

A Scenario-Driven Cyber Security Awareness Exercise Utilizing Dynamic Polling: Methodology and Lessons Learned

Maria Leitner^{1,2} 

¹*AIT Austrian Institute of Technology GmbH, Center for Digital Safety & Security, Vienna, Austria*

²*University of Vienna, Faculty of Computer Science, Vienna, Austria*

Keywords: Cyber Security, Awareness, Cyber Security Exercises, Cyber Security Education, Methodology.

Abstract: As cyber security capabilities are becoming more relevant for society, the need for cyber security skills and teaching methods have increased. For example, cyber security exercises have emerged to train and test skills and abilities of people in emergency situations (e.g., under cyber attacks). While cyber security knowledge has become essential for everyone, we propose a cyber security awareness exercise that targets people with or without cyber security knowledge. Our novel approach uses dynamic surveys to visualize decisions during the exercise. In this paper, we describe the idea behind the exercise and specify the design, implementation and evaluation of this method. We validate our methodology with a cloud-based implementation that enables a low-barrier entry and a responsive design for the participants. We apply our methodology to four case studies. Our findings show that this methodology is an easy tool for organizers and helps participants to learn about cyber security. For future work, we aim to develop the methodology further and increase the scenarios to conduct more experiments with a diverse audience.

1 INTRODUCTION

With the ongoing digitization and the increased interconnectedness, the surface of information systems for cyber security attacks has increased significantly. Furthermore, new business models (such as cyber crime as a service) allow to launch large-scale attacks by just one mouse click. Hence, with the constantly increasing threat and attack landscape, it is only imminent that skills and capabilities to prevent, identify, stop and mitigate security incidents and cyber attacks have become highly relevant. Security incidents are, for example, events that may indicate a breach in confidentiality, integrity or availability of data (e.g., a data leak, a data manipulation or a interruption of a service).

For organizations and individuals of the digital society, it has become essential to know how to handle security incidents and attacks. This has evoked the development of a variety of methods and tools for cyber security education (e.g. (Daimi and Francia III, 2020)). For example, table-top-exercises, cyber security exercises or simulation games that focus on conveying knowledge and skills to a variety of people

have been designed (Kucek and Leitner, 2020). Cyber security exercises can be utilized to test, train and validate the organizational and technical competencies of organizations and individuals. Cyber security exercises can be set up in various ways (cmp. (ENISA, 2015)) such as Capture-The-Flag (CTF) competitions (e.g., (Werther et al., 2011; Vigna et al., 2014)) or as cyber defense exercises (Vykopal et al., 2017). In recent years, cyber security exercises have increased significantly (ENISA, 2015). Many cyber security exercises aim to increase capabilities, skills and competences of individuals and strengthen the resilience and preparedness of organizations against threats and attacks. Cyber security exercises utilize forms of experiential learning (Gentry, 1990) but also other learning theories such as challenge-based learning (Cheung et al., 2011). They are suitable for cyber security training (Hendrix et al., 2016).

The target audience of cyber security exercises (such as CTFs or technical exercises) are often IT experts or security experts (Vykopal et al., 2017; Leitner et al., 2020; Andreolini et al., 2020). However, table-top-exercises (Angafor et al., 2020), board or card games (e.g., (Denning et al., 2013)) often raise awareness and target a wider audience.

In this paper, we outline a methodology for a cyber

^a  <https://orcid.org/0000-0003-1371-5446>

security awareness exercise utilizing dynamic polling. In literature, this exercise might be also referred to as “strategic exercise”, “awareness game” or “simulation game”. We present the idea, design, setup and implementation of the method of this cyber security awareness exercise. The novel idea of our approach is that we are using dynamic surveys that allow that participants make an active decision. Then, the decision of the whole set of participants is visualized. These visible results aim to engage fruitful discussions of the participants. We describe our implementation using a cloud-based application that uses dynamic polls that allow the responses to be shown directly throughout the exercise. This opinion-sharing stipulates the discussion among the participants. Furthermore, we demonstrate our findings with an elaborate evaluation in four case studies. We show that our methodology is easy-to-use, has a low barrier entry and can support raising the participants’ awareness. For organizers of exercises, we have received feedback that it has a very short learning period at the beginning.

