AI-Driven Communication Training for Cybersecurity with the Talk to Transform Simulator

Friederike Lindauer, Martha Damus, Carmen Winkel, Katharina Frosch

Suggested citation:

Lindauer, Friederike, Martha Damus, Carmen Winkel, and Katharina Frosch. 2025. "AI-Driven Communication Training for Cybersecurity with the Talk to Transform Simulator." In *KI-Forum 2025 : KI in Forschung und Lehre an Hochschulen*, edited by Hanno Homann, Cedric Rohbani, and Jens Christian Will, 106–13. Hannover: HsH Applied Academics. https://doi.org/10.25968/opus-3790.

Abstract

Effective communication skills are increasingly recognized as critical for leadership in digital transformation contexts. Recently, AI-Chatbots such as Talk to Transform (T2T) have been developed to enhance leadership competencies through interactive role-plays and feedback. This paper proposes their adaptation for cybersecurity training. We discuss the current landscape of cybersecurity training, highlight the importance of communication, and present T2T as an innovative approach to bridge this gap through chatbot-driven role-plays.

AI-Driven Communication Training for Cybersecurity with the Talk to Transform simulator

Friederike Lindauer[*], Martha Damus[†], Carmen Winkel[‡], Katharina Frosch[*]
Brandenburg University of Applied Sciences
[*]*Department of Business Management,* [†]*Digitalization of teaching,* [‡]*Project SCALE-C*

***Abstract*—Effective communication skills are increasingly recognized as critical for leadership in digital transformation contexts. Recently, AI-Chatbots such as Talk to Transform (T2T) have been developed to enhance leadership competencies through interactive role-plays and feedback. This paper proposes their adaptation for cybersecurity training. We discuss the current landscape of cybersecurity training, highlight the importance of communication, and present T2T as an innovative approach to bridge this gap through chatbot-driven role-plays.**

***Index Terms*—Cybersecurity training, role-play, simulation-based training, organizational learning, AI-chatbot**

I. Introduction

Communication plays a crucial role in navigating digital transformation within organizations. In their digital skills framework, Bouwmans et al. highlight that employees need to be "proficient in crafting compelling narratives that captivate audiences ... with the goal to persuade or inspire others" [1, p. 27]. Complementing this perspective, research on strategic internal communication [2] demonstrates that traditional, synchronous communication methods remain highly relevant in the digital age: Leaders frequently employ information-rich, face-to-face interactions during organizational transformations, and this approach correlates positively with employee satisfaction. This underscores the importance of effective communication in engaging stakeholders during digital change processes. Moreover, communication is considered an integral part of knowledge transfer and persuasion of employees, which suggests integrating communicative aspects during the learning process.

While often seen as a technical field, many cybersecurity risks stem from human behavior, with the literature underscoring that breaches frequently result not from technical flaws but from human error, miscommunication, and unclear responsibilities.[3]. The growing frequency and complexity of cybersecurity incidents indeed highlight the critical need for effective communication and clarity within organizations.

Recent findings underscore that even younger, digitally fluent employees are increasingly uncertain about their ability to handle emerging cybersecurity threats. According to a 2024 survey of 1000 American employees by Ernst & Young, 72% of Gen Z employees reported having clicked on a suspicious link at work, while only 31% expressed strong confidence in recognizing phishing attempts. Moreover, a significant portion of younger employees—64% of Gen Z and 58% of Millennials—admitted fearing job loss if they inadvertently triggered a security incident [4]. These results point to a critical gap in technical awareness. This highlights the urgent need for training formats that not only raise awareness but also empower employees to respond confidently in real-time situations. Cybersecurity leadership particularly demands strong communication skills for effective risk management and security culture cultivation [5]. However, traditional training methods are not only costly and time-consuming but also often fail to sustainably change behaviors [6]. This emphasizes the need for innovative, interactive approaches, in particular, scalable, AI-supported or interactive solutions to address these constraints [6].

Building on previous work in leadership training, this paper explores how the T2T chatbot-based simulation can be adapted for cybersecurity education [6,7]. We illustrate this through a concrete use case focused on phishing awareness and dialogue-based behavior change. We refer to this format as 'T2T' and introduce an extension called 'T2T-Cy' focused on cybersecurity topics. T2T is a digital training format that uses an AI chatbot to simulate realistic conversations between leaders and employees. It guides learners through a structured process of preparation, role-play, and feedback to improve communication. For the application of T2T, AI chatbots are key. We define them as "generative AI software using machine learning, that responds automatically to (users') messages in a natural language"[7, pp. 142–143]. These chatbots have become part of modern education, with various studies underlining their potential to improve the educational experience [8,9,10] as well as learning outcomes [11].

To thoroughly connect T2T to cybersecurity training, we will first look at cybersecurity training and analyze possible gaps in research (second section). In the third section, we look at the T2T as an AI-based communication training format and elaborate on the previously applied use case in leadership communication. The fourth section analyzes how the T2T approach could be beneficial for cybersecurity training and presents a hands-on use case. Lastly, we discuss further AI-Chatbot approaches for cybersecurity training as well as the limitations.

II. Bridging the Gap: The Role of Communication in Cybersecurity Training

Cybersecurity training has been and will be one of the most important approaches to mitigate the risks of complex cyberthreats and incidents to individuals and organizations [6]. The issue is gaining importance due to its cross-sectional nature; cybersecurity is not the task of specialists but of every member within an organization. Therefore, education and development in this field need to be tailored towards different target groups, besides IT-specialists and cybersecurity experts, also towards the so-called end users, which would be an average employee, but also students and employees in sectors such as healthcare and other areas of critical infrastructure [12,13,14].

