Idea 02 ms-final

Script Outline: Prof Margit Scholl, Technical University of Applied Sciences in Wildau
Topic: Increasing Security Awareness in German Small and Medium-Sized Businesses with "Awareness Lab SME (ALARM) Information Security"
Reference: Preprint paper http://dx.doi.org/10.13140/RG.2.2.13519.29600

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

In this episode, we're looking at innovative support that can boost information security awareness.

Recent cybersecurity reports show that the security of firms' online presences is under ever-greater threat from cyberattack. Small and medium-sized enterprises (SMEs) are attacked disproportionately often. There is also a link between people's level of knowledge and the number of attacks, so Professor Margit Scholl and her team at TH Wildau have developed the Awareness Lab SME (ALARM) Information Security program. Their goal is to raise security awareness and increase safety education within SMEs.

The overall aim of this research is to highlight the need for greater operational awareness among executives and employees in SMEs and provide innovative holistic support to raise their information security awareness. This project delivers a tangible, interactive personnel development package to increase organization-wide information security in SMEs.

Motivated by the increase in cyberthreats, for both German firms and those operating internationally, Professor Scholl identified the shortcomings of traditional educational approaches, which have not succeeded so far in boosting mindfulness in work processes that are becoming more and more digitized. The conventional reactive approach to cybersecurity is not enough.

A proactive adaptive strategy is needed to provide a sufficient level of security, but simply increasing the level of technology involved is unable to deliver this. Humans are now playing a critical role in increasing information security, and SMEs need to advance their cyber resilience with their employees.

The TH Wildau project team were assisted by four subcontractors, three partners from the Association of German Chambers of Industry and Commerce and additional pilot SMEs. To establish a baseline for where information security and awareness in SMEs currently stands, the research team carried out online surveys and a detailed review of international literature. A subcontractors also performed in-depth psychological interviews.

The project team had already established in previous projects that serious games (an educational application that uses the principles of game design in non-game contexts to engage and motivate users) could raise awareness of information security, so they set about developing a series of analog and digital serious games for this purpose. Target groups tested the games during development and their feedback prompted improvements for the final versions.

The team created seven analog serious game. Each learning scenario has a set of golden rules for the debriefing phase of raising awareness to minimize the risks for users. Resources include a moderation guide, a construction guide, and a handout, together with the print templates. The German versions are all available for free via the project website, linked in this episode's show notes.

Dear listeners, how safe is your own home office?
The first analog serious game, "Home Office", outlines important information security and data protection risks that occur in your own home and offers preventive measures to minimize them.

Are you familiar with passwords?
And do you use multi-factor authentication yourself?
Do you know what this means?
The second game, "Multi-Factor Authentication," covers password protection and shows that protecting information relies largely on secure authentication. It demonstrates how to create a "strong" password and explains how more than one factor is necessary for the protection of very sensitive information.

Are you the managing director of a company and have you made it secure against fraud attacks?
Analog serious game three, "The Five Phases of CEO Fraud," reviews the entire CEO fraud attack process, whereby attackers impersonate a company's executive, and looks at preventive measures. This includes the prelude to an attack—for example, where employees receive urgent email from what appears to be the CEO.

Almost everyone, young children included, regularly uses smartphones today. Do you know how to protect yourself from attacks?
The fourth game, "Mobile Communication, Apps & Co.," considers the potential dangers involved with mobile communication and the use of apps and raises awareness of the measures that can be taken to reduce these risks.

Are you familiar with what can happen to you with analog and digital communication?
Do you know the common attack methods?
The fifth serious game, "Cyber Pairs," looks at how attackers use social engineering in attempts to launch a social engineering attack on the SME to get into their IT network or access information under false pretenses. This serious game aims to clarify different terms and the names of cyberattacks. It helps learners understand the risks and what can be done to minimize them.

Are your personal data and business secrets securely protected in your company?
The sixth game, “Data and Information Protection,” explores how protecting data and information from customers, business partners, and employees has to be a part of every modern company’s business process, together with high-quality protection strategies.

Is the information in your company classified? And do your employees know how to deal with it?
The final analog serious game, “Information Class Roulette,” explains the function of information classification and why every organization needs it. Information classification involves assessing the data and the level of protection it requires. Choosing appropriate classes depends on the possible impact of the information’s availability, loss, or damage.

Professor Margit Scholl describes how these analog serious games are suitable for station learning. Each game can be set up as a learning station with groups of 4 to 20 learners moving from one station to another when they have completed a task. A group member acts as moderator at each learning station. Groups collect points for tasks completed correctly; this means that these serious games can also be played competitively.

