Proceedings of the 51^{st} Hawaii International Conference on System Sciences | 2018

Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices

Margit C. Scholl
TUAS Wildau
margit.scholl@th-wildau.de

Frauke Fuhrmann
TUAS Wildau
frauke.fuhrmann@th-wildau.de

L. Robin Scholl
TUAS Wildau
lscholl@th-wildau.de

Abstract

Comprehensive digitization leads to new challenges because of cybercrime and related security countermeasures. There is no doubt that this will fundamentally affect our lives and is leading to an increase in the importance of information security (IS). However, technology solutions alone are not sufficient to ensure IS countermeasures. The human side of security is important to protect organizational assets like user information and systems. The paper illustrates these relationships in terms of information security awareness (ISA), examining its goals and the factors influencing it through the systematic analysis and review of scientific literature and the transfer of scientific knowledge for practical purposes. We reviewed the publications of leading academic journals in the field of IS over the past decade.

1. Introduction: Overcoming Digitization Challenges

Through the cross-sectional nature of information and communication technologies (ICT), digitization affects almost all areas of life. Computer-aided technologization is a key feature of industrialized nations and is having an increasing effect on (working) life all over the world. The threat potentials are elevated by the increasing degree of digital networking, the increasing spread and penetration of information technology (IT), and a higher degree of interactivity coupled with increasingly high-quality attacks. Previous IT security mechanisms have reached their limits, and reliability and controllability cannot be assumed as before [11]. These challenges affect both individuals and organizations. Government digital agendas (see the Federal Government of Germany or the Digital Agenda for Europe [12]) seek to keep abreast of digital networking and the digital changes in society.

However, information security (IS) is more comprehensive than simple IT security [32, 10]. In 2000 IT security expert Donald Pipkin addressed all the different aspects of IS and saw the value of information assets as a key issue in business [53].

Now in its tenth year, Verizon's 2017 Data Breach Investigations Report[1] reveals 2,000 data leaks and shows who is hit hardest by online spying: about 20 percent of all successful attacks hit manufacturing companies, government agencies, and educational institutions. The results of a survey on the threat posed by ransomware conducted by the Federal Office for Information Security (BSI) in Germany in early 2016 suggest a more severe threat.[2] More than a third of the institutions interviewed had been affected by encryption Trojans in the past six months. In 75 percent of these cases, the malware sneaked in via infected e-mail attachments. For 22 percent, the infection resulted in the significant loss of parts of their IT infrastructure.

In awareness training, in particular, it seems that over the past fifteen years organizations have not put their main focus on developing IS awareness and training responsible information users [78]. Verton finds that less than 50 percent of organizations have an IT security and training program for employees [73]. The relevant standard for IT security is 27001 "Information Security Management Systems" (ISMS) of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) [32]. 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 [51]. In Germany, ISO/IEC 27001 IT protection certificates have been available since 2006 [9]. However, a survey

[1] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/ [accessed May 30, 2017]

[2] https://www.heise.de/security/meldung/BSI-Umfrage-Ein-Drittel-der-Unternehmen-ist-von-Erpressungs-Trojanern-betroffen-3189776.html [accessed May 31, 2017]

URI: http://hdl.handle.net/10125/50168
ISBN: 978-0-9981331-1-9

of 424 German organizations shows that only 63 percent perform measures to raise IS awareness [2] and 40.5 percent of these organizations do not measure the effectiveness of their trainings.

Technical solutions for IS are necessary to address certain vulnerabilities such as viruses, denial of service attacks, etc. Nevertheless, IS is about more than technology [41], because information systems involve human beings, and users do not always act the way they are supposed to [3]. Against this backdrop, the next section introduces the historical importance of the human factor in IS. We end with a summary of our research questions and an explanation of the structure of the paper.

2. Introduction: Human Actors and IS

A lack of understanding of security issues coupled with the pervasive use of computers makes employees a "critical factor" in the IS equation [20]. However, as Dark points out, 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 [20]. Thus, technology solutions alone are not sufficient to ensure IS countermeasures. This addresses the challenges of IS management (ISM) in organizations, because management and behavioral aspects are pivotal to building an ISMS in organizations [62]. To protect the organizational assets, including user information and systems, the human side of security should also be managed [37, 67], as is particularly evident in social engineering (SE) attacks [77]. 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 [6].

Solms [74] discusses the development of IS in terms of five "waves": his third (institutional) wave, which includes questions about IS policy, brought the role of the employee as an end user of the system into the spotlight, and the importance of the human dimension within IS was accepted [74]. This development was pushed in the fourth wave with growing emphasis on IS Awareness (ISA) and the risk posed by uninformed employees, who might compromise IS measures. There is one main difference between Solms's fourth (IS governance) and fifth (cybersecurity) wave: organizations rolled out more and more systems based on the Internet and its services, making it possible for millions of clients and customers to use such systems externally without an adequate IS [74]. One direct result was that criminals 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!" [74].

