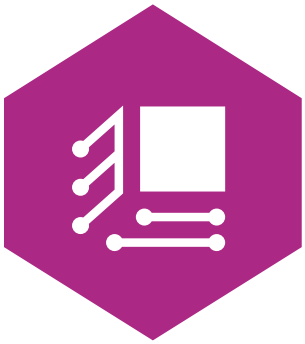

VOLUME 18 ISSUE 2

The International Journal of

# Technology, Knowledge, and Society



## Scenarios as a Tool for Professional Training in Information Security Dialogues

JOHAN LUGNET AND ÅSA ERICSON

COMMON GROUND

TECHANDSOC.COM

**THE INTERNATIONAL JOURNAL OF TECHNOLOGY, KNOWLEDGE, AND SOCIETY**
https://techandsoc.com
ISSN: 1832-3669 (Print)
https://doi.org/10.18848/1832-3669/CGP (Journal)

First published by Common Ground Research Networks in 2022
University of Illinois Research Park
60 Hazelwood Drive
Champaign, IL 61820 USA
Ph: +1-217-328-0405
https://cgnetworks.org

*The International Journal of Technology, Knowledge, and Society* is a peer-reviewed, scholarly journal.



Common Ground Research Networks, a member of Crossref



**PEER REVIEW**
Articles published in *The International Journal of Technology, Knowledge, and Society* are peer reviewed using a two-way anonymous peer review model. Reviewers are active participants of the Technology, Knowledge, and Society Research Network or a thematically related Research Network. The publisher, editors, reviewers, and authors all agree upon the following standards of expected ethical behavior, which are based on the Committee on Publication Ethics (COPE) Core Practices. More information can be found at
https://cgnetworks.org/journals/publication-ethics.

**ARTICLE SUBMISSION**
*The International Journal of Technology, Knowledge, and Society* publishes biannually (June, December). To find out more about the submission process, please visit
https://techandsoc.com/journal/call-for-papers.

**ABSTRACTING AND INDEXING**
For a full list of databases in which this journal is indexed, please visit https://techandsoc.com/journal.

**RESEARCH NETWORK MEMBERSHIP**
Authors in *The International Journal of Technology, Knowledge, and Society* are members of the Technology, Knowledge, and Society Research Network or a thematically related Research Network. Members receive access to journal content. To find out more, visit https://techandsoc.com/about/become-a-member.

**SUBSCRIPTIONS**
*The International Journal of Technology, Knowledge, and Society* is available in electronic and print formats. Subscribe to gain access to content from the current year and the entire backlist. Contact us at cgscholar.com/cg_support.

**ORDERING**
Single articles and issues are available from the journal bookstore at https://cgscholar.com/bookstore.

**OPEN RESEARCH**
*The International Journal of Technology, Knowledge, and Society* is Hybrid Open Access, meaning authors can choose to make their articles open access. This allows their work to reach an even wider audience, broadening the dissemination of their research. To find out more, please visit https://cgnetworks.org/journals/open-research.

**DISCLAIMER**
The authors, editors, and publisher will not accept any legal responsibility for any errors or omissions that may have been made in this publication. The publisher makes no warranty, express or implied, with respect to the material contained herein.

# Scenarios as a Tool for Professional Training in Information Security Dialogues

Johan Lugnet,[1] Luleå University of Technology, Sweden
Åsa Ericson, Luleå University of Technology, Sweden

*Abstract: This article presents scenarios designed to support abstract and reflective thinking necessary to inculcate information security awareness among IT service designers. Data for the study was obtained in empirical interventions and through an action research approach in cooperation with an IT company. The findings highlight the need for training that, in combination with traditional contents, also integrates organizational, business, and social aspects into information security awareness. Rethinking a strategy for training to be grounded in scenarios from day-to-day business activities is one implication of the study; another is the suggestion to frame the scenarios as dilemmas, that is, problematic and realistic situations having multiple solutions depending on interpretations and perspectives, and a final conclusion is the importance of enabling structured in-depth dialogues among employees.*

*Keywords: Information Security Awareness, Social and Organizational Aspects, Scenario-Based Learning, Professional Education, Gamification*

## Introduction

The digitalization of products and services has progressed toward an interconnected business world where technological cyber security measures have been in focus. Today, those technical solutions, for example, firewalls, VPN and antivirus software have proven utterly important for consumers, whether they are representing businesses or acting as private persons. The societal benefits that are expected from the implementation of digital solutions are high. It is, for example, concluded that they will enable a sharing economy (Huckle et al. 2016), and that Industry 4.0 will drive sustainable development (Smart Services Welt 2015). The efforts to fulfil sustainable development goals by introducing new digital and interconnected solutions suggest that solutions will become a mix of both goods and services, or products-service systems which are firmly service-oriented (Vargo and Lush 2004). Typically, the introduction of product-service solutions as a digital and sustainable business model is seen from a positive standpoint, for example, reporting on expected efficiency by 15 to 20 percent for companies (Parida, Sjödin, and Reim 2019).

