

Idea 03 ms-final

Script Outline: Prof. Margit Scholl, Technical University of Applied Sciences in Wildau
Topic: German SMEs and the “home office”: Narrative-driven game-based awareness raising with long-term efficacy

Reference: <https://www.intechopen.com/chapters/1171513>

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

In this episode, we look at an innovative research project in Germany that’s designed to help small and medium sized businesses—SMEs—learn more about information security.

Based at the Technical University of Applied Sciences in Wildau (TH Wildau), near Berlin, the ALARM, or Awareness Lab SME Information Security project, is led by Professor Margit Scholl.

Using gaming as a tool for education and training, researchers and corporate partners have developed so-called “serious games” to help employees understand the risks associated with remote working.

Covid-19 drove many of us online as we worked from home. But despite workplaces having since reopened, many employees still want to work remotely at least one or two days a week.

The problem is that, in their rush to get everyone online to keep their businesses going, many SMEs failed to think about the information security risks associated with home-working, for example that corporate data is being accessed via an external network.

We might be careful to close a laptop lid if a friend pops round while sensitive data is on our screens. But look around. From smart appliances such as fridges and televisions, to thermostats, video doorbells and even children’s toys, we’re surrounded by technology that has the potential to let cybercriminals into our homes to steal the data we’re working on.

The Internet of Things makes individuals—and the businesses they work for—vulnerable, and the size of the threat is enormous. It’s estimated that by 2025 there will be 30 billion smart devices worldwide—that’s four devices for every person on the planet.

Crimes range from phishing and hacking to data breaches and ransomware attacks, any one of which could bring a business down.

A literature review carried out for the ALARM project found the average cost of a data breach is US\$4.5 million. And global experts Cybersecurity Ventures currently predict that the global cost of cybercrime will rise to US\$10.5 trillion by 2025.

In addition to financial harm, cyberattacks can cause physical and/or digital damage, as well as psychological distress, reputational loss, and social and societal harm.

Employees working from home are an easy target, one that organized crime is well aware of. The question is no longer what happens *if* a business is targeted, but rather *when*.

Professor Scholl argues that employees have to do more to protect themselves and their employers from cybercrime. Employers also need to do everything they can to make protection a tangible and comprehensible subject for every employee.

One goal of the ALARM project is therefore to discover how employees can be made more aware of the problem, and how their behavior can be adapted to be more secure when working from home.

One solution identified by the researchers was the development of “serious games”—games that are used for education and training rather than entertainment.

They began by interviewing pilot companies about the information security issues they face. They also conducted a survey to develop security profiles for the businesses involved.

The concerns that emerged included password security, phishing, fraud, social engineering, and manipulation. They also included apps and software, home office environments, data protection, secure transmission, storage and encryption, and information classification.

These topics were then used by experienced game developers to design, test, and revise seven analog and seven digital games, each around 15 minutes long.

For example, the analog game “Living safely and working securely from home” was designed as a group game for participants to work on together. It centers on a board depicting a large family house containing 17 different IT usage scenarios in and around the home.

They include a teenager trying to use their parents’ Amazon account, a child gaming on their computer, and young adults setting up a smart TV. They also show adults video-conferencing for work, and another adult being reminded by “Alexa” to expect a call from their boss. Outside a burglar is trying to steal the family car, which has a digital key, and a thief is going through a dustbin looking for personal and financial information.

To start the game, a moderator introduces the learning topic and asks participants about their experience of the scenarios depicted. The participants are then given cards describing 17 information security risks which they have to discuss and match to the scenarios on the board. Once they’ve done this, they are given 17 more cards describing protective measures which they again have to discuss and match to the scenarios. According to Professor Scholl, talking about security and your own experiences is extremely important as a means to increase security awareness.

For example, for the video-conferencing scenario, the text on the risk card tells them that this provides everyone on the call with insights into their private life. The text on the matching protection card warns them that they should only exchange sensitive information via a VPN (virtual private network) and, if necessary, switch off the video function on their laptop.