This is why the human factor in IS has often been seen as "critical" or the "weakest link" or the "greatest threat" in the safety chain, especially because the majority of incidents of information or data collision in organizations are due to unconscious behavior or the deliberate fault of employees [7, 21, 23, 27, 72]. However, in the recent past, a rethink has started highlighting the strength of human actors as a security factor in an organization-wide ISMS as well as the need for ISA. For example, Elliot emphasized the idea of doing security *with* the organization and not *to* it [22]. Winkler turned against critics who claim that consciousness efforts are useless. She showed how technology, process, and awareness should combine to stop human failings, and that if a single user action can compromise an entire security program, the problem is the security program itself [76]. Moreover, one should differentiate between the sensitization and training of employees [8]. "Security communication, education, and training (CET) is meant to align employee behavior with the security goals of the organization, but it is not always designed in a way that can achieve this" [6]. In our paper we will come back to this point. What does ISA really mean? And how should security CET be designed to achieve lasting behavioral change in people? The objective of this paper is a systematic compilation of past scientific insights into ISA and a possible transfer of these insights into practical implementation. Our research questions (RQ) are as follows:

RQ#1: What *is* ISA actually? What factors are used in the scientific literature to define it? How can the correlation to an organizational IS culture be interpreted and rules for livable security created?

RQ#2: What are the dependencies/connections/correlations between these factors and the ISA in practice? What are the consequences for individual and organizational learning processes in the area of IS?

RQ#3: What and how is ISA measured? How is ISA related to IS compliance?

RQ#4: How can ISA trainings (ISAT) be designed in practice to be efficient, effective, and sustainable? What methods are relevant from a scientific point of view?

In section three we review the relevant scientific literature relating to ISA aspects, IS culture, and ISA measurements, theories, and trainings. Section four summarizes the discussion surrounding our RQ and their further ramifications. Our conclusions and future work are presented in section five.

3. Literature Review

We reviewed the publications of leading academic journals in the area of IS over the past decade. We focused our research on studies of the "human factor". The purpose was to identify the main research interests and to derive impact for practice and future research.

3.1. KAB: knowledge, attitude, behavior

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. The concept of ISA is widely used here. But at the same time this concept is defined differently in the literature. An important step toward a contemporary and conceptualized definition of ISA has been made through the naming of the three dimensions of *knowledge*, *attitude*, and *behavior*—also known as the KAB model [40]. The proposition is that ISA comes out of what employees or users know about IS and its vulnerabilities, what they think or what opinion they have about it, and their actual behavior in this context. This model has been adopted by other researchers and modified [47, 49].

In using the KAB model, the question arose as to whether knowledge and attitudes are directly connected to behavior or if this influence is only assumed. Some authors answered that question with "knowing is doing" and filled the knowing-and-doing gap [16, 47] by showing, on an organization's management level, that managerial ISA and managerial actions toward IS are positively connected.

A large spectrum of theories has been consulted in this research field to obtain knowledge about the real security behavior and influencing factors. The theories most applied to explain IS behavior are the Theory of Planned Behavior, General Deterrence Theory, Compliance Theory, Protection Motivation Theory, the Technology Acceptance Model and the Theory of Reasoned Action, Social Bond Theory, and Involvement Theory [4; 15; 17; 24; 42; 46; 47; 50; 56; 63; 65; 68].

Our literature review in the field of IS behavior reveals that companies' information security efforts are often threatened by employee negligence and insider breaches [14]. The lack of ISA, ignorance, negligence, apathy, mischief, and resistance are at the root of user mistakes [56]. Herath and Rao find that employees underestimate the probability of security breaches [29]. The findings of Chu, Chau, and So suggest that misuse may be both an intentional type of behavior and an unreasoned action [17]. However, the paper by Kruger, Drevin, and Steyn indicates that divisions can be identified where guidance is needed and shows the specific types of threats that users are exposed to [41]. And Hanamura, Takemura, and Komatsu conclude that the ability to collect and process information and ISA decrease the probability that an individual will encounter information security incidents, but overconfidence regarding information security knowledge increases the probability of phishing and spoofing [28]. However, the constructs of organizational impact and attacker assessment generated stronger path coefficients with ISA than technical knowledge [46]. Their research model results also indicate that ISA is strongly associated with IS risk [46]. And Pattinson et al. found a strong correlation with ISA for the measure relating to the three behaviors Internet use, mobile computing, and email use [50]. However, Parsons et al. conclude that even if there is a reasonable level of ISA overall, weaknesses were identified in the use of wireless technology, the reporting of security incidents, and the use of social networking sites [49].

In the German banking sector, Bauer and Bernroider find strong empirical evidence showing the importance of ISA programs, protection motivation, and monitoring [4], while the findings of Fagade and Tryfonas suggest that security by compliance as a campaign to secure information assets in Nigerian financial institutions is a far-fetched approach [24]. This might relate to sociocultural influences on ISA. McCrohan, Engel, and Harvey confirm that when users were educated about the threats to e-commerce and trained in proper security practices, their behavior could be changed to enhance online security for themselves and the firms where they are employed [45].

