Caring Not Scaring - An Evaluation of a Workshop to Train Apprentices as Security Champions

Menges, Uta; Hielscher, Jonas; Kocksch, Laura; Kluge, Annette; Sasse, M. Angela

Published in:
EuroUSEC '23

DOI (link to publication from Publisher):
10.1145/3617072.3617099

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

Caring Not Scaring – An Evaluation of a Workshop to Train Apprentices as Security Champions

Uta Menges
Jonas Hielscher
Ruhr University Bochum
Germany
firstname.lastname@rub.de

Laura Kocksch
Aalborg University Copenhagen
Denmark
firstname.lastname@ikl.aau.dk

Annette Kluge
M. Angela Sasse
Ruhr University Bochum
Germany
firstname.lastname@rub.de

ABSTRACT

Security champions are regular employees who have deeper knowledge in information security and a direct connection with the security team. Through this connection, they can facilitate the diffusion of security knowledge to employees and back to the security team. We worked with a German organization with more than 20,000 employees that decided to create such a program, starting with a three day in-person workshop with $n = 17$ young apprentices to train them to become security champions. Internal and external speakers were invited, to pass on their security knowledge to the apprentices. We contributed to the workshop program with Serious LEGO, security mythbusting exercises, and Q&A sessions. However, our main goal was to evaluate the workshops' impact on the participants. We gathered data through interviews, surveys and observation before, during and after the workshop. We found that the workshop did indeed influence the security behavior of young employees. However, the external security experts presented outdated or incorrect security knowledge, and recommended secure behaviours that contradicted company security policies. We identified incentives and motivations that participants brought to the role. In addition to tailoring security training content appropriately, we identify preparatory steps, and support that organizations need to put in place to support security champions who take on the role.

KEYWORDS

Security Champions, Human Centered Security, Security Training, Security Intervention

ACM Reference Format:
Uta Menges, Jonas Hielscher, Laura Kocksch, Annette Kluge, and M. Angela Sasse. 2023. Caring Not Scaring – An Evaluation of a Workshop to Train Apprentices as Security Champions. In *The 2023 European Symposium on Usable Security (EuroUSEC 2023), October 16–17, 2023, Copenhagen, Denmark.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3617072.3617099

1 INTRODUCTION

Most organizations want to influence their employees towards secure IT security behaviors, invest a lot in training, mostly online. Evaluation studies have shown that success is limited [6, 48]; a common complaint from staff is that the content is generic and recipients struggle to apply training contents in their daily work. This is where *security champions* [10, 11, 24] come in – the idea to build a network of employees interested in extra training, regular consultations with security specialists, and helping colleagues in their departments with reminders, explanations and practical demonstrations.

So far, security champions are described as employees that are intrinsically motivated to improve the security in their teams [1, 3, 36].[1] Such security-savvy employees have received no formal mandate or training by their organizations and must coordinate security work with their regular work tasks. However, it is a promising low-threshold approach to promote secure behaviors throughout the organization, which is why we teamed up with a German industrial organization that aimed at training young apprentices (from all types of trades: mechanics, sales, information technology) to become security champions. The training was organized as a three day in-person workshop where apprentices met with security teams and participated in various sessions with internal and external speakers from the security community to receive insights into different aspects of information security[2] (e. g., Internet of Things (IoT) security, social engineering, network security, social media security policies).

The workshop was conducted with $n = 17$ apprentices. To find out how such a workshop format helps in the development of security champions, we accompanied the workshop scientifically by taking observational notes, conducting interviews before the workshop and an online questionnaire three months afterwards. At the workshop itself, we held an intervention where the apprentices modeled their perception of the champion role. Here we also collected their security questions and tried to bust security myths [29]. In our analysis of the material, we focused on (I) the change of the apprentices' security behavior and self-identification with the role of security champions over time, (II) the impact of the workshop content on the apprentices and (III) the relationship-building between the apprentices and the security team. We identified *mutual trust* between employees, security champions and the regular security team as an important prerequisite to create a security champion program and build on previous work that shows that security teams need to be approachable, should not work with blaming and act on eye-to-eye level [4, 19, 45, 53, 59]. We formulated the following research questions:

[1] With the exception of security champions in software development teams, where e. g., the OWASP foundation suggests a security champion program [23].
[2] The terms *information security*, *IT security* and *cybersecurity* are often used to describe the same principle. In this paper we will use the term *information security*, which includes technical and organizational aspects in the protection of data and systems.

EuroUSEC 2023, October 16–17, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0814-5/23/10.
https://doi.org/10.1145/3617072.3617099

Q1: How can apprentices without specific security knowledge be attracted and empowered to take on the role of security champions in organizations?
Q2: What conditions must be in place and fulfilled by the organization – in terms of planning, implementation, delivery and content of an appropriate security champions workshop – to enable the process of apprentices' willingness and empowerment?

To the best of our knowledge, we are the first who followed a program to form security champions in an organization in a multi-step empirical observation. We found that young employees are indeed a plausible target group for a security champion program. They changed their own security behavior according to what they learned from the security experts and wished to sustain a network among each other and with the security team. We identified a missing follow-up strategy after the workshop and problematic security advice to be main blockers for a successful champion program.

2 RELATED WORK & BACKGROUND

2.1 Security Champions

To help employees balance their primary work tasks with secondary compliance tasks, e.g. security tasks [8, 9], security champions can help find feasible security that leads to more secure performance of primary tasks [10]. Security champions are employees from different departments at different hierarchical levels who want to volunteer for security [37] and who perform these tasks in parallel to other work tasks [26]. They take on the role of multipliers [3] and can receive and relay communication about security-related issues from their respective departments and support colleagues on their team [3, 57]. For the related concept of cybersecurity advocates [25–27], it is emphasized that they should not have exclusively technical skills, but especially soft skills (spreading optimism, being able to listen, etc.) and be able to educate and promote best security practice [25, 27]. To do their job, they should try to reduce the gap between security experts and non-security experts by building trusting relationships with employees [26]. Security champions should increase employees' skills and confidence in security as they provide a more direct and contextual source of security knowledge for employees [16] and promote interactive engagement and awareness of the topic among them [18]. They can also support the information security team in ensuring that employees internalize security awareness [3]. Research congruently shows that (organizational) framework conditions are necessary for the success of a security champions program: security champions can only exist in organizations if there are policies in the organization that are worth advocating. However, if relevant policies neglect or even hinder business processes, champions will not promote them as a consequence [11]. Security champions organized in information security champion networks are key to the success of a champion program [3, 10], they can especially be found in software development teams [36, 67, 71], and are generally suggested for such teams by the influential OWASP foundation [23].

2.2 Security Education

To protect against threats, organizations are increasingly using so-called SAET campaigns (security awareness, education and training) to sensitize employees to security risks [60]. These programs are often implemented in the belief that non-compliance with security rules and measures is due to a lack of understanding [42] and knowledge [11] among employees. Hielscher et al. [33] have shown that security awareness and education training is the (sole) tool of choice for Chief Information Security Officers (CISOs) to change employees' security behavior. Although these campaigns are well received in the organizational context, in many cases there is no evaluation of their effectiveness in terms of improving certain skills of employees over a long period of time (e.g. duration of effectiveness of a measure) [60]. Other research shows that traditional and generic awareness-raising and training programs are not very effective [6, 35] and that certain criteria need to be taken into account in order to bring about behavioral change. Instead of flooding employees with information and warnings and trying to turn them into security experts, employees' perspectives and decision-making processes should form the basis for developing security solutions [43]. Effective measures should be tailored to employees from different departments, foregoing organization-wide advice [40]. These factors include refraining from instilling fear of security breaches [40, 53] and not merely providing information about security [6, 32, 63] or repeating rules alone [11], but designing security education in such a way that it is targeted and actionable and also provides feedback to employees [6]. In this context, adaptation processes are necessary: security awareness and education should always be human-centered, the security behavior required of employees should be tailored to their primary tasks [62], and the value of security should be emphasized for the achievement of organizational goals [40].

2.3 Apprentices in Germany

Germany has a unique form of tertiary education; the so called *German Dual Education System* [12] for vocational training. Apprentices are taught academic knowledge relevant to their trade in schools provided by the government and practical training relevant to skills necessary in an organization. There are 324 officially recognized types of skilled trades for which people can qualify through apprenticeships lasting 3-3.5 years.[3] In 2021, 1.25 million people in Germany were in an apprenticeship, compared with 2.95 million university students.[4]

3 METHODOLOGY

We followed a three day in-person workshop of a German industrial organization, where $n = 17$ of hundreds of apprentices in the whole organization were trained to become and act as security champions. We interviewed them before the workshop, took notes during the workshop and conducted a post-questionnaire three months later. Our methodology is summarized in Figure 1.

[3]List of recognized training occupations 2022 [German]: https://www.bibb.de/dienst/veroeffentlichungen/de/publication/show/17944, accessed September 11, 2023.
[4]DESTATIS Berufliche Bildung [German]: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bildung-Forschung-Kultur/Berufliche-Bildung/_inhalt.html, accessed September 11, 2023.

