

## Idea 01 ms-final

Podcast script: Prof Margit Scholl, Technical University of Applied Sciences in Wildau (TH Wildau)  
Topic: Awareness Lab SME (ALARM) Information Security Training

### Script begins:

Hello and welcome to Research Pod! Thank you for listening and joining us today.

In today's episode, you'll be taken on an expedition into the world of information security, where people stand as the guardians of digital integrity. Today, homage is paid to the visionary mind behind the German "ALARM Information Security" project, Margit Scholl, at Technical University of Applied Sciences in Wildau (TH Wildau). With her pioneering spirit and unwavering dedication, Scholl—along with her research team and project partners—has sculpted a landscape where digitization harmonizes seamlessly with robust security measures.

In this podcast, we investigate the backdrop to breakthroughs in innovation, guided by Scholl's principles of security education: "Digitization only with information security. Information security only with awareness." You'll learn about the subject of Security Awareness, with an understanding of the significance of mindfulness.

From TH Wildau's research hub of education to the SME ecosystem, Scholl's influence is pervasive, shaping a paradigm where high-quality materials intertwine with strategic collaborations. Let's explore how psychology intertwines with cybersecurity!

// Music Break //

Chapter 1 of the German project documentation sets the stage for the "ALARM Information Security" project, introducing its comprehensive approach. From concept development and practical tests to awareness measurements and the building of a company-wide security culture, the objectives are clear. This chapter outlines a roadmap encompassing instructions for action, potential certifications for moderators, and sustainability considerations. It lays the groundwork for a holistic security strategy aimed at fortifying organizations to defend against digital threats.

In Chapter 2, the nitty-gritty of the procedures and methodologies employed in Professor Scholl's research project are explored. The focus here is on integrating various approaches to heighten information security awareness. It all starts with the foundation laid by in-depth psychological interviews conducted by project partner known\_sense. These interviews formed the basis of three pivotal studies, shedding light on the psychological landscape of information security.

From there, online surveys and international literature research were conducted by the TH Wildau research team. These endeavors helped to gauge the current state of information security awareness in SMEs.

Chapter 2 zooms in on the development and application of *analog* serious games in the increasingly digital world—an innovative means of raising awareness. Through extensive testing and feedback

sessions with various target groups, these analog learning scenarios were refined into their final versions. But analog isn't the only realm Prof Scholl explored. The project looks at the effectiveness of digital serious games, developed by Gamebook Studio HQ GmbH. These games serve as powerful supplementary tools for bolstering information security awareness, with additional iterative feedback ensuring their efficacy.

Continuing on, the author explored simulated "on-site attacks," a critical component of the integrative method mix. Developed and monitored by Thinking Objects GmbH, these simulations highlighted the importance of communication and prompted the derivation of low-threshold security concepts for SMEs.

Moving forward, Chapter 2 also introduces the "Security Self Check (SeSec)," a digital add-on designed for self-assessment. It's a supplementary method aimed at identifying knowledge deficits and closing security gaps through targeted training measures.

Toward the end of Chapter 2, Professor Scholl reflects on the experiences and findings from awareness training, particularly in the face of the challenges posed by the Covid-19 pandemic. The latter part of the chapter is dedicated to the complexities of "awareness measurements." While knowledge queries are common, quantifying awareness and behavioral change poses challenges, prompting a deeper examination of this intricate topic. And finally, at the end of the chapter, awareness maturity models are explored, with an outline of their purpose and significance in the realm of information security.

// Music Break//

Moving on! Chapters 3 and 4 of the project documentation provide crucial insights into public relations and the learnings gleaned from the ALARM research project in German SMEs. Chapter 3 illuminates the selected events and challenges faced, accompanied by photos capturing the vibrant experience-oriented atmosphere of the awareness-raising measures. Additionally, the research team's publication list from 2020 to 2023 is showcased, reflecting their dedication to advancing knowledge in the field.

Chapter 4 gets to the heart of the matter: What have we learned from the ALARM project about information security, awareness, and security culture in German SMEs against the backdrop of the Covid-19 pandemic?

