Martin Brehmer, Vanessa Steinherr, Raphaela Stöckl

Toward A Higher Resilience Against Cyberattacks

Two new impulses for awareness training programs

Effective information security awareness programs are crucial for building resilience against cyberattacks, and they are thus, a major part of an organization's security investments. However, studies reveal that they are often ineffective and perceived to be burdensome. Thus, we share insights from two new approaches that are effective in both, building information security awareness and motivating participants to engage with information security learning content profoundly.

1 Introduction

The European Union Agency for Cybersecurity reports that human-centered cyberattacks such as social engineering attacks, but also data breaches (often traced back to human errors), are among the most considerable threats to information security and data privacy [1]. As human behavior plays a crucial role, information security education, and training awareness (SETA) programs are important measures to strengthen the resilience of organizations. [2] However, many training approaches are rather ineffective and neglect participant-centered aspects. As a result, such programs are perceived to be burdensome, not engaging, moderately boring, unspecific, lack real-life hands-on experiences, and do not convey tangible relevance to the users. [3–5] In other words, they are not participant-centered. They fail to motivate participants and further, to provide tangible real-world relevance for why they should change unsafe behaviors. As a result, organizations might invest in such SETA programs but could still be vulnerable without knowing it. In order to address this problem, we present two scalable concepts for training programs that consider the mentioned shortcomings and focus on a participant-centered delivery. More precisely, we outline two concepts for realistic training scenarios, a) an interactive video that enables participants to experience the consequences of their behavior in a motivating manner, as well as b) a business game that enables the participants to take different angles of information security within an organization. Both approaches have been developed and tested in higher education contexts and students report them to be engaging and realistic.

Martin Brehmer

Wissenschaftlicher Mitarbeiter an der Universität Augsburg. Forschungsschwerpunkte in den Bereichen Informationssicherheitstrainings, sowie generative KI und Gamification im Bildungskontext.
E-Mail: martin.brehmer@uni-a.de

Dr. Vanessa Steinherr

Wissenschaftliche Mitarbeiterin an der Universität Augsburg. Forschungsschwerpunkte in den Bereichen IT-gestützte Verhaltensänderung und computergestütztes Lernen.
E-Mail: vanessa.steinherr@uni-a.de

Raphaela Stöckl

Wissenschaftliche Mitarbeiterin an der Universität Augsburg. Forschungsschwerpunkte in den Bereichen Learning Analytics und Datenanalysen.

E-Mail: raphaela.stoeckl@uni-a.de

2 Theory-informed considerations for our training approaches

In order to develop participant-centered approaches, we considered current research articles and literature reviews on factors that lead to the success and failure of SETA programs. Accordingly, a major success factor is to make training approaches *engaging*. This means they should include, e.g., a variety of training formats, options for interactivity, rich media for delivery (e.g., videos), collaborative learning techniques, and motivating learning content. A critical aspect of motivation is making the content relevant to users, e.g., by providing real-world examples that allow them to have their own 'hands-on' experiences. Simulations of real-world scenarios like the story of a cyberattack are one way to cover this aspect if fear appeals are not overstressed. This being said, simulations can be engaging, have the potential to foster good behavior, and change false beliefs by providing feedback on decisions and experiencing consequences in a comfortable way. [2–5]

Another major success factor that contributes to engaging and successful training is the *effective mediation of relevant information*. It is not about quantity, as training programs might fail if too much content and abstract information are provided. The participants might simply not understand the relevance and its ties to specific practices, so they react with disinterest and cognitive overload. Consequently, only providing information, e.g., by hanging up posters, is not enough. Instead, active learning requires practice and repetition which is, e.g., enabled by simulations. [2, 3]

To sum up, learners need to experience in an engaging and motivating way that the training is of great value and provides specific and relevant information to their daily tasks.

