"Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security

Jonas Hielscher and Uta Menges, *Ruhr University Bochum;* Simon Parkin, *TU Delft;* Annette Kluge and M. Angela Sasse, *Ruhr University Bochum*

https://www.usenix.org/conference/usenixsecurity23/presentation/hielscher

This paper is included in the Proceedings of the 32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Open access to the Proceedings of the 32nd USENIX Security Symposium is sponsored by USENIX.

"Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security

Jonas Hielscher
Ruhr University Bochum

Uta Menges
Ruhr University Bochum

Simon Parkin
TU Delft

Annette Kluge
Ruhr University Bochum

M. Angela Sasse
Ruhr University Bochum

Abstract

In larger organisations, the security controls and policies that protect employees are typically managed by a Chief Information Security Officer (CISO). In research, industry, and policy, there are increasing efforts to relate principles of human behaviour interventions and influence to the practice of the CISO, despite these being complex disciplines in their own right. Here we explore how well the concepts of human-centred security (HCS) have survived exposure to the needs of practice: in an action research approach we engaged with $n = 30$ members of a Swiss-based community of CISOs in five workshop sessions over the course of 8 months, dedicated to discussing HCS. We coded and analysed over 25 hours of notes we took during the discussions. We found that CISOs far and foremost perceive HCS as what is available on the market, namely awareness and phishing simulations. While they regularly shift responsibility either to the management (by demanding more support) or to the employees (by blaming them) we see a lack of power but also silo-thinking that prevents CISOs from considering actual human behaviour and friction that security causes for employees. We conclude that industry best practices and the state-of-the-art in HCS research are not aligned.

1 Introduction

The role of a Chief Information Security Officer (CISO) is generally seen as assessing an organisation's IT security risks, and proposing ways of managing those risks appropriately. Since most businesses today make extensive use of IT, they need to be concerned about IT security – and globally, organisations spend more than 130 billion dollars every year on IT security products and services [31]. There is growing evidence that many CISOs struggle to define their role [8], lack support from upper management [70], suffer from enormous stress [49], and are afraid that they might be fired after security incidents occur [21].

The security manager community has wrestled with the human factor of the organisation setting – that security is provided for and around a workforce – for decades [2, 13]. The origins of this space, treating humans as a "weak link", have been left behind by further developments in tools and techniques incorporating a range of disciplines (such as psychology and behaviour change), in a race to address the critical need for people within organisations to be able to work securely. What is not certain is how much of the growing body of research and solutions in this space reaches practitioners, how it is interpreted, when it reaches them, and how well it meets their needs.

To explore this, we worked with a Swiss partner organisation to conduct five half-day workshops on the topic of human-centred security (see Section 4) in a practitioner community setting with $n = 30$ participating CISOs, with three authors present. We prefaced these workshops with briefings on basic concepts and recent empirical findings from human-centred security (HCS) research, with a specific focus on where concepts meet productive tasks (as employees have jobs to do). Discussion was driven by the interests of the participating CISOs, where we found participants adding topics to the agenda, such as their relationship with organisational leadership. The CISOs represent a diverse set of experiences, organisational background and were exclusively located in Switzerland, partly working for multinational organisations or local public sector agencies.

We particularly sought to answer the following questions:

Q1: How do CISOs respond to foundational concepts from human-centred security?

Q2: What obstacles, enablers, and touchpoints do CISOs see for applying these concepts to security in their organisation?

We found that the attending CISOs – with a general interest into HCS topics – implement HCS, but in the absence of better solutions (which would account for real human behaviour and aim at supporting behaviour change in accordance with productive tasks [35]) they use what is available on the market

and considered best-practice in their community: Awareness and security training out-of-the-box and phishing simulations to generate numbers they can present to their superiors. We conclude this work with suggestions for closing the gap in knowledge-transfer between the HCS research- and the security management-community.

The paper is organised as follows: In Section 2 we take a look at the role of a CISO and research of organisational HCS. In Section 3 we explain how we conducted the workshops, collected, and analysed the data. In Section 4 we shortly explain what happened at each of the five workshops. Section 5 presents the results and insights gained from formally analysing the discussions. In Section 6 we categorise our findings and derive lessons for academia and industry and in Section 7 we conclude our work.

