Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2021 Research-in-Progress Papers | ECIS 2021 Proceedings

6-14-2021

Towards Designing A Method To Create Sticky Information Security Training For SMEs: Identifying Design Factors

Martin Brehmer
Faculty of Business and Economics, martin.brehmer@wiwi.uni-augsburg.de

Antragama Ewa Abbas
Delft University of Technology, a.e.abbas@tudelft.nl

Nageswaran Vaidyanathan
Copenhagen Business School, naggoma@gmail.com

Follow this and additional works at: https://aisel.aisnet.org/ecis2021_rip

Recommended Citation

Brehmer, Martin; Abbas, Antragama Ewa; and Vaidyanathan, Nageswaran, "Towards Designing A Method To Create Sticky Information Security Training For SMEs: Identifying Design Factors" (2021). *ECIS 2021 Research-in-Progress Papers*. 28.
https://aisel.aisnet.org/ecis2021_rip/28

This material is brought to you by the ECIS 2021 Proceedings at AIS Electronic Library (AISeL). It has been accepted for inclusion in ECIS 2021 Research-in-Progress Papers by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

TOWARDS DESIGNING A METHOD TO CREATE STICKY INFORMATION SECURITY TRAINING FOR SMES: IDENTIFYING DESIGN FACTORS

Research in Progress

Brehmer, Martin, University of Augsburg, Germany, martin.brehmer@wiwi.uni-augsburg.de

Abbas, Antragama Ewa, Delft University of Technology, Delft, The Netherlands

Vaidyanathan, Nageswaran, Digitalization, Copenhagen Business School, Frederiksberg, Denmark

Abstract

The risk of being impacted by a cyberattack is high, because of more professional attacks. Thereby, cyber criminals are bypassing technological countermeasures through tricking users. Recently collected data during the SARS-CoV-2 pandemic demonstrate, that cyberattacks including social engineering are among the main threats, especially for Small and Medium-sized Enterprises (SME). (Information) Security Education and Training Awareness (SETA) is proposed to be an effective countermeasure. However, the effects of SETA fade rapidly over time and learnings are not applied in practice sustainably. Thus, we state that a method is required to create SETA programs with sustainable learning outcomes for SME. To develop such a method, we follow the Design Science Research Methodology and share insights of our first design cycle in this article. We conducted a literature review and analyzed factors of failure and success regarding the design of sustainable SETA programs. Furthermore, we sketch our plans for design cycle 2.

Keywords: information security; training; education; awareness; SETA; DSR; SME

1 Introduction

Although the total costs of data breaches are much higher in larger organizations, SMEs have much higher costs relative to their size, e.g., in 2019 large companies reported an average cost of US$ 204 per employee compared to US$ 3,533 in medium-sized organizations (Ponemon Institute, 2019). So, cyberattacks are more business critical for SMEs than they are for larger companies, because SMEs struggle to recover due to the high costs per employee (Ponemon Institute, 2020). This, in extreme cases, can even lead to company shut down (Cimpanu, 2020). Regarding the anatomy of cyberattacks in general, harmful attacks predominantly require human intervention through unaware users. For example, 84% of cyberattacks rely on social engineering, such as phishing emails, and in 71% malware, such as ransomware, was spread from one employee to another. Further, phishing, but also malware attacks are often combined, worth mentioning that in 99% of emails distributing malware, infections required user intervention, such as clicking on a phishing link. Humans are in focus within cyberattacks as user authentication data are among the top 5 targets of criminals to commit financial fraud or to carry out follow-up attacks, e.g., in order to attack supply chains by abusing "trusted" but compromised SME accounts as multiplicators for phishing attacks. (Lourenço and Marinos, 2020)

Moreover, due to the coronavirus pandemic, many SMEs have shifted their work to remote working, and many reported to shift to remote working permanently (Baker, 2020; Lavelle, 2020). Nevertheless, employees often use a less secure personal IT infrastructure to access and process corporate information. Additionally, online interactions such as the use of cloud services or participating in online meetings have become a new normal. (Buil-Gil et al., 2020; Lallie et al., 2020; Mandal and Khan, 2020; Whitmore and Parham, 2020) Thus, remote work has significantly increased the attack surface for SMEs and their connected business partners. Moreover, SMEs have higher significant risks because their information security policy is disconnected from everyday work practice (Sadok et al., 2020) or rely on an informal environment, which may trigger many security risks (Milosz et al., 2018; Gundu and Flowerday, 2013). Besides, criminals are getting better and are adapting their methods to specific contexts, e.g., phishing campaigns related to the coronavirus pandemic increased by 667% in one month (Lourenço and Marinos, 2020). An Australian governmental report confirms that SMEs are generally unprepared, as half of them spend less than A$ 500 per year for all cybersecurity measures. SMEs also often lack the expertise to implement them. Thus, 52% of SMEs adopt a "do-it-yourself" approach, although only 1 of 5 SMEs know the term phishing. (ACSC, 2020)

In summary, we state a necessity to create cybersecurity awareness programs to empower SME employees and managers to counter cyberattacks, particularly social-engineering-based attacks such as phishing. Security Education Training and Awareness (SETA) programs are significant ways to reduce incidents (Puhakainen and Siponen, 2010). SETA should foster knowledge about potential threats and good practices on avoiding cybersecurity incidents and also change information security-related behaviors towards more compliance and lower risks (Hina and Dominic, 2017; Gardner and Thomas, 2014; Wilson and Hash, 2003). For this article, we use the term 'sticky' SETA programs as a construct, referring to learning outcomes that remain in participants' memory sustainably and change their behavior permanently.

