authentication—this refers to the property that guarantees that a person, an IT component, or an application is actually the person or object it is presenting itself to be. When information is authentic, then it is ensured that it was generated by the specific source.
- Commitment—here we have two aspects: technical commitment means the sender has provided verification of his or her identity and the recipient is unable to deny having received the message; organizational commitment is the individual's psychological attachment to the organization.
- Reliability—is also called dependability of IT components and consists of their *quality* in terms of correctness, robustness, and failproofness so that their typical functions can be executed with the necessary precision and during the normal period of use.

So we have two things to look at: first, all (business) processes must be analyzed to determine the *acceptable* security level to be achieved. This also means determining which risks the institution must live with. Second, *adequate* safeguards (meaning security rules) must be set up in such a way that they can be implemented by all employees. For this, the management must necessarily take on a role model function [05, 10]. 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 [49], because information systems involve human beings, and users do not always act the way they are supposed to [04].

3. LITERATURE REVIEW AND DISCUSSION

A more intensive literature research was originally conducted in 2016. The initial criteria included limiting the search to scientific publications from the past ten years—i.e., starting from the year 2006. Some ten scientific journals were used, including *Information Systems Quarterly*, *Information Systems Research*, *European Information Systems*, *Information Security & Information Security Journal: A Global Perspective*, and *International Journal of Information Security*. The keywords "information security," "awareness," and "human factor" were chosen in a more broad-based approach. In line with this, the following topics were grouped: awareness raising and training and applied awareness measures; security awareness measures and factors influencing information behavior and IS culture; human factors influencing the vulnerability of information security; knowledge, attitudes, and behavior; social engineering (SE) methods; the role of information security managers; the measurement of information security awareness; history and theories. In addition, there were some articles with a more particular focus on measures relating to the *effectiveness* of awareness trainings and scientific literature on *psychological* aspects as well as game-based learning methods. In mid-2016, around 150 scientific articles were identified, around 80 of which were used more intensively for references. Here, the basis of this literature review is shown for the first time (in tabular form, see table 1–3 in the appendix). The author continued to study the scientific literature as an ongoing process, so that further and current scientific publications are included in this article.

3.1 Information security awareness (ISA)

Awareness is the ability to directly know and perceive, to feel, or to be cognizant of events, and is a *relative* concept. Awareness may be focused on an internal state, such as a visceral feeling, or on external events by way of sensory perception. Insects do not have consciousness in the usual sense because they lack the brain capacity for thought and understanding. More broadly, it is the state of being conscious of something.[v] But the question of what consciousness actually *is* leads to the realization that consciousness can have a multitude of meanings [27]. Analogous to this, the term "security awareness" is also characterized by a variety of possible interpretations.

From the past scientific literature review different studies produce different definitions of ISA in terms of the variety of aspects involved (see annex, table 1). However, many researchers support the KAB model with the three dimensions of *knowledge*, *attitudes*, and *behavior* [47]. This model suggests that ISA is the product of what employees or users know about IS and its vulnerabilities, the opinion they have of IS, and their actual behavior in this context. These three dimensions have been further divided into different focus areas, and the model has been adopted and modified by other researchers (e.g., [57], [56]). The paper of [65] outlines five dimensions of ISA, namely its organizational, general public, sociopolitical, computer ethical, and institutional educational dimensions, along with the target groups within each dimension who require different kinds of information. Al-Daeef et al. (2017) have combined [35], [66], [77], and [02] in their current definition: ISA is "the security knowledge that has been gradually acquired through a continuous and updated catchy training manner to influence trainees' behavior" [01].

However, there is no easy linear way to explain human IS behavior. Warkentin et al. (2011) indicate that certain social conditions within the organizational setting contribute to an informal learning process. This process is distinct from formal compliance-training procedures and is shown to influence employee perceptions of the efficacy of compliance activities, which contributes to the behavioral intention to comply with information privacy policies [75]. For the purposes of practice and to foster learning through vicarious experience, IT managers can pair new employees with mentors and organize group learning exercises [75]. Kirlappos et al. (2013) conclude that effective problem detection and the adaptation of security measures need to be decentralized, and employees should be the principal agents deciding how to implement security in specific contexts. Therefore, the first step is to recognize employees' primary task focus and design security that fits with individual tasks and business processes—only when this has been achieved should organizations focus on communication [42]. As Willison & Warkentin (2013) point out, numerous studies have focused on the security behavior of employees without regard to the *motivational* factors. They suggest that violations are largely due to non-malicious non-compliance, poor employee awareness training, low motivation and commitment, or weak oversight from management [76]. However, they believe the interplay between thought processes and context may significantly impact the efficacy of IS security controls, and specifically deterrence safeguards [76].