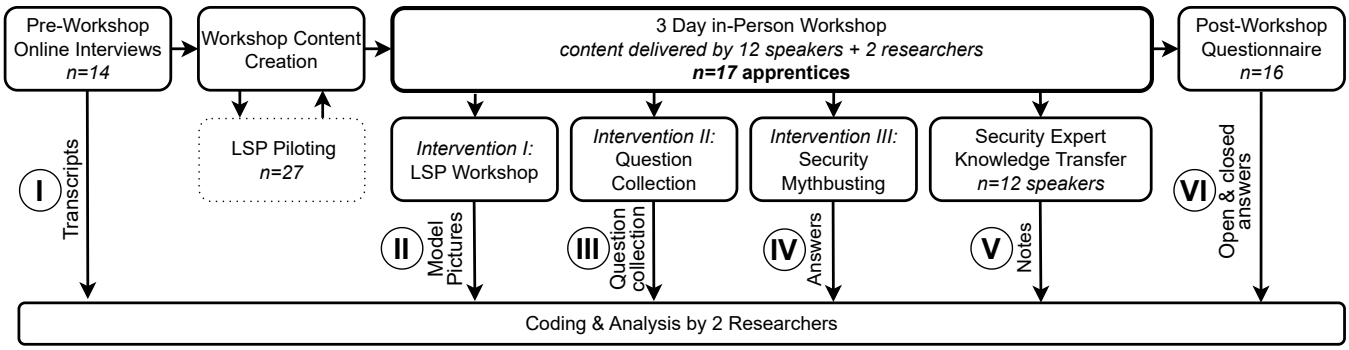

Figure 1: Our methodology, showing the procedure and the six data points we used: (DP-I) the transcripts of the pre-workshop interviews, (DP-II) the pictures taken of LSP (LEGO) models, (DP-III) the questions written on cards by the apprentices, (DP-IV) the answers on our mythbusting posters, (DP-V) the notes we took during the observations at the three workshop days, and (DP-VI) the answers from the post-workshop questionnaire.

3.1 Organization & Setting

The organization that invited us to evaluate their security champion program (we will call it *AutoCorp* from now on) is an industrial conglomerate with more than 20,000 employees around the world, headquartered in Germany. It produces advanced industrial components in various sectors, e. g., as a supplier for the automotive industry. In early 2022, we discussed a possible evaluation of a security awareness training package with the security awareness lead of AutoCorp; the concept of security champions arose in the discussion, and it emerged that the organization wanted to conduct a workshop with selected apprentices from all their German sites, where they would learn about security threats and AutoCorp's security policies. The idea was that the apprentices would become what he called *ambassadors for security*. We used this opportunity to evaluate the workshop and the impact and design options of such programs in general. The workshop content was created by the security awareness lead in collaboration with the corporate CISO, and the head of the apprenticeship program (which three we will call *leaders* in our evaluation). In addition to designing and conducting the evaluation, we were invited to contribute some content to the workshop. We (three researchers attending the workshop) had mixed roles: (I) we collected qualitative and quantitative data through interviews, questionnaires and observations, but (II) we also contributed to the content of the workshop with a three-fold intervention (see Section 3.3).

3.2 Recruitment

AutoCorp recruited the workshop participants. The awareness lead and the head of the apprenticeship program at AutoCorp contacted managers of various sites in Germany and asked each of them to send one apprentice to the workshop. As researchers, we were not involved in this internal recruitment process, but AutoCorp tried to recruit at least one apprentice per site and informally told us that apprentices that were considered "the best" in their jobs would be preferred. To recruit for pre-workshop interviews, the awareness lead asked every apprentice whether they could share their email addresses with us. We then sent out personalized invitations via email. We did the same for the post-workshop questionnaire.

3.3 The Workshop

The workshop was held in-person at AutoCorp's headquarters and lasted three days (an overview of the schedule can be found in Appendix A). The agenda was worked out by the awareness lead in collaboration with the apprenticeship lead. Since the organization in our study is German and all participants were native German speakers, the workshop itself, as well as all data collection was carried out in German. In the course of the three workshop days, the apprentices participated in 14 sessions, organized by 12 different security experts. Five experts came from external organizations. The workshop included live hacking sessions (Expert 1 /S1), talks about internal security policies (S3), IoT security (S4), law enforcement (S4), the visit of the organization's security headquarters (the Security Operation Center/ SOC) and an address by a member of AutoCorp's board (S2). We ourselves performed a three-fold intervention at the workshop, with the two goals of explaining the idea of security champions from a research perspective and preventing the apprentices from follow false, unusable security advice:

Intervention I At the first day we held two identical two-hour sessions for half of the group each. After a small presentation by one researcher, participants built building block models displaying their security situation, following the **LEGO Serious Play (LSP)**[5] **method** [34, 54] as the core of the session. We chose this method as it has already proven to be one of many creative methods in IT security research to engage participants in a playful way [15] and to make abstract issues tangible [28]. The building tasks included the modeling of the security champion role (see Appendix D for task descriptions). We piloted this intervention two months before the workshop with $n = 27$ students.

Intervention II We then asked all apprentices to **anonymously write down any question** they had about information security at AutoCorp or in general on cards, and told them that we would try to find the answers to these questions. We answered the questions by email three weeks after the workshop. The aim was to teach the

[5]LSP is a clear process following format that focuses on a complex problem or question that participants approach successively by building their thought models in Lego models, sharing them, and reflecting on them together [34].

apprentices exactly the security knowledge they miss, as well as getting insights into what they relate with information security.

Intervention III As the third part of our intervention and in reference to the security-usability trade off myth [64, 65], we hung up **mythbusting posters** at the workshop venue. On those posters, we presented 25 statements, which the apprentices could mark whether they deemed them true or false (see Appendix E). During the second day, we hung out posters with the correct answers and offered written explanations. With the posters, we aimed at counteracting common security misconceptions [29]. The list of myths was created based on a short literature review of security literature (e. g., summarized by Herbert et al. [29]) in combination with a discussion in our research team.

3.4 Data Collection & Instrument Development

In a first step, one month before the workshop, we conducted 14 semi-structured online interviews with the apprentices. We asked questions on four topics: (I) their daily work routine, (II) personal experience with information security, (III) professional experience with information security and (IV) their wishes for the workshop. The interview guide was developed by two authors and approved by the AutoCorp awareness lead. After an initial topic selection – guided by the research questions – questions were gathered and refined in multiple iterations (see Appendix B for the full interview guide). The first interview served as a pilot interview but we did not make any changes afterwards and included it in our analysis. We did chose semi-structured interviews (rather than an online questionnaire) because they offer more flexibility, and the opportunity to create a first trust relationship with the apprentices.

We could not record audio- or video-content during the workshops for data protection and ethical reasons. Instead, one of the authors took detailed and anonymous notes of what was said during the three days of the workshop. We ensured that at least one researcher was present at every session. We cleaned and summarized the notes after the workshop. We took pictures of the LSP models created, and of a *topic collection wall*, where the apprentices collected their questions and ideas through all three workshop days. We also collected the anonymous question cards, which the apprentices filled out during our second intervention. Three months after the workshop, we sent out an invitation to complete an online questionnaire, asking the apprentices closed- and open-ended questions about (I) changes in their own security behavior, (II) their perception of their new security champion role, and (III) experiences in trying to fulfill it. We developed the questionnaire after the workshop and the questions were partly shaped by the workshop content itself. Again, two of the authors developed and refined it in multiple iterations (see Appendix C for the full questionnaire). In figure 1 all six data points (DP-1 to DP-VI) are shown.

3.5 Data Analysis

The data we collected are of different types (e. g., full paragraphs from the interviews vs. bullet points from the question cards) and were collected using mixed methods. Since the majority of our collected data was qualitative (open-ended to some degree) a good coding strategy was essential. After some discussion, we decided to code every data point (interview transcripts, notes, pictures, questionnaire answers) independent of each other: with a slightly different strategy and distinct codebooks. For the derivation of key topics we took the full material into consideration. Hence, codes from different data points were combined in the evaluation and discussion rounds.

Generally speaking, we followed Kuckartz et al. [47] and applied inductive and deductive coding strategies. Every step of the coding process was accompanied by meetings between two researchers where the code books and interpretation of the results were discussed. This was key to increase the agreement about interpretation. Over one dozen of those meetings took place over the course of three months – accompanied by individual work between those sessions. For the **pre-workshop interviews** (I) two researchers independently created deductive codebooks based on the interview guide, followed by (II) the deductive and inductive coding of two interviews. (III) The codebooks were merged following a discussion and (IV) all remaining interviews were coded by one researcher. Because the coding was done in such a collaborative way, we did not calculate an inter-coder-reliability. The **notes taken during the workshop** were coded in a similar way, again by two researchers. For **all other qualitative data** we applied a simpler, more descriptive coding approach: one researcher created inductive categories simply to allow the grouping of similar content, which was then again discussed between both researchers. The analysis of the **quantitative data** (e. g., the scaled answers in the post-workshop questionnaire) was performed descriptively.