However, although there are many providers for SETA programs, a high number of incidents still occur because SETA is often "not carried out at all or delivered in an insufficient or inadequate manner". (Verizon, 2020) For example, SME managers often do not recognize the relevance and importance of SETA and tend to ignore the risks of uninformed employees (Gundu and Flowerday, 2013). Furthermore, although informal and instructional content is often freely available, SME managers have limited knowledge on how to conduct such SETA programs (Gierow et al., 2020). From a financial perspective, SMEs often do not have strong financial support to purchase or conduct formal training. In addition, SMEs lack human resources to develop in-house training because specialists, e.g., information security experts, are missing (Ayat et al., 2011). Despite the limitations, there is renewed interest in developing SETA programs in SMEs and improving training materials (Ozaki, 2020; Lugnet et al., 2020). However, there has been little discussion about applicable methods

to create feasible and effective SETA programs for participants of SMEs (Ozaki, 2020). This indicates that existing solutions are generally non-explicit, do not always reach real-world practices and needs, or are based on specific case studies (Bada and Nurse, 2019). Other studies on meta-design factors for SETA programs, such as those conducted by Karjalainen and Siponen (2011) or Alshaikh et al. (2019), seem too abstract to be applied in practice by an SME manager.

Consequently, we argue that there is a need for a formalized method for SMEs to develop a comprehensive, straightforward, simple, and effective SETA. It should consider design factors as well as theoretical knowledge and address the challenges we have outlined above, to counter cyberattacks that focus on exploiting insecure or unaware human behavior, such as phishing attacks. Knowing these critical design factors related to 1) *what fosters sticky learning outcomes and* 2) *what leads to SETA programs' failure* is a mandatory basis for deriving a suitable method relevant for practice. Thus, it is an important basis for our further research. Therefore, in this *research in progress* article, we identify design factors contributing to SETA programs' success or failure based on a literature review. Overall, to reach our final goal, we will use the Design Science Research (DSR) approach, which is discussed in more detail in section 2. In section 3, we discuss the design factors that contribute to the success or failure of SETA programs. Then, in section 4, we outline the next steps of our research towards a method to create sticky SETA. Finally, in section 5, we outline limitations and further research.

2 Research approach

This study uses a Design Science Research (DSR) approach to attain our final objective, e.g., a method to create sticky SETA programs for SMEs. The DSR strives to create cutting-edge Information System artifacts within multiple iterations to address real-world problems (Hevner, 2007; Hevner et al., 2004). It should also focus on creating and contributing to existing knowledge within one or more design cycles (Hevner and Chatterjee, 2010). The DSR is appropriate because it reconciles real-world issues with theoretical knowledge to create relevant artifacts, i.e., our prospective method to create sticky SETA for SMEs or valuable design knowledge like quality factors to set up sticky SETA programs. To guide our DSR approach, we employ a well-adopted Design Science Research Methodology (DSRM) proposed by Peffers et al. (2007) and Peffers et al. (2018). Therefore, we define our starting point (Baskerville et al., 2018) and answer three research questions (RQ) as part of our first cycle:

1. **Identify problem & motivation** - *RQ 1: Why do SME managers need a method to develop sticky SETA programs?*

   We answer this first RQ in section 1 and section 3 by outlining problems, related works, as well as the focus of our research and our motivation to conduct this study.

2. **Define objectives of a solution -** *RQ 2: What are design factors that contribute to the success and failure of SETA programs?*

   We conducted a literature review to identify design factors that lead to the success and failure of SETA programs in section 3.

3. **Design & development -** *RQ 3: What are the next steps towards developing a method to create sticky SETA programs?*

   We sketch our ongoing iterative research and next steps for our second design cycle in section 4.

3 Factors of failure and success for creating SETA programs

3.1 Literature Review: theoretical knowledgebase

As previously stated, SETA programs are more necessary than ever for SMEs, but the existing solutions are insufficient. SME managers need to know which design factors lead to success or failure in learning outcomes before determining specific activities to design a SETA program. Hence, outlining these quality factors is a necessary first step towards a formalized method that organizes such design activities to support managers creating sticky SETA programs with practical value.

In order to systematically derive these factors and build on existing knowledge we follow the recommendations of design science research. SETA related literature provides several articles about descriptive theories such as the Protection Motivation Theory (Rogers, 1975, e.g., cited by Hina and Dominic, 2017; Wang et al., 2018) or the Theory of Planned Behavior (Ajzen, 1985, e.g., cited by Wang et al., 2018), explaining single aspects of information security-related behavior, but lack an overview of pragmatic findings for sticky SETA. Thus, we conduct a rigorously documented systematic literature review to provide a theoretical but relevant contribution to a real-world problem space following the guidelines of vom Brocke et al. (2009) and vom Brocke et al. (2015). Therefore, we propose that our results are a key contribution towards a method to create sticky SETA programs for SMEs. To ensure a shared understanding of our research topic, we first briefly outline the research area, the specific objective of this literature review, and our methodological setup.

SETA and technological countermeasures, e.g., anti-virus or intrusion detection systems, are recommended to reduce the risk of security incidents (Marinos and Lourenço, 2019). However, technological mechanisms can be more easily bypassed by computer users behavior either intentionally or unintentionally, e.g., by clicking on a malicious (phishing) link within an email, which leads to the installation of further software such as backdoors or stolen user credentials (Willison and Lowry, 2018). In fact, most cybersecurity incidents involved a tricked user as a necessary attack element to be harmful (Marinos and Lourenço, 2019). We, therefore, declare that SETA programs are at least as important as technological solutions to mitigate security incidents.

