A Competence-Based Screening of Instructional Designs in Trainings for IT-Security at the Workplace

Patricia Köpfer[1] Julia Warwas[1] Florian Schütz[2] Florian Rampold[2] Kristin Masuch[2] Simon Trang[3]

[1]University of Hohenheim, Germany; [2]University of Göttingen, Germany; [3]University of Paderborn, Germany

Correspondence: Patricia Köpfer, Email: patricia.koepfer@uni-hohenheim.de

Abstract

Building competences for employee behavior enhancing Information Technology Security (ITS) is crucial. While cybersecurity attacks are rising in numbers and sophistication, deficient knowledge and behaviors of employees present greater weaknesses in companies than insufficient hardware/software components such as firewalls. However, ITS trainings are time-consuming and often only temporarily effective. We address these shortcomings and model the required competences for ITS behavior in everyday work, identify their qualification needs, and recommend needs-based training programs. In this paper, we examine to which extent available ITS trainings cover the dimensions of our competence model. We pursue the question on which specific dimensions of ITS competence are addressed/omitted. Results show that especially the implication of the important dimension of justification needs to be improved.

Keywords: information technology security, competence, structured literature review, training, qualitative content analysis, small and medium-sized enterprises

1. Introduction

Cybersecurity attacks in small and medium-sized enterprises (SME) are rising in numbers (Bitkom 2018) and sophistication (Ahmad et al. 2020). Greatest weakness aren't insufficient hardware/software components such as firewalls, but deficient knowledge and behaviors of employees in these companies (Herath & Rao 2009). Building competences for employee behavior that enhance Information Technology Security (ITS) is crucial, particularly in SMEs that lack specialized IT departments. However, ITS trainings are time-consuming, cognitively demanding and often only temporarily effective (D'Arcy & Lowry 2018; Hu et al. 2021). Furthermore, previous studies on the target groups' readiness and abilities to adopt ITS-related behavior mainly examine their (self-reported) intention to comply with ITS policies. Our interdisciplinary project addresses these shortcomings. We model the required competences of employees for ITS behavior in everyday work conceptually, identify their qualification needs, and recommend needs-based training programs.

Based on the cognitivist view of competence and following Chomsky (1965), we distinguish between competence (cognitive structures and rules required to produce a particular ability) and performance (practical application of that ability). Following a general definition of competence by Weinert (2001), we define ITS competence as "the (measurable) cognitive abilities and skills that are present (or can be learned) in individuals to act in an IT-secure manner in everyday work, as well as the associated motivational and social dispositions and skills to successfully and responsibly avert or manage a threat in variable situations."

For the development of a model for ITS competence, general and vocational competence modeling as well as action regulation theory (e.g., Dörner et al. 1989) must be considered and theoretical and empirical findings from the IT security literature must be stringently integrated.

Regarding the (intraindividual) determinants of ITS behavior, there are various explanatory approaches such as Social Cognitive Theory (Bandura 1977) or Social Bond Theory (Ifinedo 2014). However, as mentioned earlier, most ITS studies primarily examine employees' *intention* to behave in a rule-compliant manner. Another variable – both target and influence – in the ITS literature is usually employee's *awareness* of ITS threats. However, the investigation of actual *competence* has yet to be conducted.

According to the above definition, a situation in which an ITS threat occurs can be viewed as a problem that needs to be managed. Consequently, the person facing the problem must go through an action that includes, for instance, the following phases (Betsch, Funke & Plessner 2011): Analysis and evaluation of the initial situation, definition and prioritization of action goals, generation of several possible action plans, evaluation of the plans, decision and execution, action control.

In developing our model, we therefore focused on the problem-solving process within the domain "IT-secure behavior". Occupation-specific threat scenarios, defined and precisely identified as "threat vectors", are considered as action-relevant reference variables for competence modeling. With a focus on concrete action, seven competence dimensions were developed (see Figure 1; definitions of the individual dimensions can be found in Table 1).

2. Objectives and Research Questions

The aim of this paper is to examine published recommendations for ITS training contents as well as actual existing ITS trainings with reference to the competence model underlying our research project. We thus pursue the question on which specific dimensions of ITS competence at the workplace are addressed (or omitted) in the ITS training literature and in ITS trainings. This allows us to map the level of awareness of ITS competence in research as well as the status quo of actual implementation of ITS competence in training.