While one of the most significant findings of a study in Turkey is that the higher the education level, the more ISA there is [48], Ngoqo and Flowerday illustrate the poor security behavior among student mobile phone users, despite courses covering certain principles relating to information security [47]. The survey of Slusky and Partow-Navid revealed that the major problem with the ISA of students is not a lack of security knowledge but the way that knowledge is applied in *real-world situations*. The authors conclude that the compliance with ISA is lower than the understanding of it [64]. Kim also showed that college students understand the importance and the need for ISA training (ISAT) but many of them do not participate in trainings [37]. Moreover, many student smartphone users employ some security measures, but a high percentage of them are ignoring potential risks [35]. This suggests a need for increased education, training, and awareness at university level.

3.2. Influencing factors / Antecedents

To reduce vulnerability to a variety of attacks, several organizations have made ISA a top priority. However, Shaw, Chen, and Harris see three main *barriers* to ISA in organizations: the general level of security awareness, employees' computer skills, and organizational budgets [61]. As the reviewed literature shows, an important influencing factor in IS is not necessarily insufficient knowledge but rather the *lack of compliance with ISA and IS behavior* [64]. Using the vocabulary of the KAB model, this is the attitude or the will and ability to convert the knowledge into IS-compliant behavior. Looking at *antecedents of IS compliance*, these factors can be divided into individual and organizational levels.

For example, at the individual level, Flores et al. show that computer experience at work, helpfulness, and gender had a significant correlation with behavior reported by respondents in the scenario-based survey [25]. Significant differences between the genders are also seen vis-à-vis the intention to comply with data protection regulations in German hospitals [26]. The general results of Foth suggest that psychological factors, such as attitude, subjective norms, and perceived behavior control, play an important part [26]. The findings of Safa, von Solms, and Furnell show that commitment and personal norms affect employee attitudes, and that the attitude toward compliance with IS organizational policies also has a significant effect on the behavioral intention regarding IS compliance [56].

At this point, it is important to identify the role of top management. The top management can play a proactive role in shaping employee compliance behavior [31]. Moreover, managers should compartmentalize roles and allocate information on a "need to know" basis [75]. Managers should ensure that employees fully understand what behaviors are expected, how their behaviors will be evaluated, and what rewards they may receive if they perform these behaviors. This knowledge can be shared through effective security education, training, and awareness initiatives [30]. The IT managers could pair new employees with mentors, organize group learning exercises, and facilitate on-the-job training to enhance the practical learning of information privacy procedures [75]. Formal or informal mechanisms can be provided to enhance interaction among employees. Frequent interaction is the basis for forming interpersonal rapport and psychological attachment [30].

Siponen, Pahnila, and Mahmood show that threat appraisal, self-efficacy, and response efficacy have a significant impact on the intention to comply with IS policies, and that sanctions have a significant impact on actual compliance with IS policies. The stronger the intention to engage in the behavior, the more likely it is to be performed [63]. The results of Herath and Rao suggest firstly that threat perceptions about the severity of breaches and response perceptions relating to response efficacy, self-efficacy, and response costs are likely to affect policy attitudes. Secondly organizational commitment and social influence have a significant impact on compliance intentions; and, thirdly, resource availability is a significant factor in enhancing self-efficacy, which, in turn, is a significant predictor of policy compliance intentions [29].

Boss et al. [7] examine elements of control and conclude that the perception of mandatoriness is effective in motivating individuals to take security precautions, so if individuals believe that management is watching, they will comply. In contrast to a previous study, Liang, Xue, and Wu reveal that punishment expectancy is a strong determinant of compliance behavior, while reward expectancy is not significant [43]. In line with these findings, Chen, Ramamurthy, and Wen indicate that when punishment is severe, adding a remunerative control mechanism may not overly affect compliance [15].

By contrast, for Kirlappos, Beautement, and Sasse, IS has adapted to the modern collaborative nature of organizations and abandoned the "command-and-control" approaches of the past [38]. The authors state that "whilst many organizations are aware that this 'comply or die' 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" [38]. Moreover, a clear set of IS principles needs to be identified and communicated to develop employees who are risk-aware and know how to manage the risks that apply to them [38]. Based on the research into IS knowledge sharing [56], collaboration, intervention, and experience have a significant effect on the attitude of employees toward compliance with organizational information security policies.

In addition, the results produced by Sun, Ahluwalia, and Koong revealed a nonlinear relationship between security levels and *information security readiness* (ISR) [68]. In a general way, ISA programs 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 [4].

However, Tsohou et al. argue that ISA processes are associated with interrelated changes that occur at the organizational, technological, and individual levels [71]. This is also shown by Da Veiga, who found firstly that the overall IS culture average scores, as well as individual statements, were significantly more positive for employees who had read the IS policy compared with employees who had not, and secondly that the overall IS culture also improved from one assessment to the next [19].

The summary research results show that a variety of nonlinear, complex interactions influence the behavior of humans with respect to IS. Likewise, necessary changes in approach in modern organizations are clarified. There is a clear need for further work in the field of ISA and end-user security behaviors.