Furthermore, official government institutions try to foster SETA programs and a common awareness knowledge. Consequently, information on training content is now available through several internet sources, including content from e.g., NIST, ENISA or EUROPOL. However, the problem remains that the training effects fade over time, as SMEs usually do not know how to use this information and to conduct such persuasive SETA programs. (Marinos and Lourenço, 2019; Ozaki, 2020) In order to avoid misconception of SETA or the repetition of already known factors for failure, it is necessary to know why SETA have failed so far. To the best of our knowledge, yet, there are no systematic reviews focusing on the factors of failure and the success altogether in relation to the implementation and design of SETA in SMEs. Instead there are some articles focusing on specific use cases like Bada and Nurse (2019) and single aspects, e.g., persuasion techniques (Bada et al., 2015). Thus, we conduct the following systematic literature review to cover a broad area of design knowledge, while creating a first systematically derived knowledge base for further research, including both sides of quality aspects, analyzed from 27 articles in total. First, we analyze a literature sample why SETA programs have failed so far. Then we analyze and derive possible design relevant success factors. This is followed by a discussion, highlighting meta-requirements of sticky SETA programs design activities. To find the relevant articles, we used the following search term in the most prominent information technology database IEEE Xplore:

(("Document Title":information security OR "Document Title":IT-Security OR "Document Title":cybersecurity OR "Document Title":"cyber security" OR ("Document Title":training AND "Document Title":awareness)) AND (("Abstract":training OR "Abstract":design OR "Abstract":edu) AND ("Abstract":recommendation* OR "Abstract":guideline* OR "Abstract":effect* OR "Abstract":challeng*)) AND ("Abstract":phishing OR "Abstract":human OR "Abstract":awareness OR "Abstract":"social engineering"))*

The search string is derived from RQ 2 (see section 2). It was constructed by considering the keywords to cover key aspects that could offer insights about quality aspects for SETA programs, such as "design", "recommendations", and "guidelines". We did not find a significant number of articles focusing on the success or failure of SETA programs, especially in the context of SMEs. Thus, we decided consciously not to be restrictive regarding narrowing the results with more keywords or by restricting the time period of publication date but by filtering the articles by personal selection, and interpreting our results regarding SME characteristics at the end of section 3. Our criteria for this selection process will be outlined below. We found 90 articles, of which we filtered out 63 articles by the criteria of being a) not related to SETA particularly or b) focusing only on operational information security management in general, c) representing reports of training without outlining factors for

success or failure, as well as d) representing articles which focus on technological aspects within the title, abstract or if still unclear, full text. Instances for excluded articles focus on (situational) "awareness" sensors of cars or algorithms for phishing detection.

To analyze the articles, we defined criteria when to include a failure or success factor to our list. These criteria are as follows: First, the authors of these papers must emphasize factors that influence the success or failure of SETA programs and cover these statements either through empirical studies or logical deduction. Second, to rigorously outline and separate fail and success factors, we analyze the literature sample twice. This is necessary, because it is not appropriate to conclude from the nonexistence of a fail factor to be a success factor and vice versa. So, a previous synthesis of these both categories of factors would not fulfil the criteria of rigorously analysis. Consequently, towards creating a method for sticky SETA we conclude that it is necessary to first know and erase factors of failure, and second to foster successful SETA through implementing the success factors. Third, regarding a rigorous extraction of these factors we did not consider statements which implicated obvious uncertainty regarding these factors, e.g., if authors state that the results are not sufficient enough to draw clear conclusions. Thus, to present our review results, we use a condensed concept-centric listing, instead of a concept matrix as this would be too complex for this format. The main concepts are represented as highlighted terms, associated aspects, e.g., root causes and implications are underlined. Table 1 provides an overview of the factors which lead to SETA program failure.

Influencing design factors why SETA programs fail in the long term
1. SETA are seldomly people-centered and do **not focus on the personal interests or learning types** of employees but rather focus on imparting too broad theoretical knowledge, leading to disinterest and cognitive overload. (Ghazvini and Shukur, 2017; Al Sabbagh et al., 2012; Nagarajan et al., 2012; Caulkins et al., 2016)
2. User **motivation** to engage with the training content **is usually low** (if not explicitly addressed) as it is perceived as temporary necessary burden (Abawajy et al.; 2008), without relevance to working tasks (Nagarajan et al., 2012; Caulkins et al., 2016; Willems et al., 2011), without modern ways of delivery (Aldawood and Skinner, 2019; Bowen et al., 2011), taught by unexperienced persons without instructional design knowledge, which leads to low concentration during a training (Aldawood and Skinner, 2019; Ghazvini and Shukur, 2017).
3. Learning content **is not designed to fit the demands of the target group and job roles** regarding personality attributes, consideration, and extension of **prior as well as mandatory knowledge**. (Ghazvini and Shukur, 2017; Neupane et al., 2016)
4. Learning content and training contain too many details, which hinders learning. It is not part of daily business tasks for many participants, so they **struggle to distinguish and comprehend relevant content from additional content**, leading to feelings of overwhelming, amotivation and mental dropout. Thus, the content is not internalized if delivered with high complexity. (Alshomrani and Mehdim, 2012; Nurse et al., 2011)
5. Usability regarding easily accessible information **is a neglected aspect**, so getting access to learning content itself and relevant information within complex structured ways of content provisioning is a complex task or not available on demand. (Neupane et al., 2016; Nurse et al., 2011)
6. Training **scenarios are too abstracted** from their daily tasks, so users cannot detect and map their insecure behavior to the learning content and thus are not able **to tackle their false beliefs or malicious behavior**. (Innab et al., 2018; Waly et al., 2012; Alahmari and Duncan, 2020).
7. Training **without ad hoc feedback in addition to repetitive training** lead to undetected and thus not addressed false beliefs or existing knowledge gaps. (Ghazvini and Shukur, 2017; Waly et al., 2012; Caputo et al., 2013; Nagarajan et al., 2012; Wang et al., 2018)
8. Training conducted only once or twice is not taken as an integral part of the daily work environment and, therefore, is not subject of discussion and daily communication, **fostering common understanding and informal exchange between colleagues**. (Al Sabbagh et al., 2012; Alnatheer, 2015)
9. SETA programs are perceived as **expensive security mechanisms** regarding internal costs or buy-in decisions with uncertain learning outcomes. Thus, the SETA budget is usually low, or SETA is not considered within SMEs due to limited financial resources. (Aldawood and Skinner, 2019; Innab et al., 2018)

Table 1. Results of the literature review (part I: failure factors for designing SETA).