Cybersecurity training typically pursues several goals. It aims to protect against threats, reduce typical human error building competences, knowledge and behavior change [15,16,17,18]. There are different formats of training in the cybersecurity field, e.g., classical approaches like presentations, lectures, text-based materials, or e-learning [14,16,19]. On the other hand, there are also more innovative approaches, e.g., serious games, context-based micro training, virtual labs, or AI-assisted learning [14,16,19]. Even though the cybersecurity training and development landscape seems to evolve towards more innovative approaches, there are still fundamental gaps in research, e.g.:

- Focus on technical aspects rather than pedagogy and interpersonal skills [17,20]
- Many current training approaches are not based on empirical evidence of their effectiveness or sound theories [12]
- There is a lack of clear, quantifiable metrics to measure the actual impact of training programs on threat and incident reduction [21]

Focusing on the three presented gaps – a numbering that does not claim to be complete - one thing becomes clear: there is a lack of interdisciplinary approaches in the cybersecurity field. The integration of pedagogical, educational, and psychological aspects into cybersecurity training goes beyond the core technical cybersecurity knowledge. If we focus on the first of the named gaps, the advances of AI and chatbots could provide a cost-efficient and low-threshold way of training soft skills via chatbot formats. Two recent studies in the field of cybersecurity training show that chatbots can support the development of effective communication skills, e.g., regarding active listening and communication of complex technical information clearly and concisely, by offering a conversational training format where knowledge and skills are acquired through dialogue and interaction [17,22]. Such conversational training formats are also promising because, up to now, there is a lack of training approaches in many cybersecurity training scenarios that help to practice communication strategies or to understand communication frameworks, although communication is essential for knowledge transfer and persuasion [23]. Furthermore, there are communication barriers between cybersecurity experts and non-technical users, often due to a lack of common ‘language’ [24], an issue that conversational learning with a chatbot could simulate and improve. In this regard, the field of cybersecurity could learn from the leadership-communication training approaches with chatbots, e.g., the T2T format.

According to Triplett, “leaders are an often-overlooked human factor influencing an organization's vulnerability to cyberattacks” [25]. Therefore, it is inevitable to not only train them in matters of cybersecurity but to convince them to be an advocate for cybersecurity within the organization. To advocate for cybersecurity within the organization, leaders need to communicate regularly on current issues to make individuals more sensitive [26]. Additionally, leaders can support employees in understanding cybersecurity strategies and ensure they participate in the provided training programs [25,27,28]. As emphasized by the Ernst and Young report, cybersecurity is no longer a purely technical matter but a leadership issue that requires transparent, organization-wide communication to build a culture of resilience. Therefore, training leadership communication should be viewed as a key intervention point in developing effective cybersecurity cultures, since humankind and cybersecurity are inseparable [4,25].

III. T2T: An AI-Based Communication Training Format

To better understand how chatbot-based simulations like T2T can support communication training, this section outlines the structure and pedagogical foundation of the original T2T format. Its core methodology combines didactically guided workshops, chatbot-based role-play and structured reflection. This combination can be exciting for learners in a positive sense. But also, it can be demanding and challenging. Therefore requires – on the developer side – an in-depth understanding of educational principles, technological capabilities, limitations, and data protection.

First evaluation results from the original T2T training suggest high learner satisfaction and perceived learning gains in communication skills. When compared to a control group using traditional face-to-face role plays, learning outcomes were similar, indicating that the chatbot based approach can be equally effective. These findings provide an initial basis for assuming that T2T-Cy may also be effective in promoting communication awareness and behavioral reflection in cybersecurity contexts.

a) Didactic Design and Feedback System

The T2T simulator is based on a large language model (GPT-4o) and uses prompt-engineered role profiles to simulate employee responses in realistic leadership conversations. In contrast to generic chatbot use, T2T integrates the AI into a pedagogically framed process: each conversation includes briefing, interaction, automated feedback, and structured reflection. The simulation is embedded in a broader didactic setting and serves not only for practice but also provides feedback and encourages self-assessment and reflection. The prompt design followed an iterative approach of the whole team. Learning through rapid-prompting, testing, reflecting, and re-prompting. The final prompt was quite long and very detailed (see Table 1 for excerpts of the prompt). The T2T simulator acts as a role player for different scenarios within an organization, in our case, the role of the employee.

By training with the T2T simulator, learners take on the role of a supervisor and practice their leadership communication skills with an AI-powered chatbot that first acts as a team member and then provides feedback on the quality of the learners' communication strategies. Interaction between learners and the chatbot takes place exclusively through text. [29]. The used scenarios are derived from reallife organizational case studies and focus on leadership, feedback conversations, and conflict resolution. Learners interact with the AI-Chatbot to experience dynamic dialogue situations and receive targeted feedback on their communication performance [Fig. 1]. The training particularly addresses 'Future Skills' such as feedback literacy, agility, and adaptive leadership in disruptive contexts.

The concept follows a 'Reflect–Act–Reflect' logic, in which learners engage in individual reflection before and after simulated dialogues with a text-generative AI. By personalized, context-sensitive feedback, learners are enabled to refine their techniques in a supportive environment [30]. For example, the T2T simulator gives learners reflection questions and displays text passages from the conversation that are marked as good and bad practices. This provides learners with starting points for individual improvements in the next conversation.