The game ends with a debriefing session in which the moderator discusses participants' choices, and corrects the placement of the cards where necessary.

The digital games are designed for online use by a single employee in their chosen location. They cover similar topics as the analog games but are designed for people who learn in different ways and have varying degrees of cybersecurity knowledge.

The games follow the format of a visual novel. Narrative text is combined with static or animated illustrations with which participants interact. In this way, players become part of the story and their decisions influence the course of the games. Information is given to them as on-screen text, audible instructions, and feedback—even music can set the mood.

The digital scenarios explored by the games include the first day at work and password protection, hacker attacks, the search for clues in relation to fraud, AI in the home office, ransomware attacks, and password hacking.

For example, in the "AI in the home office" game, the scene is set by an on-screen Information Security Officer who tells the player about the game and how they will be tested. The officer also introduces an AI avatar who interacts with the on-screen action as the player dictates.

The player must first choose to investigate one of three characters who are working from home—a business's dispatcher, boss, or trainee. Once chosen, the AI avatar then looks around the character's home office and comments on what it finds.

For example, AI avatar learns the names of the employee's Wireless Local Area Network, laptop, and Android tablet. The player is then asked to choose one of three options describing why these are a risk to information security: the router still has its default password; the laptop's microphone is always on; the WiFi signal is weak.

If the player correctly chooses the router, the AI avatar recommends that the employee change their password and network. When the employee asks why, because their password is long, the AI avatar explains that standard passwords are easy to find, and that hackers can quickly access home networks.

The digital game continues in this way until the Information Security Officer finally gives the player feedback on what they have learned and scores them using a star rating.

The serious games developed for the three-year ALARM project are part of a series of measures researchers have designed to support and raise SMEs' awareness of the need for greater information security.

The games are available to businesses from ALARM's website and can be used free of charge for internal, non-commercial purposes. Other support includes such things as free awareness testing and security analysis.

The pioneering project has been well received, and although targeted at German businesses, it has international relevance, not least because of its novel approach to information security training.

Rather than being bombarded with hard-to-remember facts and stats, for example in a Powerpoint presentation, users can learn about cyberattacks in a safe, enjoyable, and interactive way, with time to think about the best way to respond.

The research team finds the games are successful because they provide a storytelling context for information security information. By presenting meaningful narratives that invite users to become emotionally involved, learners are more likely to retain the learning content.

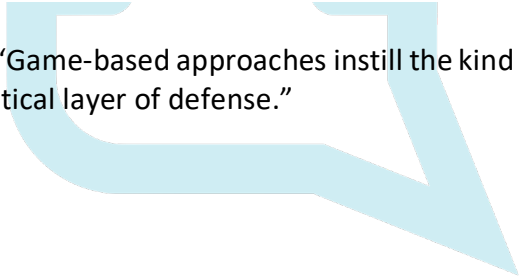
Professor Scholl argues that all businesses, and SMEs in particular, need to think more about the risks associated with the information technology that is essential to their business. They also need to work with staff to build a security culture together.

Current information security training for many employees amounts to no more than a couple of hours a year. This fails to produce the knowledge and behavioral change that managers and employees need, particularly when working from home.

The advantage of serious games is that they are short—in ALARM’s case around 15 minutes’ long. They can also be played more often alone (digital games) or in a team (analog games), making learning a continuous process. The analog games provide a good framework for more intensive discussions and exchanges, which can last longer than 15 minutes if there is enough time. For the digital games, an operational debriefing is recommended in order to make “Talking about Security” a lasting experience.

As Professor Scholl explains, “Game-based approaches instill the kind of security thinking that can turn employees into a critical layer of defense.”

That’s all for this episode—thanks for listening, and stay subscribed to ResearchPod for more of the latest science and ideas. See you again soon.



researchpod