However, all digital systems need to be maintained and upgraded to be kept secure from threats and breaches. As a rule of thumb, the costs allocated for the yearly maintenance of solutions are 20 percent of the development cost (e.g., WestArete 2019). This means that the tipping point for maintenance costs to exceed the development costs comes after five years. This does not align with the sustainable requirements, like for example, prolonging the lifecycle of products by digital services. Due to the interconnectivity, and its consequence of increased complexity in relationships between actors, for example, digital service developers, digital service providers, clients, and users, the threat landscape becomes more complex and the risks for all partners who are interacting with the systems change drastically. The cooperation increases the chances of entry for an underground economy of cybercriminals, and the encompassing digitalization in society gives them a wider attack sector. The, by now well-known, attack on a casino in USA where 10 gigabytes of data were stolen from their customer database through an interconnected thermostat in an aquarium (Mathews 2017) is one such

[1] Corresponding Author: Johan Lugnet, Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, SE- 97187, Sweden, email: johan.lugnet@ltu.se

*The International Journal of Technology, Knowledge, and Society*
Volume 18, Issue 2, 2022, https://techandsoc.com

ISSN: 1832-3669 (Print)
https://doi.org/10.18848/1832-3669/CGP/v18i02/65-77 (Article)

example showing that such attacks are stealthier and more ambitious (Symantec 2019). The attack on Kaseya, a US-based manager of IT structure for major stores worldwide, in July 2021 is another recent example of wide-reaching consequences of such attacks, where 800 groceries stores in Sweden were forced to close down for a week (Osborne 2021).

IBM (2014) concluded that over 95 percent of information security-related incidents were recognized as caused by "human error." In relation to this, it is important to consider the concept of trust, which is what cyber criminals misuse for their fraudulent purposes when manipulating people's behavior to, for example, respond to malicious emails (so-called social engineering). Trust is a basic element in interactions is related to a human state of mind, that is, we assume that what we do or say should be received respectfully and constructively, that is positively or in a worst case, neutrally (e.g., Kramer 1999), and, vice versa—we suppose what others do or say have good intentions. Digital trust—in short people having confidence in service providers creating a secure digital world—is influenced by a number of factors, such as, regulations, standards, dependability, reliability, honesty, motivation, and ethics (Yan and Holtmanns 2008). As can be seen, some are agreed and articulated, for example, regulations and standards, and some are subjective and intrinsic in culture and beliefs, for example, honesty and motivation. The CIA triad, which is an acronym for Confidentiality, Integrity, and Accessibility, is an important model for information security, but is certainly a challenge to apply when designing services. An international study found that 81 percent of respondents from organizations perceived that connected products and services were critical for their businesses, but only 39 percent of those respondents considered that they had control over security, integrity, and ethical aspects (PwC 2019). The fact that employees need better knowledge and education in information security is typically seen as the responsibility of the IT (information technology) department (e.g., Wilson and Hash 2003). However, not all organizations have dedicated information security specialists. The digitalization of all business activities brings new responsibilities for all employees, since any of them can become the weak link in the chain which can be used by criminals as an entry into the organization's IT systems and to get access to critical information.

In the case of an IT company, the challenges of managing clients' information and designing digital services have to be included in the training programs. IT consultants may possess expertise in the design of technical solutions, but may lack experience in information security, that is, information management, regardless of its format (von Solms and von Solms 2018). However, they have to manage both, adding to the complexity of the situation where clients may themselves lack understanding of the nature of their own information. Hence, preparedness for information security situations caused by the people factor needs to be included in general training programs (Alshaikh et al. 2018). Previous studies have concluded that training programs for professionals often lack theoretical grounding (e.g., Abraham and Chengalur-Smith 2019), but it has also been concluded that if the implementation in practice is perceived as too ambitious, the interest goes down (Saban, Rau, and Wood 2021). Taking this perspective, this article attempts to present and reflect on the design of scenarios emerging from practice to later be incorporated in a training program in information security awareness for professional digital service developers.

This article is disposed to first describe the research approach; second, to provide a theoretical background of training programs; and third, present and reflect on our empirical findings. Finally, the article concludes with implications and ideas about future studies.

## Research Approach: Action Research and a Participative Approach

The study was based on an action research approach. Action research exists in different forms but can generally be described as iterations of simultaneous understanding and changes—so-called informed actions, where each new iteration is preceded by reflection. According to Checkland and Holwell (1998), three elements essentially need to be clarified when doing

action research. Those are (1) a framework of ideas to clarify the pre-understanding, (2) the methodology per se, and (3) the area of concern. The framework of ideas is important to explain the motivation for the study in relation to how qualitative data is interpreted. The motivation for this study was found in the analyses of previous research efforts in information security training (as presented in the section titled Information Security Training below), but also from interactions with companies in applied research projects. Furthermore, acting as course developers, teachers and examiners at the University's information security master program also contributed to the motivation of studying and designing training programs.

The methodology for this study can be described as participative, since the respondents, mainly IT service designers and digital service developers, were active actors in the research stages, that is, data acquisitions, analyses, and reflection. Thus, they also influenced the results. Gathering of qualitative and empirical data and its analytical interpretations are simultaneous, which is natural for participative methods (Checkland and Holwell 1998; Miles and Huberman 1994). Data in this study was gathered jointly by the researchers and by the respondents over a period of one year. The researchers undertook literature studies within information security training and participated in bi-monthly meetings and workshops with the respondents. In addition, the respondents, in internal workshops, discussed what they perceived as troublesome when managing information in the design of services and in customer relationships. The analysis of the results from the interactions and workshops with representatives from the company resulted in nineteen identified challenging situations. The nineteen situations were further analyzed in collaboration with the company CIO (chief information officer) and the chief business manager. The situations were thereafter aggregated into scenarios. The scenarios were further jointly analyzed in two meetings with the respondents. Three of the situations are generalized into scenarios and presented in the empirical finding section in this article. The presented examples are to some extent simplified to align with the requested anonymization from the company. The analyses of the situations can be described as open and non-cross sectional, meaning that a pattern and categorization emerged from the material (Silverman 2000; Mason 2002). This implies that the described situations are central in the construction of the scenarios, thereby putting the challenge into a context and into a specific (realistic) setting. This method was decided, since the joint analyses found that the situations were typical dilemmas, that is, there was no single correct answer, but several possible solutions to each scenario. The scenarios and the training approach were later put into a test with seventeen information security students. The focus in the tests was to investigate the scenarios and learning process in a digital format. After some refinement in how to present the scenarios, a user test with ten employees from the company was conducted.