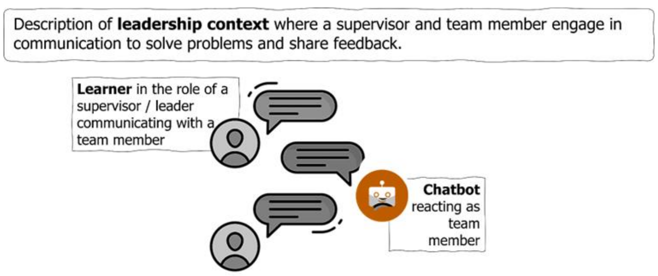

Figure 1. Conversational Design T2T

The T2T format is rooted in experiential learning theory and emphasizes metacognitive development by promoting self-observation and communication awareness. Reflection prompts and feedback loops guide learners to assess their own conversational strategies and to iterate on improvement [30]. Importantly, this approach provides an opportunity to bridge theoretical content and practical communication competencies.

b) *Technical Implementation and Data Protection*

The T2T was implemented on the fobizz-plattform a GDPR-compliant digital learning platform for teachers, that offers an interface to prompt agents using state-of-the-art LMMs. T2T utilized Open-AI GPT4.0 and made use of different personas with a range of employee archetypes. To enhance a human-like conversation, the personas signaled non-verbal cues in brackets within the dialogue (e.g., "[nods slowly]", "[sighs]"). Designing the cues, personas, and scenarios outlined above requires a sound understanding of the AI software's technical capabilities and limitations to ensure an effective and safe learning experience. In addition, AI chatbots facilitate conversations across various languages and help alleviate the discomfort often associated with face-to-face interactions. This makes them a good choice also for international students, beginners, or shy learners [31].

However, these systems also have limitations. AI models may struggle with understanding context or nuances in human communication, such as sarcasm or cultural subtleties [32]. Additionally, they rely heavily on the quality and diversity of the training data, which can lead to biases if not adequately addressed. Furthermore, technical issues like latency, data privacy concerns, and the need for robust infrastructure can cause challenges. Consequently, within the T2T project, an introductory manual was developed to raise awareness of these issues and to draw attention to the functional limitations and ethical use of AI. To ensure data protection, a national tool provider was chosen that acts as an interface to major large language models (LLM) providers and encrypts the learner data. Technical problems were handled and 'caught' by human personnel of the university.

c) *First Application Scenarios in Practice*

In December 2024, the T2T format was piloted with 30 students from a management degree program at a German university of applied sciences. The training was integrated into a regular seminar and accompanied by a qualitative and quantitative evaluation. Students received a communication task that involved delivering negative feedback in a challenging leadership situation, using a role-play scenario with an AI chatbot. The chatbot impersonated for example a resistant employee and responded dynamically to the learner's communication style. [33]. Looking into the evaluation of the format, we see that the learner satisfaction with T2T and the self-assessment of the resulting learning outcomes were very positive [33]. In contrast to the control group, which received classical face-to-face role-plays, the T2T rankings revealed minimal differences, contradicting our initial expectations. The findings suggest that, in the context of student learning, there is minimal distinction between T2T and traditional face-to-face role-plays in terms of learner satisfaction and learning outcomes. The positive feedback from students has been a significant motivation for T2T, resulting in its testing with various non-academic user groups in professional development and continuing education programs. These tests have highlighted the system's scalability and adaptability to different learning environments [34].

IV. EXTENDING T2T TO CYBERSECURITY TRAINING - A NEW USE CASE

T2T is a promising innovative training for leadership communication that focuses on conveying communication skills like active listening, goal setting, etc. It embodies an approach that is based on sound theory, incorporates feedback, and, if desired, quantifiable metrics to measure the training's outcomes. Cybersecurity training frequently lacks quantifiable metrics and a solid foundation in sound theories from pedagogy and psychology. It is our professional opinion that an extension of T2T towards cybersecurity is an apparent solution to begin addressing the current gaps in the cybersecurity training research.

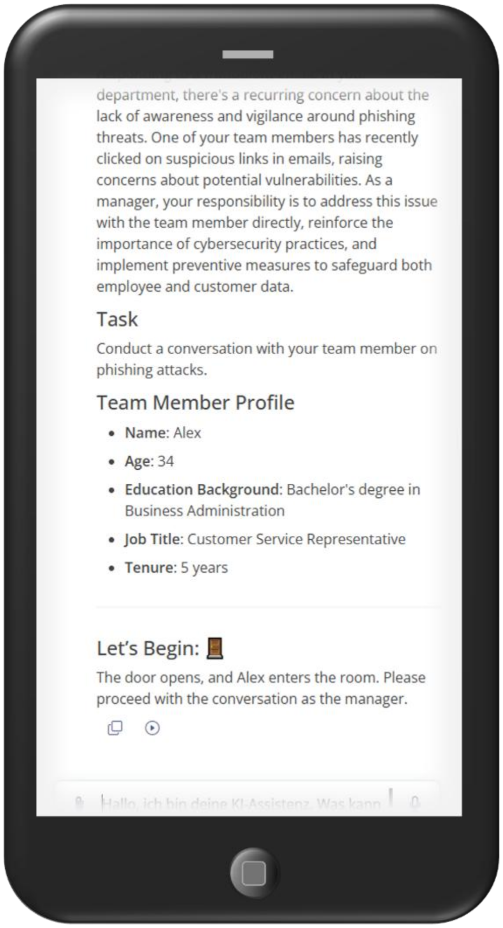

Figure 2. Start of the T2T-Cy role-play scenario

To address this, the T2T format has been adapted for awareness building in cybersecurity (T2T-Cy). In the updated version, leaders engage in a chatbot-based role-play with employees who don't take cybersecurity seriously. The objective is to practice how to raise awareness and encourage more responsible behavior through persuasive, dialogue-based interaction. The T2T-Cy includes, as an exemplary scenario, a realistic phishing conversation. The setup is similar to the T2T; the learners assume the role of a manager at a fictive organization, for critical infrastructure reasons, we chose a bank. To underline the differences between T2T and T2T-Cy contexts and conversational focus, we provide excerpts of the original prompts within Table 1.