3.6 Ethics & Data Privacy

Our institution does not have an institutional review board (IRB) nor an ethics review board (ERB) for security research. Nonetheless, we followed best practices of user research [69] and European GDPR. Every apprentice was asked for permission to be contacted by us via email, by the awareness lead. All apprentices agreed to this. Before the interviews, we sent a data privacy statement to the participants informing them about their rights – especially that the interview participation is voluntary, anonymous to everyone else and that we delete the audio files after six months. At the workshop itself, we again informed all apprentices that we not only deliver content, but also collect data from the workshop for anonymized scientific evaluation. Due to the small sample size and unique attributes of the participants (e. g., type of apprenticeship), we only report in aggregated form about the data we gathered to keep the apprentices' statements anonymous towards AutoCorp.

3.7 Limitations

In order to be able to identify and evaluate the research relevance of our study in a well-founded way, we have drawn on components of Thomas and Thymon [68], which were developed to classify the criticism of a lack of practical relevance of organizational (theoretical) research. They serve as a reflective framework for the present study: e. g., emphasis was placed on concrete guidance for practitioners in their organizational setting (descriptive relevance). However, as with any study involving human subjects, there are several limitations to our research: Information security is attached to moralities [45] and in our position as researchers and experts, we functioned as a type of moral authority by the apprentices which

may have lead to a *social desirability* phenomenon [21] and may also have been reinforced by the authoritative relationship between AutoCorp's leaders and the apprentices. In terms of external validity – the question of transferability and applicability of results to different contexts [14] – we have to acknowledge that our findings stem from a specific organization. This can limit transferability. To address external validity, we have followed Johnson's [38] recommendations by describing the information on possible generalizability in a transparent and dense way. As researchers, we were in the role of passive observers as well as active security experts. This might have influenced the analysis of our results. We address this by being transparent whenever an observation was made in reaction to content we delivered.

4 RESULTS

Here, we report the results from the analysis of the data we captured before, during and after the workshop. Where necessary, we directly relate our findings to previous literature. Every quote is marked with the data point where we captured it (DPI-DPVI, see Figure 1). Participants' quotes are marked P1-P19, speakers (internal and external) with S1-S12. When we asked the apprentices to rate their security skills on a scale from 1 to 10, 6 out of 14 apprentices answered with a 6 or above (*DP-I*). From 14 apprentices who participated in the pre-workshop interviews (*DP-I*), two could not attend the workshop in the end and were replaced by two other apprentices. However, we still considered their answers in our analysis. Hence, we quote 19 apprentices (P1-P19). In some cases, we could not relate a statement to a concrete apprentice (especially in the data we collected during the workshop). In those cases, the statements are marked with *Px*.

4.1 Demographics

17 apprentices participated at the workshop, 14 took part in our pre-workshop interviews, and 16 filled out our post-workshop online questionnaire. We only explicitly collected demographic data at the pre-workshop interviews. Among the 14 apprentices, the youngest were 18 and no one older than 30. Three identified as female, 11 as male. Eleven were in their first year of apprenticeship, three in their second year. A majority of eight apprentices worked in technical jobs (mechanics, electricians, mechatronics technicians), four in the commercial area and two in information technology. Two participants reported that they dropped out of university before they started their apprenticeship. The participants worked at AutoCorp sites all over Germany (with a majority working in south and west Germany).

4.2 Between Secure Behavior And Expectations: Security Champions

The analysis of data we collected before and after the workshop revealed that AutoCorp leaders, the apprentices and we as researchers had partly contradictory ideas about what *security champions* should be. In a preparation meeting with the awareness lead, we briefly explained our definition of security champions (based on academic literature [10, 24]) to him, and especially stressed that voluntariness would be key [1, 3, 36] – since voluntary security champions are more likely to self-sustain their champion behavior without external prompting or supervision. We told the apprentices the same in our presentation as part of our intervention I.

Volunteers? The awareness lead told us that no apprentice would be forced to take on the role of security champion. What we considered to be at least partly inconsistent with the principle of voluntariness as well as internalized motivation and the concept of security champions was that during the workshop we learned that the apprentices would have to give a presentation on the content of the workshop to their local teams and other apprentices. The theme of upcoming presentations dominated throughout the workshop, so a whole workshop day was used to find presentation topics for all apprentices. During intervention I, six apprentices built LSP models (*DP-II*) that show themselves in a class-room setting, standing in front of their fellow apprentices, teaching them about security (see Appendix F). The LSP models also showed that the apprentices see themselves as future aides to their teams: not only delivering knowledge, but also guiding those that they see as *not young and naturally tech-savvy*. As one apprentice explained: *"You also have to think about people who actually have nothing to do with IT. Even 65-year-old Udo, who still uses his Nokia 6310, has to be able to understand it."* — [Px:*DP-V*].

"Network Building". AutoCorp's leaders had not planned for an active network between the apprentices after the workshop – which would be key for a successful champion program [10, 36, 55] – and were surprised when the apprentices started to organize themselves via instant messengers.

While the apprentices wanted to form a network and chose an effective means of communication – like they would, for instance in a sports team –, they clashed with company policy on only using company-provided tools for work-related communication: *"Of course, you only use WhatsApp for private things. But when it comes to business communication you only do it via email!"* — [apprenticeship lead:*DP-V*]. From the organization's perspective not using WhatsApp is completely understandable, since it harvests metadata which potentially is a threat to the organization. But then AutoCorp would need to provide them with a secure tool that offers the utility to run a network – email is not that tool, which young people know. AutoCorp's leaders stressed several times that the apprentices could and should stay in touch with the security team. They conveyed this through an abstract and implicit statement: *"We would like this to become something long-term, and you know us now [...] If you encounter any resistance at your sites, please do not hesitate to contact us."* — [awareness lead:*DP-V*]. In line with the security champion concept, the CISO hoped to get insights into the different teams through the champions [24]: *"You, as ambassadors, should once a month ask at your location if there are any important [security related] topics that arise there."* — [CISO:*DP-V*]. The CISO introduced the function of the champions as responding to an external need: reporting to him and the security teams, not as representatives of local teams' practices and needs. By stating that he *would not blame employees*, he acknowledged that security champions be suspected to be 'snitches' or spies in the local teams. To dispel this notion, he was quick to add he planned a regular virtual *security coffee break* in the near future, where employees could ask the security team any type of questions and where the

apprentices could also update their security knowledge. By subtly grappling with the social implications of champions becoming spies, the CISO showed his implicit conviction that having such a direct hot line into the teams would be desirable, reflecting recent research showing that CISOs in larger organizations in particular are reluctant to communicate directly with employees [33].

Post-Workshop status. In the post-workshop questionnaire (*DP-VI*), 13 of 16 apprentices stated that they saw themselves as security champions now. Seven of those, however, said that they would not have/be allowed sufficient time in their working days to fulfill the role as they understood it. Nevertheless, all 13 stated that they felt comfortable in their role. Seven apprentices told us how they defined their security champion role: Four (P5, P6, P10, P12) said that they served as contact persons in their teams now. Four (P5, P10, P12, P19) stated that they were now teaching about information security and reacting to misbehavior: *"It is rather the simpler things that I like to point out. In fact, one encounters situations in which the famous post-it note with the password is stuck to the screen. Or moments in which a colleague is asked to change the password on the computer and then changes it with the comment 'Well, let's change the last number again'."* — [P19:*DP-VI*]. P10 and P18 wrote that they were unsure how to exactly fill out their role, with P18 demanding more support: *"The training was completed and a lot of knowledge was taken away. [...] More information about [...] the role of the employee would be great and consolidate the knowledge."* — [P18:*DP-VI*]. P12 stated that they were explaining security to other team members, but that they were reaching the limits of their own knowledge. Only one apprentice reported to have held the planned presentation at their local site so far.

Short summary: The workshop fulfilled at least some of AutoCorp's initial intentions: the apprentices accepted their role, reported some activities that would be part of it and they wanted to become security aides for their less tech-savvy colleagues. The idea of the CISO and awareness lead, however, was primarily about apprentices disseminating what they learned at their local sites, and stay in contact with the corporate security team.

4.3 Security Expertise Is Not Enough

The apprentices came into the workshop with a diverse understanding of security (and privacy) and brought their own local security knowledge with them. Most defined information security not solely as the protection of IT systems, but also of all types of analogue information – for which we found the root in a basic data protection briefing at the beginning of their employment, e. g.,: *"I have to be careful, of course, because I also come into contact with classified information, so I also have to be careful who I tell certain things"* — [P3:*DP-I*]. This shows that the apprentices are already highly willing to take care of the IT systems as well as analogue organizational information based on their understanding of information security.