The content of the paper can be of high interest to organizers of exercises, participants and cyber security educators. Organizers of training courses may be introduced to the simulation game for the first time. This may shift their view on how lectures and exercises can be designed for local or remote training courses. Organizers of cyber exercises may be interested in learning on the variety of scenarios and the complex scenario building. The example can also help people who would like to start hosting their own cyber security exercises. Cyber security educators may be interested in incorporating the methodology into their security lectures to activate their audience.

The rest of the paper is structured as follows. Section 2 outlines background for cyber security awareness exercises and cyber security education. Section 3 describes the methodology of the cyber security exercise, in particular, the idea, design, implementation and evaluation. Section 4 demonstrates the cyber exercise using four case studies. Lastly, Section 5 concludes the paper.

2 BACKGROUND

2.1 Cyber Security Awareness Exercises

In the past years, cyber security exercises have become a typical method to enable cyber security awareness or develop cyber security competencies (e.g., (ENISA, 2015; Peker et al., 2016; Pham et al., 2016; Brilingaitė et al., 2020)).

Many serious games have been developed to con-

vey cyber security competencies (Hendrix et al., 2016; Tioh et al., 2017). For example, table-top exercises for incident response have been systematically reviewed in (Angafor et al., 2020) and serious games in cyber security in (Tioh et al., 2017). Both reviews show that there is a big variety in table-top exercises and gamification in cyber security education. Furthermore, many board games or card games exist for cyber security. For example, a card game in (Denning et al., 2013) was developed to raise security awareness. Another example in (Frey et al., 2019) assesses security decisions in a cyber-physical systems game and many other examples can be found (e.g., (Sedjelmaci et al., 2019)).

Cyber security exercises can be utilized to test, train and validate the organizational and technical competencies of organizations and individuals. Hence, it is self-evident that exercises should not be limited only to experts participants but also to all diverse participants of organizations. Cyber security exercises enable here a good method for training and testing of skills and competencies (ENISA, 2015; Werther et al., 2011). However, most solutions in the area of cyber security exercises focuses on testing advanced technical knowledge (e.g., in CTFs (e.g., (Vigna et al., 2014; Kucek and Leitner, 2020)) or in cyber defense exercises (e.g., (Vykopal et al., 2017; Beuran et al., 2017))).

In summary, while there are many approaches for cyber security exercises, to the best of our knowledge, we did not identify a method that allows all participants to play the same scenario, make decisions and visualize their and the other participant’s decisions. We could not identify a method where the participants could either work together in groups or individually but had overall the same story line. Furthermore, we did not find any tool that supported an active decision-making in groups or individually. Therefore, we will propose in the next section our methodology for a cyber security awareness exercise that allows active decision-making, using the same scenario as well as enables and supports group discussions.

2.2 Cyber Security Education

In the past years, research has focused on new methods such as cyber security exercises to develop cyber security education further (see for example a variety of topics is described in (Daimi and Francia III, 2020)). Several learning theories have been applied to cyber security exercises such as challenge-based learning (Cheung et al., 2011), cognitive learning (Wellington et al., 1996), behavioral learning (Byrne and Wolfe, 1974) and active learning (Sanders et al.,

2017).

Furthermore, the authors in (Katsantonis et al., 2019) describe a conceptual framework how to develop serious games for cyber security. Our proposed methodology in Section 3 follows these aspects and includes scenarios, missions and goals related to the target audience and therefore introduces the actions (injects as text, image or poll). The challenge tuning can be mainly conducted with the scenario complexity.

In summary, new teaching methods such as cyber security exercises support the active and dynamic learning in cyber security education (see e.g., (Beuran et al., 2017; Frank et al., 2017)). Our proposed methodology provides a method that could be utilized in educational settings. However, it is not limited and may be used in other domains as well for educational purposes.