In the beginning of the simulation, the key aspects about the organization, the situation the manager needs to solve, and the information about the conversational partner are provided to the learner [Fig. 2]. In the T2T-Cy use case, the learners converse with one of their employees who has recently clicked on suspicious links in emails, leading to concerns about potential vulnerabilities at the organization. The learners as managers have the responsibility to address the issue with the employee and reinforce cybersecurity practices [Fig. 3]. As well as to implement preventive measures to safeguard both the employee and the customer. The employee is prompted to be resistant, disliking changes and new training. This makes it harder for the learners to convince the employee of their agenda, but likely makes it more realistic.

Table 1. Conversational Context – prompt excerpts

T2T	**T2T-Cy**
Title: termination of working contract, T2T Conversational context: Imagine you are a manager in a medium-sized company that develops board games. You lead an 8-member project team. One of the team members has repeatedly drawn attention over the past few months for arriving late and logging excessive work hours. Despite several warnings, the behavior has not improved, which has significantly disrupted the team's workflow. After careful consideration, management has decided that termination of employment is necessary in order to maintain team dynamics and work quality. As the manager, it is your responsibility to communicate the termination clearly and directly, and to issue it in a legally compliant manner. Explain the reasons for the decision and refer to the previous warnings in order to make the situation transparent.	Title: Phishing Conversational context: Imagine you are a manager of GreenBank Financial, (…) a mid-sized commercial bank offering a range of services including personal banking, business loans, and digital banking solutions. (…) GreenBank's IT department has recently observed a spike in phishing attempts targeting employees. (…) In your department, a recurring concern has emerged: lack of awareness and vigilance around phishing threats. One of your team members, has recently clicked on suspicious links in emails, raising concerns about potential vulnerabilities. As a manager, your responsibility is to address this issue with the team member directly, reinforce the importance of cybersecurity practices, and implement preventive measures to safeguard both employee and customer data.

Once the dialogue comes to an end, e.g., through a goodbye, the T2T-Cy takes the learner through a reflection [Fig. 4], asking different questions, e.g., “What was the biggest challenge during the conversation, and how did you handle it?” The reflection provides the space for learners to think about the conversation. From the reflection part, the T2T-Cy flow provides feedback [Fig. 5] to the learner based on the conversation. With the provided feedback, learners can find out about their strengths or mistakes, and they learn what they could have done to convince the employee. When learners engage with the T2T-Cy more than once, experiential learning will likely be triggered.