What is Security? The protection of social media accounts and data privacy was an overarching topic for the apprentices. They talked about this in the pre-workshop interviews, e. g., *"we're just dealing with the internet, social media. Now whether it's online shopping, whether it's here on Instagram, [...], or WhatsApp, if you're on all the messengers and that's one thing you use every day, but you've never really engaged with the security of it."* — [P12:*DP-I*] and during the workshop (*DP-V*). The majority of the question cards the apprentices wrote as part of intervention II were about this topic (*DP-III*). And, by coincidence, some external security experts addressed the topic in their presentations, but without giving concrete advice beyond the two claims to (I) stay away from social media, and if you can not (II) do not post company-internal information there, e. g., *"Information security shouldn't start in your head when you drive to work. It starts in your private environment, including what you post online. You have to create a holistic concept here."* — [S4:*DP-V*]. Other topics mentioned by the apprentices were secure communication, the capabilities of attackers, and technical measures like antivirus and encryption. What the question cards from intervention II (but also our observation during the workshop) itself especially showed us was that the level of security knowledge differed among the apprentices, which is also due to the different professional apprenticeship backgrounds, as particularly the apprentices in information security asked very technical questions. While others asked very general questions like *"Does Snapchat see or store my pictures?"* — [Px:*DP-III*] they sought expert knowledge: *"How should the new EU law on protection against child abuse (analysis of messages & images) be implemented in the context of end-to-end-encryption?"* — [Px:*DP-III*][6].

"Expert" knowledge. This expert knowledge was to be provided by the external experts at the workshop. However, those had not been briefed by AutoCorp to relate their expertise in a way that would have been more helpful to the apprentices in their specific work situation, e. g., by focusing on risks that are known and relevant to the apprentices [43] and on advice that can be handled in line with their primary work task [62]. Instead, all external experts talked about their own realm of expertise, without referring to AutoCorp's security goals and practices or to content provided by other experts. Several of them contradicted each other in their talks on the use of password managers, the security of email communication and the correct handling of incidents. All external talks focused on worst-case scenarios, and referred outlandish threat models, to convey the message that "information security is important". They presented

(1) attacks for which security **champions can not prepare** (e. g., the sophisticated Pegasus spyware [51] by S5),
(2) **outdated threats** (e. g., that attackers can easily spy on private information in public WiFi (S6), which is not the case anymore [29], as https encryption is common and even mandatory under the GDPR, or the myth that emails are like postcards and anyone can read them (S4), which is not the case anymore for the same reason),
(3) **attacks that are impossible** outside of an artificial lab environment (e. g., a reverse proxy on the own local machine of the expert to read and manipulate website traffic that would otherwise be encrypted, by S5), and

[6]While intervention II was anonymous, we know this, since some apprentices approached us afterwards to add thoughts towards their questions.

(4) **advices that are unusable** for the majority of people (e. g., that one should in general surf the web via the Tor browser[7] (S1), which would in practice shrink the number of websites and services one can access dramatically).

Additionally, the vast majority of advice was just a list of *don'ts* that significantly restrict users instead of providing useful and secure behaviors: do not use wireless keyboards, no public WiFi, no public USB charging stations, do not plug a foreign flash drive into your computer, deactivate Bluetooth on your devices, do not use foreign cloud providers, do not store corporate data on private devices, do not use TikTok. Usable security advice was to use multi-factor authentication (MFA), create backups, store account backup keys on smartphones, and use password managers.

Thus the external experts ended up scaring many of the apprentices, rather than provide actionable advice. Apprentices expected they would need some of what they heard later on, but found it difficult to integrate into their own local knowledge – producing some unorthodox suggestions: *"I am also afraid that someone can access my social media account or my online banking. However, I have already learned that the Tor browser is a good alternative."* — [Px:*DP-V*]. Here, the apprentices referred to an external expert recommending that one should "always" use the Tor browser to stay secure and anonymous. This is not a usable advice (given by S1) for average internet users because some services will not work over Tor and there are significant usability issues [49]. It led the apprentices to believe they would be able to use social media securely as long as they used Tor. Content-wise, the workshop provided the apprentices with a lot of information on various security topics, but those might not all be very usable or applicable in their personal and work life. Still, the apprentices competently engaged in navigating various goods. This gives a hint of the difficulties of integrating expert security knowledge with local practice (e. g., using social media) leading to ambiguity and awkward compromise.

Short summary: In addition to scaremongering, the presentations to educate the apprentices in the workshop were far from giving objective, up-to-date and usable information: some contained outdated knowledge or recommended unsuitable ways of "being secure". The apprentices nevertheless tried to integrate the newly learned knowledge into their previous local knowledge.

4.4 Security Scaremongering: a Blocker for Empowerment

The external experts sent fear appeals – a concept under harsh critique in the HCS community [6, 39] – mainly through their description of current threats with sometimes drastic examples and explanations, as well as attack possibilities that have little to do with the concrete threat risks. One expert used a proxy on his own device to read and manipulate the otherwise TLS-encrypted content of a website (S5). The wrong impression was created that an attacker could easily extract sensitive data, especially in case one uses a public WiFi. Another expert stressed the problems of insecure home IoT devices and explained that a compromised smart fridge could ultimately lead to a compromised bank account, if online banking is used in the same home WiFi (S4). This was clearly incorrect, since even a compromised home network would not lead to compromised online banking protected by encryption. The impact of these scary messages was reflected in the questions and statements of the apprentices during the workshop (*DP-V*). For example, they stated that they now had to change all passwords, that they were afraid that their social media or bank account could be accessed, or that they had realized that they previously underestimated many threats and types of attacks.

Destruction of Self-Efficacy. The workshop should have reduced the feelings of *insecurity about information security* that the apprentices already expressed in the pre-workshop interviews, e. g., *"[...] because I am personally very afraid that someone can get access to my system."* — [P7:*DP-I*]. Unfortunately, security communication aimed at non-experts uses scaremongering in a misguided attempt to motivate, which increases rather than reduces the feeling of insecurity [70, 72]. Instead, the workshop should have addressed the feeling of fear and focused on positive actions they can do in their work environment to improve the apprentices' security self-efficacy [7, 61]. This is a prerequisite to act as a security champion: self-efficacy is the only psychological construct measurably related to secure behavior [22] and it would also be desirable if apprentices in their role as security champions could in turn convey the feeling of self-efficacy to their audience as well [26]. Prior to the workshop (*DP-I*), the apprentices reported divergent feelings they associated with information security. In addition to apprentices who felt a sense of trust and security because they had no personal negative experiences, or did not associate any emotions with this topic because security is part of their everyday work, others reported that they felt insecure due to a lack of knowledge and transparency (*DP-V*): *"[...] there is a certain uneasiness. You don't know, it's an issue that's a bit hidden. So you don't really know if you are secure or not [...]"* — [P13].

Short summary: The speakers worked with fear to stress the importance of information security. However, employees who are scared are unlikely to try new actions and are not empowered in their sense of security self-efficacy.

4.5 Organizational Rules as an Opportunity for Collaboration

As Beris et al. [11] point out, a security champion program can only succeed if the organization has security policies that the champions want to advocate. Hence, we were interested in the apprentices' perception and execution of policies. We asked them about their experience in the pre-workshop interviews.

Organizational Policies. Independent of their apprenticeship occupation, the apprentices reported a variety of policies they were aware of (*DP-I*): Five told us that they were not allowed to use private flash drives *"If we take flash drives, they are first checked by the IT department to make sure that there is no malware in them"* — [P5:*DP-I*]. A corresponding company-owned flash drive would have to be requested from the IT department. This requirement was also evident in one of the LSP models. P11 described that employees

[7] The Tor Project: https://www.torproject.org/download/, accessed September 11, 2023

working in the home office have to connect to the VPN. Other rules mentioned by four apprentices were locking computers with passwords and changing passwords regularly. P10 outlined that they verify separately at the printer with a card or send important data via a special program instead of email. The apprentices also described that they were not allowed to dispose of documents unchecked or leave them open and that they must always lock all cabinets in the office. Some also had to show identification to enter the company premises. In line with the findings on work routines, organizational rules and measures should have been given more weight in the workshop planning. Especially because organizational rules also influence the design and corresponding tasks of security champions in an organization, as they should also convey messages tailored to their audience [26]. Among the apprentices with a technical trade, only one mentioned security policies that were specific to their environment: *"What we also have to consider are the machines [industrial controllers] we work on, because they also run on a program and we are not allowed to change anything in those programs."* — [P12:*DP-I*]. This shows that specialized security competencies are required in some types of jobs and security training needs to be adapted to them. However, at the workshop, these topics were not covered, even though the majority of apprentices are trained in such technical jobs.

Security Friction. Regarding possible difficulties and challenges (*DP-I*), some responded that they had not experienced any limitations so far. Others described specific examples or general procedures perceived as a hassle. P2 explained that they found it tedious to have to re-enter their password five to six times a day to log on to the computer, but that they also recognized the high importance of this. P14 reported that it was annoying to have to deal with password management. P1 described a similar experience: *"But this... Logging into the whole... being registered in this system, that was very tedious [...]"* — [P1:*DP-I*], adding that it took some time getting used to the mass of security. Other examples were reported by P12: an employee from an external company always had to come with his computer to log into the program, and they had to contact this external company even for small changes, and the ticket sometimes took up to four days to be processed. P13 summarized their perception as follows: *"You walk through a door, but to get through the door you have to open 10 locks in a row. That's how it is here sometimes with the IT systems, but that's the way it should be, otherwise anyone could get in somehow"* — [P13:*DP-V*]. Others pointed out that it was not feasible in terms of time to meticulously take care of security in addition to their actual work, suggesting that they feel constrained by security policies in meeting their productivity goals [52]. Problems also became clear in the LSP models, e.g. the apprentices built a model that showed that a multitude of information security policies and slow IT department delay learning and working in the organization. These perceived problems sometimes have an impact on everyday work and can, e. g., promote security friction [9, 30] or shadow security [41, 42]. If these already existing guidelines and practical troubles had been included in the planning of the workshop, it would have been possible to discuss with the apprentices their assessment of current measures as well as about their perception of related hurdles, difficulties and challenges in their daily work – in the sense of a joint dialogue [4] and a collaboration process [66].