3 METHODOLOGY AND CONCEPT

3.1 Idea

Background. Originally, the idea for this exercise was developed for a security conference. The challenge was to allow more than 100 people to play a fun “game” together and talk and learn about cyber security. The basic concept was that decisions in the game should be actively made and the opinion of each participant is valued. The first idea came up in 2017 and was continuously developed and tested until today. Initially, many people should be able to play together in the game and learn about cyber security. The people’s knowledge level on information security was unknown. The game should be interactive, i.e. participants can actively make decisions. These initial thoughts were specified in the next step.

Aims. The aim of the cyber security exercise is to raise awareness and can be used for educational settings. We designed an exercise methodology based on the following requirements:

- Participants should be able to participate with or without knowledge on information security or cyber security.
- Participants should be able to make individual decisions in the exercise.
- Participants should be able to see the results of their and the other participants decisions instantly.

- Participants should be able to experience the challenges after a cyber security attack.
- Participants may be able to discuss the results.

Similar to other cyber security exercises, this exercise can be structured into three phases preparation, implementation and evaluation (ENISA, 2015).

3.2 Exercise Design

This section describes the preparation and requirements scenario design, participant setup and infrastructure setup.

3.2.1 Preparation and Requirements

In this phase, one has to identify the aims and learning goals of the exercise. For example: Should they play themselves or a persona? Should they face easy or difficult situations? Should they experience difficult decisions? Once the objectives, learning goals and overall settings (e.g., target audience, duration) are specified, the scenario design may start.

3.2.2 Scenario Design

In general, a cyber exercise consists of a scenario (often in literature also referred to as playbook). A scenario can consist of one or more stories. For example, a scenario of a critical infrastructure consists of a first story about a ransomware attack and a second story about a phishing campaign against employees. The number of stories, however, need to be carefully considered (see the discussion below on a good scenario). Each story can be further divided into injects. An inject is a piece of information or question that the participants receive and progresses the scenario of the exercise. An inject is later represented as a single slide (see implementation in Section 3.3). The injects can be arranged in any arbitrary sequence. Figure 1 depicts an example scenario that includes two story lines and several injects. It shows that there are injects that consist of text, images or polls. This list of injects does not have to be exhaustive. In future exercises, new injects might be added (e.g., video injects).

What Contributes to a Great Scenario? Saying “*let’s start crafting a scenario*” is in general easy to say but the actual steps to develop a scenario are in the beginning often challenging for inexperienced exercise organizers. Unfortunately, it takes some experience to learn and know where the pitfalls are. As part of the lessons learned, we would like to share our experience. A great scenario is one that is...:

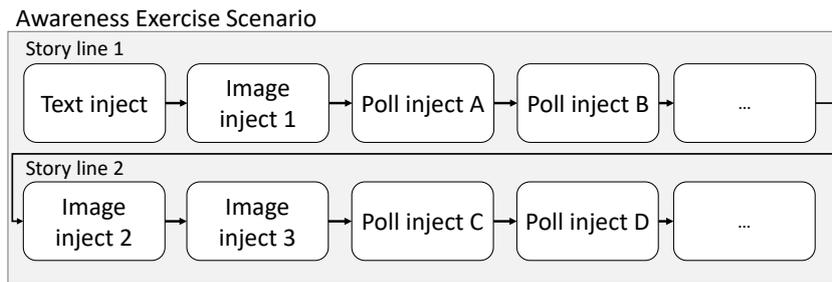


Figure 1: Scenario Design Schema.

- **captivating:** The participants should be thrilled and focus on the exercise.
- **interactive:** The participants have the ability to be part of the exercise by making decisions and participating actively.
- **informative:** The participants will receive instantly feedback to their decisions. In particular, they will see instantly (or if the moderator releases) the results of all participants.
- **anonymous:** If the responses are visible, one cannot easily recognize the answer of another person. Hence, participants remain anonymous (unless their name or another personally identifiable piece of information is written into an open text field).
- **security-aware:** The story should include one or more security incidents.
- **relatable:** The stories need to be relatable and should not be far away from the reality of the participants.