2 Related Work

Here, we explain what the role of a CISO is (2.1), as well as fundamental aspects of human-centred security (HCS) in organisations (2.2).

2.1 The CISO

A Chief Information Security Officer (CISO) can be found mainly in larger organisations or in the role of consultants that offer their services to multiple organisations. While there is no consensus of what exactly a CISO is, we deem persons with some executive power (i.e., reporting to the board) and with a team to lead as a CISO. There is no uniform reporting structure for CISOs [1, 25, 60]. CISOs often face difficulties in gaining credibility within their organisation due to, among other things, their unclear role, identity, and their perceived lack of power [8]. Critically, regardless of their resources and formal training, CISOs are the individuals who define human-facing security policies and rules that are applied to everyone in the organisation.

Multiple organisations choose the following strategy to anchor security responsibility: the CEO delegates IT security oversight to the Chief Information Officer (CIO), who in turn reports to the CEO. In other organisations, however, the CIO hands over IT security oversight to the CISO, making the CISO both the CIO's appointee and the CEO's sub-appointee [25].

Historically, most CISOs have a background in computer science or engineering [26]. However, the required skill-set of CISOs includes but is not limited to: *IT security skills* to defend, monitor, and protect [10, 36, 39, 68], *strategic security management and government* [5, 10, 33, 36, 39, 45], *leadership and communication skills* [5, 36, 68] and *security teaching skills* [5, 10, 39, 68]. Independent of their tasks, CISOs are under immense pressure and experience unhealthy levels of stress [49]. In general, CISOs become increasingly important for many organisations: Following a proposal of the US Securities and Exchange Commission, every US corporation traded on the stock market might soon be forced to recruit a CISO for their board.[1]

The experiences and opinions of CISOs and other security managers have been studied previously with regards to their security experiences in small and medium-sized enterprises [28, 38], their security budgeting decisions in agreement with the management [48], and their perceived role and collaboration in their organisation [4, 6, 20–22, 27, 44, 52, 55]. Family businesses are less likely to hire CISOs [64], while the appointment of CISOs of stock corporations triggers positive market reactions [30].

2.2 Human-Centred Security in Organisations

Human-centred security (HCS) builds on academic research that started as "usable security" 25 years ago. Zurko & Simon [69] argued that "normal users" as well as technically-minded ones (such as software developers and system administrators) struggled with the workload in everyday practice and the complexity of security solutions that specialists had created, and often made mistakes as a result. Adams & Sasse [2] documented the impossible memory tasks that password policies created for employees in an IT-heavy organisation. Their work demonstrated the link between provisioned systems and impact upon security-related workload for users within organisations. Whitten & Tygar [67] evaluated a PGP mail client with a graphical user interface in a lab-based study and found that most of their participants were not able to use it successfully despite detailed prior instruction; they identified a number of design flaws, but also suggested that users do need a detailed understanding of public-key cryptography. The majority of research studies in usable security since has focused on providing new or better user interfaces to security and privacy tools (easier ways to security and privacy settings), or to motivate and/or train users to follow secure behaviours (recognise phishing emails, heed certificate warnings, etc.).

A path of research has followed, first carved out by [2], to study security behaviours in organisations, to understand why employees do not comply with user-facing security policies. With depressing regularity, the authors found that while occasionally, it was because employees are unaware about risks or about secure behaviours, it was almost always because the employees found the security tasks created too much friction with main production tasks [13, 62]. Steves et al. [62] found that employees experienced authentication as a "wall of disruption", and started to re-organise workflows to reduce their exposure to those mechanisms. Cormac Herley [34] argued that the time users needed to invest to follow security advice on passwords and phishing was simply not worth it, and that

[1] The SEC Is About To Force CISOs Into America's Boardrooms: https://www.forbes.com/sites/bobzukis/2022/04/18/the-sec-is-about-to-force-cisos-into-americas-boardrooms/amp/, accessed October 11, 2022.

security advocates treat user time as a free resource. Parkin et al. [52] suggested a tool for tracking employee security effort in an organisation, and Kirlappos et al. [40] suggested that adapting technology and processes to secure employee routines would be more effective and efficient than trying to change employees' behaviours for the sake of security.