Short summary: Security friction and the impact of security policies were no part of the workshop, except in our LSP models. Here and in the pre-workshop interviews, the apprentices identified some forms of friction and harsh security policies that might hinder the successful advocacy of security rules to their colleagues.

4.6 The Ultimate Goal: Secure Behavior

In the security community awareness is often presented as a self-serving goal: one must raise it and the organization is more secure. A misconception, because what needs to be achieved in the end is actual behavior change towards secure routines [6, 32, 63]. And since security champions can only succeed if others are willing and able to follow their advice, they need to implement those secure routines themselves. Hence, the awareness lead had the right idea to bring in security experts that would help to shape the behavior. And indeed, in our post-workshop questionnaire (*DP-VI*), the apprentices reported changed behavior: a switch to stronger passwords (P9, P10, P14-P17, P19), the prevention of public WiFi (P8, P11, P12, P18), and more care with private data sharing (P8, P12, P16, P18). Newly introduced security measures included the use of a password manager (P17), MFA (P9,11), switching to a non-admin-account on the private PC (P18) and increased WiFi security at home (P17, P18). The apprentices also reported heightened awareness in general (P9), higher threat awareness (P5) and higher suspicion at clicking on links (P6) and generally against social engineering (P7). These behavioral changes reflect what apprentices were taught during the workshop.

Implementing Unusable Security. Despite the deficiencies in the design of the workshop and the presented information, the apprentices managed to make use of the workshop contents. Although we acknowledge that the results may be affected by social desirability effects, we still see them as overwhelmingly positive and could not observe any differences in this respect with regard to the different professions of the apprentices. The apprentices seem to have taken on secure behaviors that (probably most end-users) would deem hard to use – either because they are in conflict with a primary task [44, 62] (e. g., the avoidance of public WiFi is the avoidance of a service that gets increasingly widely adapted) or are complex to implement (e. g., the separation of home WiFi networks, tedious and time consuming and potentially impossible for non-tech-savvy users). Although, the workshop has been a success in that way, we suspect the new behavior might not sustain for long. Firstly, because the created friction can grow over time and secondly, because although apprentices may have changed their own behaviors, translating that into local teams or in collaborative situations may proof difficult.

The behavior change we hoped for following such workshop and induced with our mythbusting intervention III would have been e. g., more password manager and more MFA usage, the usage of E2EE messengers over non-E2EE (e. g., Signal over Telegram), a diversification of passwords (stored in a password manager), etc. – most of which were not reported by the apprentices, but would be

rather simple steps that would increase security & privacy, without sacrificing usability. Our third intervention presented some of those solutions, but we could not get through with those messages. In conclusion, this intervention did not have the desired effects.

Short summary: The apprentices reported to have changed their behavior in agreement with the expert knowledge they received at the workshop. However, it is unlikely that this new behavior will sustain: it causes friction and other team members might not be able to follow along.

5 DISCUSSION

AutoCorp's awareness lead was in the process of reorganizing the security awareness program in the whole organization. As a part of this he set out to build a security champion program with apprentices. He organized a workshop where manifold security expertise was transferred to the apprentices, e. g., in the form of live hacking and the presentation of sophisticated attacks, as is common in expert talks on conferences but also at security awareness days in organizations. The quotes in the previous section suggest that apprentices are a plausible target group for security champion training. During the apprenticeship – a study program that includes learning situations with authorities in a vocational school and in the organization on a daily basis – the apprentices were open to listen to security experts (another form of authority) and to adapt their security behavior. And indeed, they reported having changed their behavior – although, in often unintended ways. Firstly, they brought in their own local security knowledge, especially around social media data security and the protection of analog information in their job. When they received the expert knowledge, they tried to combine both realms, with interesting results, expressed e. g., in the statement of one apprentice, who now wants to use the Tor browser to increase privacy in their social media accounts. Although this approach is unlikely to achieve the desired result (as Tor does not protect anonymity in social media, where one needs to log in with their credentials anyways), it shows that the apprentices were willing to transfer the newly learned to their own security routines.

Secondly, the external and internal experts did not question whether security advice they gave was practically applicable or at least *correct*, or *state-of-the-art*. We noticed dozens of statements and advice that we would describe as *security myths* [29]: threat models that do not apply to the apprentices (e. g., attacks by the Pegasus spyware), attacks that were outdated (e. g., credential stealing in public WiFi) or attacks that did only work in the artificial environment at the workshop (e. g., website manipulation through a reverse proxy). Additionally, we would deem the majority of given advice as non-usable, or at least as not easy to implement (e. g., the creation of two separate networks at home). We tried to hold against this with our intervention III (mythbusting), but did not succeed (e. g., 12 apprentices indicated that the statement "If I lose my smartphone, I don't have to worry much about someone else reading the data on it. Because the data storage is encrypted" is a false statement). We suspect that the changed behavior reported by the apprentices will not increase their security in further parts and they will not be able to convince others of this. However, a further survey would be needed to verify this assumption.

The concrete task of the apprentices as new security champions remained opaque after the workshop. Some apprentices showed interest in becoming security aids for their local teams (e. g., expressed by one apprentice, who said that even the non-tech-savvy colleagues should be helped). This idea is built on a positive perception of security, where it is natural that one cares for the security of each other [45]. However, some of the statements of the AutoCorp leaders suggested that they might hope to gain insights into the security behavior of the teams. If this was the case, it would be a dangerous idea based on the concept of blaming (employees for their non-compliance). The potential mistrust might hinder the apprentices from introducing new security knowledge in the teams. The apprentices might already be walking on thin ice when they directly hint their colleagues towards their insecure behavior (e. g., sticky notes with passwords on their monitors). A more promising and sustainable concept of the champion role would have been to collectively support the security team in introducing new security routines. In a classical change management process [46] they could act as *agents for change* [32, 50] and help with the replacement of old insecure routines by introducing new, better alternatives (e. g., password managers instead of sticky notes, fast biometric authentication instead of complex passwords, encrypted messenger for data transfer instead of flash drives). This, however, would require the release of such alternatives by the security team. The apprentices were also beginning to subvert formal channels AutoCorp considered secure, by organizing themselves in a WhatsApp group; an idea of a lasting network, which is described as key for a successful security champion program [3, 10]. The fact that this approach was deprecated by AutoCorp's leaders with company email addresses as the only alternative suggestion, shows that they could only think along in their own trodden paths, existing official tools. Instead of learning from the digital natives and providing them with a secure alternative that offers the same functionality (e. g., Slack, Yammer, etc.) they pushed them onto an antiquated communication tool that does not have the functionality needed for effective collaboration.

5.1 Implications From our Case Study for Security Champion Programs

It should be emphasized that a security champion program does not necessarily need to get implemented with apprentices, but could be aimed at young or new employees in an organization. The challenge with a program with new employees is that they may not have the needed knowledge of local practices and routines that would be desirable for a security champion. However, we expect that the apprentice role can be beneficial: as novices to the organization, apprentices are taught local practices and they are able to comment or correct undesirable routines. On the one hand apprentices can transparently present to their teams what is currently not (yet) working in the context of information security measures in the organization, so that an open approach to organizational challenges can be taken from the beginning. On the other hand, young employees are digital natives, to whom a higher level of digital competence is attributed. However, it should be stressed here that even young employees with high digital competence can not be left alone with security responsibilities, and, in fact, allotting

security tasks to them reproduces those as invisible and potentially undervalued. Instead of the principle of control, Kocksch et al.'s [45] characterization of security as a "discipline of care" (continuous and collaborative efforts) could provide a framework for a workshop format that helps participants to practice security and adapt their own practices by refraining from blaming, stoking fears and delegating responsibility to certain groups of people (such as apprentices). From a caring approach, recommendations for the design of e.g. a security workshop are to refrain from imposing standards, rules and prohibitions, and instead to enable participants to form new bonds and try out practices. It should be taken into account that lay people currently perceive security as a mystical or even scary expert system [17], thus a workshop should help to gradually dissolve this image. Viewing security as a collaborative process and a collective achievement [20] and planning and acting accordingly is important. The one-sided view of security experts as mediators of unusable or too impractical security knowledge seems just as unproductive as the view of employees as unwilling learners. Workshops that enable such an approach as well as an exchange and cooperation at eye level could be a suitable approach. Such cooperation could also be supported by organizations communicating openly and transparently which current information security deficits exist. Organizations should also ensure further convergence and exchange among the security champions but also between the security champions and the security experts. As a prerequisite for security champions to be able to take care of the organization's security in collaboration with the security experts, the organization must create a suitable structure for them so that they can also take care of each other. A suitable follow-up and knowing what happens after the workshop are, in our opinion, necessary framework conditions.