Based on this theoretical core knowledge, we developed the two conceptual elements for SETA programs that we mentioned in the introduction: An interactive video and a business game. In order to engage the participants to delve into the learning content and to internalize its relevance for their personal lives as well as for business contexts, both approaches are based on a specific narrative that is strongly connected to the real-world environment of our target group, in this case, higher education students. We chose students because they are prospective full-time employees, represent a great share of IT users at a university, and are often already partially employed, e.g., as assistants either at the university or in other organizations. However, even though we implemented tailored narratives for students in both approaches, the narrative concept itself diverged. We will now outline this, and further underlying considerations based on our previous work along both approaches, before explaining the implementation in more detail within the next chapter. This also means that we share more details about the conceptualizations instead of content creation. For the latter, we can refer to our previous work on applying generative artificial intelligence to create learning content efficiently [6].

The first approach is an interactive learning video that employs choice-based storytelling because we found in our previous work that narratives can have a strong positive effect on the motivation of participants (for further information – see [7]). This means that participants of this training start a video that includes real-world camera footage of the organizations' environment and a narrative leads them to decision situations. Each decision leads to a different story path and different story endings, e.g., a cyberattack was stopped vs. the organization was hacked. For this reason, every participant has the possibility to experience the consequences of good and bad decisions within a safe space and in a very personal way. The narrative makes them curious, and 'retry' options allow for repetitions until the right path is found. With that, we address the named success factors for information security training programs of our previous research, but also adapt to current practices as learning videos are among the dominant ways of delivery for such approaches. For instance, KnowB4, ESET, or Proofpoint offer various forms of learning videos; however, to the best of our knowledge, there is no such approach as ours. Furthermore, there is scarce evidence that video-based training approaches are effective. Contrary, our approach provides first empirical evidence for its effectiveness (for more information see [8]).

For the second approach, we chose a business game because it encourages participants to take different perspectives on information security while the narrative simulates a realistic scenario, e.g., specific business processes for the organization. Furthermore, a business game allows instructors to split a course into smaller groups and the creation of a collaborative learning environment. Given this, we grouped all students of our lecture into teams of 3 up to 4 people. We also considered that collaborative learning could take place either online, hybrid, or in local classes. In general, instructors could carry out such business games by developing paper-based material or using collaboration technology to scaffold the players, respectively the learning process. We tested both, a PDF-based version and a collaboration software.

Despite the concept of the training that we depicted above, we briefly depict the content that has been taught when carrying out both training approaches. Overall, the content addressed issues of information security as well as data security. We strived to sensitize our participants that there is no data privacy without both, legal privacy regulations and information security, as the latter provides the technological means to enforce the technical security of private data. The focused content of the interactive video addressed the topic of bad USB sticks and reporting security incidents. Instead, the business game covers four lecture dates that focus on threat assessment (for non-information systems managers), phishing attacks, handling sensitive data, and incident response. During all lectures, we strived to cover both perspectives – the private perspective and the work perspective to make the content more accessible and relevant to the participants.

Lastly, we want to emphasize that every instructor should carefully consider a positive formulation for the role of humans in the cybersecurity context, as we did. For instance, in case a human is unintentionally involved in cyberattacks, e.g., being tricked into plugging a malicious USB stick into the working computer, in literature, this human is considered as one compromised link in the security chain and often declared as a 'human error' or 'the weakest link within the security chain'. Thus, we emphasize using more sensitive and positivistic wording, e.g., to declare all humans as 'one of the most important links within the security chain'.

3 Two engaging approaches to build information security awareness training

3.1 Interactive videos based on choice-based storytelling

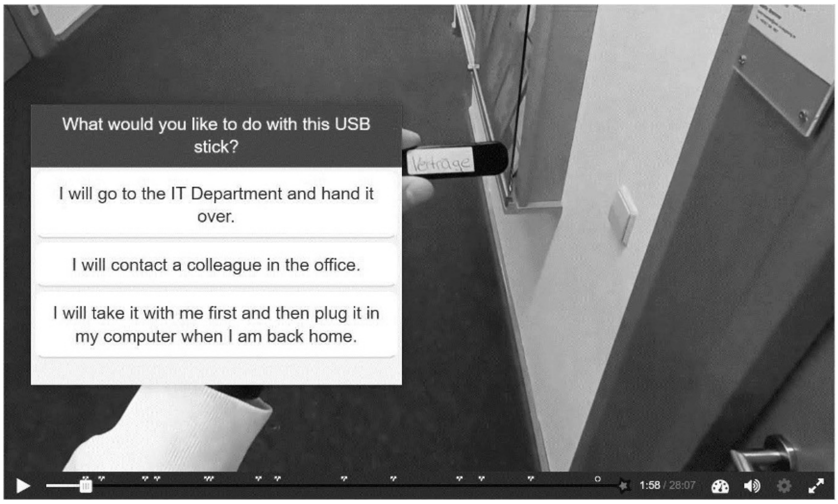
As introduced in the previous chapter, we aimed to create a narrative-based training approach for students of the lecture on data privacy and information security at a German university. This training scenario is based on a real-world scenario in order to increase personal relevance, reduce the emotional distance between the learning content and the participants, and to make it more authentic. In order to achieve this, we recorded real-world footage of the university environment to tell the narrative within the learning video. This also means that we developed a real-world inspired narrative instead of a general narrative that applies to all companies or branches. Thereby we argue that, e.g., the organizations' brand logo or specific information are one attempt to provide customized experiences, however, they could appear to be too generic. As a result, the customization might not achieve the intended effect of a tailored training instance.