3.2 Information security (IS) compliance

Humans often fail to perform the security behaviors their organization requests to protect informational assets ([08], [44], [14]) and employees' poor compliance with information security policies (ISP) is an ongoing problem ([45], [72]). However, Vance et al (2012) point out that prior studies have not examined the influence of relevant past experience and automatic behavior on employee decisions to comply [74]. Moreover, current information security analysis methods do not allow IS managers to capture the rationalities behind employees' compliance and non-compliance [45]. This is the motivation of Kolkowska et al. (2017) to provide managers with a tool to make them more knowledgeable about employees' information security behaviors [45]. The question of whether a tool is really the right way merits discussion. More important might be the findings of Hu et al. (2012), that the participation of high-level managers in IS initiatives has a significant direct and indirect influence on employees' attitudes toward, subjective norms of, and perceived behavioral control over compliance with IS policies [32]. They also find that top management participation strongly influences organizational culture, which in turn impacts employee attitudes toward, and perceived behavioral control over, compliance with IS policies [32].

Tables 2 and 3 list all the prior studies on IS compliance that could be located. These factors can be divided into individual and organizational levels. For the sake of clarity, these factors were put into two separate tables. It should be noted that there are factors that cannot be assigned to only one level but, in reality, affect both levels (e.g., technological influences).

Kruger et al. (2007) work on informational cyber threat awareness with an email awareness experiment [49]. Siponen et al. (2007) investigate employees' adherence to IS policies with a web-based questionnaire [64]. Workman (2007) does surveys (self-reports) and observations (an empirical field study) of reactions to phishing mails concerning SE attacks [78]. Herath & Rao (2009) describe various factors relating to employee intentions to comply with an organization's IS policies according to different theories (General Deterrence Theory (GDT), Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), Decomposed Theory of Planned Behavior (DTPB), Organizational Commitment (OC)) [29]. Boss et al. (2009) use questionnaires to measure how organizations motivate individuals to take precautions in accordance with extant policies and procedures and the role of individual perceptions of mandatory safeguards [09]. Kruger et al. (2010) develop a questionnaire consisting of a vocabulary test as an aid to assess awareness levels and an evaluation of the respondents' IS behavior [48]. McCrohan et al. (2010) give lectures on cyberthreats caused by poor password management to promote awareness intervention on user security behavior [54]. Sun et al. (2011) do observations to find factors influencing attitudes toward security measures for protecting data of differing importance for "information security readiness" (ISR) [70].

Warkentin et al. (2011) do a survey of healthcare professionals to answer the question "How does the informal social learning environment influence employee perceptions of the efficacy of complying with information privacy policy and their intention to comply"? [75]. Hu et al. (2012) do a survey concerning the role of organizational culture in shaping employee intentions to comply with IS policies, and how the top management influence employee intentions to comply with IS policies [32]. Slusky & Partow-Navid (2012) do a survey to gain insight into compliance via the ISA of students [67]. Hanamura et al. (2013) do an Internet survey to ascertain the attributes of victims in IS incidents [25]. Kirlappos et al. (2013) do an interview analysis of real-world non-compliance examples to understand drivers for non-compliant actions in IS [42]. Liang et al. (2013) develop surveys and questionnaires according to the Regulatory Focus Theory to get input in compliance behavior instead of compliance intention based on control [52]. Styles (2013) combines online surveys, SE experiments, and behavioral observations to assess user awareness [68]. Chen et al. (2014) do a web-based field experiment to find relations between coercive control, remunerative control, and certainty of control [13]. Flores et al. (2014) do surveys, phishing experiments, and interviews to investigate security behavior in practice [21]. Jones et al. (2014) do a survey on the smartphone security practices of undergraduate college students [37]. Parson et al. (2014) do surveys and interviews to get information about knowledge, attitudes, and behavior across eight policy-based focus areas [57]. Mejias & Balthazard (2014) do questionnaires based on the Technological Threat Avoidance Theory (TTAT) and General Deterrence Theory (GDT) to define an IS risk model [55].

Chu et al. (2015) do a web-based survey based on the Theory of Planned Behavior (TPB) to investigate the actual behavior and employees' IS resource misuse [15]. Hsu et al. (2015) do surveys based on Social Control Theory (SCT) to gain insight into the consequences of organizational in-role and extra-role security behaviors on the effectiveness of IS policies and the role of formal and social controls [31]. Ngoqo & Flowerday (2015) do surveys to find factors contributing to student mobile phone users' poor IS behavior in South Africa [56]. Pattinson et al. (2016) run questionnaires to investigate non-malicious computer-based behavior and how it is influenced by individual, organizational, and interventional factors [58]. Tsohou et al. (2015) do interviews to define a framework that combines Actor-Network Theory (ANT), Structuration Theory, and the Theory of Contextualism [72]. Da Veiga (2016) creates an information security culture assessment (ISCA) questionnaire to describe the influence of security policy on the security culture of employees [19]. Fagade & Tryfonas (2016) do a survey concerning the behavioral dimension of compliance to IS standards concerning employees of selected banks in Nigeria [20]. Pattinson et al. (2016) use self-reporting online survey and one-on-one repertory grid technique interviews to get facts about attitudes toward naive and accidental IS behavior among students [58]. Safa et al. (2016) do data analysis of a web-based questionnaire according to Social Bond Theory (SBT) and Involvement Theory (InvT) to define a conceptual framework of different aspects of involvement (IS knowledge sharing, collaboration, intervention, and experience, as well as attachment, commitment, and personal norms) [60].