5.2 Recommendations For Industry: 6 How-to's for Security Champion Programs

From our observations, we derive recommendations for organizations seeking some form of security training: employees (apprentices in our case) do not need to know the most sophisticated, dangerous, or technically complicated attacks and maximum strength countermeasures – and they do not need information delivered by *top security experts*, which is consistent with Kirlappos and Sasse's [43] finding that users are most motivated to take up awareness and training offers if they relate to risks they know and care about and are communicated, e. g., by peers. Security research is already familiar with this under the saying ***more [security] is not the answer*** [13, 31]. In line with previous advice for designing successful security campaigns, employees need appropriate and relevant knowledge, with the chance to get feedback on [6]. They should be able to build self-confidence and experience the benefits of their own control and the fun of helping each other with security. In Section 4.6 we gave hints on possible advice that would fulfill those requirements. The type of security knowledge transfer we observed at the workshop is not unique in this workshop setting, but rather common in the security community where experts seek to impress each other with novel attacks. We advocate for a shift in the security community: fellow experts are not the same target group as security-novices. Any talk addressing the later one should include concrete and usable (easy-to-implement) security advice. If such advice is not possible, the talk should not be held. Especially if the target group is security champions, whose task it is to give low-level advice on a collegial basis, usable methods instead of lists of *don'ts* are vital. Based on our experiences during this study, we suggest the following additional points to implement a successful security champion program: **(I) Tailor the content** of the workshops to the security practices in use [6, 30, 43], the knowledge and the questions of the participants. To avoid the risk Herley [30] describes, that a convincing cost-benefit risk of security advice should actually relate to the costs and benefits that users care about, rather than those we think users care about, pre-workshop interviews or surveys are suitable for this, as well as online focus groups to calm participants. **(II) Select security experts** with great care. Attention should be paid not only to what they present (possibly spreading panic or worst-case scenarios), but also on how they present it. As CISOs, security experts often seem to be far removed from daily work [5], so the content should be checked to see if it is in line with the company's security policies, if it corresponds to the participants' work realities [2, 6, 9] and to review it for correctness, inconsistencies, and tone, to be able to brief experts if necessary. Include an **(III) interdisciplinary team from different departments [33]**, e. g., human resources or the corporate training department. As described in *security dialogues* [4], this could create collaboration and discourse by presenting (local) challenges from organization's real contacts, which contributes to authenticity and connectivity for the participants. **(IV) Teach soft skills**, not solely technical security knowledge. In line with and partly complementary to the recommendations derived from their research [25–27, 55], we advocate that security champions need to be taught and trained on how to recognize that colleagues need help, how to help colleagues without devaluing themselves and belittling those seeking advice, how they can encourage and motivate others to communicate difficulties and how to ask for suggestions and feedback themselves. Follow **(V) change management practices** [46]. Workshops can only be one element of an overall plan, in which appropriate preparation and follow-up in the form of tools and procedures, should be implemented and carried out [5, 56]. This is in line with Poller et al.'s [58] suggestion in their software development research that security initiatives should not only take a technical but also a change management perspective. Follow up and **(VI) evaluate** [6]. One approach could be debriefing interviews with participants, as they give them the opportunity to reflect on their role and the workshop. Also, organizations should ask for feedback in order to improve themselves [10], which would also address the fundamental criticism that employee feedback on security measures is in most cases insufficiently listened to [42].

6 CONCLUSION

In this paper we followed $n = 17$ apprentices on their way to become security champions in their organization. Most apprentices reported to be willing to take on the role of security champions. They would like to build a network among each other and take care for the information security of their teams, especially for the less tech-savvy team members. Security knowledge delivered by external and internal experts during a three-day workshop shaped the security behavior of the apprentices. These young employees

showed to be open to learn and adapt: they aimed at combining their own local security knowledge and digital competences with the newly learned. The CISO, awareness and apprenticeship lead of the organization did not provide a suitable platform to build a security champion network following the workshop. For a sustainable security champion program organizations would need no scaring but caring to ensure that the future security champions are exposed to correct, up-to-date knowledge linked to actions that can be applied in the organizational context.

ACKNOWLEDGMENTS

We want to thank our partner organization and all *Security Champions* that participated in the workshop and interviews. We would like to thank Steven Ehleringer, Markus Schöps, Jennifer Friedauer, Verena Lörsch, Marco Gutfleisch and Alina Tausch for their support and proof-reading. The work was supported by the PhD School "SecHuman - Security for Humans in Cyberspace" by the federal state of NRW, Germany and partly also by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

REFERENCES

[1] Hege Aalvik. 2022. *Towards an Effective Security Champions Program.* Master's thesis. NTNU.
[2] Anne Adams and M Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46.
[3] Moneer Alshaikh and Blair Adamson. 2021. From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing* 25, 5 (2021), 829–841.
[4] Debi Ashenden and Darren Lawrence. 2016. Security Dialogues: Building Better Relationships between Security and Business. *IEEE Security & Privacy* 14, 3 (2016), 82–87.
[5] Debi Ashenden and M Angela Sasse. 2013. CISOs and organisational culture: Their own worst enemy? *Computers & Security* 39 (2013), 396–405.
[6] Maria Bada, M Angela Sasse, and Jason R. C. Nurse. 2019. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?
[7] Albert Bandura. 1977. Self-efficacy: toward a unifying theory of behavioral change. *Psychological review* 84, 2 (1977), 191.
[8] Adam Beautement, Ingolf Becker, Simon Parkin, Kat Krol, and M Angela Sasse. 2016. Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours. In *Proceedings of SOUPS 2016, Twelfth Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, 253–270.
[9] Adam Beautement, M Angela Sasse, and Mike Wonham. 2008. The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms*, Angelos Keromytis, Anil Somayaji, Christian W. Probst, and Matt Bishop (Eds.). Association for Computing Machinery, New York, 47.
[10] Ingolf Becker, Simon Parkin, and M Angela Sasse. April 29, 2017. Finding Security Champions in Blends of Organisational Culture. In *Proceedings 2nd European Workshop on Usable Security*, Yasemin Acar and Sascha Fahl (Eds.). Internet Society, Reston, VA, 1–11.
[11] Odette Beris, Adam Beautement, and M Angela Sasse. 2015. Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the Risk Perceptions and Emotions That Drive Security Behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop* (Twente, Netherlands) *(NSPW '15)*. Association for Computing Machinery, New York, NY, USA, 73–84.
[12] Hans-Peter Blossfeld. 1992. Is the German dual system a model for a modern vocational training system? *International Journal of Comparative Sociology* 33, 3 (1992), 168.
[13] Joseph Bonneau and Sören Preibusch. 2010. The Password Thicket: Technical and Market Failures in Human Authentication on the Web.
[14] Donald T Campbell and Thomas D Cook. 1979. Quasi-experimentation. *Chicago, IL: Rand Mc-Nally* 1, 1 (1979), 1–384.
[15] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Claude P. R. Heath. 2020. Too Much Information: Questioning Security in a Post-Digital Society. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14.
[16] W Alec Cram, John D'arcy, and Jeffrey G Proudfoot. 2019. Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly* 43, 2 (2019), 525–554.
[17] Joseph Da Silva and Rikke Bjerg Jensen. 2022. "Cyber Security is a Dark Art": The CISO as Soothsayer. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 365 (nov 2022), 31 pages.
[18] Duy Dang-Pham, Siddhi Pittayachawan, and Vince Bruno. 2017. Applications of social network analysis in behavioural information security research: Concepts and empirical analysis. *Computers & Security* 68 (2017), 1–15.
[19] Albese Demjaha, Tristan Caulfield, M Angela Sasse, and David Pym. 2019. 2 Fast 2 Secure: A Case Study of Post-Breach Security Changes. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, New York, 192–201.
[20] Paul Dourish, Rebecca E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (2004), 391–401.
[21] Michael Eid, Mario Gollwitzer, and Manfred Schmitt. 2013. *Statistik und Forschungsmethoden: Lehrbuch. Mit Online-Materialien* (deutsche erstausgabe, 3., korrigierte aufl. ed.). Beltz, Weinheim.
[22] ENISA- European Union Agency for Network and Information Security. 2019. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity.
[23] OWASP Foundation. 2022. OWASP Security Culture: Security Champions.
[24] Trevor Gabriel and Steven Furnell. 2011. Selecting security champions. *Computer Fraud & Security* 2011, 8 (2011), 8–12.
[25] Julie M Haney and Wayne Lutters. 2017. Skills and Characteristics of Successful Cybersecurity Advocates. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX, Santa Clara, CA, 1–7.
[26] Julie M Haney and Wayne G. Lutters. 2018. "It's Scary…It's Confusing…It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 411–425.
[27] Julie M Haney and Wayne G Lutters. 2021. Cybersecurity advocates: discovering the characteristics and skills of an emergent role. *Information & Computer Security* 29, 3 (2021), 485–499.
[28] Claude P.R. Heath, Peter A. Hall, and Lizzie Coles-Kemp. 2018. Holding on to dissensus: Participatory interactions in security design. *Strategic Design Research Journal* 11, 2 (2018), 65–78.
[29] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, M Angela Sasse, Yasemin Acar, and Markus Dürmuth. 2023. A World Full of Privacy and Security (Mis)Conceptions? Findings of a Representative Survey in 12 Countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 582, 23 pages.
[30] Cormac Herley. 2009. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop* (Oxford, United Kingdom) *(NSPW '09)*. Association for Computing Machinery, New York, NY, USA, 133–144.
[31] Cormac Herley. 2013. More is not the answer. *IEEE Security & Privacy* 12, 1 (2013), 14–19.
[32] Jonas Hielscher, Annette Kluge, Uta Menges, and M Angela Sasse. 2022. "Taking out the Trash": Why Security Behavior Change Requires Intentional Forgetting. In *New Security Paradigms Workshop* (Virtual Event, USA) *(NSPW '21)*. Association for Computing Machinery, New York, NY, USA, 108–122.
[33] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M Angela Sasse. 2023. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *USENIX Security 2023*. USENIX Association, Berkeley, 1–19.
[34] David Hillmer. 2021. *PLAY! Der unverzichtbare LEGO SERIOUS PLAY Praxis-Guide für Trainer, Coaches und Moderatoren (German)*. Hanser, München.
[35] ISF. 2014. From Promoting Awareness to Embedding Behaviors, Secure by choice not by chance.
[36] Martin Gilje Jaatun and Daniela Soares Cruzes. 2021. Care and Feeding of Your Security Champion. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. IEEE, IEEE, New York, 1–7.
[37] Lennart Jaeger, Clara Ament, and Andreas Eckhardt. 2017. The closer you get the more aware you become–a case study about psychological distance to information security incidents.
[38] R Burke Johnson. 1997. Examining the validity structure of qualitative research. *Education* 118, 2 (1997), 282–292.
[39] Johnston and Warkentin. 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly* 34, 3 (2010), 549.
[40] Iacovos Kirlappos, Adam Beautement, and M Angela Sasse. 2013. "Comply or Die" Is Dead: Long live security-aware principal agents. In *Financial Cryptography and Data Security: FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers 17*. Springer, Springer, Berlin, 70–82.
[41] Iacovos Kirlappos, Simon Parkin, and M Angela Sasse. 2015. " Shadow security" as a tool for the learning organization. *Acm Sigcas Computers and Society* 45, 1 (2015), 29–37.
[42] Iacovos Kirlappos, Simon Parkin, and M Angela Sasse. February 23, 2014. Learning from "Shadow Security": Why Understanding Non-Compliant Behaviors Provides