The narrative itself tells the story of a student assistant who receives an e-mail, including a request from a colleague to come to work for a job-related issue. Upon arriving at the organization, the protagonist finds a USB stick and has to decide how to deal with this situation. This is called choice-based storytelling, where a player has the opportunity to control the storyline through their own decisions. For instance, the player can decide whether to plug in this USB stick, walk to the computer department, or ask a colleague what to do. The journey in the video leads the person to different decision situations that are represented through pop-up questions within the video at the given time. We provide two screenshots of such decision situations in the Figures 1 and 2. The first figure depicts the first decision situation that we described previously – the protagonist has to decide what to do with the USB stick that he found in front of a colleague's door. The second figure is a decision situation where the protagonist was informed by a fellow student that he and students found several USB sticks on the campus, and these sticks seem to be empty. Now, the viewer has to decide whether to ignore that or to report it to the IT department. If a participant chooses a path that violates information security, they are led, e.g., to the scenario that either he or the organization has been hacked but allowed to retry. We prepared different endings for bad decisions to reflect different preceding circumstances and consequences. For instance, if the player decides to plug the USB stick into the personal computer of the protagonist, the story continues with footage of the protagonist's computer that acts strange for some seconds. Then, an instructor sequence explained what happened. In contrast, now referring to Figure 2, where the player has to decide whether to report the situation when fellow students found 'empty' USB sticks or not, the protagonist gets informed about a cyberattack that hit the organization severely, including details of the incident. This allows participants to experience possible specific consequences of their actions in a safe learning environment. We also included humor for both good and bad behavior to make the students feel more comfortable.

In order to develop the narrative, we oriented on the Human-Aspect-of-Information-Security-Questionnaire [9] to cover relevant topics and to assess the level of information security awareness after the training is completed. Another way to cover that aspect would be to consider documents and recommendations of local official institutions, e.g., the 'Federal Office for Information Security' (Bundesamt für Informationssicherheit) in Germany, or the National Institute of Standards and Technology in the United States. In addition to that, we recommend identifying relevant topics based on the organization's risk assessment, if available. Subsequently, we modeled our narrative as a process chain to create an overview of all decision situations. This is highly relevant to shooting the video footage efficiently. We experimented with both an action camera and a smartphone camera (in combination with a gimbal) to capture all scenes. It was an intentional decision to choose this setup over a professional camera team as we strived to cover the aspect that creating training content should be lightweight and affordable.

A pre- and post-test (n=60) revealed a significant and strong effectiveness of the video for the topic 'incident response' in enhancing information security awareness. The qualitative feedback from students was largely positive, e.g., 29 out of 32 statements mentioned engaging aspects of the video, such as it is enjoyable and exciting, but mainly that it is literally engaging and supporting them in active learning; three negative statements related to technical issues. Further remarkable is that among all evaluation categories, many students positively referred to the interactive real-world scenario as it enabled them to experience the consequences of their own decisions and reflect on them. (see [8] for details)