The study conducted by Yazdanmehr et al. (2016) explores the role of norms in employees' compliance—within US companies—with an organizational information security policy (ISP). Their results show that ISP-related personal norms lead to ISP compliance behavior, and the effect is strengthened by ISP-related ascription of personal responsibility [79]. Moreover, social norms related to ISP—the product of a principled ethical climate in an organization—an awareness of consequences, and the ascription of personal responsibility shape personal norms [79]. Future research might explore factors that were not examined such as employees' personal characteristics or organizational culture to enhance the understanding of ISP compliance [79].

Foth et al. (2016) use General Deterrence Theory (GDT) and the Theory of Planned Behavior (TPB) to examine the psychological factors that influence employees' intentions to comply with data protection regulations in hospitals [22]. Bélanger et al. (2017) propose a model grounded in TBP and information security literature to study the determinants of early conformity with technology-enforced security policies. They tested the model respondents from a university that implemented new password policies [08]. Grounded in TPB, their study argues that attitude and security self-efficacy, but not subjective norms, affect behavioral intention [08]. One of their findings is the critical role that attitude plays in affecting intention [08].

Ifinedo's (2013) study investigates employees' information systems security policy (ISSP) compliance behavior in organizations, viewed through the theoretical lenses of social bonding, social influence, and cognitive processing. Data from a survey of business managers and IS professionals confirmed that social bonds that are formed at work have a major influence on attitudes toward compliance and subjective norms, with both constructs positively affecting employees' ISSP compliance [34]. Employees' locus of control and capabilities and competence related to IS security issues also affect ISSP compliance behavior [34].

To improve users' compliance, Bauer et al. (2018) utilize a multiple case design to investigate three banks from central and eastern Europe that have IS practices and established IS processes in common. Before users are allowed to begin their work and receive the necessary privileges, they have to sign an acknowledgment and acceptance of the ISP [06]. The analysis of Bauer et al. (2017) reveal that the unintentional and intentional behaviors of users are likely to trigger IS incidents from the perspective of the users themselves as well as from IS managers overseeing their behaviors [06]. Moreover, the IS managers mention that the majority of users are aware of IS risks, but it seems that many intentionally act in a way that is non-compliant with their ISP [06]. Additionally, all banks have established different annual e-learning strategies addressing IS—however, the IS managers are not satisfied with the impact of e-learning on the users, meaning that the employees do not take the courses seriously enough [06]. According to IS standards, Bauer et al. (2018) recommend the organizational implementation of a *full* PDCA cycle model with regard to IS and show a positive impact in terms of lowering levels of perceived IS risks, acknowledging responsibilities, attributing importance to IS, and building up knowledge of ISP [06].

Our own review results show that, on the one hand, a great deal of research is being done, while, on the other, the different ways in which ISA is measured illustrate a variety of non-linear, complex interactions that influence the behavior of humans with respect to IS. A newer review of 114 influential security policy-related journal articles is done by Cram et al. (2017) with the aim of synthesizing what is known and what remains to be learned about organizational information security policies, focusing the holistic understanding of this research stream and identifying promising paths for future studies [17]. Likewise, necessary changes in the approach in modern organizations should be clarified. Bauer et al. (2018) recommend a mix of ISA design interventions—e.g., in terms of diverse media visualizing IS risks and threats, engaging stories about real-life IS incidents to encourage users to share their own experiences, and a target-oriented evaluation with suitable metrics [06].

3.2 Information security awareness trainings (ISAT)

There are numerous methods that can be used to measure the effectiveness of ISA and organizational programs, and they differ widely in their suitability and applicability for evaluating knowledge, willingness, and/or possible behavior. For example, Kim (2014) conducts a survey on the status of ISA trainings (ISAT) among college students [40]. Bauer & Bernroider (2015) examine how ISA programs affect the intention of German bank employees to practice IS-compliant behavior [07]. However, there have only been a few KAB studies carried out that give (general) recommendations for the *design* of training measures ([58], [67]).

A time-alignment proposal comes from Kirlappos & Sasse (2012) to create short tutorials for a potential user-training approach. Their example of security education being delivered in the context of phishing would be a game in which users can collect or lose points by answering questions about the trust and assurance indicators (identified above) on a professional-looking website [43]. Because phishing has been common for years, there are some early training examples related to this type of attack. As an example, Sheng et al. (2007) present the design and evaluation of Anti-Phishing Phil, an online game that teaches users good habits to avoid phishing attacks. Their findings show that *interactive games* may be a promising way to educate people on how to protect themselves against phishing attacks [62]. Moreover, Kumaraguru et al. (2008) discuss an *embedded* digital training system geared to phishing attacks, called PhishGuru, as an effective way to teach users to identify phishing scams [50]. An app-based learning game for home computer users to protect against phishing attacks is presented by Arachchilage & Cole (2011), proposing that *mobile games* can be easily integrated into a user's natural environment. They applied Technology Threat Avoidance Theory (TTAT) to define the game design principles and produced the prototype game using the Google App Inventor Emulator [03].