the Basis for Effective Security. In *Proceedings 2014 Workshop on Usable Security*, Matthew Smith and David Wagner (Eds.). Internet Society, Reston, VA, 1–10.
[43] Iacovos Kirlappos and M Angela Sasse. 2011. Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy* 10, 2 (2011), 24–32.
[44] Iacovos Kirlappos and M Angela Sasse. 2015. Fixing security together: Leveraging trust relationships to improve security in organizations. In *USEC 2015*. Internet Society, NDSS, San Diego, California, 1–10.
[45] Laura Kocksch, Matthias Korn, Andreas Poller, and Susann Wagenknecht. 2018. Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 92 (nov 2018), 20 pages.
[46] John P Kotter. 2012. *Leading change* ([nachdruck], with a new preface by the author ed.). Harvard Business Review Press, Boston, Mass.
[47] Udo Kuckartz. 2012. *Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung [German]*. Beltz Juventa, Weinheim and Basel.
[48] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. 2022. Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York, 842–859.
[49] Linda Lee, David Fifield, Nathan Malkin, Ganesh Iyer, Serge Egelman, and David Wagner. 2017. A usability evaluation of tor launcher. *Proceedings on Privacy Enhancing Technologies* 2017, 3 (2017), 90–109.
[50] Fred C Lunenburg. 2010. Managing change: The role of the change agent. *International journal of management, business, and administration* 13, 1 (2010), 1–6.
[51] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. 2018. Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries.
[52] Peter Mayer, Nina Gerber, Ronja McDermott, Melanie Volkamer, and Joachim Vogt. 2017. Productivity vs security: mitigating conflicting goals in organizations. *Information & Computer Security* 25, 2 (2017), 137–151.
[53] Uta Menges, Jonas Hielscher, Annalina Buckmann, Annette Kluge, M Angela Sasse, and Imogen Verret. 2021. Why IT Security Needs Therapy. In *European Symposium on Research in Computer Security*. Springer, Springer, Berlin, 335–356.
[54] Uta Menges, Jonas Hielscher, Annette Kluge, and M Angela Sasse. 2022. (Work in Progress) Brick by Brick: Using a Structured Building Blocks Method to Engage Participants and Collect IT Security Insights. In *12th International Workshop on Socio-Technical Aspects in Security (STAST)*. Springer, Springer, Berlin, 1–12.
[55] James Nicholson, Ben Morrison, Matt Dixon, Jack Holt, Lynne Coventry, and Jill McGlasson. 2021. Training and Embedding Cybersecurity Guardians in Older Communities.. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 86, 15 pages.
[56] Shari Lawrence Pfleeger, M Angela Sasse, and Adrian Furnham. 2014. From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management* 11, 4 (2014), 489–510.
[57] Hiep Cong Pham, Duy Dang Pham, Linda Brennan, and Joan Richardson. 2017. Information Security and People: A Conundrum for Compliance. *Australasian Journal of Information Systems* 21 (2017).
[58] Andreas Poller, Laura Kocksch, Sven Türpe, Felix Anand Epp, and Katharina Kinder-Kurlanda. 2017. Can Security Become a Routine? A Study of Organizational Change in an Agile Software Development Group. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Portland, Oregon, USA) *(CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 2489–2503.
[59] Lena Reinfelder, Robert Landwirth, and Zinaida Benenson. 2019. Security Managers Are Not The Enemy Either. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–7.
[60] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana Von Landesberger, and Melanie Volkamer. 2020. An investigation of phishing awareness and education over time: When and how to best remind users. In *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*. USENIX, Berkeley, 259–284.
[61] Hyeun-Suk Rhee, Cheongtag Kim, and Young U Ryu. 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & security* 28, 8 (2009), 816–826.
[62] M Angela Sasse. 2015. Scaring and bullying people into security won't work. *IEEE Security & Privacy* 13, 3 (2015), 80–83.
[63] M Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. 2022. Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours. In *European Symposium on Research in Computer Security*. Springer, Springer, Berlin, 1–18.
[64] M Angela Sasse and Matthew Smith. 2016. The Security-Usability Tradeoff Myth [Guest editors' introduction]. *IEEE Security & Privacy* 14, 5 (2016), 11–13.
[65] M Angela Sasse, Matthew Smith, Cormac Herley, Heather Lipford, and Kami Vaniea. 2016. Debunking security-usability tradeoff myths. *IEEE Security & Privacy* 14, 5 (2016), 33–39.
[66] Nader Sohrabi Safa, Carsten Maple, Tim Watson, and Steve Furnell. 2018. Information security collaboration formation in organisations. *IET Information Security* 12, 3 (2018), 238–245.
[67] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy Champions in Software Teams: Understanding Their Motivations, Strategies,and Challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 693, 15 pages.
[68] Kenneth W Thomas and Walter G Tymon Jr. 1982. Necessary properties of relevant research: Lessons from recent criticisms of the organizational sciences. *Academy of Management Review* 7, 3 (1982), 345–352.
[69] U.S. Department of Homeland Security. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research.
[70] René Van Bavel, Nuria Rodríguez-Priego, José Vila, and Pam Briggs. 2019. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies* 123 (2019), 29–39.
[71] Charles Weir, Ben Hermann, and Sascha Fahl. 2020. From needs to actions to secure apps? the effect of requirements and developer practices on app security. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX, Berkeley, 289–305.
[72] Kim Witte. 1994. Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs* 61, 2 (1994), 113–134.

Table 1: An overview of the different sessions of the three workshop days and the external security experts (numbered S1-S7).

Day	Topic	Security Experts (Speaker)
1	Welcome	CISO, awareness lead, apprenticeship lead
	Academic concept of security champions, LSP model building (**intervention I**), question card collection (**intervention II**)	3 researchers
	Live hacking	2 hacking experts IT provider (S1)
2	Visit Security Operation Center (SOC)	CISO, SOC team
	Feedback Day 1	CISO, awareness lead, apprenticeship lead
	Resolve security myths (**intervention III**)	3 researchers
	Motivational speech	member of the executive board (S2)
	Security structure of an international corporation, communication about corporate security	AutoCorp security team member (S3)
	Police perspective on the topic of IT and information security	police officer cybercrime unit (S4)
	Message encryption, structure and components URIs, certificates of web pages	telecommunications expert (S5)
	Social engineering, strong passwords	intelligence service employee (S6)
	Targets of cyber attacks, types of hackers, possible solutions for companies	security product vendor (S7)
	Introduction to P4wnP1 and scripting language	CISO
3	Sorting and discussing topics collected topics	apprenticeship lead
	Topic preparation for presentations in the teams	apprenticeship lead
	Feedback, discussion of next steps	CISO, awareness lead, apprenticeship lead

A WORKSHOP SCHEDULE

B PRE-WORKSHOP INTERVIEW GUIDE

Introductory questions

(1) We would be pleased if you could first tell us a little about your apprenticeship.
(2) What are your daily tasks?