3.3. IS Awareness Training (ISAT)

Awareness remains a critical issue of IS [69]. Increasing the level of users' security awareness through education and training may be an effective way to encourage the adoption of security tools, which leads to safer technology use [34]. However, the importance of appropriate awareness and training is often overlooked [44], although scientific research indicates a general need for (cyberthreat) education and training [35, 37, 45, 61]. Furthermore, Tsohou et al. conclude that "recent global security surveys indicate that security training and awareness programs are not working" [70]. Our review of the scientific literature shows that the *design* of the ISA trainings has not been the subject of significant research. Only a few studies from the literature on KAB give (very general) recommendations for the design of training measures [50, 64].

Why have mainstream ISA techniques failed? 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 [65]. Moreover, it might ignore the daily mix and overlap between work and home and therefore ignore an insight from practice that "if you don't change home security behavior, it is hugely more difficult to effect change in the office" (Ian Kilpatrick, chairman of the Wick Hill Group) [13]. A second aspect might be policies "ending up as long lists of dos and don'ts located on web pages most employees only access when they have to complete their mandatory annual 'security training' and which has little to no effect on their security behavior" [38]. A third aspect relating to IS campaigns is that a training with the hope of addressing security awareness gaps cannot be sufficient to ensure compliance with security culture [24]. Moreover, the Dimensional Research Survey showed in 2011 that companies were lacking proactive ongoing trainings for employees and more than 30 percent did not currently make any attempt to educate employees [37]. In the field of ISA, current information security awareness activities fail [33] and CET approaches are far from efficient. Nevertheless, Shaw, Chen, and Harris [62] report on a laboratory experiment that investigates the impacts of hypermedia, multimedia, and hypertext on increasing ISA on the three awareness levels (perception, comprehension, and projection) in an online training environment with meaningful ISA materials [61].

The secret is to *engage* your people in the right way, so they can convert learning into tangible action and new behavior [6]. Research shows that besides the theoretical approach of knowledge transfer and the promotional approach of *emotionality* a systematic communicational approach in the form of *team-based* applications is needed to achieve lasting ISA that results in the intention and behavior to protect confidential information [36, 54]. The combination of these three approaches is called ISAT 3.0 [60]. This corresponds to the idea that ISA is role-based learning, detailing the roles and responsibilities of a user in the use of ICT systems within their organization [14] and may be based on *situational learning* as an effective user-centered approach.

Besides situational target orientation, ISAT needs individual emotionality and team-based communication and exchange for motivation. To achieve this, creative techniques and digital and analogue serious games become more important in the field of IS, ISA, and ISAT. Prime examples of this are the software "Operation Digital Chameleon" [55], a card game, where the staff members target the topic of SE [5] and the "Security Parcours"[3] of the company T-Systems developed in cooperation with the firm known_sense.

3.4. Measuring awareness

At the very least, the common goal is to achieve a change in human behavior to create more IS. However, most employees will not adopt security behaviors that severely hamper their ability to perform primary tasks [6]. Before mandating a certain security behavior, the organization needs to ensure that behavior can be complied with, without routinely blocking productivity—a step called "security hygiene" [52]. IS awareness-raising measures and their evaluation should be an indispensable part of today's organizations. However, in an international survey with 369 respondents (70 percent from US-based organizations and 30 percent from outside the United States) 26.6 percent indicated that they do not use any metrics to measure their awareness program [57]. The most common methods and their advantages and disadvantages

[3] https://sicherheit.eco.de/2013/events/security-parcours.html [accessed June 4, 2017]

are summarized and discussed in [58]. But before appropriate measures for assessing the effectiveness of IS awareness-raising programs can be chosen, organizations should consider which metrics they want to use to monitor the effectiveness of the programs applied [58].

3.5. Information security culture

At this point one should also question the relationship of ISA to the security culture of the organization. Van Niekerk and Solms explain the development of organizational culture at three levels [72]: level one shows only the "artifacts." At level two the "espoused values" are considered, meaning the organization's official viewpoints, which give a deeper insight into the reasons, thoughts, and perceptions that drive the observable behavior. The third level is called "shared tacit assumptions" and reveals those values, beliefs, and assumptions that have become shared and taken for granted in an organization. These shared tacit assumptions result from a joint learning process [72]. Moreover, for Beyer et al. [6] it is necessary to use an approach that motivates employees to play an active role in corporate security. "Employees should understand what to protect, why they should want to protect it, how the organization can help them with this, and how successes and mistakes can be used as opportunities to learn and improve" [6].

4. Discussion, RQ, and Consequences

RQ#1: Although there is no uniform and binding definition of ISA, many articles in the international scientific literature are based on the KAB model and show that knowledge/education about the IS of users is a basis for reflecting on their own attitudes. The overall goal of most literature in this context is a better understanding of people's behavior as a means to develop it in the proper way.

There is, however, no simple linear cause-and-effect relationship between knowledge and attitudes, and certainly not with regard to the real IS behavior practiced by people. A main problem for human beings seems to be the application of IS knowledge in real-world situations. It seems that commitment and personal norms affect employees' attitudes. In addition to the proactive role of management, 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. Moreover, there is no doubt that psychological factors, subjective norms, and the sociocultural and gender background in nonlinear and complex interactions have a major influence on human ISA and IS behavior.

In the context of the practices currently being examined, rewards and incentives such as remuneration rules are hardly ever used as an enforcement mechanism for IS. It is, however, to be expected that the "comply or die" approach [38] that has hitherto been practiced will work less and less for modern organizations.