It paints a concerning picture, highlighting the unchanged risk situation for German SMEs. The latest BSI report underscores the persistent threat of cybercrime, with ransomware attacks reigning supreme. Despite this, German SMEs exhibit a paradoxical blend of confidence and vulnerability, often lacking adequate cybersecurity measures.

The ALARM project's in-depth psychological interviews reveal a glaring gap in security awareness strategies among SMEs. However, hope emerges in the form of experience-oriented learning scenarios—serious games—designed to foster communication and raise awareness effectively.

Throughout these chapters, it becomes evident that bridging the gap between cyber resilience and business resilience is imperative. With personalized learning opportunities and tailored awareness programs, SMEs can enhance their security stance and navigate the evolving threat landscape with confidence.

Chapter 4.2 of the project documentation unveils the intricate dynamics surrounding the use of serious games and simulations as tools for raising awareness in SMEs. While English-speaking countries have embraced these tools, German SMEs are just beginning to explore their potential.

The chosen titles for the learning scenarios merely scratch the surface of the underlying narrative. Understanding information security requires a holistic view, integrating narratives relevant to the target audience's daily lives.

The varying levels of security culture and awareness maturity among German SMEs pose challenges to the effectiveness of individual learning scenarios. However, the modular design of the analog serious games offers flexibility, enabling SMEs to tailor the experience to their unique needs. Despite concerns about impact assessment, the ALARM project sheds light on the complexities of awareness measurements and maturity models, urging further interdisciplinary research to tackle these challenges head-on.

In Chapter 4.3, unexpected hurdles within the German pilot SMEs are detailed. As soon as preparation for the interviews started, anomalies emerged, making recruitment a daunting task. Time-consuming arrangements and canceled appointments left the team scrambling. Management directives sometimes coerced employee participation, complicating the sample selection.

Despite high expectations, many SMEs struggled to grasp the project's intricacies. The term "security awareness" was unfamiliar, and information security was often seen as a technical issue rather than a holistic concern.

Over the project's duration, the strain on SMEs was prominent, owing to the demands of evaluations. However, amidst the challenges, there were silver linings. Following the final event, the "Awareness Forum," pilot SMEs expressed gratitude, highlighting the impact the project had had.

Throughout this chapter, Prof Scholl delves into the critical role that management in German SMEs plays in fostering information security and awareness. While some strides have been made, a cohesive strategy for security awareness remains elusive in most SMEs. The existing culture of "talking security" presents an opportunity to develop and advocate for such a strategy on a long-term basis.

Despite the commendable outcomes of the ALARM Information Security project, it's clear that merely providing high-quality awareness materials isn't enough. The project identified three key areas for improvement:

- Supporting SMEs in effectively using awareness materials internally.
- Training moderators to implement awareness measures.
- Providing tailored materials for managers to enhance security communication.

The goal of future projects must be to empower SMEs with the knowledge and resources to combat cyberthreats effectively, emphasizing systemic advice and effective tools for management.

// Music Break //

The potential transferability of awareness-raising measures developed in the ALARM Information Security project to other sectors was explored. While initially designed for SMEs, the analog and digital

learning scenarios are freely available for non-commercial use. Given the current low awareness levels in German SMEs, these materials can serve as a foundation for broader awareness initiatives. From craft businesses to healthcare and beyond, the knowledge and tools from this project have the potential to make a significant impact across various sectors.

In Chapter 5, steps were taken for German SMEs to enhance their information security. From updating data-backup strategies to fostering a security culture, the need for a comprehensive approach is evident here. Employees play a crucial role as the last line of defense against attackers, highlighting the importance of their awareness and sensitivity to security. Recent research emphasizes the interdisciplinary nature of information security teams, combining creative perspectives with technical expertise. Despite unresolved questions, the tools developed in the ALARM Information Security project offer practical solutions.

While the journey with the “Awareness Lab SME Information Security” project was arduous, it’s clear that Professor Scholl’s efforts were not in vain. The desire for continued collaboration underscores the significance of her work. Though the new project awaits funding, the seeds of change have been sown, promising a brighter future for SMEs in information security.

That’s all for this episode—thanks for listening. And, as always, stay subscribed to Research Pod for more of the latest science.

See you again soon.

**Script ends**



researchpod