This study is in progress in the context of professional training at different companies, that is, its area of concern (Checkland and Holwell 1998). In this article, we address one of those companies, namely an IT company that designs, develops, and sells digital services. It is a medium-sized, and nationwide firm, which works in a distributed manner across several offices at different geographical locations. Most employees have an educational background in IT-related areas, like programming, system architecture, interaction design, user-interface, and service design, but also in areas such as business, sales, and marketing. The company works with a range of clients, for example, companies, municipalities, and authorities, and hence experiences several types of information security challenges in its different tasks. Recently, a specific role of information and cyber security expertise has been introduced to support the company's design and development function and can be seen as being responsible for the implementation of the suggested training program. Due to the distributed business sites, a key requirement is that training must be conducted online, because the employees find it difficult to join co-located meetings. Preferably training should also be self-paced, so that the employees can start at different times, complete it at their own pace, and without external facilitators being available.

## Information Security Training

The so-called DIKW pyramid (Ackoff 1989; Rowley 2007), that is, data, information, knowledge and wisdom, is commonly used to describe and classify the relationships between concepts. The DIKW pyramid indicates that information is a valuable resource, consisting of formal guidelines, informal experiences, and contextual interpretations. Information is a prerequisite to build business wisdom. The term wisdom represents the organization's values, insights, and principles for innovation and development (Ackoff 1989; Rowley 2007). Development and innovation need an increase in wisdom, while expansion comes from the capability to benchmark, copy, and do more of the same (Ackoff 1989). Information is a basic prerequisite for creating business value based on the ability to innovate and create new solutions, products, services, processes, and the like (Jacoby and Rodriguez 2007). Information, due to its embeddedness with knowledge and wisdom, is a resource that is not straightforward to capture, formalize, or to classify in terms of protection and security measures for organizations.

Uncertainty about how to manage information security causes hesitance when developing or outsourcing new digital services (Osborn and Simpson 2018), so the subject is important to include in the design sector. Reports show that not only large, but also small- and medium-sized companies are increasingly attracting the attention of cybercriminals (Symantec 2019). For example, it is shown that 43 percent of cyberattacks target small- and medium-sized companies directly, and that 60 percent of those will be gone from the market within six months (Verizon 2019). Small- and medium-sized companies have in particular demonstrated a low and slow uptake of information security training efforts (Saban, Rau, and Wood 2021). Reasons for few training efforts are lack of time, lack of budget, lack of planning, and lack of relevant training (O'Brien and Hamburg 2013). To overcome the barriers, on-the-job training, which is contextualized, situated, and problem-based, is commonly suggested.

Information security training has in earlier studies been concluded to be centered around traditional formats of education (e.g., Lacey 2010), that is, individual reading and tests that have simple answers to theoretical questions. It has been suggested that learning programs need to go beyond such standardized formats and incorporate the dynamic that is embedded in information security management (Crossler et al. 2013). Traditional formats of training have been criticized for making people believe that they already know the answer, which happens when people are exposed to a question and provided with one correct answer. Furthermore, we tend to think that we have always known the answer when we get the correct one. These mental mistakes of thinking are so-called hindsight bias, and foresight bias (South 2007). We are tricked by our own brain to believe that we know more than we actually do when the training program is based on simple single-solution problems. It is suggested that professional training programs should incorporate realistic problems, and more complex problems, since those make people mindful of the topics and committed to company policies (Bulgurcu, Cavusoglu, and Benbasat 2010). Aligning training programs with expectations from executives and the requirements to keep employees interested are found to aid design, implementation, and assimilation of the programs (Saban, Rau, and Wood 2021).

There are a mix of different, but to some extent similar concepts used in relation to the security topic, for example, information security, information technology security, computer security, and cybersecurity (Paulsen and Byers 2019). Publications of NIST (National Institute of Standards and Technology) in the US provide guidance for training programs in information technology security (Wilson and Hash 2003). The definition of information technology security, also provided by NIST, is somewhat confusing since it does not explain "technology" but denotes the concept as the entire range of technology, its applications, and support systems (National Institute of Standards and Technology [NIST], n.d.). However, von Solms and von Solms (2018), in their study of definitions provided in other families of standards and guidelines, conclude that cybersecurity and IT security are subsets of information security.

Information security, as defined by von Solms and von Solms (2018), includes the activities to assign appropriate security measures to information in any form. Thus, organizations need to know what information resources they have. The suggested procedure to consider this is to follow a classification scheme also assessing probability of risks and consequences (e.g., International Organization for Standardization [ISO] 2013). The definition of information security provided by NIST prescribes that information and information systems should be protected from unauthorized access, use, modification, and the like, with the goal of ensuring confidentiality, integrity, and availability (NIST, n.d.). The CIA-triad, which stands for confidentiality, integrity, and availability is, as evident in the definition from NIST, well-established within the information technology security domain. Over time, research efforts have addressed the subject of whether the CIA-triad has the breadth to cover socio-technical issues. The efforts commonly conclude that re-conceptualizing the meaning of security controls needs to be done, rather than discarding the model as such (Samonas and Coss 2014). The CIA-triad suggests, in short, that unauthorized persons should not be able to:

- read and use the information—confidentiality
- modify or make changes to the stored information—integrity
- deny use of the stored information for those that are authorized—availability.

The inclusion of not only digital, but all types of information formats align with the operational and practical definitions found in organizations and companies, that is, that information security encompasses all types of information resources (Saban, Rau, and Wood 2021). Finding absolute definitions for each concept does not seem constructive, but organizations benefit from describing how different concepts relate to their businesses, to the different roles, and different responsibilities (Wilson and Hash 2003). It is hence important to create a shared vocabulary.