3. Methods

3.1 Structured Literature Review of Literature on ITS Trainings

In order to get a broad overview of recommendations on effective ITS design and conceptualization, a structured literature review is conducted that follows the approach of Webster and Watson (2002) and vom Brocke et al. (2015). The objective of this approach is to identify current state-of-the-art research in the information security awareness domain. The exact procedure is described in Rampold et al. (2022). In summary, it should be mentioned that several prominent databases in IS research and economics have been selected. Inclusion criteria were as follows:

- Search Terms “security education” OR “security awareness” OR “security training” OR “security education training awareness” OR “security program” OR “security competence”
- Publication date between 1998 and 2021
- Search Terms are part of the publication’s abstract, keywords or title
- Publication type peer-reviewed journal or conference
- Language is English

This structured review provided a number of 57 relevant articles for further analysis.

3.2 Selection of ITS Trainings

The selection of information and cyber security training offers in this paper follows the same approach as used for the selection of the literature in section 3.2, and as there, the search is exclusively online. The search for the training offers was conducted using the Google search engine, which is considered the most popular and leading search engine with a market share of over 90% worldwide. To improve the effectiveness of the search, Google’s Advance Search Tool was used, which provides additional parameters to customize the search and narrow down the results. The general search constrains for information and cyber security training offers for this study were: publicly available trainings, free, but also fee-based trainings, training language German or English, available for participants located in Germany,

wide variety of training methods and content. The following keywords were used for the search: "cybersecurity training". The search with the English keyword combination yielded several thousand results, the German keyword combination several hundred results. In order to select a manageable number of representative cybersecurity training providers from this huge number of hits, market overviews such as those from TechRadar and NIST were consulted. The final selection includes 343 information and cyber security training offers. Of these 343, 71 were included in the analysis in this paper that are not offered in e-learning format.

3.3 Data Analysis

Both ITS literature and ITS trainings were analyzed for references to the competence dimensions using Qualitative Content Analysis (Schreier 2012). Computer assisted categorization was performed with the software MAXQDA 2022. All 57 papers were fully coded, and for the 71 trainings, the descriptions of the trainings available on the respective websites were coded. The category building followed a deductive approach and the main categories were formed according to the theoretically established competency dimensions. Both data sources were coded by three raters each, and 15% each of the data were triple coded during the coder training. In the final step, interrater reliability was a Cohen's kappa of $.81 < \kappa < .98$.

4. Results

As first results of the qualitative content analysis, the frequencies of occurrence of the competence dimensions are presented. A category (dimension) was counted as soon as it occurs at least once in a document (research paper or training). Regardless of how often it was coded in a document. An overview of the frequencies, each with an example from the data, can be found in Table 2.

4.1 Results from ITS Literature

The most frequently occurring category is Threat Awareness, with 29 mentions. Tactic Justification, in contrast, was coded only 2 times. An interesting aspect is the combination of dimensions in the papers. Threat Awareness alone occurs most frequently (14 times). In two research papers, all dimensions except Tactic Justification are combined, and once all dimensions except Threat Awareness were coded. In six papers, no reference to the competence dimensions could be found at all.

4.2 Results from ITS Trainings

The results are quite similar for the existing training offers. Threat Awareness occurred 55 times, followed closely by Tactic Choice (37 times) and Threat Impact Assessment (27 times) and Threat Identification (26 times). In contrast, Tactic Control and Tactic Mastery occurred only six times and twice, respectively. No reference to Tactic Justification could be found. Within two trainings the largest combination of different competence dimensions occurs: once Threat Awareness & Threat Identification & Threat Impact Assessment & Tactic Choice and once additionally Tactic Control.