Fig. 1 | Decision situation: how to deal with the USB stick



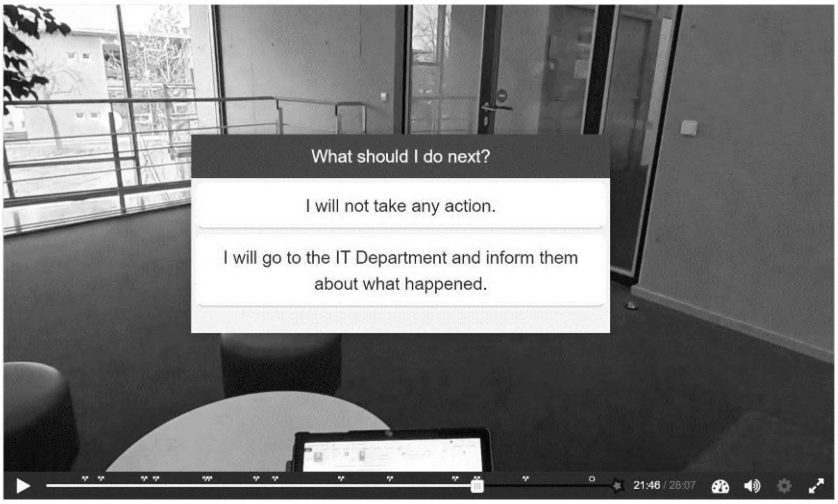
What would you like to do with this USB stick?

I will go to the IT Department and hand it over.

I will contact a colleague in the office.

I will take it with me first and then plug it in my computer when I am back home.

Fig. 2 | Decision situation: reporting an incident



What should I do next?

I will not take any action.

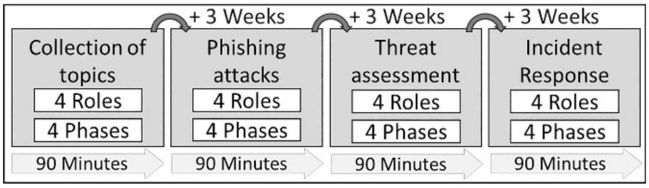
I will go to the IT Department and inform them about what happened.

3.2 Business game for online and local setups

Implementing a business game is a further possibility to provide a real-world context that addresses the topic of information security awareness. More precisely, a business game is an educational method that uses simulations to build realistic scenarios and allows participants to gain practical experience as well as to make decisions without having to face real consequences. This enables a hands-on approach to various relevant information security topics. Participants do not just passively consume new content but are given an active role in which they have to discuss, apply, and evaluate new content. The content of business games can be closely aligned with the relevant content of any organization.

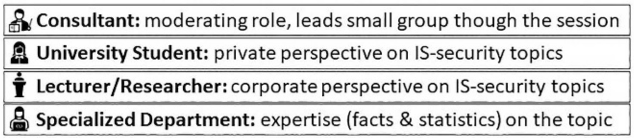
Based on these considerations, we have developed a simulation game for a German university where students deal with data protection and information security at their university during one semester. At regular intervals of circa 3 weeks, we have scheduled 4 sessions of 90 minutes each (see Figure 3). Every session addresses one specific information security-related topic.

Fig. 3 | Structure of the business game with four sessions



The business game simulates the storyline of a fictitious IT consultancy that advises a potential customer (our university) on the topics of data protection and information security. While in the first session, the participants collect relevant information security topics by conducting a simplified threat assessment, the following three sessions focus on one specific topic in detail. Within the business game, there are four roles that students can be assigned to: A representative of IT consulting, a university student, and two university employees. One as a lecturer/researcher and one of a specialized department (e.g. IT, law). Each role enables a different perspective on information security topics (see Figure 4).

Fig. 4 | Assigned roles within the business game



Consultant: moderating role, leads small group though the session

University Student: private perspective on IS-security topics

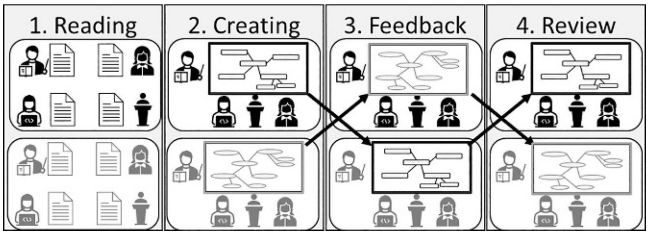
Lecturer/Researcher: corporate perspective on IS-security topics

Specialized Department: expertise (facts & statistics) on the topic

Each of the four sessions of the business game has a workshop character and is moderated by the role of the Consultant. Besides each session is structured into four phases: **1. Reading**: Getting to know the assigned role and learning about corresponding information security; **2. Creating**: Working together in the small group and creating a product to summarize the previously learned information security knowledge of all roles; **3. Feedback**: Exchanging and analyzing this product with members of other small groups and documenting the comments; **4. Review**: Reflecting on the received feedback for the product.