These analog games can be used to initiate competition between groups or teams, or they can be used as a starting point for in-depth information security training. Each game can be played in around 15 minutes, split into 3 stages: introduction, game, and debriefing. This can be extended for anything up to an hour to allow for more discussion between participants. “Talking about security” is an important part of raising information security awareness!

The digital games expand on the topics covered in the analog games without duplicating them. They allow employees to work autonomously. These digital games can also be used independently of the analog games and played in any order.

An overarching story set in a fictional SME links the digital games together. Users meet the same characters in the individual stories and become more familiar with the imaginary company and its employees with each game.

The overall story concept and descriptions of each of the digital games are available for download and the games can be played online on the project website. There is also a self-test and an additional password-hacking game.

If the digital serious games are to be used as part of a company awareness campaign, Professor Scholl recommends initiating a discussion afterwards in which participants talk about what they experienced. This can be done via video conference or in analog form and will be an active reminder of the protocols of information security.

Have you ever been selected to improve information security in your company?
Digital serious game 1, “The first day,” introduces information security. The player has just joined the fictional company and has been tasked with handling IT security. This includes some challenges and pitfalls. They select options from a list of suggested actions. At the end of the game, their decisions are evaluated.

Has your company ever been attacked? Have you tried to understand how hackers operate?
In game 2, “The Hacker’s Attack,” the player takes the role of an attacker launching a social engineering attack in a bid to get unauthorized access to the company’s network. There is a choice of possible approaches, but only one will lead to success.

How can you detect attacks and the extent of any damage that has occurred?
How can you prevent something worse from happening?
The third game, “The Search for Clues,” has the player taking the role of a forensic scientist, who has just received an anonymous tip that the company has fallen victim to CEO Fraud. If the player can identify the attacker and the scam that was employed, the company may just be able to get its money back.

Do you use AI privately or at work?
Would you like to slip into the role of an innovative AI?
The fourth digital game, “AI in the Home Office,” sees the player adopting the function of an artificial intelligence, monitoring the SME employees’ computers, and assisting them with any security issues. Visiting the home offices of three employees from different departments shows how the same mistakes occur repeatedly.

Cloud computing and cloud data backup are becoming increasingly important for companies?
What should you pay attention to?
The fifth game, “Everything Just CLOUD,” looks at password hacking and protection and examines the topics of data storage in the cloud and password security from both the attacker’s and the trainer’s perspectives.

What exactly is operational information classification?
What does it offer in everyday life and how is it used sensibly in companies?
Digital game 6, “Information Classification,” has the player return to the artificial intelligence role to look at how information classification is used within the company.

Are you aware of the most common attack that is currently being used against companies?
Digital serious game 7, “Ransomware,” starts with the company falling victim to a ransomware attack. Their data has been encrypted and only the attacker has the ability to unlock it. The player adopts the role of the forensic scientist hoping to limit the damage and solve the case.

With players switching roles between security specialists, investigators, hackers, and artificial intelligence, they get to experience the topics from different viewpoints. The choices they make determine their learning journey, and they receive feedback in the form of messages displayed during each game and a summary of their performance at the end.

The “Security Self Check (SeSec)” can be used to identify gaps in individual employees’ knowledge and pinpoint security weaknesses within the company. Targeted training can address these gaps.

The project has also developed seven on-site attack simulations. These focus on CEO Fraud, email checking, hacking, phishing (where attackers use scam emails to trick people into providing their personal access data), smishing (i.e., phishing attacks via SMS), tailgating

(where a person attempts to gain unauthorized access to a company, often by following an authorized employee through a secure door), and incident response.

Each simulation comes with two downloadable resources: an information sheet and a low-threshold (in terms of harm reduction) security concept. The researchers have taken care to ensure that the simulations don't have any negative consequences or impacts on the atmosphere and culture of trust within the company. This means that if "on-site attack" simulations are to take place as part of a company awareness campaign, very clear agreements must be made between management and the service provider in order to support the employees by creating an atmosphere of trust and not embarrassing them.

The Awareness Lab SME (ALARM) Information Security project has come to the end of its three-year run. When the proposal was being developed, Professor Scholl never imagined that the project would have to negotiate the challenges of the Covid-19 pandemic. Notwithstanding these difficulties, the "ALARM Information Security" project has delivered a creative practice-oriented blend of materials in both analog and digital form.

Professor Scholl notes that while technology plays a fundamental part in building a company-wide information security culture, the process won't work without people. She also makes clear that—as the project evaluation shows—participants take these gamified security awareness measurements seriously! This modern game-based awareness building program's performance far exceeds that of traditional learning theory approaches and has positive long-term effects on data protection and information security.

That's all for this episode—thanks for listening. Do stay subscribed to ResearchPod for more of the latest science.

See you again soon.

Script ends