Idea 04 ms-final

Podcast script: Prof Margit Scholl, Technical University of Applied Sciences in Wildau (TH Wildau)

Topic: Security sensitization and awareness

Reference: doi.org/10.13140/RG.2.2.12630.22082, https://hdl.handle.net/10125/103369

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

In today's episode, we look at innovative strategies for improving information security awareness in small and medium-sized enterprises (or SMEs), explored through research led by Professor Margit Scholl from TH Wildau. The research, conducted in an evolving landscape of cybersecurity threats, highlights how important it is to equip SMEs in Germany with robust mechanisms to improve their security attitudes and their resilience against cyberthreats.

The study fits into the context of escalating cyber dangers, activity interruptions, and natural calamities, identified as the main risks to businesses worldwide. In Germany, in particular, SMEs are showing increasing concern over business interruptions and cyberattacks, which marks a significant change in the perception of risk and the recognition of cyberthreats as a significant challenge. Despite the technical safeguards in place, there is a notable gap in organizational measures relating to information security, particularly in the areas of awareness and emergency preparedness.

// Music Break //

Carried out in cooperation with corporate partners, Professor Scholl's research is centered on the exploration of effective workplace training and educational measures designed to instill and perpetuate a culture of security awareness in SMEs. The research advocates a holistic approach that not only fosters the necessary skills but also actively involves individuals in confronting specific information security challenges.

The methodology of this study involves a variety of tools and approaches designed to dissect and understand patterns of behavior relating to information security. The ISO/IEC 27001 standard emerges as a critical reference, highlighting the need for continuous improvement of information security practices, the integration of security into everyday business operations and the establishment of trust between interested parties.

This research elucidates the essence of **I**nformation **S**ecurity **A**wareness (ISA) as a multifaceted domain, influenced by cognitive, emotional, and systemic factors. By using analog and digital games, on-site attacks, and exhaustive assessments, the study aims to uncover new dimensions in security training methodologies, ensuring that they are engaging, relevant, and effective.

The analog and digital areas of this research feature innovative game-based learning scenarios, leveraging narrative design and interactive storytelling to simulate real-world information security challenges. With the analog games, “talking about security” is initiated in a targeted manner, which is important for raising awareness. The digital games were designed to respond to diverse learning preferences, allowing players to navigate various scenarios from multiple perspectives, thus enriching the learning experience and promoting a deep understanding of cybersecurity principles.

At the same time, the research is pioneering the use of on-site attacks, a methodical approach to simulating real cyberthreats in a controlled environment. This initiative aims to raise awareness among SME workers about the nuances of cybersecurity threats, enabling them to identify and respond to these threats proactively.

Chapter 5 of the study presents a relevant and comprehensive analysis by synthesizing the findings of three key research studies. The goal is to explore the effectiveness and efficiency of different strategies and methodologies with a view to promoting a solid culture of cybersecurity awareness among SME employees.

The first study presented discusses the behavioral aspects of information security in SMEs. It highlights the human factor in cybersecurity, which is often neglected, thus suggesting that although technical defenses are of crucial importance, employee behavior and awareness play a fundamental role in safeguarding companies’ digital and analog assets. The research also highlights the need for ongoing education and training programs adapted to the needs of SMEs. The authors also defend an approach that goes beyond periodic training sessions, asserting that information security needs to be integrated into employees’ daily lives.

The second study is centered on the mental motivators that influence staff adherence to cybersecurity protocols. Through a collection of dialogues and questionnaires, researchers identify key elements that affect staff commitment to secure procedures, such as the importance of policies, the transparency of leadership directives, and the sense of individual responsibility. This research recommends that more engaging and relevant educational content be created that resonates with staff on a psychological level, thus increasing their willingness to adhere to security guidelines.

Finally, the third study addresses the impact of gamification on the efficacy of information security training. By integrating gaming elements into training programs, research suggests that significant improvements can be made with regard to employee involvement and best practices for ensuring the retention of information security. The study presents case studies in which gamified training produced improvements in employees’ ability to identify and respond to phishing attempts as well as other common cyberthreats. The results recommend the inclusion of interactive and competitive elements in training programs as a way to break the monotony of traditional educational methods and promote a deeper understanding of cybersecurity principles.

// Music Break //

Another important contribution of Professor Scholl's work is the article "Sustainable Information Security Sensitization in SMEs: Designing Measures with Long-Term Effect" presented in the Proceedings of the 56th Hawaii International Conference on System Sciences in 2023. The article draws on the findings from the three studies, offering an in-depth analysis of a multifaceted approach to raising cybersecurity awareness in SMEs. The document describes the implementation of a comprehensive awareness program that encompasses a variety of methods such as workshops, seminars, cyberattack simulations, and feedback sessions. The creation of the program is based on the idea that raising awareness of cybersecurity risks and best practices should be an ongoing process and not a one-off event.

One of the main contributions made by this article is its emphasis on the importance of personalization in the development of cybersecurity awareness programs. Recognizing that SMEs operate in diverse sectors with different risk profiles, the document advocates the development of tailored programs that address the specific threats and challenges faced by each company. This strategy not only improves the relevance of training content but also increases employee involvement and participation.

In addition, the study emphasizes the critical role of leadership in promoting a culture of cybersecurity awareness in SMEs. It also emphasizes that the commitment and involvement of senior management are essential factors in signaling the importance of information security to the entire company. By setting an example and actively participating in awareness-raising activities, leaders can inspire a collective sense of responsibility for ensuring the security of digital resources.

Professor Scholl's research highlights the complexity of human behavior in the cybersecurity ecosystem and calls for innovative and engaging education and training approaches implemented on an ongoing basis. This research is a key resource for SMEs looking to navigate the complex cybersecurity landscape, offering practical guidance on developing comprehensive, tailored, and effective information security awareness programs. With this knowledge, SMEs are better placed to cultivate a proactive and resilient cybersecurity culture, thereby safeguarding their digital and analog assets against the ever-evolving array of cyberthreats.

Thanks very much for listening. Don't forget to check out the links to the original research papers linked in the notes for this episode and stay subscribed to ResearchPod for all the latest in research news.

See you again soon.