To make this generic structure of the business game sessions more tangible, we will describe the concrete concept of the first session. This is depicted in Figure 5, showing an example of two small groups. The first session represents the first contact of the IT consultancy supporting the university in the area of information security. Therefore, it is about collecting relevant information security topics (simplified risk assessment) in the context of the university and creating a structured overview of these topics, including threats. The session starts with the students being divided into small groups of four, and then each student is assigned a role.

Fig. 5 | Structure of one session on two exemplary groups



In the first phase of every session, each student is provided with information about their role. The aim of this phase is for each student to understand the perspective of the role and to learn about topics relevant to information security. The **consultant** is given information about the structure and process of the session. The role also receives information on how to lead the small group through the process and how to ensure that all roles are actively participating and responding to each other. The **student** receives an experience report, including experiences with a hacked social media account, sharing private information online, and creating weak passwords. The **lecturer/researcher** role includes an experience report that deals with the topic of phishing emails, handling sensitive data and storage media, as well as regular backups. Within the first session, the fourth role of the department is an **employee of the university computer deparment**. This role is provided with an overview of cyber-attacks and related statistics.

The second phase begins with a welcome from the consultant, who asks each role to briefly introduce themselves. In addition, during this phase, the small groups work together to create an overview of information security issues in the form of a mind map. Each role is asked to engage and share the information provided. The aim of this phase in the first session is for the students to reproduce, analyze, and link information security topics. At the end of this phase, each small group has created a mind map summarizing the information security topics they have identified.

In the third phase, the mind maps of the small groups are exchanged, and each small group receives the mind map of another small group. The task of this phase is to analyze the received mind map for its completeness and logic. The small groups should document their thoughts on the received mind map, again under the moderation of the consultant.

In the fourth and final phase, each small group receives its annotated mind map back from the assigned group. The roles discuss the comments and reflect on what they have learned. At the end of the phase, the consultant closes the session by thanking the other team members for their participation and saying goodbye.

If any questions remain unanswered in the small groups after a session, they are discussed with the students in an open plenary with the teacher and any ambiguities are clarified.

Over two semesters, 35 students returned a survey about their experiences after completing the business game. The overall feedback from the participating students was positive, with 72% saying they (highly) enjoyed the simulation and 67% saying they were (highly) interested in the addressed topic. In this context, students emphasized that they liked the group interaction and the role-specific tasks. In addition to the high level of motivation, there is also a measurable increase in information security knowledge.

4 Implications and conclusion

The evaluations of our interactive video and the business game show that participants found both approaches engaging and that they enjoyed participating, despite minor technical issues such as lost Wi-Fi connections. Moreover, student feedback emphasizes that realistic training approaches allow them to take different perspectives, stimulate interest, and support the internalization of relevance. It also supported them in active learning. This supports our assumption that our narratives and the simulation of real-world scenarios were both successful in connecting the students' world with the security goals of the organization, our university.

With special emphasis on the interactive video, we suggest incorporating realistic decision situations in SETA programs in combination with narratives that are borrowed from the participants' real-world context to create tangible relevance to the users. This goes in line with current research that emphasizes the importance of real-world training scenarios as they link abstract knowledge with the organization's environment and the personal habits of the participants. [3, 10] Moreover, tangible relevance makes SETA programs engaging and fosters resilience against cyber threats.

Referring to the business game, we recommend using suitable collaboration software instead of a paper-based version and basing the game on a realistic use case that allows for different user roles and perspectives. Since there was no adequate collaboration software available for our learning management system (based on Stud.IP), we co-developed a dedicated plugin in a funded interdisciplinary research project (for further information – see 'Acknowledgements'). The plugin offers the necessary functionalities for this, and related use cases. For instance, the use of the plugin allowed us to address the three types of participants, namely online, hybrid, or local class students, and provided the lecturer with more control options during the business game, e.g., monitoring the status of each group within every phase of the game. Consequently, instructors can not only detect and intervene in problems but also review the outcomes of all groups simultaneously.