Wilson and Hash (2003) provides instruction for information technology security training as a NIST guideline which is established for an IT security learning scale. It prescribes the categories awareness, training, and education as:

- Awareness is for all, and it focuses attention on security and allows individuals to recognize and respond to such situations. Awareness is not training since the learner receives information and has no active role.
- Training is for all users of IT systems, that is, digital systems. Training is a formal activity and strives to build relevant security skills and competencies to support the job to be done. The learner takes a more active role.
- Education is for IT security professionals and is described as multidisciplinary integration of technological and social aspects to produce specialists. Education is described as degree programs or certificate programs at colleges or universities.

The separation in the explanation between awareness and training according to Wilson and Hash (2003) may lead to the idea that each element can be seen as a standalone unit, and make it seem that awareness does not relate to training. However, the elements should be interpreted in terms of relationships between the elements, that is, awareness-training-education. This relationship is clearly described in the guidelines for how to design a learning program and includes the development of awareness (the behavior to reinforce) and training (skills to learn and be able to apply) (Wilson and Hash 2003).

Awareness (of different topics) lays the foundation for training (the learning process) for all users of IT systems. Wilson and Hash (2003) suggest that all—internal and external—users should:

- Comply with the organization's policies and regulations.
- Be trained in the systems and applications they use (behavior, code of conduct, and similar).
- Be aware of, for example, password usage, data backup, antivirus protection, violation of security policy, how to report incidents, and how to avoid social engineering attacks.

Using software tools to enable self-paced training is of interest, especially in distributed businesses. Furnell, Gennatou, and Dowland (2002) tested a prototype that was extended with multimedia functions in an interactive online training setting. The learners were provided descriptions of situations and were encouraged to apply countermeasures that they could select from a database. An improved version of the tool was presented adding audio-visual content, graphics, and texts to represent real-life situations from an organization, and a set of multiple-choice questions to further improve the learning (Furnell, Warren, and Dowland 2003; Sharfaei and Furnell 2003–2004). Shaw et al. (2009) conducted a study on three levels of awareness, namely, (1) perception of threats, (2) comprehension of how to handle those, and (3) the ability to anticipate future situations. From this study, it was concluded that learners presented with only text material performed better at the perception level, while learners presented with multimedia material performed better at the comprehension level and demonstrated the ability to foresee future situations. Another prototype was tested to measure awareness, by using questionnaires and applying the answers in a three-dimension scoring model: (1) knowledge, what was known, (2) attitude, toward the topic, and (3) behavior, the kind of actions the learner would have conducted (Kruger and Kearney 2006). This kind of support was found useful for evaluation of the maturity level of awareness of the organization as a whole. Also, a pilot study of information security training included features like a discussion forum, newsletter, and article sharing (Chen, Shaw, and Yang 2006).

The pedagogical training material as such has gained attention when using software tools. Puhakainen and Siponen (2010) investigated two types of approaches. One approach emphasized instruction-led teaching having one-way interaction and quantitative measurements in line with a traditional format of learning. The other approach stressed interactive two-way discussions between learners, where each learner's own thinking, critical reflections, and conversational forms of evaluation were central. It was concluded that the interactive training was preferred by the learners. Furthermore, non-technical learners were also provided with a software tool and followed a three-fold training session addressing social engineering attacks by email (Puhakainen and Siponen 2010). The first part was instructor-led discussions that focused on risks in relation to the use of emails. In the second part, the learners were approached with emails and documents which they analyzed. The third part was to reflect on behavior and the possible consequences of it.

From their study, Puhakainen and Siponen (2010) concluded that information security training should:

- utilize methods and learning tasks that activate and motivate the learners' cognitive processing by having personal relevance and by becoming visible and realistic,
- encourage continuous and integrated dialogues into the daily work.

From previous studies in training of information security awareness (e.g., Kruger and Kearney 2006; Shaw et al. 2009; Puhakainen and Siponen 2010) it can hence be concluded that the idea of non-active learners can be questioned.

### *A Brief Review of the Pedagogical Foundation*

Problem-based learning is, in short, an instructional approach where doing and creating forms the object for learning. Simplified, it goes through three main stages: (1) understand the problem, (2) explore and generate possible solutions, and (3) decide and present the solution. Problem-based learning is in line with the Conceive Design Implement Operate (CDIO) framework (n.d.), which is guiding the pedagogical idea for several institutions of higher education. The acronym CDIO stands for Conceive, Design, Implement, and Operate, and has evolved to progress beyond traditional engineering education to include the realistic and complex processes of both problem-definition and problem-solving. This type of learning objective is related to personal development, or to train high-order-thinking skills (e.g., Anderson and Krathwohl 2001), which are important for envisioning novel future situations.

Dweck (2017) presents two different types of mindsets, a fixed one and a growth one. The latter is related to personal development. A fixed mindset is shown in the urgency to prove oneself right, that one already is knowledgeable about a topic. This mindset renders a judgmental stance and so-called summative feedback on what people already master. The personal development mindset is based on a belief that your basic qualities can be cultivated, and collaboration and communication with others are means to do that (Dweck 2017).

Training related to problem-based learning tries to encourage the learners to evaluate their own effort in relation to others, and also generalize their knowledge to an envisioned future situation (e.g., Feisel 1986; Biggs 1996). As a pedagogical approach, problem-based learning rests upon effective teaching and active learning, including the principles of, for example: (Ramsden 2003):

- Stimulate interest and quality in explanation.
- Create concern and respect for learners and learning.
- Give appropriate assessment and feedback to progress.
- Provide an intellectual challenge.
- Enable independence, control, and engagement.