After analyzing the literature again to identify the success factors, we found 8 factors for SETA programs and outline them in Table 2. We assume that some design factors are applicable to other training domains or larger enterprises as well. However, these design factors are crucial to change the mindset of users and to foster basic engagement with SETA, for now, focused on SME.

Influencing design factors that foster successful SETA programs
1. Different modern **ways of delivery**, **knowledge bases**, **learning types,** and preferences. (Aldawood and Skinner, 2018; Holdsworth and Apeh, 2017; Innab et al., 2018; Elmelhem et al.; 2018; Nurse et al., 2011, Waly et al., 2012).
2. Short, **comprehensible, motivating learning content** (consider gamification) with **high usability**. (Aldawood and Skinner, 2019; Hina and Dominic, 2017; Holdsworth and Apeh, 2017; Labuschagne et al., 2011; Nagarajan et al., 2012; Nurse et al., 2011; Waly et al., 2012)
3. Create awareness **specific to the target group,** e.g., phishing awareness for office workers. (Aldawood and Skinner, 2019; Caputo et al., 2013; Hina and Dominic, 2017; Holdsworth and Apeh, 2017; Le Compte et al., 2015)
4. On-demand, easily accessible learning content to give it a value and application in daily tasks. (Aldawood and Skinner, 2018; Burns et al., 2011; Caputo et al., 2013; Labuschagne et al., 2011; Nurse et al., 2011; Willems et al., 2011)
5. Measurement of performance through simulation, hands-on training, and evaluation. This enables SME managers to give employees feedback, train them with more focus, **mirror false beliefs and risky behavior,** or even cautiously deter intentional abuse (but prefer reinforcement instead). (Bowen et al., 2011; Caputo et al., 2013; Hina and Dominic, 2017; Holdsworth and Apeh, 2017; Innab et al., 2018; Jama et al., 2014; Labuschagne et al., 2011; Elmelhem et al., 2018)
6. Reinforce learning content and **repeat** SETA regularly, several times a year but not too often as it could lead to the perception of being bullied. (Aldawood and Skinner, 2018; Holdsworth and Apeh, 2017; Hina and Dominic, 2017; Innab et al., 2018; Nagarajan et al., 2012)
7. Create **(risk) awareness as part of their daily work tasks**, implement policies, take in all stakeholders, set SMART goals, and foster good habits towards an organizational culture. (Aldawood and Skinner, 2018; Alnatheer, 2015; Amankwa et al., 2015; Awawdeh and Tubaishat, 2014; Holdsworth and Apeh, 2017; Al Sabbagh et al., 2012; Waly et al., 2012)
8. Choose **inexpensive SETA** elements regarding time and financial costs with high usability to enable training repetition. (Innab et al., 2018; Nurse et al., 2011; Wang et al., 2018)

Table 2. Results of the literature review (part II: success factors for designing SETA).

3.2 Meta-requirements to design sticky SETA for SME

In summary, we identified failure factors for designing SETA programs, such as SETA contents that are too theoretical or not comprehensible. In addition, SETA programs often do not fit people's needs, and it lacks integration into daily life. They also do not address motivation to learn, share knowledge, and question learnings, as well as their own beliefs or behavior. Besides, learning outcomes are difficult to measure. The lack of budget for customized training or the lack of in-house experts to design them fosters inefficient implementations or the absence of SETA. As a result, SME employees and managers perceive SETA as expensive and ineffective without value.

The findings reveal **human-centered designed learning content** as a crucial success factor for sticky SETA, especially in SMEs. Reasons for this are, employees often have versatile responsibilities and related knowledge, but many aspects of their work do not fit to common job roles, e.g., in a small business a person handles both, sales and purchasing activities to substitute colleagues. Jama et al. (2014) state that only 30% of companies have different or adapted learning content. However, more learning content could also lead to problems regarding the precise measurement of specific awareness aspects. Thus, the focus should be on **how to deliver the content** comprehensibly and **how to align it to the demands, real-world challenges, and daily tasks** of individuals, respectively, the

target-groups they belong to. In consequence, focusing on the sheer quantity of learning content is not appropriate. Furthermore, SETA programs need a **comprehensible structure of relevant content** instead of providing too many details as this could lead to amotivation, low concentration, to cognitive overload. In this regard, we found that **motivation** is one of the key aspects for successful training, as it leads to engagement with the learning content or perceiving it as useful or not. On the contrary, SETA programs are not perceived to be motivating and sticky in general (Abawajy et al., 2008; Nurse et al., 2011), due to the often neglected but highly relevant aspect of **usability** regarding **easy access** to the training platform, the content or information during the learning process but also applicability to daily tasks. Thus, **on-demand** availability and easy access to SETA content foster intrinsic motivation to engage with the content as it confirms the **relevance** of the topic and provides real **value** to users in their daily tasks when needed. Simulated real-world scenarios are necessary to test whether the training meets individual aspects, but also to disprove users' false or risky beliefs regarding overconfidence and knowledge gaps in security threat detection. Moreover, SETA programs should be repeated regularly. Therefore, SETA programs have to be **lightweight and inexpensive for SMEs**. In addition to motivation, SETA requires performance-based feedback mechanisms regarding **rewards for good practice, appreciation of the supervisor, and threat of deterrence**. In particular, the commonly flatter hierarchies of SMEs may encourage a compliant behavior through sticky SETA as part of an **information security culture** because individual performances are more focused and more addressed. Without that, users do not transfer what they have learned to their real-world environment because they are not aware of the consequences of their behavior and the importance of solutions in their daily work (Nagarajan et al., 2012), although their behavior can be business-critical, especially for SMEs. The following graphic is presented to synthesize the outlined aspects to meta-requirements for sticky SETA for SMEs in a more comprehensive way:

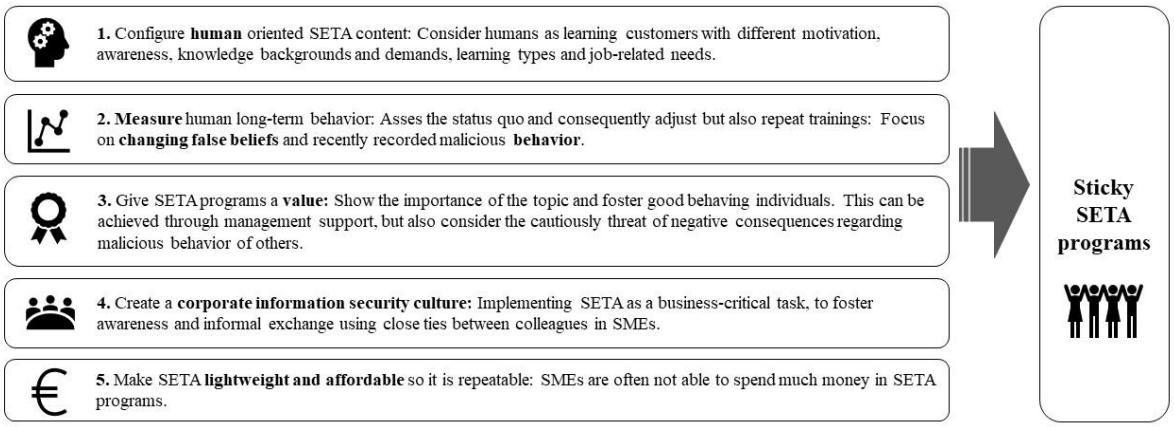

Figure 1: Meta-requirements for creating sticky SETA programs

4 The next design cycle

The conducted literature review represents the main part of our first design cycle and offers rigorously derived insights about essential design factors for creating sticky SETA programs. In order to derive appropriate evaluation criteria for our design, we extracted all applied theories and models from our literature review, resulting in six different applied theories, with only Protection Motivation Theory (Rogers, 1975) mentioned twice (Hina and Dominic, 2017; Wang et al., 2018), and two applied models. However, we did not identify a single well-known theory related to all our meta-requirements for sticky SETA. Thus, we analyzed recent independent literature for theoretical constructs to give straightforward design and evaluation recommendations for specific steps and prospective method instances. We found the theoretical model of Yoo et al. (2018) to fit our purpose as they integrate the Theory of Psychological Ownership with the Theory of Flow to form a conceptual model for measuring the effectiveness of SETA programs. According to Google Scholar, although this model is relatively new, it has already been part of the discussion in more than 50 articles to date. Further, all

constructs, such as social interaction, feedback, autonomy in the learning process, challenging content, immersion in the content, and SETA effectiveness, seem to cover aspects of our meta-requirements. Thus, based on NIST SP 800-50, the work of Yoo et al. (2018), and our meta-requirements, we derived the first ideas of specific activities and preliminary 5 steps towards a method to design sticky SETA for SME: **1. Co-develop SETA elements and a compliance policy with a specific target group**. Consider incident reports of the industry as a starting point for initial discussions and align SETA on members of a department or base it on clusters of personal preferences. Further, ensure the training is motivating, challenging but also feasible. This should create value for participants, foster commitment (psychological ownership) and social interaction between colleagues and management. **2. Implement and update the training** in an easy, repeatable, inexpensive way, e.g., present a monthly cyber security poster, implement a 10-minute team stand-up meeting every other day, discuss recent incidents or questions of employees on security issues, and also establish a readily accessible knowledge base. These efforts encourage social interaction and immersion in the training process as part of an information security culture, and promotes autonomy as employees can access and discuss learning content on demand. **3. Test and evaluate SETA** through simulation, e.g., by sending sporadic fake phishing emails using a fake mailer like "emkei.cz", conducting surveys, and providing feedback on security performance. **4. Reinforce training** based on the outcomes of step 3 and foster self-efficacy, e.g., in the detection of phishing emails to strengthen the value of SETA for users. **5. Establish an on-going process** which includes the identification of champions to recognize good behavior by using gamification elements like high score or free-to-use serious games like *What.hack* from Wen et al. (2019). This helps to strengthen user motivation to engage in the topic and immersive learning processes. In addition, define a realistic budget for SETA, claim management sponsorship and communicate it to the participants as this creates commitment on both sides. In addition, track learning outcomes, user motivation, and incidents to identify gaps and strengthen information security within the organization in the long term. For the first evaluation, we discussed these ideas with a team of experienced practitioners in IT security and a seasoned IT professional and current CTO of a mid-sized personal loans provider company in the US and implemented their feedback. We asked them if they assume our literature review findings and our suggestions to be realistic and useful. In total all participants agreed that our approach is realistic and useful. Thus, our concluding next step to start in design cycle 2 is to extend the knowledgebase with further theoretical, also pragmatic knowledge and to define core activities for the proposed method, considering our previous findings and further well-adopted design literature for SETA programs in general, e.g., Ruhwanya and Ophoff (2019) but also Herold (2010). We will then derive a clear sequence of design instructions for the prospective method. Finally, to contribute to the rigorous creation of design knowledge, the method should be applied to a target group and rigorously evaluated, e.g., using SME departments as a case study, and measuring SETA effectiveness using the Yoo et al. (2018) model. After formalizing these activities towards explicit steps of a method, it is necessary to test the usefulness of the solution (vom Brocke et al., 2020, Hevner and Chatterjee, 2010). Therefore, we suggest using summative evaluation, which is often conducted once the artifact has been developed (Venable et al., 2016, Sonnenberg and Vom Brocke, 2012).