RQ#2: The improvement of perception and comprehension can advance a person's ability to project real-life situations. And it seems that the constructs of organizational impact and attacker assessment have a stronger influence on the ISA than technical knowledge. Management and employees have to learn their pivotal role for the IS of an organization.

Thus, the learning process in organizations must be based on the user-centered approach, paying attention to target groups, gender, and culture, which is based on individual knowledge and skills as well as on concrete work connections. The user-centered approach should also enable exchange in informal learning processes in certain social conditions within the organizational setting. The integration of formal and informal mechanisms can enhance the interaction between employees. 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 the IS guidelines, such aspects of emotionalization and motivation should be incorporated into the sensitization to and training of ISA.

We have developed the *spiral of transformative interaction* between an organization and its staff with regard to (IS) learning processes (see fig. 1 and [59]). The spiral shows the interaction between top-down specifications and individual bottom-up influences on the establishment of a future-oriented modern organizational security culture.

RQ#3: With regard to the third complex of research questions, we found that only a few organizations use different metrics for a deeper and continuous measurement of their awareness program [58]. 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 [39]. Therefore, ISAT should not overwhelm employees with information or take up excessive paid work time [72].

It seems that attitudes toward compliance with IS organizational policies also have a significant effect on the behavioral intention regarding IS compliance, whereby policies must be livable. Here the top management must play a proactive role in shaping employees' compliance with IS behavior. Advice should be seen as an enabler that supports the organization's goals [6].

Creating an effective ISA program requires targeted communication and training that caters to specific employee groups. The optimal IS culture must be carefully defined in each case. If this is not done explicitly, staff may conclude that the organization lacks the proper commitment to security. Rather than relying on generalized computer-based packages, IS training should be geared to the specific work environment.

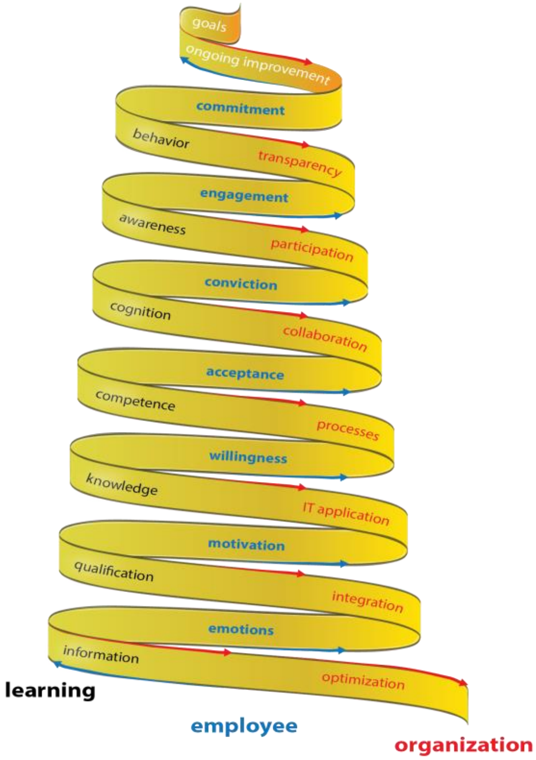

Fig 1 Spiral of transformative interaction

RQ#4: The fourth complex of research questions aims to provide concrete instructions for the design of the ISAT and useful learning methods. Game-based learning 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 ISA. In this way, learners directly see the consequences of their actions and can get a sense of their knowledge level in dialogue. Games also support IS abilities that we increasingly need in daily life and in the workplace—for example, communication, cooperation, social interaction, and creativity. 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 [60]. Integrated analogue and digital game-based ISAT with interactive elements leads to the further involvement of human actors. Our own extensive experience with such learning materials and methods in projects and events suggests that ISA and associated knowledge could be improved in almost all participants and behavioral changes triggered. To this end, we have proposed a future project with a correspondingly extensive organization-oriented measurement scenario, designed for a systematic study.

5. Conclusion and Outlook

The extensive research of scientific literature on the subject of ISA shows a wide range of studies and specific theories, mainly taking the point of view that human actors are the *weakest link* [44] in IS and geared to creating a better understanding of the factors influencing their IS behavior. However, we must overcome this misleading perception and realize that employees are a strong security and safety barrier, especially in the area of SE attacks. For IS "human beings are an essential part of the prevention, detection, and response cycle" [20]. It is therefore very important to provide humans with the knowledge, attitudes, intention, and skills to behave in a security-oriented way and build up ISA. The need for more intensive ISAT is postulated from the research, but ways of making such trainings effective and sustainable are not really addressed.

Studies show that frequently used awareness-raising and training measures, such as campaigns (e.g., flyers, brochures, posters, films), purely IT-based trainings (e.g., web-based trainings, simple video games), or the sharing of information in lectures, are ineffective and do not lead to a lasting sense of security among the addressees [1, 18, 66]. Instead, training that provides opportunities for personal communication and interaction is a promising means to promote ISA and the triggering of security-related behavior. To be effective, security training must be based in the work context and address specific security needs, with regular ongoing reminders of the key messages and awareness campaigns tailored to employees' needs [6]. As a result, the acceptance of the corresponding technical, organizational, individual, and administrative measures may also increase [1]. But there is no shortcut to developing an effective ISAT program, because every organization must define for itself the security culture it seeks to promote [6].