Gibbs (1999) elaborated on feedback, and, quite provokingly for traditional education formats, he stated that it is a cliché that learners require feedback from an instructor to be able to learn. Instead, Gibbs promotes peer dialogues for feedback, since the social dimensions of dialogues internalize understanding on a personal level, that is, the reaction of a colleague matters, since people tend to care about what others think about them. Gibbs (1999) described that feedback, however, has to be instant—for instance, when you play darts, you improve when you are able to see where the darts land. Furthermore, Gibbs (1999) concluded that learners should spend time on the task and tackle a lot of variants of the problems.

## Empirical Findings

The interaction with the company in this study rendered nineteen scenarios, of which three examples are presented here. The scenarios are outlined as wicked problems, that is, they have several alternative interpretations depending on perspective, similar to dilemmas. The scenarios as tested with users were presented as short videos or filmed sketches, supported by text and graphic pictures. Three examples of scenarios that digital service developers can experience and have to manage are:

- *Integrity of People*—Your customers must share information with you, but over time it becomes evident that a customer has shared sensitive information about people. When trying to investigate what has happened, it is clear that the customer has no understanding that the information was sensitive. The responsible person at the customer's place is not interested in figuring out how to solve the problem, and tells you to continue the work since the situation is none of your business. You consider the situation as a conflict with the integrity of people. How will you manage the situation?
- *Confidentiality and Trust*—You must always be available to respond to customer requests, but you are often in meetings with other customers in their premises. You are busy with a client when your company's most important customer calls to inform you about an urgent matter. You explain that you need to answer the call, but where to take the call? And your laptop is open, showing your presentation in the meeting room. You consider the situation as being in conflict with confidentiality and trust. How will you behave in this situation?
- *Ethicality and Privacy*—You are designing a new digital solution and are discussing its functionality with your most important customer's CEO. The CEO says that you should add a monitor and control function for logging the employees' movements and activities. The function can easily be added to the order, but a surveillance function is in conflict with labor policies and regulations. You consider gathering such information as a conflict with ethical design and privacy. How will you communicate with the customer in the situation?

When the results were presented to the company after the compilation into scenario descriptions, the scenarios were found as consisting of "mundane" work task. This was unexpected, since the company representatives had the perception that their information security challenges probably would be more "typical," for example, how to comply with data protection regulations, managing access to systems, and the like. An analysis of the unexpected result indicated that training to complement the "traditional" approach was a good decision but it was maybe also an indication that the implemented training thus far had increased the insights in formal policies and regulations, since these were not considered as the main problems in the scenarios.

In the analyses and construction of the scenarios, it became clear that the main problems occurred in interactions with customers, and reflections concerning the consequences were most troublesome. The user test showed that the scenarios generated dialogues providing new upcoming perspectives and solutions. In pedagogics, the Johari window (e.g., South 2007) conceptualize three perspectives of personal development, namely, known known, known unknowns, and unknown unknowns. These concepts are, in a popular view, often associated with the former US Secretary of Defense, Donald Rumsfeld, in a speech from 2002, and make fun of that speech. However, the concepts originate from teaching and learning to better understand how to achieve critical and reflective thinking and by that awareness, going from what is known to analyze a range of unknowns. The scenarios described a situation in which a risk could be identified (known known). The scenarios generated analyses of whether or not that risk could be related to the developers' situations or if they have experienced a similar challenge. Thus, the probability for the risk, or any other similar risk to occur or not, was investigated (known unknowns). The suggested training passes through three stages from known to unknown, thus as a whole creating an intellectual challenge to manage new situations (Ramsden 2003), to assimilate novel thinking for future situations (Shaw et al. 2009), and to, in dialogues, confront the individuals' cognitive model for learning (Dweck 2017). The following three stages outlined in Table 1 combine awareness and training.

Table 1: Overview of Active Elements in the Training Program

| *Risk/Scenario Investigation* | *Probability/Analyses* | *Consequence/Dialogues* |
|---|---|---|
| Something perceived as a vulnerability, which is articulated in the scenario. Known familiar scenarios and recognizable risks, i.e., known known. | The likelihood that risks will happen. Identified risks expressed as first-hand experiences, but unknown if it will happen again, i.e., known unknowns. | The impact of an identified risk. Unknown if, when, where, and how it will happen, situation and context are unidentified since each digital service project is unique, i.e., unknown unknowns. |

*Source: Lugnet and Ericson*

The three-stage process of training integrates declarative knowledge (facts, basics, theory) in the presentation of the subject for training, conceptual knowledge in the analyses and adaptations of scenarios, and procedural knowledge where the participants in dialogues make connections and simulate plausible actions for novel situations (Pintrich 2002).

## Implications and Future Research Directions

This study describes the design of scenarios for the purpose of reflecting on their application in a training program in information security awareness for professional digital service developers. The empirical data was obtained through action research and participatory research methods in cooperation with an IT consultancy firm. The information security challenges found in the study can be described as social and interhuman, often denoted as "soft questions" in technical company contexts. The "softness" typically indicates that the issues have several possible solutions, each depending on the individuals' different perspectives and their different interpretation of situations. Theory suggests that awareness training for learners implies practicing the ability to ask stimulating questions and analyze several alternatives, that is, to train high-order-thinking skills (Biggs 1996; Ramsden 2003; Anderson and Krathwohl 2001). This article presents and reflects the basic contents for such a training format.