We achieved the best results by following this approach. However, the aforementioned aspects of a good scenario are part of several aspects to make the exercise interesting. For example, while the scenario is important to have interesting content, it is also important to formulate the questions in an understandable manner. The text should be adapted to the knowledge of the target audience. For instance, if the participants have not heard about certain terms such as malware or ransomware, then other descriptions might be used or the moderator explains the terms during the event. Other examples that are out of the scope of this paper are the moderator's style and qualities to guide the participants through the exercise (see e.g., (Brownell et al., 2006)).

3.2.3 Exercise Participant Roles

In our exercise, we suggest five roles. The *moderator* guides the participants through the scenario. They read the scenario, wait for enough responses and continue. The *support* helps the moderator by managing

the slide deck or by helping the participants to join the online system. The *participants* take part in the exercise and answer questions. *Observers* may oversee the exercise but do not interact with the participants. There may be a *technical staff* that supports the setup of the local infrastructure.

These five suggested roles are flexible. Moderator and participants are the mandatory roles for this cyber security exercises. However, additional roles might come in handy if there is a large target audience. Then, support, for example, is highly recommended. Or if the position of the moderator is not close to the device where the exercise application is controlled.

3.2.4 Infrastructure Requirements and Setup

The setup of the exercise is rather straightforward. A speaker setting at a conference or at a university is expected. Therefore, the main requirements for this exercise are: First, all participants have Internet-enabled devices (e.g., mobile phones or tablets). Secondly, the location should be able to provide Internet access to the number of participants. Third, there is a video wall that displays one screen at least. Fourth, speakers and a microphone are available in the location. Lastly, the software application for the exercise is accessible from the location (e.g., via Internet browser).

3.3 Proof-of-Concept Implementation

3.3.1 Implementation Choice and Selection

When the scenario is specified, the implementation of the exercise is the next phase. In the following, we summarize how we selected an implementation or proof-of-concept for our methodology.

There are several options to develop a software application that can support our proposed methodology. First of all, it is possible to develop its own software application. This option would allow maximum support of many features. However, for some organizers the development of its own application would require a lot of resources. As there was a time constraint, in

our case, a faster solution was preferable. Second, we investigated software applications that support digital surveys or polls (e.g., LimeSurvey¹, SurveyMonkey²). We found that LimeSurvey and SurveyMonkey are very helpful for preparing and processing surveys. However, in a setting where we aim to display text and images to tell a story, survey tools provide only limited support. Third, in the past years, several cloud-based applications have been developed that focus on supporting interactive meetings with presentations such as Mentimeter³ or Slido⁴. These tools allow the support of text or image-based presentation slides and provide also features for dynamic polls. For example, participants take part in a poll that is outlined on a slide and the voting results are shown instantly (or when the moderator releases them to the audience). These applications support the sequence of injects but do not support decision points where different injects would be selected afterwards. Also these meeting applications often provide means that (external) participants can join the presentation such as by using a PIN or a QR code. Forth, other online video call software such as BigBlueButton⁵ provide surveys in their respective applications. For example in BigBlueButton, the survey can be conducted but have limitations such as no support to integrate or upload pre-designed polls. In our methodology where we plan to have 20 or more polls, this automated support would be needed to facilitate the creation of polls. Furthermore, the use of BigBlueButton would entail that the scenario and the polls are not visible in the same screen. In summary, there are various ways to develop an implementation for our proposed methodology. Many of them provide advantages and drawbacks to support the cyber security awareness exercise. However, the meeting and presentation applications seem to support the most features (e.g., dynamic polling, visibility of results, fast response) for our purpose.

In this paper, we have selected *Mentimeter*, a cloud-based meeting and presentation application that allows for dynamic polling, as an easy-to-use tool for implementing the scenario. Many other meeting and presentation applications might be also easily adaptable for our approach. Another reason why we have selected this application is that it is affordable and does provide a human-centered user interface not only

¹<https://www.limesurvey.org/> (last access: 29/08/2022)

²<https://www.surveymonkey.com/> (last access: 29/08/2022)

³<https://www.mentimeter.com/> (last access: 29/08/2022)

⁴<https://www.slido.com/> (last access: 29/08/2022)

⁵<https://bigbluebutton.org/> (last access: 29/08/2022)

for designing the injects but also for the participants when they join. The application also provides a responsive design that changes depending on the screen sizes or resolutions of the devices. Furthermore, it offers a wide variety of formats for the presentation slides (including figures, text, etc.) and allows multiple different visualizations for the results of the polls (e.g., bar chart, pie chart, point chart).