Today, "serious games" are in fact widely accepted in the security sector—even at management level it is rare that one has to apologize for a "potential waste of time". According to the Gartner IT Glossary,[vi] "gamification is the use of game mechanics to drive engagement in non-game business scenarios and to change behaviours in a target audience to achieve business outcomes. Many types of games include game mechanics such as points, challenges, leaderboards, rules and incentives that make game-play enjoyable." The literature review of Hamari et al. (2014) indicates that gamification provides positive effects, although the effects are greatly dependent on the context in which the gamification is being implemented and on the users' behavior, and therefore important for the design of the gamified system [24]. However, following Hendrix et al. (2016), it is very difficult to answer generically whether games are effective cybersecurity training tools. They conclude that "perhaps the focus should be more on the type of scenario-based training that is already common in the security field which often includes gaming elements. Games could then represent specific case studies and facilitate a case-based learning approach." [28].

In addition, even if the security personnel structure has been significantly overhauled, cyber-criminal "success strategies" such as CEO Fraud or Ransomware cannot be prevented either with technical tools or through the use of purely cognitive training measures—the real work situation must be trained, too. The reason for this is that security awareness relies on the factors relationship, attachment, discourse, and development—i.e., elements of what is called systemic communication, which aims to improve the communication with oneself and others in a respectful and purposeful way [61]. Developed and tested short-term analog and digital game-based learning scenarios[vii] combined with multiple learning methods such as theoretical information, a handbook with tasks, the exchange of experience, and discussions seem to be a successful, innovative mix of sensitization and training methods to help learners to more easily understand the abstract and complex theme of IS in all its facets and make the topic tangible and open to their direct experience [61]. The combination of these three approaches— *knowledge* plus *emotionalizing* plus *interaction* with *exchange of experience*—is called ISAT 3.0 with systemic sensitization measures [61]. This corresponds to the idea that ISA is role-based learning, detailing the roles and responsibilities of a user vis-à-vis ICT systems within their organization, and may be based on situational learning as an effective user-centered approach that improves the ability (in terms of perception, comprehension, and projection) to secure one's surroundings ([12]).

Following Cone et al. (2006), training and awareness are generally accomplished using a combination of several techniques: *formal* training sessions that can be instructor-led, brown-bag seminars, or video sessions; *passive* computer-based and web-based training (CBT/WBT), representing a centralized approach with the flexibility of self-paced training; *strategic* placement of awareness messages; *interactive* computer-based training, such as video games, which can be divided into two kinds, first-person interaction games or resource management simulations [16]. Since personal, class-room trainings often seem to be elaborate and costly, many rely on online/offline trainings like WBT with the risk that "a monotonous slide show fails to challenge the user and provides no dialogue for further elaboration" [16]. For example, Kim et al. (2017) developed an Internet-based cyberinformation security education & training and monitoring & reporting system to address the security breaches of malicious email and the attachment of documents commonly found in public institutions and private companies. As a result, the security education rate of 78 percent was raised throughout the system, and the user sense of security has been strengthened [41]. However, the participation rate does not say anything about the sustainability of the measure.

5. SUMMARY AND OUTLOOK

The literature review of ISA measurements reveals that there is a need for further work in the field of ISA and end-user security behaviors. Much of the research on ISA is about staff and students at the university level, with a certain amount focusing on company employees, and there are few e-government studies, even though public administrations have electronically processed sensitive and critical information for decades—this is, of course, a limitation. However, in future, the human side of IS needs to be proactively guided and continuously monitored, which also requires managers to act as role models in order to develop an active IS culture in their organization. IS culture is part of the general organizational culture and needs communication, collaboration, and participation.

As the CIP Report pointed out, "technical challenges can present given the lack of security in IoT devices and the fact that interconnectivity and interdependencies dramatically increase vulnerabilities—e.g. Smart Cities have already experienced malicious attacks, unintentional collapses of critical infrastructure, and systemic failures that have cascaded across networks. In addition, new technologies can generate their own risks—for example, system failures can occur due to unexpected security flaws caused by connecting smart networks to older, insecure devices" [23]. Smart regions with IoT technologies should pay attention to IS. One dimension includes business and professsional values like integrity, honesty, and trust at the individual level and competency as a professional, while the other dimension has to do with management and leadership skills, including the maintenance of a positive attitude, team building, empowerment, coaching and training others, and influencing decision makers to embrace new standards of achievement and social behavior that lead to appropriate IS and organizational resilience [69].

Moreover, when cybersecurity insider threats are associated with malicious users, their attacks are far less numerous than threats such as malware attacks, hacking, denial-of-service attacks, and ransomware. However, if the unintentional incidents of employees and contractors are added in, then these insider threats are the most prevalent instances.[viii] Companies' information security efforts are often threatened by employee negligence and insider breaches [14]. An important insider threat is a breach of confidentiality access policies. Employees' poor compliance with IS policies is a perennial problem and current IS analysis methods do not allow IS managers to capture the rationalities behind employees' compliance and non-compliance [45]. However, the study by Vance et al. (2013) shows that information systems with more sophisticated design artifacts can enhance the perception and responsibility of insiders [73]. Understanding and diagnosing information security systems (ISS) and related cultural artifacts can help ISS practitioners formulate, implement, and manage ISS strategies [33]. "Organizations need security training, education, and awareness because many times the first line of defense is the human line of defense. Human beings are an essential part of the prevention, detection, and response cycle" [18].