The initial tests and analyses of the basic format for the suggested training program showed a number of implications and future research directions. These were mainly consequences related to the online requirement of pursuing self-paced training, and to the learning objectives for personal development. The considerations from this study are, in summary:

- The training can be self-paced in a small team, that is, three persons collaborating in the training program to enable reflective dialogues. The learners can come from the same design project team, thereby also creating a shared vocabulary for the specific challenges in the project, as well as assessing plausible security risks in the work. The interaction with others supports instant feedback, helped also by being able to see face expressions and body language. Using a camera is thus suggested. The non-verbal elements are highly important in the learning situation.
- The learners should be able to participate and engage in the training on an equal level. The online solution is therefore suggested as an independent facilitator for the learning steps. If not, the learners have to keep track of (next) step. Hence, focus will be drawn to the process rather than to the format and contents.
- Professional training must be efficient. It cannot take too much time away from ordinary, and also invoiced, business work. Simultaneously, awareness training cannot be too short to fulfil its purposes; it has to challenge the routine and business-as-usual perspectives, that is, known single-solutions problems. A timer, keeping track of time, is important to avoid a situation where learners end up in long discussions, which is likely to happen since each scenario can be scrutinized from many points of view. Identifying a time limit for a reasonable training program and for each step to create learning is an important suggestion for future research.
- Presenting the scenarios merely as written text (2/3 of a A4) has in our study shown to fail. The learners found the text "too long." Sharfaei and Furnell's (2003–2004) prototype used audio-visual material and multimedia. This study also tested the possibility of combining very short texts with 2-minute movies, and visual storyboards (i.e., 3-square images with speech bubbles, as can be seen in comic strips). Those were found better at communicating the challenge in the scenarios. Furthermore, it was also found that each scenario had to have a prescriptive "tag line" indicating the main information security challenge, as in the three examples above—integrity of people, confidentiality and trust, and ethicality and privacy. The tag line is a condensed description of the challenge and supported the learners in starting the dialogues.
- Theory differentiates between discussion and dialogue, such as showcasing the difference between arguing for a standpoint or investigating an issue to learn more (e.g., Shaw et al. 2009; Dweck 2017). How the learners communicate when analyzing the scenarios is hence important. Also, the training process drives the learners toward the unknown unknown stage (South 2007). High-order thinking skills develop in that stage, but learners have different preferences to manage undetermined or abstract issues. There is, for example, a tendency among some to simplify the challenge into a single-solution situation, turning the conversation into an argumentation of one correct solution (Cox et al. 2014). In the case of online-facilitated and self-paced training, it is thus particularly important to further investigate how to prevent or break single-solution discussions and get the learners on track again. Here, capturing and feeding in the essence from other (previous) groups of learners' results might be one possibility to change behavior, for example, by using gamification techniques or applying behavioral design models as tested by Alshaikh et al. (2019).

There are other aspects that have not been covered in our study but are interesting for professional training. For example, the possibility of developing joint designer and customer training as initialized by Kävrestad and Nohlberg (2020) is one such effort. If so, the issues of

low customer competence in information security can be managed simultaneously. The terminology provided by NIST (Wilson and Hash 2003), especially for the concept of awareness as having the purpose to only draw attention to IT security, feels a bit outdated considering modern pedagogics and the progress in digitalization over the last decade. Despite strictly differentiating between awareness and training in the definitions, Wilson and Hash (2003) prescribe "awareness *and* training" as a combined concept in learning situations. It should be noted though, that a new version of the guideline for the design of information security awareness programs is drafted and planned to be integrated with the 800-16 guideline. This will probably align the terminology with modern pedagogics and will be more in line with the contemporary digitalization era. Furthermore, "a free and robust dialogue" on digitalization and higher education studies is suggested by Brabazon (2017, 89). In particular, her arguments of a shift from learner mobility to content mobility, from just-in-case to just-in-time, and from isolated learners to virtual learning communities are interesting in relation to lifelong learning in practice. Her conclusion that higher education has failed to reach outside the normal target groups (e.g., young students) points toward research and development of courses and programs that are agile and receptive to industry needs. Finally, the execution of training programs may also be considered in respect of formal examinations and accreditation.

## Acknowledgement

Support from Vinnova through PiiA project Undis is gratefully acknowledged. Financing from the CYNIC project (20201650), from the EU program INTERREG North 2014-2020, and Region Norrbotten and Lapin Liitto is also gratefully acknowledged.

## REFERENCES

Abraham, Sherly, and InduShobha Chengalur-Smith. 2019. "Evaluating the Effectiveness of Learner Controlled Information Security Training." *Computers & Security* 87:101586. https://doi.org/10.1016/j.cose.2019.101586.

Ackoff, Russell. 1989. "From Data to Wisdom." *Journal of Applied Systems Analysis* 16 (1): 3–9. http://www-public.imtbs-tsp.eu/~gibson/Teaching/Teaching-ReadingMaterial/Ackoff89.pdf.

Alshaikh, Moneer, Humza Naser, Atif Ahmad, and Sean B. Maynard. 2019. "Toward Sustainable Behaviour Change: An Approach for Cyber Security Education Training and Awareness." Paper presented at the Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm and Uppsala, SE, June 8–14, 2019.

Alshaikh, Moneer, Sean B. Maynard, Atif Ahmad, and Shanton Chang. 2018. "An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations." Paper presented at the Proceedings of the 51st Hawaii International Conference on Systems Sciences. https://doi.org/10.24251/HICSS.2018.635.

Anderson, Lorin W., and David R. Krathwohl. 2001. "Report Writing Vignette." In *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*, edited by Lorin W. Anderson, David R. Krathwohl, Peter W. Airasian, Kathleen A. Cruikshank, Richard E. Mayer, Paul R. Pintrich, James Raths, and Merlin C. Wittrock, 212–218. New York: Longman.

Biggs, John. 1996. "Enhancing Teaching through Constructive Alignment." *Higher Education* 32:347–364. https://doi.org/10.1007/BF00138871.