5. Implications

As described above, awareness is frequently treated in the ITS literature as an influencing variable and also as a target variable of IT-secure behavior, so it is not surprising that the Threat Awareness dimension is the most common category. Awareness is also the primary focus of most training courses. The same is true for the need to recognize threats (Threat Identification). Both the literature and the trainings address the choice of actions, which we capture as Tactic Choice. It is important to recognize that the importance of threat justification, i.e., an employee's valid reasons for the chosen action, appears to be too poorly understood. Only when a strategy or action is chosen with justification can it be assumed that the action was professional, planned, and purposeful. The same is true for Tactic Mastery and Tactic Control. These should be important elements in future trainings so that direct practice

is given on how to perform actions and the employee's responsibility is not complete until the action performed is controlled. Interestingly, Tactic Control is only found in trainings when the training was geared towards the board level or for security chiefs and coordinators.

This study has some limitations. First and foremost, only a selection of trainings was coded. The selection is limited to one format, and by the time of the conference, the other training offers will have been evaluated. In addition, the analysis of the trainings is initially based on the descriptions of the trainings by the providers. To what extent the same results regarding the competence dimensions are reflected in the actual implementation of the trainings remains to be investigated. A major challenge, for instance, is the distinction between Tactic Choice and Mastery, i.e., whether strategies or measures are only discussed or also implemented. Thus, a next step is to participate in free-access trainings and re-run the analysis based on these insights.

Further research could also address the media-didactic analysis of the e-learning formats as well as the motivational dimensions that should be included in the competence model.

Acknowledgements
This work was supported by the German Federal Ministry for Economics and Climate Action (Grant number 01MS20008B).

Figure 1 Model of ITS competence

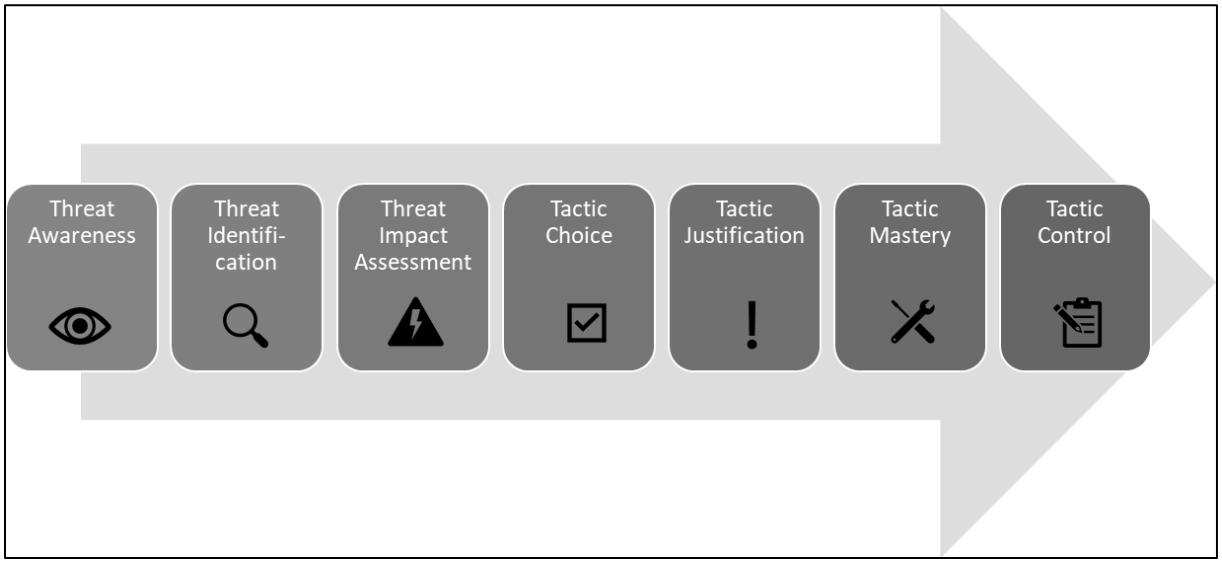

Table 1 Dimensions of the Competence Model

Competence Dimension	Definition
Threat Awareness	The employee is informed about possible threats and therefore alerted for threats; is able to decide a threatening situation from a non-threatening situation
Threat Identification	The employee accurately identifies that a security threat exists and what it consists of.
Threat Impact Assessment	The employee accurately recognizes what the consequences will be if the threat is not addressed.
Tactic Choice	From a variety of more or less suitable action options (measures) to avert threats, the employee selects the option for action (measure) that (a) is in accordance with generally safety guidelines and (b) is the most appropriate in the respective threat situation.
Tactic Justification	The employee proceeds in a planned, professional, and goal-oriented manner; can thus provide a valid justification for the chosen security strategy in terms of its relevance, effectiveness and/or superiority over other strategies.
Tactic Mastery	The employee is able to implement the chosen strategy.
Tactic Control	The employee evaluates the effectiveness of the implemented measure and, if necessary and possible, carries out appropriate follow-up actions.