Security Awareness from a psychological point of view is less concerned with conveying knowledge like this—perhaps through a single training—and focuses rather on conscious awareness of one's own perception. [26] The decisive factor is the particular context to which awareness measures refer. [27] We need to differentiate between sensitization measures to increase information security awareness and more in-depth trainings for special issues. A primary task of awareness campaigns is to generate attention (impact) for the topic IS [26]. To raise awareness sensitization through GBL trainings is an important first step within a broad and ongoing process according to the KAB model. ISA is the direct perception of everything that animates a person with regard to IS and what attracts his/her current attention. For that, GBL in the field of ISA should integrate knowledge with emotionalizing, interaction, and exchange of experience [61]. The broad themes of IS can and should be elaborated with time-limited, reality-based, target-group-specific simulations (game units) and team-oriented communication and human-centered exchange as circuit trainings, which could also be used to raise awareness in public places. In addition, *analog* game-based learning scenarios in the digital world are more important than is currently accepted.

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. Sensitization and security trainings should be carried out on an ongoing basis. Awareness-raising activities should be offered for all people in a concrete context. Sensitization can be achieved using game-based methods including analog simulations, digital simulations, and interactive methods. However, further research and, above all, more evaluation are certainly needed in the non-linear and complex field of ISA and ISAT.

6. REFERENCES

[01] Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security Awareness Training: A Review. In *Proceedings of the World Congress on Engineering* (vol. 1, pp. 5-7).

[02] Anderson, J. R., & Schunn, C. (2000). Implications of the ACT-R learning theory: No magic bullets. *Advances in instructional psychology, Educational design and cognitive science*, 1-33.

[03] Arachchilage, N. A. G., & Cole, M. (2011). Design a mobile game for home computer users to prevent from "phishing attacks". In *2011 International Conference on Information Society (i-Society)* (pp. 485-489). IEEE.

[04] 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

[05] BAköV [Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern]/Federal Academy of Public Administration in the Federal Ministry of Interior (2009). Manual „IT Security Officer in the Public Administration", version 3.0, edition 2009, which was produced by the BAköV & BSI in co-operation with the Fraunhofer Institute for Secure Information Technology (SIT).

[06] Bauer, A., Newbury-Birch, D., Robalino, S., Ferguson, J., & Wigham, S. (2018). Is prevention better than cure? A systematic review of the effectiveness of well-being interventions for military personnel adjusting to civilian life. *PloS one*, *13*(5), e0190144.

[07] Bauer, S., & Bernroider, E. W. (2015). The Effects of Awareness Programs on Information Security in Banks: The Roles of Protection Motivation and Monitoring. In T. Tryfonas, & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust*. HAS 2015. Lecture Notes in Computer Science, (vol. 9190, pp. 154-164). Springer, Cham.

[08] Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), 887-901.

[09] Boss, R. S., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

[10] BSI [Bundesamt für Sicherheit in der Informationstechnik/Federal Office for Information Security] (2016a). *Self-Declaration and IT-Grundschutz Certificate*. Retrieved from https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCertification/OrganisationofCertification/organisationofcertification_node.html. Accessed: December 1, 2016.

[11] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548.

[12] Chen, C. C., Medlin, B. D., & Shaw, R. S. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security, 16*(4), 360-376.

[13] Chen, Y., Ramamurthy, K., & Wen, K.-W. (2014). Information Security Policy Compliance: Stick or Carrot Approach?. *Journal of Management Information Systems, 29*(3), 157-188.

[14] Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing. An empirical validation of the relationship between managerial information security

awareness and action. *Information Management & Computer Security, 16*(5), 484-501.

[15] Chu, A., Chau, P., & So, M. (2015). Explaining the misuse of information systems resources in the workplace: A dual-process approach. *Journal of Business Ethics, 131*(1), 209-225.

[16] Cone, B. D., Thompson, M. F., Irvine, C. E., & Nguyen, T. D. (2006). Cyber security training and awareness through game play. In *IFIP International Information Security Conference* (pp. 431-436). Springer, Boston, MA.

[17] Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26*(6), 605-641.

[18] Dark, M. J. (2006). Security Education, Training and Awareness from a Human Performance Technology Point of View. In M. E. Whitman, and H. J. Mattord (Eds.), *Readings and Cases in Management of Information Security* (pp. 86–104). Course Technology, Mason.

[19] Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. Illustrated through an empirical study. *Information & Computer Security*, *24*(2), 139-151.

[20] Fagade, T., & Tryfonas, T. (2016). Security by Compliance? A Study of Insider Threat Implications for Nigerian Banks. In T. Tryfonas (Ed.), *Human Aspects of Information Security, Privacy, and Trust*, HAS 2016, Lecture Notes in Computer Science (vol. 9750, pp. 128-139). Springer, Cham.