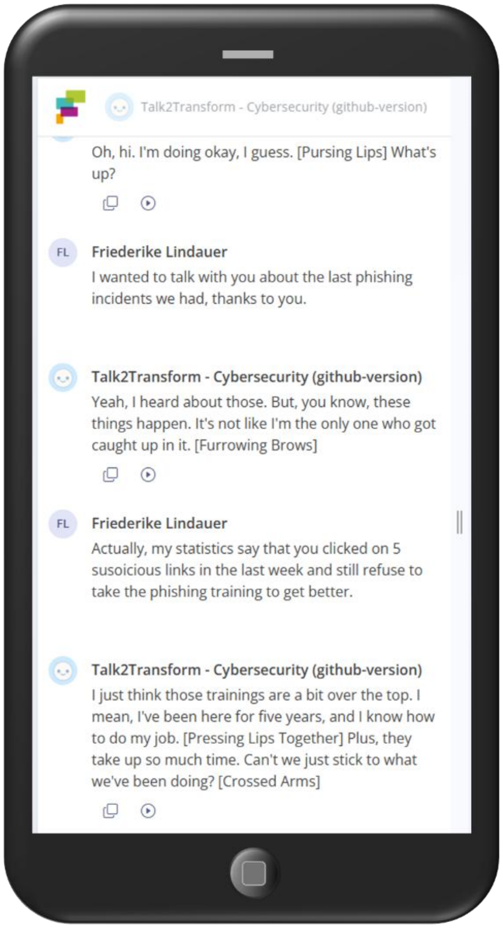

Figure 3. Excerpt from a T2T-Cy test run

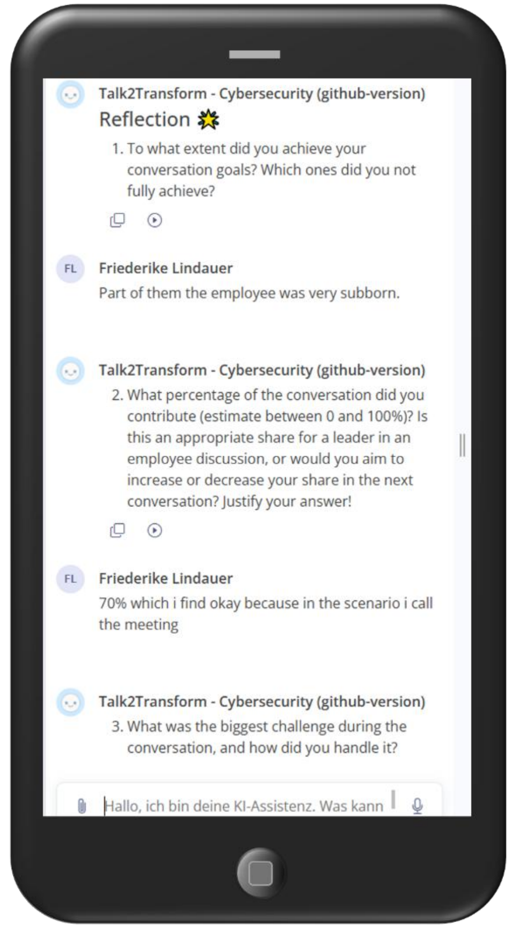

Figure 4. Excerpt of the T2T-Cy reflection flow

Research supports the value of such realistic training approaches: one study found that chatbot-based phishing simulations significantly improved learners' ability to detect fraudulent emails when active learning methods were used [23]. Another study showed that role-play exercises in small groups increased both learners' confidence and their willingness to report phishing attempts, suggesting that realistic simulations can foster not only awareness but also a proactive security culture [23].

The T2T-Cy was not yet tested with a larger user group, but from our experience with the previous version (T2T), we assume similar positive results. To measure the effects of T2T-Cy with the scale from Kron et al as well as from Nair, both scales rely on self-reporting [35,36]. Another aspect for evaluation are the conversation transcripts themselves. With qualitative analysis, the delta between different runs with the T2T-Cy can be analyzed by coding, e.g., active listening, motivational language, or providing feedback, etc. The reflection part of the simulation can provide additional qualitative data to offer a more nuanced view of the overall results. It should be noted that the T2T-Cy has not yet been tested in this regard, but such evaluation is planned.

Our approach and the mentioned training insights in the cybersecurity training field highlight the potential of AI-supported, conversation-based cybersecurity training to offer a psychologically safe environment in which employees can build and strengthen their communication skills. In order to scale the T2T chatbot-based training format for organizational cybersecurity education, considerations of technical feasibility and cost-efficiency are critical. Tymoshchuk et al. demonstrate that scalable simulation-based cybersecurity training systems can be successfully implemented using open-source tools and virtualized infrastructure [37]. For T2T-Cy, however, we rely on a classical Chat-GPT-like chat interface and the readily available tools at the university. In this regard, our approach is technically detailed but still on a lower threshold than open-source tools and virtualized infrastructure.

T2T-Cy approach supports personalized and modular scenario design while ensuring integration with real-world technologies. Scenarios can be updated rather quickly to new organisational contexts or new topics, e.g., secure passwords, which is essential to address the evolving cybersecurity landscape.

I. Future Research directions

T2T-Cy primarily focuses on awareness building for cybersecurity topics by building on the insights of T2T for leadership communication. Beyond the communication aspect of training, additional cybersecurity training approaches can be implemented using AI-Chatbots.

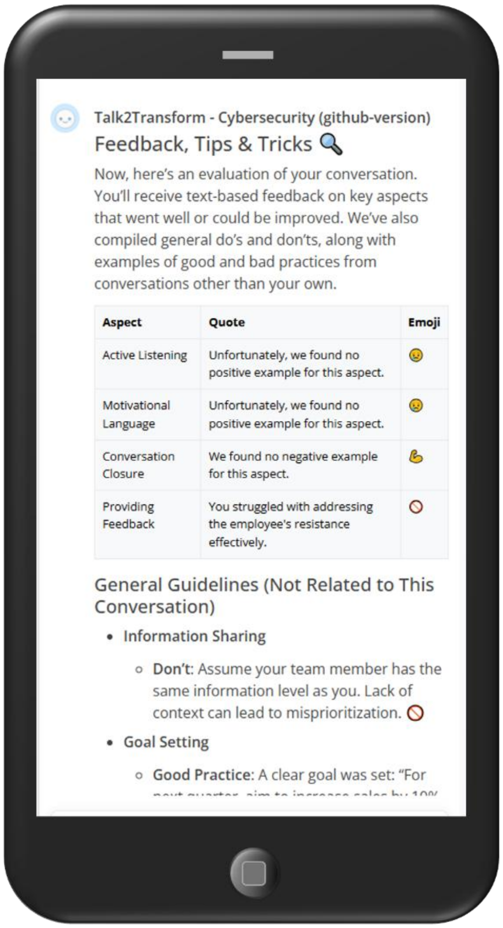

Figure 5. Excerpt of the T2T-Cy feedback flow

An example that is closely linked to communication and also with a management focus is incident response and crisis communication. It could be implemented in AI-Chatbot scenarios, including real-time crisis communication, coordination with IT teams, and stakeholder notification procedures during cybersecurity incidents. As research shows, clear and timely communication during incidents is essential for limiting damage and restoring trust, yet many are often insufficiently trained in classical security awareness programs [38].

For IT specialists and cybersecurity experts, training in the *analysis of ransomware messages and the prediction of ransomware threats* via an AI-Chatbot could have potential, especially to build an organizational routine and common understanding. Research indicates that while ChatGPT is already being utilized, at least experimentally, for the analysis and prediction of ransomware threats [39], the opportunity to turn it into a training approach seems to be less critical than relying on AI-Chatbots to do the analysis and prediction.