Much of the research on ISA is about staff and students at the university level, with a certain amount focusing on company employees. There are few e-government studies, although public administrations have electronically processed sensitive and critical information for decades. In order to overcome this limitation, we are particularly keen to stimulate projects in this area. More research in the nonlinear and complex field of ISA and ISAT is necessary.

6. References

[1] Albrechtsen, E., “A Qualitative Study of Users’ View on Information Security”, *Computers & Security*, Vol. 26, No. 4, 2007, pp. 276–289.

[2] Allianz für Cyber-Sicherheit/Alliance for Cyber Security, *Awareness-Umfrage 2015*.

[3] Aytes, K., and C. Terry, “Computer security and risky computing practices: a rational choice perspective”, *Journal of Organizational and End User Computing*, Vol. 16, No. 3, 2004, pp. 22–40.

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

[5] Beckers, K., and S. Pape, “A serious game for eliciting social engineering security requirements”, *Requirements Engineering Conference*, 2016, pp. 15–25.

[6] Beyer, M., S. Ahmed, K. Doerlemann, S. Arnell, S. Parkin, A. Sasse, and N. Passingham, *Awareness is only the first step: A framework for progressive engagement of staff in cyber security*, Hewlett Packard, Business white paper, 2016.

[7] Boss, R.S., L.J. Kirsch, I. Angermeier, R.A Shingler, and R.W. Boss, “If someone is watching, I’ll do what I’m asked: Mandatoriness, control, and information security”, *European Journal of Information Systems*, Vol. 18, No. 2, 2009, pp. 151–164.

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Federal Office for Information Security), *ORP.3: Sensibilisierung und Schulung*, 2016.

[9] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Federal Office for Information Security), *Self-Declaration and IT-Grundschutz Certificate*, 2016.

[10] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Federal Office for Security in Information Technology), *BSI-Standards 200-1. Managementsysteme für Informationssicherheit (ISMS). Community Draft – Version*, 2017.

[11] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Federal Office for Information Security), “Knowing risks, accepting challenges, designing solutions: Preface”, *Conference Proceedings of the 14th German IT Security Conference*, Bonn, Bad Godesberg, 2015.

[12] Bundesministerium für Wirtschaft und Energie (BMWi) (Federal Ministry of Economics and Energy), *International Dimension: EU – Digital Agenda*, 2014.

[13] Caldwell, T., “Making security awareness training work”, *Computer Fraud & Security*, Vol. 6, 2016, pp. 8–14.

[14] Chen, C.C., B.D. Medlin, and R.S. Shaw, “A cross-cultural investigation of situational information security awareness programs”, *Information Management & Computer Security*, Vol. 16, No. 4, 2008, pp. 360–376.

[15] Chen, Y., K. Ramamurthy, and K.-W. Wen, “Information Security Policy Compliance: Stick or Carrot Approach?”, *Journal of Management Information Systems*, Vol. 29, No. 3, 2014, pp. 157–188.

[16] Choi, N., D. Kim, J. Goo, and A. Whitmore, “Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action”, *Information Management & Computer Security*, Vol. 16, No. 5, 2008, pp. 484–501.

[17] Chu, A., P. Chau, and M. So, “Explaining the misuse of information systems resources in the workplace: A dual-process approach”, *Journal of Business Ethics*, Vol. 131, No. 1, 2015, pp. 209–225.

[18] Cone, B.D., C.E. Irvine, M.F. Thompson, and T.D. Nguyen, “A Video Game for Cyber Security Training and Awareness”, *Computers & Security*, Vol. 26, No. 1, 2007, pp. 63–72.

[19] Da Veiga, A., “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*, Vol. 24, No. 2, 2016, pp. 139–151.

[20] Dark, M.J., “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,* Course Technology, Mason, 2006, pp. 86–104.

[21] DSV-Gruppe, EnBW, <kes>, known_sense, nextsolutions, and Pallas (eds.), *Entsicherung am Arbeitsplatz: Die geheime Logik der IT-Security in Unternehmen,* Cologne, Munich, 2006.

[22] Elliot, J., “How to Do Security WITH Your Organisation, Not TO It” (Video), *RSA Conference*, 2017.

[23] EnBW, known_sense, Pallas, SAP, Sonicwall, Steria Mummert Consulting, and Trend Micro (eds.), *Aus der Abwehr in den Beichtstuhl: Qualitative Wirkungsanalyse*, CISO & Co., Cologne, 2008.

[24] Fagade, T., and T. Tryfonas, “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, Springer, Cham, 2016, pp. 128–139.

[25] Flores, W.R., H. Holm, G. Svensson, and G. Ericsson, “Using phishing experiments and scenario-based surveys to understand security behaviours in practice”, *Information Management & Computer Security*, Vol. 22, No. 4, 2014, pp. 393–406.

[26] Foth, M., “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*, Vol. 25, No. 2, 2016, pp. 91–109.