For the implementation of the scenario, we created one presentation deck and then added several slides. Each slide is then filled with text, images or polls depending on the scenario design. For example in Figure 2, we outline a text and image inject that introduces the exercise.



Figure 2: Text and Image Inject (Screenshot).

Participants can join the presentation by going to a website in the browser and entering a PIN code or by using a QR code that directly opens a URL in a browser. Once they have joined the presentation, they can see the same slide that the moderator shows. As participants might join with different devices, however, the slide and the polls might be displayed in a slightly different design. The application supports responsive design that handles the various screen sizes and resolutions.

3.3.2 Hosting the Exercise: Course of Action

The following sequence of actions is recommended to host this cyber security awareness exercise.

1. **Welcome:** The first inject consists of the title page.
2. **Exercise mechanics introduction:** This action introduces the exercise / game mechanics of the current exercise.
3. **Start and access the tool:** This action introduces the participants to the cloud-based implementation and how they can access it. They typically can join via PIN or QR code.
4. **Warm-up phase:** The warm up phase allows the

user to get familiar with the implementation and its user interface. Two to three questions are prepared that allow the user to play with the tool and get familiar. Many examples can be found on the web⁶.

5. **Start the scenario:** Then, the moderator starts the game and the first inject of the scenario is shown. The moderator narrates this inject and continues in case of text or image to the next one. For poll injects, however, the moderator should explain the question and poll and then wait for a few minutes until the majority has voted. For example, Figure 3 depicts a poll inject that shows the question and the responses. During this voting phase, the participants are free to discuss any matters with their neighbors. Once the voting has been done, the moderator can display the voting results. The moderator may take a few questions or opinions from the audience.
6. **End of scenario:** The scenario ends. The moderator provides an ending of the story lines and the scenario.
7. **Evaluation:** If the exercise is evaluated, questions could be still answered within the cloud-based implementation or utilizing another digital survey
8. **Conclusion:** The exercise is concluded and all the participants are thanked for their participation.

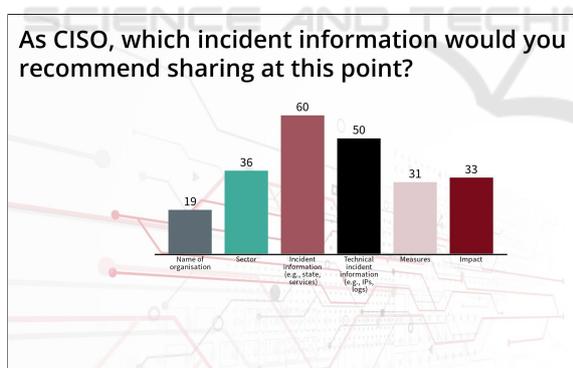


Figure 3: Scenario: Poll inject with Results (Screenshot).

As can be seen from the list, only after a thorough introduction and warm-up phase, the scenario is started. The reason behind this is that the participants should feel taken care of and not overwhelmed when starting the exercise. They will work on complex situations in the scenario, so they should be able

⁶<https://www.mentimeter.com/blog/awesome-presentations/85-poll-questions-for-every-occasion> (last access: 09/08/2022)

to not stress (a lot) about the application and how to participate in the exercise.

Another highly relevant aspect is the ending of the scenario and the story lines. It is frustrating if the end of a scenario is short and not well-explained. Often, participants feel left alone or that something is still missing. However, it is important to close the story lines. In reality the story lines also end somewhere and not just vanish.

After the end of the scenario, there is always the possibility to assess its impact or learning in the evaluation phase in the next section.

3.4 Evaluation

In the evaluation phase, the participants may receive an online survey or answer several questions at the end of the actual exercise in the cloud-based application.