5 Limitations and further research

A limitation of this study is that our literature review was conducted in only one database and should be extended to other disciplines like psychology and other databases. We tried to cover the critique by starting with a broad literature base in combination with an in-depth-analysis of only peer-reviewed articles to ensure enough information value. There may be more literature available in other databases which support or objects to some of our assumptions. Thus, further research would help to strengthen the validity of our findings. The outlined design factors indicate that there are relationships between aspects of the different factors, e.g., between personal interests and motivation to participate in SETA programs. To foster a deeper understanding of these relations and underlying core mechanisms, we suggest analyzing them. In summary, we conclude that we have created the first overview of design factors for sticky SETA in SMEs and, thus, be a basis for further research and our next DSR iteration.

References

Abawajy, J., Thatcher, K. and T.-H. KIM, (2008). "Investigation of stakeholders commitment to information security awareness programs. " In: *International Conference on Information Security and Assurance (ISA 2008)*. IEEE, pp. 472-476.

ACSC (2020). "Cyber Security andAustralian Small Businesses". Australian Cyber Security Centre. Kingston. URL: https://www.cyber.gov.au/sites/default/files/2020-07/ACSC%20Small%20Business%20Survey%20Report.pdf (visited on 1st April 2021)

Ajzen, I. (1985). "From Intentions to Actions: A Theory of Planned Behavior". In: Kuhl, J. and J. Beckmann (eds.) *Action Control*. *SSSP Springer Series in Social Psychology.* Springer, Berlin, Heidelberg, doi:10.1007/978-3-642-69746-3_2

Aldawood, H. and G. Skinner (2018). "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review," In: *IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE).* Wollongong, NSW, pp. 62-68, doi: 10.1109/TALE.2018.8615162

Aldawood, H. and G. Skinner (2019). "Challenges of implementing training and awareness programs targeting cyber security social engineering." In: *2019 Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, 2019. pp. 111-117.

Alahmari A. and B. Duncan (2020). "Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence," In: *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. Dublin, Ireland, pp. 1-5, doi: 10.1109/CyberSA49311.2020.9139638

Alnatheer, M. A. (2015). "Information Security Culture Critical Success Factors," In: *12th International Conference on Information Technology - New Generations.* Las Vegas, NV, pp. 731-735, doi: 10.1109/ITNG.2015.124

Al Sabbagh, B., Ameen, M., Wätterstam, T. and S. Kowalski (2012). "A prototype For HI 2 Ping information security culture and awareness training". In: *International Conference on E-Learning and E-Technologies in Education (ICEEE)*. IEEE, pp. 32-36.

Alshaikh, M., Naseer, H., Ahmad, A., and S. B., Maynard (2019). "Toward sustainable behaviour change: an approach for cyber security education training and awareness". In: *Proceedings of the 27th European Conference on Information Systems (ECIS)*. Stockholm & Uppsala, Sweden, June 8-14, 2019. ISBN 978-1-7336325-0-8, pp. 1-14. URL: https://aisel.aisnet.org/ecis2019_rp/100

Alshomrani, M. M. and M. Mehdim (2012). "The Importance and Dilemmas of Security Education in Information System". In: *WIAR 2012; National Workshop on Information Assurance Research*. VDE, pp. 1-5.

Amankwa, E., Loock, M. and E. Kritzinger (2015). "Enhancing information security education and awareness: Proposed characteristics for a model." In: *Second International Conference on Information Security and Cyber Forensics (InfoSec)*. IEEE, p. 72-77.

Awawdeh P. A. and A. Tubaishat (2014). "An Information Security Awareness Program to Address Common Security Concerns in IT Unit" In: *11th International Conference on Information Technology: New Generations*. Las Vegas, NV, pp. 273-278, doi: 10.1109/ITNG.2014.67

Ayat, M., Masrom, M., Sahibuddin, S. and M. Sharifi (2011). "Issues in implementing it governance in small and medium enterprises." In: *Second International Conference on Intelligent Systems, Modelling and Simulation*. IEEE, pp. 197-201.

Bada, M., Sasse, M. A., and J. RC. Nurse (2015). "Cyber security awareness campaigns: Why do they fail to change behaviour?". In: *International Conference on Cyber Security for Sustainable Society.* UK, Oxford. pp.118-131, URL: http://www.cs.ox.ac.uk/files/7194/csss2015_bada_et_al.pdf

Bada, M. and J. RC. Nurse (2019). "Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs)". In: *Information & Computer Security*. *Vol. 27* (3), pp. 393-410, doi: 10.1108/ICS-07-2018-0080

Baker, M. (2020). *Gartner HR Survey Reveals 88% of Organizations Have Encouraged or Required Employees to Work From Home Due to Coronavirus. Gartner Inc.* URL: https://www.gartner.com/en/newsroom/press-releases/2020-03-19-gartner-hr-survey-reveals-88--of-organizations-have-e (visited on 1st April 2021)

Baskerville, R., Baiyere, A. and S. Gregor (2018). "Design science research contributions: Finding a balance between artifact and theory". In: *Journal of the Association for Information Systems*. 19(5), pp. 358-376.

Bowen, B. M., Devarajan, R. and S. Stolfo (2011). "Measuring the human factor of cyber security," In: *IEEE International Conference on Technologies for Homeland Security (HST).* Waltham, MA, pp. 230-235, doi: 10.1109/THp.2011.6107876

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, p. and N. Díaz-Castano (2020). "Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK". In: *European Societies.* pp. 1-13.

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J. and J. F. Courtney (2015). "Assessing the role of security education, training, and awareness on insiders' security-related behavior: An expectancy theory approach". In: *2015 48th Hawaii International Conference on System Sciences*. IEEE, pp. 3930-3940.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., and M. E. Johnson (2013). "Going spear phishing: Exploring embedded training and awareness". In: *IEEE Security & Privacy.* 12*(*1), pp. 28-38.

Caulkins, B. D., Badillo-Urquiola, K., Bockelman, P. and R. Leis (2016). "Cyber workforce development using a behavioral cybersecurity paradigm." In: *International Conference on Cyber Conflict (CyCon US)*. IEEE, pp. 1-6.