[27] Guo, K., Y. Yuan, N.P. Archer, and C.E. Connelly, "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model", *Journal of Management Information System*, Vol. 28, No. 2, 2011, pp. 203–236.

[28] Hanamura, K.I., T. Takemura, and A. Komatsu, "Research Note: Analysis of the Characteristics of Victims in Information Security Incident Damages; The Case of Japanese Internet Users", *The Review of Socionetwork Strategies*, Vol. 7, No. 1, 2013, pp. 43–51.

[29] Herath, T., and H.R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47, No. 2, 2009, pp. 154–165.

[30] Hsu, J.S.-C., S.-P. Shih, Y.W. Hung, and P.B. Lowry, "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness", *Information Systems Research*, Vol. 26, No. 2, 2015, pp. 282–300.

[31] Hu, Q., T. Dinev, P. Hart, and D. Cooke, "Managing employee compliance with information security policies: The critical role of top management and organizational culture", *Decision Sciences*, Vol. 43, No. 4, 2012, pp. 615–660.

[32] 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.

[33] ISF (Information Security Forum), *From Promoting Awareness to Embedding Behaviors: Secure by Choice Not by Chance*, 2014.

[34] James, T., Q. Nottingham, and B.C. Kim, "Determining the antecedents of digital security practices in the general public dimension", *Information Technology and Management*, Vol. 14, No. 2, 2013, pp. 69–89.

[35] Jones, B.H., A.G. Chin, and P. Aiken, "Risky business: Students and smartphones", *Tech Trends*, Vol. 58, No. 6, 2014, pp. 73–83.

[36] Khan, B., K.S. Alghathbar, S.I. Nabi, and M.K. Khan, "Effectiveness of information security awareness methods based on psychological theories", *African Journal of Business Management*, Vol. 5, No. 26, 2011, pp. 10862–10868.

[37] Kim, E.B., "Recommendations for information security awareness training for college students", *Information Management & Computer Security*, Vol. 22, No. 1, 2014, pp. 115–126.

[38] Kirlappos I., A. Beautement, and M.A. Sasse, "'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, Springer, Berlin, Heidelberg, 2013, pp. 70–82.

[39] Kirlappos, I., S. Parkin, and M.A. Sasse, "Learning from 'Shadow Security': Why understanding non-compliance provides the basis for effective security", *(Proceedings) Workshop on Usable Security (USEC)*, San Diego, CA, USA, 2014.

[40] Kruger, H.A., and W.D. Kearney, "A prototype for assessing information security awareness", *Computers & Security*, Vol. 25, No. 4, 2006, pp. 289–296.

[41] Kruger H., L. Drevin, and T. Steyn, "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, Springer, Boston, MA, 2007, pp. 33–40.

[42] Lebek, B., J. Uffen, M. Neumann, B. Hohler, and M.H. Breitner, "Information security awareness and behavior: A theory-based literature review", *Management Research Review*, Vol. 37, No. 12, 2014, pp. 1049–1092.

[43] Liang, H., Y. Xue, and L. Wu, "Ensuring Employees' IT Compliance: Carrot or Stick?", *Information Systems Research*, Vol. 24, No. 2, 2013, pp. 279–294.

[44] Manifavas, C., K. Fysarakis, K. Rantos, and G. Hatzivasilis, "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, Springer, Cham, 2014, pp. 258–269.

[45] McCrohan, K.F., K. Engel, and J.W. Harvey, "Influence of Awareness and Training on Cyber Security", *Journal of Internet Commerce*, Vol. 9, No. 1, 2010, pp. 23–41.

[46] Mejias, R.J., and P.A. Balthazard, "A Model of Information Security Awareness for Assessing Information Security Risk for Emerging Technologies", *Journal of Information Privacy and Security*, Vol. 10, No. 4, 2014, pp. 160–185.

[47] Ngoqo, B., and S.V. Flowerday, "Exploring the relationship between student mobile information security awareness and behavioural intent", *Information & Computer Security*, Vol. 23, No. 4, 2015, pp. 406–420.

[48] Öğütçü, G., Ö.M. Testik, and O. Chouseinoglou, "Analysis of personal information security behavior and awareness", *Computers & Security*, Vol. 56, 2016, pp. 83–93.

[49] Parsons, K., A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "A study of information security awareness in Australian government organisations", *Information Management & Computer Security*, Vol. 22, No. 4, 2014, pp. 334–345.

[50] Pattinson, M., K. Parsons, M. Butavicius, A. McCormac, and D. Calic, "Assessing information security attitudes: A comparison of two studies", *Information & Computer Security*, Vol. 24, No. 2, 2016, pp. 228–240.

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

[52] Pfleeger, S.L., M.A. Sasse, and A. Furnham, "From Weakest Link to Security Hero: Transforming Staff Security Behavior", *Journal of Homeland Security and Emergency Management*, Vol. 11, No. 4, 2014, pp. 489–510.

[53] Pipkin, D.L., *Information Security: Protecting the Global Enterprise*, Prentice-Hall Inc., Upper Saddle River, NJ, 2000.