For end-users in an organization, AI-Chatbots could support training in the areas of, e.g., *identification of phishing or safe passwords* by generating good and bad practices that the end-users need to analyze, and in bad practice cases, identify, e.g., a phishing e-mail. A recent study shows a first application for phishing email identification training via chatbots in an experimental setting. The study also underlines the need of investigating this AI-Chatbot phishing identification further [40].

With these three examples, we want to underline the potential of AI-Chatbots for cybersecurity training that goes beyond the communication focus of the T2T format. As underlined in the cybersecurity section, cybersecurity training should integrate technical aspects, pedagogical aspects, soft skills [17,20], and base training on empirical evidence and sound theories from pedagogy, etc. [12]. To evaluate the actual training impact, quantifiable metrics should be applied [21]. Taking these gaps into account enhances cybersecurity training overall. By incorporating modern innovative training approaches like T2T or T2T-Cy, the field moves to training approaches that are possibly better perceived by learners, as our first tests indicate. However, further research is needed to gain a deeper understanding of how these approaches can be effectively applied, particularly in practical settings.

II. Limitations

AI-Chatbots continue to face significant challenges in understanding and appropriately responding to subtle contextual cues, such as sarcasm, emotion, or non-verbal signals. This limitation may hinder the authenticity of simulated dialogues and reduce the effectiveness of training [41]. In addition to that, we have not directly looked at the impact of the uncanny valley effect within our setup.

If Chatbots are used to train communication skills in organizations related to cybersecurity threats, sensitive information may be revealed by learners. Educational chatbots dealing with sensitive training content could become targets for attackers seeking unauthorized access to learner data, which poses significant privacy concerns and potential trust issues among users [42].

There remains the challenge of user engagement and acceptance of AI-driven training formats. Some learners may perceive chatbot interactions as less authentic or meaningful than human-facilitated training. It is therefore essential to integrate user feedback, adapt scenarios to organizational culture, and combine AI-based training with complementary face-to-face interventions for maximum impact [43].

Finally, our approaches T2T and T2T-Cy investigate modern training and learning formats with AI-Chatbots from a rather positive side. For future studies, we also want Chatbot simulations alter our human-to-human interactions in the long term?

III. CONCLUSION

Communication remains a critical, yet frequently underutilized, element of cybersecurity awareness and training. This paper has argued that AI-supported formats such as T2T, originally developed for leadership communication training in higher education settings [29], hold considerable potential for the adaptation to cybersecurity. Given the increasing complexity of cyber threats, there is a growing demand for training formats that go beyond technical instruction and actively foster communicative aspects and learning transfer.

The T2T format, with its reflective learning cycle and chatbot-based dialogue simulations, provides a valuable foundation for developing cybersecurity-specific extensions (T2T-Cy). AI agents and chatbots open up multiple opportunities for scalable, personalized, and scenario-based training interventions, ranging from phishing identification to incident communication.

By integrating innovative training formats (e.g., T2T-Cy), organizations may be able to reduce vulnerabilities stemming from human factors and improve their internal communication cultures. Developing a shared communicative understanding and terminology for cybersecurity emerges as a key element in this endeavor. Looking forward, future development efforts aim to build upon these insights by further refining training formats that integrate both communicative, pedagogical, and technical dimensions of cybersecurity preparedness as well as respective soft skills.

ACKNOWLEDGMENTS

We would like to extend our appreciation to Prof. Dr. Michael Pilgermann for his constructive review and valuable feedback. We also recognize the contributions of Svenja Hädicke and Steffi Haberland, whose support and expertise were important in developing the T2T. Thank you for your efforts.

FUNDING

Three of the authors gratefully acknowledge financial support for the SCALE-C project - SeCure Model for semiAutomated LEarning Content in Cybersecurity, co-funded by the European Regional Development Fund and the State of Brandenburg (StaF programme, project reference: 86003742).

REFERENCES

[1] M. Bouwmans, X. Lub, M. Orlowski, and T.-V. Nguyen, “Developing the digital transformation skills framework: A systematic literature review approach,” *PLOS ONE*, vol. 19, no. 7, p. e0304127, Jul. 2024, doi: 10.1371/journal.pone.0304127.

[2] L. R. Men, “Strategic internal communication: Transformational leadership, communication channels, and employee satisfaction,” *Manag. Commun. Q.*, vol. 28, no. 2, pp. 264–284, 2014.

[3] M. Alshaikh, “Developing cybersecurity culture to influence employee behavior: A practice perspective,” *Comput. Secur.*, vol. 98, p. 102003, Nov. 2020, doi: 10.1016/j.cose.2020.102003.

[4] Ernst & Young LLP, “New EY research reveals cybersecurity fears are on the rise among US workers, with a vast majority concerned about AI in cybersecurity,” PR Newswire. Accessed: Jul. 01, 2025. [Online]. Available: https://www.prnewswire.com/news-releases/new-ey-research-reveals-cybersecurity-fears-are-on-the-rise-among-us-workers-with-a-vast-majority-concerned-about-ai-in-cybersecurity-302136735.html

[5] W. J. Triplett, “Addressing human factors in cybersecurity leadership,” *J. Cybersecurity Priv.*, vol. 2, no. 3, pp. 573–586, Jul. 2022, doi: 10.3390/jcp2030029.