There are several advantages to use the same application at the end of the exercise. First of all, the participants are still at the exercise and are highly likely to answer few more questions. As the participants see only the same slide as the moderator, the challenge is here for the moderator to give enough time to let the participants answer and not bore the others. In a professional survey tool, this is different as the participants may respond in their own speed. The second aspect is that given these aforementioned limitations, it is crucial to not ask too many questions as people might leave or close the browser earlier. Lastly, our experience show that less participants respond to a survey sent out right after the exercise. However, they are motivated to answer more questions than in the location of the exercise using the cloud-based application.

4 CASE STUDIES

This section aims to validate our proposed methodology with four cases. It outlines the use cases, the example scenario, the main findings and lessons learned.

4.1 Overview of Cases

Our cyber security awareness exercise has been conducted since 2017. Over 400 participants have participated in the exercise. To exemplify our findings, we will outline four cases. They are very similar in the utilized design but have slightly different arrangements in the group discussions in the voting phase. In this paper, we outline four cases:

1. **EU Conference:** A European conference for stakeholders from academia, industry and government was targeted. However, as the conference had 120 and more participants, we changed the discussion-setting. Section 3.3.2 describes that there can be an open discussion between the moderator and the audience once the voting has ended. This is a challenging task for large crowds and could depend also on the moderators experience. Therefore, we changed the open discussion into a group discussion of two or three seat neighbors.
2. **National Conference:** A very similar scenario was verified at the national conference for information security for stakeholders from academia, industry and government of a European Member State. Compared to case 1, the number of participants was smaller and an open discussion was conducted.
3. **Operator of Essential Services:** This exercise was conducted for an organization that aimed to raise awareness within the management. In total, 10 managers from different departments participated in order to discuss security incidents and response measures. As the participant number was 10, we switched to a very open and motivated discussion on security challenges within the whole group of participants.
4. **Academic Conference:** This exercise was held at an academic European conference with focus on e-government. The participants of this exercise were students and academics from various backgrounds (e.g., political science and social sciences). An open discussion was conducted.

4.2 Example Scenario

The scenario of the four cases consisted of a fictive story about a fictive energy provider in a fictive EU Member State that faces a cyber attack. In each case study, the content of the scenario changed gradually as we incorporated the feedback and tried to improve the scenario.

The scenario consists of five stories. In this example, stories are not fully independent of each other but more corresponding and dependent on each other, similar to chapters in a book. Each story consisted of about two to four slides. The first story introduced the EU Member State and the energy provider such as infrastructure and personnel of the organization. Second, investing into capabilities and how the participants, as responsible person for information security, would allocate the investments (e.g., training, consulting, outsourcing) was investigated. Third, indications

of a cyber attack could be found. The participants investigate the situation and further report the incident within the organization. Forth, information sharing is discussed, for example if information is shared formally or informally. Fifth, in light of the incident, it is investigated if there are capabilities that are immediately needed and which.

4.3 Findings and Lessons Learned

Throughout our conducted cyber security awareness exercises, we have received an overwhelmingly positive and constructive feedback. In the following, we will investigate the findings from the participant and the organizer perspective.

Participants Perspective. Different stakeholders such as students, professionals (from IT and security), civil servants and scientists have participated and tested this cyber security awareness exercise. Due to confidentiality reasons, it is not possible to disclose more details to the evaluations. To present the responses in some way in this paper, we will summarize the main points. In general, the participants liked the novel idea by actively making decisions with dynamic polls throughout the cyber security awareness exercise. Furthermore, the fast response during the interactions was highly accepted. The participants often liked the scenario but had suggestions on the duration and the content in order to improve it. Many liked the discussion-based style that allows the participants to discuss their choices with everyone or a neighbor.

Responses from participants varied between their personal need to invest in cyber security preventive measures such as *"I need to do a backup"* to comments about the methodology and the setup of the exercise e.g., *"I like what I have seen and I have understood now why you have chosen to do a neighbor-based feedback instead of an open discussion"*. In summary, in each cycle we have tried to improve the exercise more based on these feedbacks. This feedback also was reflected in the number of participants. Many stayed until the end of the session. Often, the scenario stipulated many more questions (e.g., *"Whom do I contact if I have a data breach?"*) which found us many times going over time.