Cimpanu, C. (2020). " Company shuts down because of ransomware, leaves 300 without jobs just before holidays". ZDNET. URL: https://www.zdnet.com/article/company-shuts-down-because-of-ransomware-leaves-300-without-jobs-just-before-holidays/ (visited on 1st April 2021)

Elmelhem, J. EL., Bouras A. and F. Ghemri (2018). "Towards a Holistic Approach of Cybersecurity." In: *3rd Technology Innovation Management and Engineering Science International Conference (TIMES-iCON)*. IEEE, Bangkok, Thailand, pp. 1-4, doi: 10.1109/TIMES-iCON.2018.8621788

Gardner, B. and V. Thomas (2014). "What is a security awareness program?". In: *Building an information security awareness program: Defending against social engineering and technical threats*. Elsevier, pp. 1-8.

Gierow, H., Beckert-Plewka, K., Haake, V. and S. Karpenstein (2020). *Cyber Security Month – Zahl der Woche: 18 Prozent der kleineren Unternehmen sehen IT-Sicherheitstrainings als sinnlos an*. G DATA, Bochum. URL: https://www.gdata.de/news/2020/10/36433-kleinere-unternehmen-sehen-it-sicherheitstrainings-als-sinnlos-an (visited on 1st April 2021)

Ghazvini, A. and Z. Shukur (2017). "Review of information security guidelines for awareness training program in healthcare industry". In: *6th International Conference on Electrical Engineering and Informatics (ICEEI)*. IEEE, pp. 1-6.

Gundu, T. and S. V. Flowerday (2013). "Ignorance to Awareness: Towards an Information Security Awareness Process". In: *SAIEE Africa Research Journal*. 104, pp. 69-79.

Herold, R. (2010). "Managing an information security and privacy awareness and training program". *CRC press.*

Hevner, A. and S. Chatterjee (2010). "Design science research in information systems". In: *Design research in information systems*. Springer. Boston, MA, pp. 9-22.

Hevner, A. R. (2007). "A three cycle view of design science research". In: *Scandinavian journal of information systems.* 19(4)

Hevner, A. R., March, S. T., Park, J. and S. Ram (2004). "Design science in information systems research". In: *MIS quarterly*, pp. 75-105.

Hina, S., and D. D., Dominic (2017). "Need for information security policies compliance: A perspective in Higher Education Institutions". In: *International Conference on Research and Innovation in Information Systems (ICRIIS)*. IEEE, pp. 1-6.

Holdsworth , J. and E. Apeh (2017). "An Effective Immersive Cyber Security Awareness Learning Platform for Businesses in the Hospitality Sector". In: *IEEE 25th International Requirements Engineering Conference Workshops (REW)*. Lisbon, pp. 111-117, doi: 10.1109/REW.2017.47

Innab, N., Al-Rashoud, H., Al-Mahawes, R. and W. Al-Shehri (2018). "Evaluation of the Effective Anti-Phishing Awareness and Training in Governmental and Private Organizations in Riyadh". In: *21st Saudi Computer Society National Computer Conference (NCC)*. IEEE, pp. 1-5.

Jama, A. Y., Siray, M. M. and R. Kadir (2014). "Towards Metamodel-based Approach for Information Security Awareness Management". In: *International symposium on biometrics and security technologies (ISBAST)*. IEEE, pp. 316-321.

Karjalainen, M. and M. Siponen (2011). "Toward a new meta-theory for designing information systems (IS) security training approaches". In: *Journal of the Association for Information Systems.* 12(8), pp. 3.

Labuschagne, W. A., Burke, I., Veerasamy, N. and M. M. Eloff (2011). "Design of cyber security awareness game utilizing a social media framework". In: *Information Security for South Africa*, Johannesburg, pp. 1-9, doi: 10.1109/ISSA.2011.6027538

Lallie, H. S., Shepherd, L. A., Nurse, J. RC., Erola, A., Eppiphaniou, G., Maple, C. and X. Bellekens (2020). "Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyberattacks during the pandemic". In: *arXiv preprint*. arXiv:2006.11929.

Lavelle, J. (2020). *Gartner CFO Survey Reveals 74% Intend to Shift Some Employees to Remote Work Permanently.* URL: https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2 (visited on 1st April 2021)

Le Compte, A., Elizondo, D. and T. Watson (2015). "A renewed approach to serious games for cyber security". In: *7th International Conference on Cyber Conflict: Architectures in Cyberspace*. Tallinn, pp. 203-216, doi: 10.1109/CYCON.2015.7158478

Lourenço, M. B. and L. Marions (2020). *ENISA THREAT LANDSCAPE 2020*. doi: 10.2824/552242

Lugnet, J., Ericson, A., Lundgren, M. and J. Wenngren (2020). "On the design of playful training material for information security awareness". In: *The Sixth International Conference on Design Creativity (ICDC 2020), 26-28 August, 2020*. Oulu, Finland, The Design Society, 239-246.

Mandal, P. and D. A. Khan (2020). *A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic.*

Marinos, L. and M. Lourenco (2019). *ENISA THREAT REPORT 2018*. p. 7; doi: 10.2824/622757

Milosz, E., Juszczyk, M. and M. Milosz (2018). "KNOWLEDGE OF SAFE AUTHENTICATION IN INFORMATION SYSTEMS - RESEARCH RESULTS AND THEIR IMPACT ON TRAINING PROGRAMS". In: Chova, L. G., Martinez, A. L. and I. C. Torres (eds.) In: *12th International Technology, Education and Development Conference (INTEND).* Valenica, pp. 3043-3049.

Nagarajan, A., Allbeck, J. M., Sood, A. and T. L. Janssen (2012). "Exploring game design for cybersecurity training". In: I*EEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*. IEEE, pp. 256-262.