[6] Blessing Austin-Gabriel, Adeoye Idowu Afolabi, Christian Chukwuemeka Ike, and Nurudeen Yemi Hussain, “AI and machine learning for adaptive elearning platforms in cybersecurity training for entrepreneurs,” *Comput. Sci. IT Res. J.*, vol. 5, no. 12, pp. 2715–2729, Dec. 2024, doi: 10.51594/csitrj.v5i12.1787.

[7] W. Holmes, “Artificial intelligence in education: Promises and implications for teaching and learning,” *Cent. Curric. Redesign*, 2019.

[8] O. M. Schei, A. Møgelvang, and K. Ludvigsen, “Perceptions and Use of AI Chatbots among Students in Higher Education: A Scoping Review of Empirical Studies,” *Educ. Sci.*, vol. 14, no. 8, p. 922, Aug. 2024, doi: 10.3390/educsci14080922.

[9] R. Zhang, Zou ,Di, and G. and Cheng, “A review of chatbot-assisted learning: pedagogical approaches, implementations, factors leading to effectiveness, theories, and future directions,” *Interact. Learn. Environ.*, vol. 32, no. 8, pp. 4529–4557, Sep. 2024, doi: 10.1080/10494820.2023.2202704.

[10] W. Ma, W. Ma, Y. Hu, and X. Bi, “The who, why, and how of ai-based chatbots for learning and teaching in higher education: a systematic review,” *Educ. Inf. Technol.*, Oct. 2024, doi: 10.1007/s10639-024-13128-6.

[11] R. Wu and Z. Yu, “Do AI chatbots improve students learning outcomes? Evidence from a meta-analysis,” *Br. J. Educ. Technol.*, vol. 55, no. 1, pp. 10–33, 2024, doi: 10.1111/bjet.13334.

[12] J. Prümmer, T. Van Steen, and B. Van Den Berg, “A systematic review of current cybersecurity training methods,” *Comput. Secur.*, vol. 136, p. 103585, Jan. 2024, doi: 10.1016/j.cose.2023.103585.

[13] R. Beuran, C. Pham, D. Tang, K. Chinen, Y. Tan, and Y. Shinoda, “CyTrONE: an integrated cybersecurity training framework:,” in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, Porto, Portugal: SCITEPRESS - Science and Technology Publications, 2017, pp. 157–166. doi: 10.5220/0006206401570166.

[14] Z. Batzos *et al.*, “Gamification and serious games for cybersecurity awareness and first responders training: an overview,” *MDPI*, pp. 1–20, 2023.

[15] S. Jawhar, J. Miller, and Z. Bitar, “AI-Driven Customized Cyber Security Training and Awareness,” in *2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC)*, Feb. 2024, pp. 1–5. doi: 10.1109/ICAIC60265.2024.10433829.

[16] Kävrestad, Joakim, “Context-Based Micro-Training Enhancing cybersecurity training for end-users,” University of Skövde, Schweden, 2022. Accessed: Jun. 25, 2025. [Online]. Available: ISBN 978-91-984919-9-9

[17] C. Kallonas, A. Piki, and E. Stavrou, “Empowering Professionals: A Generative AI Approach to Personalized Cybersecurity Learning,” in *2024 IEEE Global Engineering Education Conference (EDUCON)*, May 2024, pp. 1–10. doi: 10.1109/EDUCON60312.2024.10578894.

[18] S. Nasir, “Exploring the effectiveness of cybersecurity training programs: factors, best practices, and future directions,” *Adv. Multidiscip. Sci. Res. J. Publ.*, vol. 2, no. 1, pp. 151–160, Jul. 2023, doi: 10.22624/AIMS/CSEAN-SMART2023P18.

[19] A. Ahmed, C. Watterson, S. Alhashmi, and T. Gaber, “How universities teach cybersecurity courses online: a systematic literature review,” *Front. Comput. Sci.*, vol. 6, Dec. 2024, doi: 10.3389/fcomp.2024.1499490.

[20] D. Tang, C. Pham, K. Chinen, and R. Beuran, “Interactive cybersecurity defense training inspired by web-based learning theory,” in *2017 IEEE 9th International Conference on Engineering Education (ICEED)*, Kanazawa: IEEE, Nov. 2017, pp. 90–95. doi: 10.1109/iceed.2017.8251171.

[21] S. Parkar and D. K. Mishra, “Cybersecurity workforce development and training: a comprehensive review on the significance, strategies, opportunities and challenges,” in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, May 2024, pp. 1–5. doi: 10.1109/ISCS61804.2024.10581241.

[22] D. Fanta, F. Sajid, M. Masssoth, and L. Kruck, “Efficiency of an Artificial Intelligence-based Chatbot Support for an IT-Awareness and Cybersecurity Learning Platform,” 2022.

[23] C. Knight, “The Effectiveness of Cybersecurity Training,” University at Albany, New York, 2024. [Online]. Available: https://scholarsarchive.library.albany.edu/etd/90

[24] R. Shillair, P. Esteve-González, W. H. Dutton, S. Creese, E. Nagyfejeo, and B. Von Solms, “Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise,” *Comput. Secur.*, vol. 119, p. 102756, Aug. 2022, doi: 10.1016/j.cose.2022.102756.

[25] W. J. Triplett, “Addressing Human Factors in Cybersecurity Leadership,” *J. Cybersecurity Priv.*, vol. 2, no. 3, pp. 573–586, Jul. 2022, doi: 10.3390/jcp2030029.