Organizer Perspective. The idea and implementation was introduced to at least four people by the author who are now actively working on these awareness exercises. First of all, the cloud-based implementation was introduced and an example exercise slide deck shown. This introduction did often not last

more than 10 minutes. This short amount of time indicates that the hand-over is straightforward. The author received often the feedback that this setup was very easy to use and highly reusable for new scenarios. This reflects partly the user interface and the responsive design of the cloud-based application. Since the introduction, our methodology has been picked up as a method for cyber security education in several research projects.

4.3.1 Discussion

With the use cases, the methodology has been demonstrated to be feasible and valuable. The methodology has several advantages such as the ease of use, the fast implementation of scenarios, the facile interaction with various target groups and the others aforementioned in the perspective of participants and organizers.

The limitations of this methodology strongly depends at the moment on the functionality that the proof-of-concept implementation provides. For example, with the presented proof-of-concept only sequential stories are supported and only the provided interaction types and visualizations can be used. With cloud-based implementations, the authors are limited to the functionality these are providing. Furthermore, even with the best proof-of-concept implementation, the success of the exercise depends also strongly on the quality of the scenario, i.e. how captivating and interesting it is to the audience (see Section 3.2.2). Even the best implementation cannot make an awareness exercise interesting, if it is not adequate for the target audience. The success of an exercise also includes trial runs. Hence, how to deal and provide great scenarios for diverse target groups could be of interest in future work.

5 CONCLUSION

A methodology for a strategic cyber security awareness exercise was presented that is based on dynamic surveys. This allows participants to make active decisions. The results of their and the other participant's decisions are shown anonymously in an instant. This exercise provides a low-barrier entry for participants and is easy to set up for organizers. We have described the exercise design including the requirements and hints for captivating scenarios. We demonstrated the methodology with a cloud-based implementation and validated it with four case studies. In general, highly positive feedback was received. Particularly, the inter-activeness of the responses is highly valued

by the participants. For future work, we aim to extend the methodology and validate it with diverse target groups.

ACKNOWLEDGEMENTS

The project INDUCE is funded by the National Foundation for Research, Technology and Development and the "Österreich-Fonds". Laura Bassi 4.0 is a research, technology and innovation funding programme processed by the Austrian Research Promotion Agency, with kind support of the Federal Ministry of Labour and Economy (BMAW).

The author thanks T. Pahi and K. Bointner for motivating discussions during the development of the initial methodology. Also, the author would like to thank all participants of the exercises and exercise organizers who have tried this methodology.

REFERENCES

- Andreolini, M., Colacino, V. G., Colajanni, M., and Marchetti, M. (2020). A framework for the evaluation of trainee performance in cyber range exercises. *Mobile Networks and Applications*, 25(1):236–247.
- Angafor, G. N., Yevseyeva, I., and He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and privacy*, 3(6):e126.
- Beuran, R., Pham, C., Tang, D., Chinen, K., Tan, Y., and Shinoda, Y. (2017). Cytro: An integrated cybersecurity training framework. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy, ICISSP 2017, Porto, Portugal, February 19-21, 2017*, pages 157–166. SciTePress.
- Brilingaitė, A., Bukauskas, L., and Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security*, 88:101607.
- Brownell, M. T., Adams, A., Sindelar, P., Waldron, N., and Vanhover, S. (2006). Learning from collaboration: The role of teacher qualities. *Exceptional children*, 72(2):169–185.
- Byrne, E. T. and Wolfe, D. E. (1974). The design, conduct and evaluation of a computerized management game as a form of experiential learning. In *Developments in Business Simulation and Experiential Learning: Proceedings of the Annual ABSEL conference*, volume 1.
- Cheung, R. S., Cohen, J. P., Lo, H. Z., and Elia, F. (2011). Challenge based learning in cybersecurity education. In *Proceedings of the International Conference on Security and Management (SAM)*, page 1.
- Daimi, K. and Francia III, G. (2020). *Innovations in Cybersecurity Education*. Springer.