Brabazon, Tara. 2017. "From Digital Disruption to Educational Excellence: Teaching and Learning in the Knowledge Economy." *International Journal of Social Sciences & Educational Studies* 3 (3): 188–203. https://doi.org/10.23918/ijsses.v3i3p188.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Quarterly* 34 (3): 523–548. https://doi.org/10.2307/25750690.

CDIO (Conceive Design Implement Operate). n.d. "Welcome to CDIO." Accessed March 12, 2021. http://www.cdio.org/.

Checkland, Peter, and Sue Holwell. 1998. "Action Research: Its Nature and Validity." *Systemic Practice and Action Research* 11:9–21. https://doi.org/10.1023/A:1022908820784.

Chen, Charlie C., Robert Shaw, and Samuel C. Yang. 2006. "Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System." *Information Technology, Learning, and Performance Journal* 24 (1): 1. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.5945&rep=rep1&type=pdf.

Cox, Charles, Johan Wenngren, Johan Holmqvist, and Åsa Ericson. 2014. "Tendencies toward Problem-Setting and Problem-Solving: A Study of Operations Derived from Motivation Strategies." *Journal of Technologies in Education* 10 (2): 1–14. https://doi.org/10.18848/2381-9243/CGP/v10i02/56470.

Crossler, Robert E., Allen C. Johnston, Paul B. Lowry, Qing Hu, Merrill Warkentin, and Richard Baskerville. 2013. "Future Directions for Behavioral Information Security Research." *Computers & Security* 32:90–101. https://doi.org/10.1016/j.cose.2012.09.010.

Dweck, Carol. 2017. *Mindset: Changing the Way You Think to Fulfil Your Full Potential*. London: Robinson.

Feisel, Lyle D. 1986. "Teaching Students to Continue Their Education." Paper presented at the Proceedings of the Frontiers in Education Conference, University of Texas, Arlington, October 12–15, 1986.

Furnell, Steven M., Alistair G. Warren, and Paul S. Dowland. 2003. "Improving Security Awareness through Computer-Based Training." In *Security Education and Critical Infrastructures. WISE 2003. IFIP Advances in Information and Communication Technology*, edited by C. Irvine and H. Armstrong, 287–301. New York: Springer.

Furnell, Steven M., M. Gennatou, and Paul Dowland. 2002. "A Prototype Tool for Information Security Awareness and Training." *Logistics Information Management* 15 (5/6): 352–357. https://doi.org/10.1108/09576050210447037.

Gibbs, Graham. 1999. "Using Assessment Strategically to Change the Way Students Learn." In *Assessment Matters in Higher Education: Choosing and Using Diverse Approache*s, edited by S. Brown, and A. Glasner, 41–53. Buckingham: SRHE and Open University Press.

Huckle, Steve, Rituparna Bhattacharaya, Martin White, and Natalia Beloff. 2016. "Internet of Things, Blockchain and Shared Economy Applications." *Procedia Computer Science* 98:461–466. https://doi.org/10.1016/j.procs.2016.09.074.

IBM Global Technology Services. 2014. "Cyber Security Intelligence Index." https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF.

ISO (International Organization for Standardization). 2013. "Information Technology—Security Techniques—Code of Practice for Information Security Controls (Standard No. ISO/IEC 27002:2013)." https://www.iso.org/standard/54533.html.

Jacoby, Ryan, and Diego Rodriguez. 2007. "Innovation, Growth, and Getting to Where You Want to Go." *Design Management Review* 18 (1): 10–15. https://doi.org/10.1111/j.1948-7169.2007.tb00067.x.

Kävrestad, Joakim, and Marcus Nohlberg. 2020. "ContextBased MicroTraining: A Framework for Information Security Training." In *Human Aspects of Information Security and Assurance*, edited by N. Clarke and S. M. Furnell, HAISA 2021. IFIP Advances in Information and Communication Technology, vol. 593. Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-030-57404-8_6.

Kramer, Roderick M. 1999. "Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions." *Annual Review of Psychology* 50:569–598. https://doi.org/10.1146/annurev.psych.50.1.569.

Kruger, Hennie A., and Wayne D. Kearney. 2006. "A Prototype for Assessing Information Security Awareness." *Computers & Security* 25 (4): 289–296. https://doi.org/10.1016/j.cose.2006.02.008.

Lacey, David. 2010. "Understanding and Transforming Organizational Security Culture." *Information Management & Computer Security* 18 (1): 4–13. https://doi.org/10.1108/09685221011035223.

Mason, Jennifer. 2002. *Qualitative Researching.* 2nd ed. London: SAGE.

Mathews, Lee. 2017. "Criminals Hacked a Fish Tank to Steal Data from a Casino." *Forbes,* July 27, 2017. https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/.

Miles, Matthew B., and Michael Huberman. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*. Thousand Oaks, CA: SAGE.

NIST (National Institute of Standards and Technology). n.d. "Glossary." Accessed July 26, 2022. https://csrc.nist.gov/glossary.

O'Brien, Emma, and Ileama Hamburg. 2013. "Organisational Problem Based Learning and Social Communities for SMEs." *European Journal of Open, Distance and e-Learning* 16 (2): 50–60. https://www.learntechlib.org/p/153618/.

Osborn, Emma, and Andrew Simpson. 2018. "Risk and the Small-Scale Cyber Security Decision Making Dialogue—A UK Case Study." *Computer Journal* 61 (4): 472–495. https://doi.org/10.1093/comjnl/bxx093.

Osborne, Charlie. 2021. "Updated Kaseya Ransomware Attack FAQ: What We Know Now." *ZDNet,* July 23, 2021. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/.

Parida, Vinit, David Sjödin, and Wiebke Reim. 2019. "Reviewing Literature on Digitalization, Business Model Innovation, and Sustainable Industry: Past Achievements and Future Promises." *Sustainability* 11 (2): 391. https://doi.org/10.3390/su11020391.