While in customer-facing industries such as online retail and banking, "making security easy" for customers has become the only way to succeed and retain their custom, in organisations such a *productivity-first* approach to HCS has still not taken root. This is in contrast to the heavy focus on security awareness packages and phishing simulations, focused on making employees and the organisation *more secure*. At present, the demands on employees' resources go unchecked. Studies over several years have demonstrated that security managers still struggle to work in harmony with the workforce [7, 41]. HCS in organisations must account for productivity at work, where the role and extent of the security workload is accounted for, toward employees being able to work securely in a sustainable manner.

3 Methodology

We conducted five workshops with $n = 30$ CISOs located in Switzerland over the course of eight months. The CISOs discussed topics around HCS and security relationships. We documented the discussions and additional content to code and analyse it. Figure 1 shows our approach. The research presented in this paper aims to contribute to the approach of closing the research gap on creating an understanding of how CISOs react to HCS-related content and concepts, and what barriers they see. Using the action research method [11], the aim was to observe for the first time a community of CISOs discussing organisational collaboration and the use of HCS, and to monitor reactions and changes over time.

3.1 Engaging with a Community of CISOs

Together with a Swiss partner organisation (*Content Team*) we organised a workshop series for CISOs. Content Team organises networking events and knowledge exchanges about security. Content Team members were a CISO headhunter, management consultant, communication specialist, and security journalist. They approached the authors because their CISO clientele had raised the topic of HCS. The initial plan of workshop topics was developed over 4 meetings between the Content Team and the researchers. Preparation started mid-2021, and the first workshop took place in November 2021. The initial scope was to gather CISOs to discuss how to implement HCS. There would be expert speakers, but knowledge and experiences should be generated and exchanged by the CISOs themselves. The gathering of scientific data was announced from the beginning, but was running alongside the workshops, not driving them. The researchers, as HCS experts, delivered an introduction to HCS concepts and implementation examples in the first two workshops. CISO feedback on each workshop shaped the agenda and presentation methods for the subsequent ones – the Content Team decided based on questions raised by the participating CISOs.

Knowledge-wise, it should have been a give-and-get between the CISOs and the researchers – an approach with roots in action research [11], as applied previously in the realm of IT security [7, 61]. In this action research approach, knowledge generation happens in a cycle and the practitioners work together with the researchers to learn from each other – the study is partly co-designed with the participants [19].

Engaging with a *community* [18] of CISOs rather than with individual CISOs (e.g., in interviews or surveys) has multiple advantages and similarities to 'security dialogues' [7]: (I) research in (security) communities invites participants to be more open [51], simply because the environment is more natural than an (artificial) interview or survey setting (in our case the CISOs gathered with people they also meet at other events); (II) The discussion among CISOs holds the chance to shed light on topics the researchers did not initially have in mind; (III) Trust: A lot of CISOs might feel more comfortable in a group together with people like themselves, compared with the pure *confrontation* with an interviewing researcher; (IV) The motivation of such a high number of CISOs to participate in multiple workshops. It seems unlikely that they would have committed to multiple interviews, where they only would get interviewed rather than also receiving input.

In the end, five workshops took place (four in-person, one virtual due to COVID restrictions) that together lasted more than 20 hours. Additionally, we held a series of virtual insight chats after the second workshop, where CISOs discussed their topics alone or in small groups with researcher 1 (R1) – the lead researcher. For those we prepared an interview guide (see Appendix A), but again allowed the CISOs to ask us questions and drive the conversation if they wanted. After workshop 1 and 4, a member of the Content Team interviewed some CISOs to collect their feedback. In total $n = 30$ CISOs participated at the workshops (while not every CISO was present at every workshop) and we collected notes from over 25 hours of discussions.