- Denning, T., Lerner, A., Shostack, A., and Kohno, T. (2013). Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In *Proc. of the 2013 ACM SIGSAC CCS, Berlin, Germany*, pages 915–928. ACM Press.
- ENISA (2015). The 2015 Report on National and International Cyber Security Exercises. Technical Report 1.0, European Union Agency for Network and Information Security (ENISA), Heraklion, Greece.
- Frank, M., Leitner, M., and Pahi, T. (2017). Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education. In *Proc. of the 2017 3rd IEEE CyberSciTech*, pages 38–46. IEEE.
- Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., and Naqvi, S. A. (2019). The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game. *IEEE Transactions on Software Engineering*, 45(5):521–536.
- Gentry, J. W. (1990). What is experiential learning. *Guide to business gaming and experiential learning*, 9:20.
- Hendrix, M., Al-Sherbaz, A., and Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training? *International Journal of Serious Games*, 3(1).
- Katsantonis, N. M., Kotini, I., Fouliras, P., and Mavridis, I. (2019). Conceptual framework for developing cyber security serious games. In *2019 IEEE Global Engineering Education Conference (EDUCON)*, pages 872–881. IEEE.
- Kucek, S. and Leitner, M. (2020). An empirical survey of functions and configurations of open-source capture the flag (ctf) environments. *Journal of Network and Computer Applications*, 151:102470.
- Leitner, M., Frank, M., Hotwagner, W., Langner, G., Maurhart, O., Pahi, T., Reuter, L., Skopik, F., Smith, P., and Warum, M. (2020). AIT cyber range: flexible cyber security environment for exercises, training and research. In *Proceedings of the European Interdisciplinary Cybersecurity Conference*, pages 1–6.
- Peker, Y. K., Ray, L., Da Silva, S., Gibson, N., and Lamberson, C. (2016). Raising cybersecurity awareness among college students. In *Journal of The Colloquium for Information Systems Security Education*, volume 4, pages 1–17.
- Pham, C., Tang, D., Chinen, K.-i., and Beuran, R. (2016). Cyris: A cyber range instantiation system for facilitating security training. In *Proceedings of the Seventh Symposium on Information and Communication Technology*, pages 251–258.
- Sanders, K., Boustedt, J., Eckerdal, A., McCartney, R., and Zander, C. (2017). Folk pedagogy: Nobody doesn't like active learning. In *Proceedings of the 2017 ACM Conference on International Computing Education Research*, page 145–154. ACM.
- Sedjelmaci, H., Hadji, M., and Ansari, N. (2019). Cyber security game for intelligent transportation systems. *IEEE Network*, 33(4):216–222.
- Tioh, J.-N., Mina, M., and Jacobson, D. W. (2017). Cyber security training a survey of serious games in cyber security. In *2017 IEEE Frontiers in Education Conference (FIE)*, pages 1–5. IEEE.
- Vigna, G., Borgolte, K., Corbetta, J., Doupé, A., Fratantonio, Y., Invernizzi, L., Kirat, D., and Shoshitaishvili, Y. (2014). Ten Years of iCTF: The Good, The Bad, and The Ugly. In *Proc. of the 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education*, page 7. USENIX Association.
- Vykopal, J., Vizvary, M., Oslejsek, R., Celeda, P., and Tovarnak, D. (2017). Lessons learned from complex hands-on defence exercises in a cyber range. In *Proc. of the 2017 IEEE Frontiers in Education Conference (FIE), Indianapolis, IN, USA*, pages 1–8. IEEE.
- Wellington, W., Faria, A. J., and Jr., R. O. N. (1996). An empirical investigation into the nature of the learning process in a computer-based simulation game. *Marketing Education Review*, 6(3):15–28.
- Werther, J., Zhivich, M., Leek, T., and Zeldovich, N. (2011). Experiences In Cyber Security Education: The MIT Lincoln Laboratory Capture-the-Flag Exercise. *Proc. of the 4th conference on Cyber security experimentation and test (CSET)*, page 9.