Neupane, A., Saxena, N., Maximo, J. O. and R. Kana (2016). "Neural markers of cybersecurity: an fMRI study of phishing and malware warnings". In: *IEEE Transactions on information forensics and security.* 11(9), pp. 1970-1983.

Nurse, J. RC., Creese, S. Goldsmith, M. and K. Lamberts (2011). "Guidelines for usable cybersecurity: Past and present". In: *2011 third international workshop on cyberspace safety and security (CSS)*. IEEE, pp. 21-26.

Ozaki, S. (2020). "Improving the Training Materials of Information Security Based on Cybersecurity Framework". In: Stephanidis, C. and M. Antona (eds.) *HCI International 2020 - Posters*.. Springer International Publishing, Cham, pp. 581-588.

Peffers, K., Tuunanen, T. and B. Niehaves (2018). "Design science research genres: introduction to the special issue on exemplars and criteria for applicable design science research". In: *European Journal of Information Systems*. 27(2). Taylor & Francis, pp. 129-139, doi: 10.1080/0960085X.2018.1458066

Peffers, K., Tuunanen, T., Rothenberger, M. A. and S. Chatterjee (2007). "A design science research methodology for information systems research". In: *Journal of management information systems*. 24(3), pp. 45-77.

Ponemon Institute (2019). "Cost of Data Breach Report 2019". Ponemon Instute LLC and IBM Security. URL: https://www.ibm.com/downloads/cas/RDEQK07R (visited on 1st April 2021)

Ponemon Institute (2020). "Cost of Data Breach Report 2020". Ponemon Instute LLC and IBM Security. URL: https://www.ibm.com/downloads/cas/RZAX14GX (visited on 1st April 2021)

Puhakainen, P., and M. Siponen (2010). "Improving employees' compliance through information systems security training: an action research study". MIS quarterly, pp. 757-778.

Rogers, R. W. (1975). "A protection motivation theory of fear appeals and attitude change". *The Journal of Psychology*. 91(1), pp. 93–114.

Ruhwanya Z. and J. Ophoff (2019). "Information Security Culture Assessment of Small and Medium-Sized Enterprises in Tanzani". In: Nielsen P. and H. Kimaro (eds.) *Information and Communication Technologies for Development. Strengthening Southern-Driven Cooperation as a Catalyst for ICT4D. ICT4D 2019. IFIP Advances in Information and Communication Technology*. 551. Springer, Cham, pp. 776-788, doi: 10.1007/978-3-030-18400-1_63

Sadok, M., Alter, p. and P. Bednar (2020). "It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs". In: *Information & Computer Security*, 28, 467-483.

Sonnenberg, C. and J. vom Brocke (2012). "Evaluation Patterns for Design Science Research Artefacts". In: Helfert M. and B. Donnellan (eds.) *Proceedings of the European Design Science Symposium (EDSS)*. 286. Dublin, Ireland: Springer Berlin/Heidelberg, pp. 71-83.

Venable, J., Pries-Heje, J. and R. Baskerville (2016)."FEDS: a Framework for Evaluation in Design Science Research". In: *European Journal of Information Systems*. 25(1). pp. 77-89, doi: 10.1057/ejis.2014.36

Verizon (2020). "2020 Data Breach Investigations Report (DBIR)", URL: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (visited on 1st April 2021)

vom Brocke, J., Simons, A., Niehaves, B., Niehaves, B., Riemer, K., Plattfaut, R. and A. Cleven (2009). "RECONSTRUCTING THE GIANT: ON THE IMPORTANCE OF RIGOUR IN DOCUMENTING THE LITERATURE SEARCH PROCESS". In: *ECIS 2009 Proceedings*. 161. URL: https://aisel.aisnet.org/ecis2009/161

vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R. and A. Cleven (2015). "Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research". In: *Communications of the Association for Information Systems.* 37(1).9. pp. 205-224, doi: 10.17705/1CAIp.03709

vom Brocke, J., Winter, R., Hevner, A. and A. Maedche (2020). "Accumulation and Evolution of Design Knowledge in Design Science Research – A Journey Through Time and Space". In: *Journals of the Association for Information Systems (JAIS)*. pp. 1-39.

Waly, N., Tassabehji, R. and M. Kamala (2012). "Improving organisational information security management: The impact of training and awareness". In: *IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems*. IEEE, pp. 1270-1275.

Wang, Y., , H. Zou, B. Qi and J. Li (2018). "Framework of Raising Cyber Security Awareness". In: *IEEE 18th International Conference on Communication Technology (ICCT).* Chongqing, pp. 865-869, doi: 10.1109/ICCT.2018.8599967

Wen, Z. A., Chen, R. and E. Andersen (2019). "What. hack: engaging anti-phishing training through a role-playing phishing simulation game". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. pp. 1-12.

Willems, C., Klingbeil, T., Radvilavicius, T., Cenys, A. and C. Meinel (2011). "A distributed virtual laboratory architecture for cybersecurity training". In: *International Conference for Internet Technology and Secured Transactions*. Abu Dhabi, pp. 408-415.

Willison, R. and P. B. Lowry. (2018). "Disentangling the motivations for organizational insider computer abuse through the rational choice and life course perspectives". In: *ACM SIGMIS Database: The database for advances in information systems* 49 (SI) pp. 81-102.

Wilson, M. and J. Hash (2003). "National Institute of Standards and Technology (NIST), Building an Information Technology Security Awareness and Training Program (NIST SP 800-50)". US Department of Commerce, Washington, DC

Whitmore, W. and G. Parham (2020). "COVID-19 cyberwar". In: *Research Insights: How to protect your business.* URL: https://www.ibm.com/downloads/cas/Y5QGA7VZ (visited on 1st April 2021)

Yoo, C. W., Sanders, G. L., and R. P. Cerveny (2018). "Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance". In: *Decision Support Systems*. 108. pp. 107-118.