[21] Flores, W. R., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security, 22*(4), 393-406.

[22] Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. *European Journal of Information Systems*, *25*(2), 91-109.

[23] Gordon, L. W., & McAleese, G. W. (2017). Resilience and Risk Management in Smart Cities. *The CIP Report*.

[24] Hamari, J., Koivisto, J., & Sarsa, H. (2014, January). Does gamification work?--a literature review of empirical studies on gamification. In *2014 47th Hawaii international conference on system sciences (HICSS)* (pp. 3025-3034). IEEE.

[25] Hanamura, K. I., Takemura, T., & Komatsu, A. (2013). Research Note: Analysis of the Characteristics of Victims in Information Security Incident Damages: The Case of Japanese Internet Users, *The Review of Socionetwork Strategies*, *7*(1), 43-51.

[26] Haucke, A., & Pokoyski, D. (2009). Das geheime Drehbuch der Security – Awareness in Gestalt- und Tiefenpsychologie. In *Security Awareness* (pp. 75–130).

[27] Helisch, M. (2009). Definition von Awareness, Notwendigkeit und Sicherheitskultur. In *Security Awareness* (pp. 9–28).

[28] Hendrix, M., Al-Sherbaz, A., & Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training?. *International Journal of Serious Games*, *3*(1), 53-61/2384-8766.

[29] Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

[30] Ho, S. M., Von Eberstein, A., & Chatmon, C. (2017). Expansive Learning in Cyber Defense: Transformation of Organizational Information Security Culture. *Goel, S.(Ed.)*, 1-6.

[31] Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness. *Information Systems Research*, *26*(2), 282-300.

[32] Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.

[33] Hwang, K., & Choi, M. (2017). Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism. *Government Information Quarterly*, *34*(2), 183-198.

[34] Ifinedo, P. (2013). Information systems security policy compliance: An. *Psychological Review*, *84*(2), 191-215.

[35] ISF (Information Security Forum). *The Standard of Good Practice for Information Security, Security Standard*. 2007.

[36] James, T., Nottingham, Q., & Kim, B. C. (2013). Determining the antecedents of digital security practices in the general public dimension. *Information Technology and Management*, *14*(2), 69-89.

[37] Jones, B. H., Chin, A. G., & Aiken, P. (2014). Risky business: Students and smartphones. *Tech Trends*, *58*(6), 73-83.

[38] Kajava J., Anttila, J., Varonen, R., Savola, R., & Röning, J. (2006). Senior Executives Commitment to Information Security – from Motivation to Responsibility. In Y. Wang, Y. Cheung, and H. Liu (Eds.), *Computational Intelligence and Security*, CIS 2006, Lecture Notes in Computer Science (vol. 4456, pp. 833-838). Springer, Berlin, Heidelberg, 2006.

[39] Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862-10868.

[40] Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, *22*(1), 115-126.

[41] Kim, B. H., Kim, K. C., Hong, S. E., & Oh, S. Y. (2017). Development of cyber information security education and training system. *Multimedia Tools and Applications*, *76*(4), 6051-6064.

[42] Kirlappos I., Beautement, A., & Sasse M. A. (2013). 'Comply or Die' Is Dead: Long Live Security-Aware

Principal Agents. In A.A. Adams, M. Brenner, and M. Smith (Eds.), *Financial Cryptography and Data Security*, FC 2013, Lecture Notes in Computer Science (vol. 7862, pp. 70-82). Springer, Berlin, Heidelberg.

[43] Kirlappos, I., & Sasse, M. A. (2012). Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy*, *10*(2), 24-32.

[44] Kitchin, R., & Dodge, M. (2017). The (in)security of smart cities: vulnerabilities, risks, mitigation and prevention. Published as an open access pre-print on SocArXiv. Retrieved from https://osf.io/preprints/socarxiv/f6z63. Accessed: October 26, 2017.

[45] Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. *The Journal of Strategic Information Systems*, *26*(1), 39-57.

[46] Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance, *Computers & Security*, *33*, 3-11.

[47] Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness, *Computers & Security*, *25*(4), 289-296.

[48] Kruger H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, Vol. 18, No. 5, pp. 316-327.

[49] Kruger H., Drevin, L., & Steyn, T. (2007). Email Security Awareness — a Practical Assessment of Employee Behaviour. In L. Futcher, and R. Dodge (Eds.), *Fifth World Conference on Information Security Education. IFIP — International Federation for Information Processing* (vol. 237, pp. 33-40). Springer, Boston, MA.

[50] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008). Lessons from a real world evaluation of anti-phishing training. In *eCrime Researchers Summit 2008* (pp. 1-12). IEEE.

[51] Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review, *Management Research Review*, *37*(12), 1049-1092.

[52] Liang, H., Xue, Y. & Wu, L. (2013). Ensuring Employees' IT Compliance: Carrot or Stick? *Information Systems Research*, *24*(2), 279-294.