[54] Pokoyski, D., "Security Awareness: Von der Oldschool in die Next Generation; Eine Einführung", in M. Helisch, and D.

Pokoyski (eds.), *Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*, Vieweg+Teubner, Wiesbaden, 2009, pp. 1–8.

[55] Rudel, S., and A. Rieb, "Technik vs. Mensch: Was nutzt ein hoher technischer Standard, wenn die Schwachstelle Mensch umgangen wird?", in Bundesamt für Sicherheit in der Informationstechnik (BSI), *Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis*, Tagungsband zum 15. Deutschen IT-Sicherheitskongress, 2017, pp. 345–352.

[56] Safa, N.S., R. von Solms, and S. Furnell, "Information security policy compliance model in organizations", *Computers & Security*, Vol. 56, 2016, pp. 70–82.

[57] SANS Securing the Human, *Security Awareness Report: Awareness Is Hard: A Tale of Two Challenges*, 2016.

[58] Scholl, M., K. Leiner, and F. Fuhrmann, "Blind spot: Do you know the effectiveness of your information security awareness-raising program?", *Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017)*, pp. 361–366.

[59] Scholl, M., and F. Fuhrmann, "Analog – digital? Wie sich mithilfe analoger Methoden Bewusstsein für Informationssicherheit in der digitalen Welt fördern lässt", in D. Rätz, M. Breidung, D. Lück-Schneider, S. Kaiser, and E. Schweighofer (eds.), *Digitale Transformation: Methoden, Kompetenzen und Technologien für die Verwaltu*ng, Lecture Notes in Informatics (LN), Vol. 261, 2016, pp. 101–112.

[60] Scholl, M., F. Fuhrmann, and D. Pokoyski, "Information Security Awareness 3.0 for Job Beginners", in J. E. Varajão, M.M. Cruz-Cunha, R. Martinho, R. Rijo, N. Bjørn-Andersen, R. Turner, and D. Alves (eds.), *Conference on ENTERprise Information Systems (CENTERIS)*, 2016, pp. 433–436.

[61] Shaw, R.S., C.C. Chen, and A.L. Harris, "The impact of information richness on information security awareness training effectiveness", *Computers & Education*, Vol. 52, No. 1, 2009, pp. 92–100.

[62] Singh, A.N., A. Picot, J. Kranz, M.P. Cupta, and A. Ojha, "Information security management (ism) practices: Lessons from select cases from India and Germany", *Global Journal of Flexible Systems Management*, Vol. 14, No. 4, 2013, pp. 225–239.

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

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

[65] Stewart, G., and D. Lacey, "Death by a thousand facts: Criticising the technocratic approach to information security awareness", *Information Management & Computer Security*, Vol. 20, No. 1, 2012, pp. 29–38.

[66] Straub, D.W., and R.J. Welke, "Coping with Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly*, Vol. 22, No. 4, 1998, pp. 441–469.

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

[68] Sun, J., P. Ahluwalia, and K.S. Koong, "The more secure the better? A study of information security readiness", *Industrial Management & Data Systems*, Vol. 111, No. 4, 2011, pp. 570–588.

[69] Tsohou A., M. Karyda, S. Kokolakis, and E. Kiountouzi, "Analyzing Information Security Awareness through Networks of Association", in S. Katsikas, J. Lopez, and M. Soriano (eds.), *Trust, Privacy and Security in Digital Business*, TrustBus 2010, Lecture Notes in Computer Science, Vol. 6264, Springer, Berlin, Heidelberg, 2010, pp. 227–237.

[70] Tsohou, A., M. Karyda, S. Kokalakis, and E. Kiountouzi, "Analyzing trajectories of information security awareness", *Information Technology & People*, Vol. 25, No. 3, 2012, pp. 327–352.

[71] Tsohou, A., M. Karyda, S. Kokalakis, and E. Kiountouzi, "Managing the introduction of information security awareness programmes in organisations", *European Journal of Information Systems*, Vol. 24, No. 1, 2015, pp. 38–58.

[72] Van Niekerk, J.F., and R. von Solms, "Information security culture: A management perspective", *Computers & Security*, Vol. 29, No. 4, 2010, pp. 476–486.

[73] Verton, D., *The Hacker Diaries*, McGraw-Hill, Inc., New York, 2002.

[74] Von Solms, S.H., "The 5 Waves of Information Security: From Kristian Beckman to the Present", in K. Rannenberg, V. Varadharajan, and C. Weber (eds.), *SEC 2010, IFIP International Federation for Information Processing AICT 330*, 2010, pp. 1–8.

[75] Warkentin, M., A.C. Johnston, and J. Shropshire, "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention", *European Journal of Information Systems,* Vol. 20, No. 3, 2011, pp. 267–284.

[76] Winkler, I., "The Human Exploitation Kill Chain" (Video), *RSA Conference*, 2017.

[77] Workman, M., "Gaining Access with Social Engineering: An Empirical Study of the Threat", *Information Systems Security*, Vol. 16, No. 6, 2007, pp. 315–331.

[78] Young, R. "Growth Perspective of Information Security", *Journal of Information Privacy and Security*, Vol. 5, No. 4, 2014, pp. 51–67.