Table 2 Frequencies of the Dimensions of the Competence Model

Competence Dimension	Frequency in ITS Literature (n=57)	Example from ITS Literature	Frequency in ITS Trainings (n=71)	Example from ITS Trainings
Threat Awareness	29	"Information security awareness is the most important factor in mitigating phishing." (1, pos. 83)	55	„Security awareness campaigns are designed to foster a longterm and sustainably security-conscious interaction with IT systems, enabling staff members to act in conformity with the envisaged protection level. Such a campaign can enhance security awareness." (66, pos. 5).
Threat Identification	14	"Network users should be trained how to identify email message threats before clicking on links or attachments […]" (32, pos. 423)	26	"With our IT security training for employees, you and your employees will learn to recognize the most important types of attacks" (1, pos. 5).
Threat Impact Assessment	7	"One component: Information about social and environmental consequences." (4, pos. 55)	27	"This Cyber Security online training course will help you to understand the potential impact of common cyber threats." (5, pos. 29)
Tactic Choice	10	"It is expected to choose the best strategy for solving the problem." (29, pos. 55)	37	"Measures to avert cyberattacks are discussed and reenacted" (11, pos. 4).
Tactic Justification	2	"Each defence player in turn describes how the selected defence would be effective in deterring or preventing the attack." (18, pos. 121)	---	---
Tactic Mastery	7	"Having the skills to perform the target behavior" (4, pos. 49)	2	"Addressing clear issues results in participants taking away specific recommendations for action from the training that they can implement immediately." (25, pos. 8)
Tactic Control	6	"Evaluation has been highlighted as a key element in the design and implementation of effective information security awareness programs." (3, Pos. 432)	6	"You can evaluate your awareness efforts." (2, pos.7)

References

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H. & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology 71 (8*), 939–953.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, *84*(2).

Betsch, T., Funke, J., & Plessner, H. (2011). *Denken–Urteilen, Entscheiden, Problemlösen*. Berlin, Heidelberg: Springer Berlin Heidelberg.

bitkom e.V. (2018). *Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie, Studienbericht 2018,* https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf

Chomsky, N. (1965). *Aspects of the Theory of Syntax*. Cambridge, MA: MIT Press.

D'Arcy, J. & Lowry, P.B. (2018). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal, 1–27*.

Dörner, D., Schaub, H., Stäudel, T., & Strohschneider, S. (1989). Ein System zur Handlungsregulation oder die Interaktion von Emotion, Kognition und Motivation. In E. Roth (Ed.), *Denken und Fühlen* (pp. 113-133). Springer, Berlin, Heidelberg.

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

Hu, S., Hsu, C. & Zhou, Z. (2021). Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems 00 (00)*, 1–13.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Rampold, F., Schütz, F., Masuch, K., Köpfer, P., & Warwas, J. (2022). Are You Aware of Your Competencies? – The Potentials of Competence Research to Design Effective SETA Programs. *ECIS 2022 Research Papers. 134*. https://aisel.aisnet.org/ecis2022_rp/134

Schreier, M. (2012). *Qualitative Content Analysis in Practice*. London: SAGE Publication Ltd.

vom Brocke, J. V., A. Simons, K. Riemer, B. Niehaves, R. Plattfault and A. Cleven. (2015). "Standing on the shoulders of giants: Challenges and recommendations of literature search in Information Systems research." *Communications of the Association for Information Systems 37* (9), 205–224.

Webster, J. and R. T. Watson. (2002). "Analyzing the Past to Prepare for the Future: Writing a Literature Review." *MIS Quarterly 26* (2), xiii–xxiii.

Weinert, F. E. (2001). Concept of competence: a conceptual clarification. In D. S. Rychen & L. H. Salganik (Eds.), *Defining and selecting key competencies.* Seattle: Hogrefe & Huber.