[53] Manifavas C., Fysarakis, K., Rantos, K., & Hatzivasilis, G. (2014). DSAPE – Dynamic Security Awareness Program Evaluation. In T. Tryfonas, and I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust*, HAS 2014, Lecture Notes in Computer Science (vol. 8533, pp. 258-269). Springer, Cham.

[54] McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of Awareness and Training on Cyber Security, *Journal of Internet Commerce*, *9*(1), 23-41.

[55] Mejias, R. J., & Balthazard, P. A. (2014). A Model of Information Security Awareness for Assessing Information Security Risk for Emerging Technologies. *Journal of Information Privacy and Security*, *10*(4), 160-185.

[56] Ngoqo, B., & Flowerday, S. V. (2015). Exploring the relationship between student mobile information security awareness and behavioural intent. *Information & Computer Security*, *23*(4), 406-420.

[57] Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security*, *22*(4), 334-345.

[58] Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., *and* Calic, D. (2016). Assessing information security attitudes: a comparison of two studies. *Information & Computer Security*, *24*(2), 228-240.

[59] Renaud K., & Goucher W. (2014). The Curious Incidence of Security Breaches by Knowledgeable Employees and the Pivotal Role a of Security Culture. In T. Tryfonas, and I. Askoxylakis (eds), *Human Aspects of Information Security, Privacy, and Trust*, HAS 2014, Lecture Notes in Computer Science (vol. 8533, pp. 361-372). Springer, Cham.

[60] Safa, N. S., Von Solms, R., and Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70-82.

[61] Scholl, M., Fuhrmann, F., & Pokoyski, D. (2016). Information Security Awareness 3.0 for Job Beginners. In J.E. Quintela Varajão, M.M. Cruz-Cunha, R. Martinho, R. Rijo, N. Bjørn-Andersen, R. Turner, and D. Alves (Eds.), *Conference on ENTERprise Information Systems (CENTERIS)* (pp. 433-436). Porto, Portugal.

[62] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, July). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In Proceedings of the 3rd symposium on Usable privacy and security (pp. 88-99). ACM.

[63] Sherif E., Furnell, S., & Clarke, N. (2015). An Identification of Variables Influencing the Establishment of Information Security Culture. In T. Tryfonas, and I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust*, HAS 2015, Lecture Notes in Computer Science (vol. 9190, pp. 436-448). Springer, Cham.

[64] Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study. In Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R. (Eds.), *New Approaches for Security, Privacy and Trust in Complex Environments*, IFIP International Information Security Conference, 232 (pp. 133-144). Boston: Springer.

[65] Siponen, M. T. (2001). Five dimensions of information security awareness. *SIGCAS Computers and Society*, *31*(2), 24-29.

[66] Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

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

[68] Styles M. (2013). Constructing Positive Influences for User Security Decisions to Counter Corporate or State Sponsored Computer Espionage Threats. In L. Marinos L., and I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust*, HAS 2013, Lecture Notes in Computer Science (vol. 8030, pp. 197-206). Springer, Berlin, Heidelberg.

[69] Sullivant, J. (2016). *Building a Corporate Culture of Security: Strategies for Strengthening Organizational Resiliency*. Butterworth-Heinemann, Oxford.

[70] Sun, J., Ahluwalia, P., & Koong, K. S. (2011). The more secure the better? A study of information security readiness. *Industrial Management & Data Systems*, *111*(4), 570-588.

[71] Topa, I., & Karyda, M. (2015). Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance. In S. Fischer-Hübner, C. Lambrinoudakis, and J. López (Eds.), *Trust, Privacy and Security in Digital Business*, TrustBus 2015, Lecture Notes in Computer Science (vol. 9264, pp. 169-179). Springer, Cham.

[72] Tsohou, A., Karyda, M., Kokalakis, S., & Kiountouzi, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*(1), 38-58.

[73] Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263-290.

[74] Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

[75] Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems, 20*(3), 267-284.

[76] Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1-20.

[77] Wolf, M., Haworth, D., & Pietron, L. (2011). Measuring an information security awareness program. *Review of Business Information Systems (RBIS)*, *15*(3), 9-22.

[78] Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. *Information Systems Security*, *16*(6), 315-331.

[79] Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, *92*, 36-46.

APPENDIX

Table 1: Different aspects in ISA definitions

Author year	**Aspects in definition**
Kruger & Kearney 2006 Parson et al. 2014	KAB model: 1. Knowledge (what you know) 2. Attitude (what you think) 3. Behavior (what you do)
Choi et al. 2008	1. Extent to which employees see IS as significant 2. Extent to which they are aware of IS objectives/standards
Khan et al. 2011	1. Extent to which staff understand the importance of IS 2. The levels of IS appropriate to the organization 3. Individual responsibility 4. Extent to which staff act accordingly
Sun et al. 2011	Knowledge about how well information assets are protected
Manifavas et al. 2014	1. Knowledge of IS 2. Attitude of employees vis-à-vis the protection of their organization's physical and informational assets
Mejias & Balthazard 2014	1. A state of knowledge enabling users or systems to perceive the potentially negative impacts of cyberattacks 2. Cognizance of their organization's IS policies
Ngoqo & Flowerday 2015	1. Awareness of security threats 2. An understanding of the way in which these threats work 3. The ability to predict/anticipate potential outcomes