Participants The largest group of participants were the CISOs. Three researchers were present at the workshops. R1 actively delivered content about HCS and participated in the discussions, while two researchers had passive roles – documenting the workshops. Together with four members of the Content Team we met online on a regular basis to prepare content for the next workshop and to lay down a road map. Our partners were also present at the workshops, with changing roles, like moderation, content presentation, or documentation. In three workshops, guest speakers were invited (from academia and industry). Two security awareness specialists participated in the workshops and discussions.

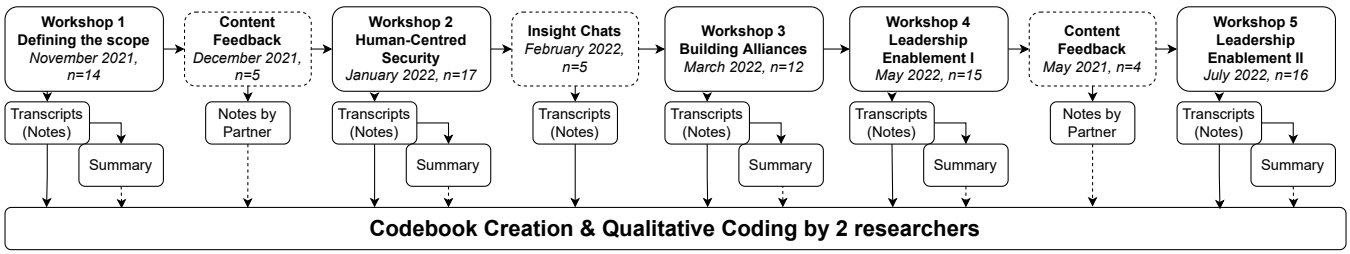

Figure 1: Our methodology: In every workshop a transcript of notes was created which then were, together with summaries, used for coding and analysis.

Content At the heart of every workshop were open discussions with the complete group, or smaller breakout groups. Those groups always had to discuss or solve specific tasks, given by the moderators. They were created by the Content Team assigning CISOs to one of two groups, trying to balance active and passive members. If the discussion went off-topic, the Content Team moderators would steer the discussion to the topic. In the larger group, content was delivered by speakers that was then heavily discussed among the CISOs. Here again, the Content Team moderators managed the discussions, ensured individual CISOs did not monopolise the discussion, and brought in more passive participants by asking them specific questions about their experiences. While some discussions between the CISOs were started by the CISOs themselves and topics were raised by them, the overall agenda was directed by presentations and tasks. Hence, we gave the CISOs stimuli for discussions. Those stimuli and the content of the workshops are presented in section 4.

Setting Four workshops took place in a large conference room in a building in a city in Switzerland. For the larger talks and presentations, the CISOs were seated at tables organised as an U-shape. For smaller group discussions the CISOs would split up and sit or stand around Flip-Charts at different corners of this room. One workshop was organised via Zoom, where the smaller groups were placed into breakout-rooms.

3.2 Recruitment

The recruitment was managed by the Content Team. Firstly, they used personal contacts to invite CISOs. Further CISOs were then invited via snowballing and by writing emails to large corporations and public agencies. In total, 92 invitations were sent, seven replied that they had no interest, 53 did not reply at all, from the remaining 32 CISOs who stated that they would be interested, only $n = 30$ could attend the workshops, mainly due to time conflicts. The main inclusion criteria were (I) the contacted person needed to hold the title of CISO, or a very similar security leadership position, and (II) they needed to work in Switzerland (even if the organisation might be international).

3.3 Data Collection

We could not record audio or video content of the workshops. Besides the problems with data privacy that such recording would pose, there was a risk that participants would be more guarded in what they said. Hence, we primarily relied on (pseudonymized) notes taken during the workshops: At every workshop, two researchers (both very skilled typists) independently recorded everything that was said. The aim was to capture the sentences and phrases as accurately as possible. In the larger group discussions the researchers would document the same content and the *transcripts* would later be validated against each other, as an additional quality check. In the smaller groups, the researchers could only document the content individually. Following every workshop we summarised what we documented, for further planning of the next workshop and to support our coding. After the first and the fourth workshop, one member of the Content Team called a number of CISOs to gather feedback on the last workshop. We included their notes on the calls in our analysis. At the insight chats between the second and the third workshop we documented the content just as we did during the workshops.