Paulsen, Celina, and Robert Byers. 2019. "Glossary of Key Information Security Terms." NIST Interagency/Internal Report (NISTIR) 7298, Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7298r3.

Pintrich, Paul. 2002. "The Role of Metacognitive Knowledge in Learning, Teaching, and Assessing." *Theory into Practice* 41 (4): 219–225. https://doi.org/10.1207/s15430421tip4104_3.

Puhakainen, Petri, and Mikko Siponen. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study." *MIS Quarterly* 34 (4): 757–778. https://doi.org/10.2307/25750704.

PwC. 2019. "The Journey to Digital Trust." https://www.pwc.com/sg/en/publications/assets/the-journey-to-digital-trust-2019.pdf.

Ramsden, Paul. 2003. *Learning to Teach in Higher Education*. 2nd ed. London: Routledge.

Rowley, Jennifer. 2007. "The Wisdom Hierarchy: Representations of the DIKW Hierarchy." *Journal of Information Science* 33 (2): 163–180. https://doi.org/10.1177/0165551506070706.

Saban, Kenneth, Stephen Rau, and Charles Wood. 2021. "SME Executives' Perceptions and the Information Security Preparedness Model." *Information and Computer Security* 29 (2): 263–282. https://doi.org/10.1108/ICS-01-2020-0014.

Samonas, Spyridon, and David Coss. 2014. "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security." *Journal of Information System Security* 10 (3): 21–45. https://www.proso.com/dl/Samonas.pdf.

Sharfaei, S., and Steven M. Furnell. 2003–2004. "Isedut: An Educational Tool for Information Security." In *Advances in Network and Communications Engineering 2*, edited by S. M. Furnell and P. S. Dowland, 49–56. Plymouth, EN: University of Plymouth.

Shaw, Ruey S., Charlie C. Chen, Albert L. Harris, and Hui-Jou Huang. 2009. "The Impact of Information Richness on Information Security Awareness Training Effectiveness." *Computers & Education* 52 (1): 92–100. https://doi.org/10.1016/j.compedu.2008.06.011.

Silverman, David. 2000. "Analyzing Talk and Text." In *Handbook of Qualitative Research*, edited by N. Denzin and Y. Lincoln, 821–834. Thousand Oaks, CA: SAGE.

Smart Services Welt. 2015. "Smart Service Welt—Recommendations for the Strategic Initiative Web-Based Services for Businesses, Final Report." https://en.acatech.de/publication/recommendations-for-the-strategic-initiative-web-based-services-for-businesses-final-report-of-the-smart-service-working-group/download-pdf?lang=en.

South, Beverly. 2007. "Combining Mandala and the Johari Window: An Exercise in Self-Awareness." *Teaching and Learning in Nursing* 2 (1): 8–11. https://doi.org/10.1016/j.teln.2006.10.001.

Symantec. 2019. "Internet Security Threat Report." https://docs.broadcom.com/doc/istr-24-2019-en.

Vargo, Steven L., and Robert F. Lush. 2004. "Evolving to a New Dominant Logic for Marketing." *Journal of Marketing* 68 (1): 1–17. https://doi.org/10.1509/jmkg.68.1.1.24036.

Verizon. 2019. "2019 Data Breach Investigations Report." https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

von Solms, Basie, and Rossouw von Solms. 2018. "Cybersecurity and Information Security—What Goes Where?" *Information and Computer Security* 28 (1): 2–9. https://doi.org/10.1108/ICS-04-2017-0025.

WestArete. 2019. "An Introduction to Maintenance Costs for Custom Software." *West Arête,* July 20, 2019. https://westarete.com/insights/maintenance-costs-for-custom-software/.

Wilson, Mark, and Joan Hash. 2003. "Building an Information Technology Security Awareness and Training Program." Washington, DC: Government Printing Office.https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf.

Yan, Zheng, and Silke Holtmanns. 2008. "Trust Modeling and Management: From Social Trust to Digital Trust." In *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions,* edited by R. Subramanian, 290–323. Hershey, PA: IGI Global.

## ABOUT THE AUTHORS

***Dr. Johan Lugnet:*** Senior Lecturer, Division of Digital Services and Systems, Luleå University of Technology, Luleå, Sweden

***Prof. Dr. Åsa Ericson:*** Professor, Division of Digital Services and Systems, Luleå University of Technology, Luleå, Sweden

***The International Journal of Technology, Knowledge, and Society*** explores innovative theories and practices relating technology to society. The journal is cross-disciplinary in its scope, offering a meeting point for technologists with a concern for the social and social scientists with a concern for the technological. The focus is primarily, but not exclusively, on information and communications technologies.

Equally interested in the mechanics of social technologies and the social impact of technologies, the journal is guided by the ideals of an open society, where technology is used to address human needs and serve community interests. These concerns are grounded in the values of creativity, innovation, access, equity, and personal and community autonomy. In this space, commercial and community interests at times complement each other; at other times they appear to be at odds. The journal examines the nature of new technologies, their connection with communities, their use as tools for learning, and their place in a "knowledge society."

The perspectives presented in the journal range from big picture analyses which address global and universal concerns, to detailed case studies which speak of localized social applications of technology.

The papers traverse a broad terrain, sometimes technically and other times socially oriented, sometimes theoretical and other times practical in their perspective, and sometimes reflecting dispassionate analysis whilst at other times suggesting interested strategies for action.

The journal covers the fields of informatics, computer science, history and philosophy of science, sociology of knowledge, sociology of technology, education, management and the humanities. Its contributors include research students, technology developers and trainers, and industry consultants.

*The International Journal of Technology, Knowledge, and Society* is a peer-reviewed, scholarly journal.



ISSN 1832-3669