Table 2: Prior studies of IS compliance (individual level)

Author	**Influencing factors investigated: predisposing factors to an SE attack**
Workman 2007	• commitment (normative, continuative, affective) • (online) trust • obedience to authority
Siponen et al. 2007	• threat appraisal • self- and response-efficacy • sanctions • intention to comply
Herath & Rao 2009	• employees' understanding of the severity of the threat • employees' belief that IS policy is a hindrance to their day-to-day job • perceived impact/benefit of ISP on/for organizational goals • IS resource availability
Sun et al. 2011	• data criticality (low/high) • IT proficiency
Kolkowska & Dhillon 2013	• different dimensions of power (resources, processes, meanings, and systems)
Warkentin et al. 2011	• perceived situational support • verbal persuasion • vicarious experience
Hu et al. 2012	• behavioral intention toward compliance (attitudes, subjective norms, and perceived behavioral control)
James et al. 2013	• perceived need of digital IS • encryption practice
Styles 2013	• motivation • recognition skills • alert capability
Liang et al. 2013	• Punishment expectancy has a much stronger effect on compliance behavior than reward expectancy. • Social influence can affect IT behavior because of the significant power of others to use reward and punishment.
Flores et al.	• degree of target information

2014	• individual's trust and risk behavior • computer experience • helpfulness • gender (females less susceptible)
Lebek et al. 2014	Theory of Reasoned Action (TRA)/ Theory of planned behavior (TPB): • evaluation of and normative beliefs toward compliance-related behavior General Deterrence Theory (GDT): • perceived severity of sanctions (PSOS) • perceived certainty of sanctions (PCOS) Protection Motivation Theory (PMT): • threat appraisal (TA) • coping appraisal (CA) Technology Acceptance Model (TAM): • perceived usefulness (PU) • perceived ease-of-use (PEOU)
Hsu et al. 2015	• Formal control is not as crucial as social control in inspiring extra-role behaviors. • Extra-role behavior is influenced by attachment to co-workers. • involvement in IS creation activities • sharing security beliefs • high degree of commitment to the organization
Topa & Karyda 2015	• perceived costs (sanctions severity/certainty, intrinsic cost, vulnerability of resources, response cost) • perceived benefits (intrinsic benefit, rewards, safety of resources) • ethical values (perceived legitimacy, value congruence) • social influence (subjective and descriptive norms) • awareness (IS, ISP, SETA programs, computer monitoring mechanisms, technology) • organizational commitment Individual only: • threat appraisal (perceived severity/vulnerability) • coping appraisal (self- and response-efficacy) • habits Individual/technology: • perceived usefulness (PU) • perceived ease-of-use (PEOU)
Pattinson et al. 2016	KAB model: • attitudes
Da Veiga 2016	• reading/awareness of an IS policy
Foth et al. 2016	• Punishment severity has no effect on the intention to comply with data-protection regulations. • Gender affects intention to comply.

Table 3: Prior studies of ISA and IS compliance (organizational level)

Author	**Influencing factors investigated**
Kajava et al. 2006	• senior management ISA, commitment, leadership
Boss et al. 2009	• declaration of security policies as mandatory
Herath et al. 2009	• IS resource availability • management communication about reality of security threats
Hu et al. 2012	• active participation in IS-related initiatives and building rule- and goal-oriented organizational cultures
Liang et al. 2013	• social influence is effective only in mandatory settings
Renaud & Goucher 2014	• establishment of an organizational security culture
Topa & Karyda 2015	• perceived costs (sanctions severity/certainty, intrinsic cost, vulnerability of resources, response cost) • perceived benefits (intrinsic benefit, rewards, safety of resources) • ethical values (perceived legitimacy, value congruence) • social influence (subjective and descriptive norms) • awareness (IS, ISP, SETA programs, computer monitoring mechanisms, technology) • organizational commitment Organization only: • facilitating conditions (availability of resources, controllability, visibility, information quality)
Sherif et al. 2015	• top management support • ISA (awareness) • ISB (behavior) • IS acceptance • ISP (policies)
Fagade & Tryfonas 2016	• top management buy-in and support • demonstration of managerial commitment to IS

[i] http://www.de.digital/DIGITAL/Redaktion/EN/Dossier/g20-shaping-digitalisation-at-global-level.html, Accessed: April 14, 2017.

[ii] https://www.egovernment-computing.de/die-wichtigsten-fragen-und-antworten-zum-bundes-hack-a-691389/. Accessed: March 7, 2018.

[iii] https://www.igi-global.com/dictionary/. Accessed: December 24, 2017.

[iv] https://www.eugdpr.org. Accessed: March 4, 2018.

[v] https://en.wikipedia.org/wiki/Awareness/. Accessed: July 5, 2018.

[vi] https://www.gartner.com/it-glossary/gamification-2/. Accessed: December 27, 2017.

[vii] http://secaware4job.wildau.biz/#lernszenarien. Accessed: August 25, 2018.

[viii] https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/. Accessed: March 8, 2018.