Personal experience with IT and information security

(3) What is your first thought when you think of IT and information security?
(4) What do you understand by IT and information security?
(5) On a scale of one to 10, how important is IT and information security to you and your personal day-to-day life, with one being "not at all important" and 10 being "very important"?
(6) To what extent is IT and information security a topic of conversation for you and your friends, acquaintances, family, etc.?
(7) What feelings do you associate with IT and information security?
(8) On a scale of one to 10, how would you rate your own prior knowledge of IT and information security, where one means "very little prior knowledge" and 10 means "very strong prior knowledge"?
(9) What experience have you already gained in the private sector with regard to IT and information security?

Professional experience with IT and information security

(10) Where do you deal with IT and information security in your daily work?
  (a) Which programs/tools do you use that are important for IT and information security?
  (b) Which IT and information security rules are important to you in your everyday work?
(11) To what extent are you concerned about the possibility of an IT security incident occurring?
  (a) To what extent have you already become aware of incidents in your company?
(12) What do you think your apprenticeship leaders understand by IT and information security?
(13) To what extent is there an exchange about IT and information security with your colleagues, the apprenticeship leads or other apprentices?
(14) On a scale of one to 10, how important is IT and information security in your apprenticeship, with one being "not important at all" and 10 being "very important"?
  (a) Can you give examples of this?
(15) What problems do you perceive with regard to IT and information security in your organization?
(16) Who would you contact if you had a problem in the context of IT and information security or wanted to report a security issue?
(17) Do you remember any IT security measures that you found particularly annoying?
(18) Do you remember any IT security measures that you found particularly helpful?
(19) If you had one wish: How should IT and information security function in your company according to your personal wishes and needs?
(20) What IT and information security courses and training have you attended so far?

Expectations of the workshop

(21) Why are you taking part in the workshop?
(22) What would you like to practice during the workshop?
(23) What would you like to take away from the workshop for your everyday work?

(24) Are there any problems that you hope to have solved by the end of the workshop?
(25) When was the workshop worthwhile for you?
(26) How would your apprenticeship leaders know that the workshop was worthwhile for you?

Vocational topics and design of a web presence for apprentices

(27) How do you rate the current (cross-location) information offer for apprentices?
  (a) Which topics would be interesting for you?
(28) Which media do you / would you use (website, app, mail/newsletter)?
(29) Should the possibility for cross-site networking be given?
  (a) Do you have any ideas about the presentation?
  (b) Would you participate yourself as an editor (article and/or design of the website)?

C POST-WORKSHOP ONLINE QUESTIONNAIRE

What has changed? We are interested in what you took away from the workshop and what has changed for you since the workshop.

(1) What impact did the workshop have on your sense of security, given everything you've heard about attacks and defenses on IT systems? Please select only one of the following answers:
  - I feel more secure
  - Nothing has changed
  - I feel less secure
(2) Who would you contact now with questions about IT and information security (feel free to name several people or departments)?
(3) Have you noticed any IT or information security issues or breaches in the workplace? Please select only one of the following answers:
  - Yes
  - No
(4) Has anything changed in your security behavior since the workshop and if so, what (feel free to describe in detail)?
(5) Do you notice any IT or information security rules that interfere with you or your colleagues' daily work?
  - Yes
  - No
(6) In which work processes/ in which work tasks do IT or information security rules bother you? [Answer this question only if previous question was answered with 'yes']

Security Champions

Now a few questions about your role as a security champion.

(7) Do you now see yourself as a security champion at your location? Please select only one of the following answers:
  - Yes, totally
  - Yes, a little
  - No, hardly
  - No, not at all
(8) What would have to happen for you to be able to act as a security champion in the future? [Answer this question only if question (7) was answered with 'No, hardly' or 'No, not at all']
(9) How would you describe your role as a security champion now (answer extensively, in bullet points if you like)? [Answer this question only if question (7) was answered with 'Yes, totally' or 'Yes, a little']
(10) Do you have enough time at your location to further engage with the workshop content, role as a security champion, etc.? [Answer this question only if question (7) was answered with 'Yes, totally' or 'Yes, a little'] Please select only one of the following answers:
  - Yes, I have enough time
  - Yes, if I ask for it, I have enough time
  - No, I don't have enough time, but that's not bad either
  - No, I don't have enough time, but I would like to have it
(11) Are you comfortable in your role as a security champion? [Answer this question only if question (7) was answered with 'Yes, totally' or 'Yes, a little'] Please select only one of the following answers:
  - Yes, very
  - Yes, rather
  - No, rather less
  - No, not at all
(12) Since the workshop, have you come into contact with colleagues about IT and information security with whom you had not spoken before? Please select only one of the following answers:
  - Yes, with many (more than 3)
  - Yes, with few (1-3)
  - No
(13) Have colleagues already approached you with their IT and information security issues (e.g. with specific questions or content for consultation hours)? Please select only one of the following answers:
  - Yes, several times (more than 3 times)
  - Yes, a few times (1 to 3 times)
  - No, not yet
(14) Did you give a presentation on the workshop content at your location? Please select only one of the following answers:
  - Yes
  - No, but a lecture is planned
  - No, and a lecture is not planned
(15) Do you have the impression that all employees feel equally responsible for IT and information security issues? Please select only one of the following answers:
  - Yes, all equally
  - No, only individuals
  - No, only the responsible department
  - No, nobody

Workshop questions

Now a few questions about the workshop content itself.

(16) Do you feel well prepared for IT security incidents and attacks through the workshop? Please select only one of the following answers:
  - Yes, very. I know what to do and when
  - Yeah, a little. I have an idea what I have to do

- No, rather not. I don't really know what I have to do
- No, not at all. I do not know what I have to do

(17) What are the concrete security recommendations you take with you (please answer in bullet points)?

Organizational issues
Finally, a few organizational questions.

(18) Did you take part in the interview before the workshop? Please select only one of the following answers:
- Yes
- No

(19) Do you have any feedback for us on the survey or anything else you would like to tell us?

D LSP TASKS

The apprentices had to build four different LSP models during our workshop intervention. We followed the LSP guide [34] and started with skill building tasks before we moved on to the main content tasks:

(1) LSP Skill building; **Build a Tower**; Individual task; Criteria: high, beautiful, stable.
(2) Security Skill building; **Build a model of the term that is on your card** (phishing, password manager, antivirus software, two-factor authentication); Task in pairs; 5 minutes time; Condition: Use a maximum of 5 bricks from the tower models per partner.
(3) Security at AutoCorp; **Build a model of IT and information security as it works or should work in your everyday work**; Individual task; 10 minutes time. "Simple Building Commandment" (not thinking first and then building, but the other way round)
(4) Security Champions; **Build a model showing your role as a possible security champion**; Task in pairs; 10 minutes time.

E MYTHBUSTING

No.	Statement	True/ False
1	[sarcastic introduction] You are here because you are the best of the best!	TRUE
2	Ordinary emails are like postcards: anyone who observes my network traffic can read them.	FALSE
3	I can trust modern biometric authentication (fingerprint, FaceID, etc.) on my smartphone: They are more secure than a PIN.	TRUE
4	If I use a VPN, website operators cannot track me.	FALSE
5	In practice, public WiFi are dangerous because others can read the data I enter online.	FALSE
6	A green lock in the address bar of my browser (HTTPS) means that the connection is encrypted.	TRUE
7	Telegram uses stronger encryption than WhatsApp.	FALSE
8	I need a third party antivirus software on my Windows computer to be secure.	FALSE
9	The messages I send on WhatsApp can only be read by me and the person I'm talking to.	TRUE
10	In public WiFi, attackers can redirect me to specially prepared websites that I cannot recognise as fake.	FALSE
11	Most important password rule: My passwords should be long and complex.	FALSE
12	Password managers are a suitable tool for storing my company passwords as well.	TRUE
13	I should not store my private passwords in the browser.	FALSE
14	If I just click on a malicious link in an email, it is possible that malware will get onto my PC (without further interaction).	FALSE
15	If I lose my smartphone, I don't have to worry much about someone else reading the data on it. Because the data storage is encrypted.	TRUE
16	I am more secure in practice with a 6-digit PIN than with a 4-digit PIN.	FALSE
17	Links in emails can lead me to fake websites in order to intercept my login data.	TRUE
18	The private browser mode effectively prevents website operators from tracking me.	FALSE
19	End-to-end encryption means that only the sender and receiver can read a message, but no one in between.	TRUE
20	Emails are encrypted end-to-end by default.	FALSE
21	Two-factor authentication significantly increases the protection of my online accounts.	TRUE
22	A firewall is there to detect and remove/block malware on my device.	FALSE
23	The private browser mode prevents malware from entering the device.	FALSE
24	It is unsecure to use Windows 7 on my personal device.	TRUE
25	Video conferences (e.g. via Zoom), are usually end-to-end encrypted.	FALSE

F WORKSHOP IMPRESSIONS

Figure 2: Results from the LSP workshop (intervention I), topic collection on a board and the mythbusting poster (intervention III).