[26] C. Şeker, “Cybercrimes in organizations: communication, trust, and leadership approaches,” *Int. Rev. Econ. Manag.*, vol. 13, no. 1, pp. 31–50, 2025, doi: http://dx.doi.org/10.18825/iremjournal.1687722.

[27] R. Müller and R. Turner, “Leadership competency profiles of successful project managers,” *Int. J. Proj. Manag.*, vol. 28, no. 5, pp. 437–448, Jul. 2010, doi: 10.1016/j.ijproman.2009.09.003.

[28] F. Hult and G. Sivanesan, “What good cyber resilience looks like.,” *J. Bus. Contin. Emerg. Plan.*, vol. 7, no. 2, pp. 112–125, 2014 Winter 2013.

[29] K. Frosch, S. Hädicke, M. Damus, S. Haberland, F. Lindauer, and C. Winkel, “Lehren mit KI: Talk2Transform (T2T),” *Hochschulforum Digit.*, vol. Arbeitpapier Nr. 87, no. Wie KI Studium und Lehre verändert, pp. 23–25, 2025.

[30] B. Yuan and J. Hu, “Generative AI as a Tool for Enhancing Reflective Learning in Students,” Dec. 03, 2024, *Institute of Electrical and Electronics Engineers (IEEE)*. doi: 10.36227/techrxiv.173324189.99227671/v1.

[31] M. Pears *et al.*, “Non-technical Skills for Urology Trainees: A Double-Blinded Study of ChatGPT4 AI Benchmarking Against Consultant Interaction,” *J. Healthc. Inform. Res.*, vol. 9, no. 1, pp. 103–118, Mar. 2025, doi: 10.1007/s41666-024-00180-7.

[32] Julanos, I. Hendriyani, I. Wulandari, and I. C. Kamsil, “Integrating Artificial Intelligence in English Teaching: Opportunities and Challenges in the Digital Classroom,” *J. Pedagogi*, vol. 2, no. 1, pp. 1–15, Feb. 2025, doi: 10.62872/9qgk5d12.

[33] K. Frosch, F. Lindauer, and C. Winkel, “Is Learning with an AI-Powered Chatbot for Everyone? A First Look at How Learning Preferences May Influence Learning Outcomes,” in *Learning in the Age of AI: Towards Imaginative Futures*, Bologna: Forthcoming, 2025. [Online]. Available: https://www.researchgate.net/publication/391781513_Is_Learning_with_an_AI-Powered_Chatbot_for_Everyone_A_First_Look_at_How_Learning_Preferences_May_Influence_Learning_Outcomes

[34] L. T. Wilhelm, X. Ding, K. M. Knutsen, B. Carik, and E. H. Rho, “How managers perceive AI-assisted conversational training for workplace communication,” May 21, 2025. doi: 10.1145/3719160.3736639.

[35] B. T. Nair, “Role play – An effective tool to teach communication skills in pediatrics to medical undergraduates,” *J. Educ. Health Promot.*, vol. 8, no. 1, Jan. 2019, doi: 10.4103/jehp.jehp_162_18.

[36] F. W. Kron *et al.*, “Using a computer simulation for teaching communication skills: A blinded multisite mixed methods randomized controlled trial,” *Patient Educ. Couns.*, vol. 100, no. 4, pp. 748–759, 2017.

[37] D. Tymoshchuk and V. Yatskiv, “Interactive cybersecurity training system based on simulation environments,” *Meas. Comput. Devices Technol. Process.*, no. 4, pp. 215–220, Nov. 2024, doi: 10.31891/2219-9365-2024-80-26.

[38] S. Abdelhamid, T. Mallari, and M. Aly, “Cybersecurity Awareness, Education, and Workplace Training Using Socially Enabled Intelligent Chatbots,” in *Creative Approaches to Technology-Enhanced Learning for the Workplace and Higher Education*, D. Guralnick, M. E. Auer, and A. Poce, Eds., Cham: Springer Nature Switzerland, 2023, pp. 3–16. doi: 10.1007/978-3-031-41637-8_1.

[39] H. Fujima, T. Kumamoto, and Y. Yoshida, “Using ChatGPT to Analyze Ransomware Messages and to Predict Ransomware Threats,” Nov. 22, 2023. doi: 10.21203/rs.3.rs-3645967/v1.

[40] S. Hobert, A. Følstad, and E. L.-C. Law, “Chatbots for active learning: A case of phishing email identification,” *Int. J. Hum.-Comput. Stud.*, vol. 179, p. 103108, Nov. 2023, doi: 10.1016/j.ijhcs.2023.103108.

[41] J. Krauter, “Bridging the uncanny valley: improving AI chatbots for effective leadership mentoring,” *Open J. Leadersh.*, vol. 13, no. 03, pp. 342–384, 2024, doi: 10.4236/ojl.2024.133021.

[42] J. Yang, Y.-L. Chen, L. Y. Por, and C. S. Ku, “A Systematic Literature Review of Information Security in Chatbots,” *Appl. Sci.*, vol. 13, no. 11, p. 6355, May 2023, doi: 10.3390/app13116355.

[43] S. V. Jin and S. Youn, “Social presence and imagery processing as predictors of chatbot continuance intention in human-AI-interaction,” *Int. J. Human–Computer Interact.*, vol. 39, no. 9, pp. 1874–1886, May 2023, doi: 10.1080/10447318.2022.2129277.