What further applies to both of our approaches is that they enable a broad application context. They are scalable and lightweight, as well as independent of the learners' and the instructors' location. In addition, the interactive video can be provided on demand.

Finally, we declare that the selection and combination of training elements, e.g., videos, business games, or group training should be carefully considered in general. There is no 'one size fits all' solution and our suggestions should not be interpreted as such. For instance, the proposed interactive video enables users to experience the consequences of cyberattacks within a real-world environment but might not be suitable to train, e.g., encrypting files. Nevertheless, we provide two concepts for engaging, interactive training approaches that could be used as elements of an effective SETA program portfolio. Moreover, these concepts can be applied on many other topics related to information security awareness. For example, we developed a second interactive video for the use of mobile devices at public locations and a business game with only one session. Lastly, we want to emphasize the importance of positively perceived training approaches, as convincing individuals is the first step to invoke positive group thinking processes and therefore, to build an effective information security culture [11].

Acknowledgment

This work was supported by the 'Stiftung Innovation in der Hochschullehre' (FBM2020: 'Facilitating Competence Development through Authentic, Digital, and Feedback-Based Teaching-Learning Scenarios') under Grant FBM2020-EA-2620-01350. The collaboration software mentioned in this article is 'CoLearn!', a Stud.IP plugin and one result of this project.

Open Access

Funding

Open Access funding enabled and organized by Projekt DEAL.

References

[1] ENISA. 2023. *ENISA Threat Landscape 2023*. EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA).

[2] Siqi Hu, Carol Hsu, and Zhongyun Zhou. 2022. Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems* 62, 4, 752–764. DOI: https://doi.org/10.1080/08874417.2021.1913671.

[3] Martin Brehmer, Antragama E. Abbas, and Nageswaran Vaidyanathan. 2021. Towards Designing a Method to Create Sticky Information Security Training for SMEs: Identifying Design Factors. In *29th European Conference on Information Systems (ECIS 2021)*, 1–13.

[4] Nabin Chowdhury, Sokratis Katsikas, and Vasileios Gkioulos. 2022. Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security* 113, 102551. DOI: https://doi.org/10.1016/j.cose.2021.102551.

[5] A. Reeves, D. Calic, and P. Delfabbro. 2021. "Get a red-hot poker and open up my eyes, it's so boring"1: Employee perceptions of cybersecurity

training. *Computers & Security* 106, 102281. DOI: https://doi.org/10.1016/j.cose.2021.102281.

[6] Martin Brehmer and Vito Buonassisi. 2024. Educators' friend – applying generative AI to create effective digital learning objects for information security education: toward initial design principles. In *Proceedings of the 57th Annual Hawaii International Conference on System Sciences*, Honolulu, HI, January 3-6, 2024.

[7] Martin Brehmer and Ramona Reinelt. 2023. Gamifying a Learning Management System: Narrative and Team Leaderboard in the Context of Effective Information Security Education: January 3-6, 2023. In *Proceedings of the 56th Annual Hawaii International Conference on System Sciences*, Honolulu, HI, January 3-6, 2023.

[8] Martin Brehmer. 2023. Decide wisely: Interactive videos as appealing educational element to attract students to information security. *Wirtschaftsinformatik 2023 Proceedings*.

[9] Kathryn Parsons, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, and Tara Zwaans. 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security* 66, 40–51. DOI: https://doi.org/10.1016/j.cose.2017.01.004.

[10] Hwee-Joo Kam, Dustin K. Ormond, Philip Menard, and Robert E. Crossler. 2022. That's interesting: An examination of interest theory and self-determination in organisational cybersecurity training. *Information Systems Journal* 32, 4, 888–926. DOI: https://doi.org/10.1111/isj.12374.

[11] A. Da Veiga and J.H.P. Eloff. 2010. A framework and assessment instrument for information security culture. *Computers & Security* 29, 2, 196–207. DOI: https://doi.org/10.1016/j.cose.2009.09.002.