Due to the speed required for this manual documentation, we could not always tell which CISO exactly made which statement. However, we were always able to document whether a statement was made by a CISO or another participant, which was crucial for the coding process. Initially, the workshop was held in English, later in German, since all CISOs were German speakers. Hence, the language of our data collection changed as well. All German quotes were translated by us before they were presented in this paper.

3.4 Analysis

We applied Kuckartz' [42] process scheme of the content-structuring analysis, combining deductive and inductive coding strategies and a category-based evaluation along main codes. Our coding happened in multiple steps: (I) The initial code selection emerged from the summaries that we created immediately after every workshop. We initially included any topic raised by the CISOs. Two researchers created deductive code sets. (II) These code sets were then merged. (III) Two

researchers independently coded all *transcripts* deductively and inductively. (IV) The different code sets were discussed, reduced (guided by our research questions) and merged again. In multiple discussions we used mind-maps to find superordinate topics. We then sorted all codes as sub-codes to those topics. (V) Both researchers then coded one of the transcripts. (VI) In a final step the *transcripts*, the summaries, the notes taken by our partners and the outputs of the workshops (slides, flip charts, etc.) were coded. During all coding steps memos were created to amplify the identification of key topics. All coding was done in MaxQDA. Experts on qualitative data analysis argue that the value of multiple coding iterations by different coders lies in the process, as much as the final coding results. Involving multiple researchers as coders is important to identify themes and disagreements, but focusing on statistics such as inter-coder reliability can actually be detrimental to the qualitative nature of the study [9, 46]. In accordance with this, the coding process was highly collaborative, but the inter-coder reliability was not calculated. The final code book can be found in the Appendix C.

3.5 Demographics

The Content Team collected the job description, gender, company sector and number of employees in the organisation of the CISOs (see Table 1). We did not explicitly collect any additional demographic data, like educational background or age (though some CISOs gave away more information during discussions, such as educational and professional history).

Table 1: Background information of the participating CISOs.

Gender			#	%
Male			27	*90%*
Female			3	*10%*
Job Title				
CISO			24	*80%*
Co-CISO			1	*3%*
Head Enterprise Risk Management			2	*7%*
Lead IT Controlling & Security			1	*3%*
ITSO			1	*3%*
CIO			1	*3%*
Industry				
Insurance			3	*10%*
Finance			2	*7%*
Industry			6	*20%*
Media			3	*10%*
Public sector			1	*3%*
Retail/Logistics			4	*13%*
Others			11	*36%*
Number of Employees				
Max	100,000	*Average*	15,300	
Min	220	*Median*	4,500	

3.6 Ethics and Data Privacy

The study received approval from the Research Ethics Board at the authors' respective institutions.

Before the first workshop, the participants were informed that the workshops would be held under the *Chatham House Rule*[2], which allow anonymous citations of all that was said. All participants agreed to these conditions. Since it remained unclear whether the CISOs would allow the pseudonymized quotations, all quotes in the following Section are not attributed to a participant. We informed the participants that we would like to perform scientific analysis and report the results back to the workshop participants. The Content Team wanted to create a white paper for CISOs, and some of the CISOs wanted to use the content for internal discussions in their organisations. Hence, the complete workshop series was designed as a give-and-get format. We pseudonymized the data before we made our notes. We did not collect any additional personal data beyond what was said. We used the demographic data collected by the Content Team only in an anonymized aggregated form.

3.7 Limitations

Like in every research study with humans, our work has several limitations. Our manual data collection is less accurate compared to audio or video recordings – due to the sensitive nature of the content and the positions of the participants in their organisation, however, this type of passive collection was almost inevitable. Taking the notes, we also could in some cases not distinguish which participants made which statement. However, whenever possible, we validated the notes made independently by researchers to increase the quality. In the workshops one of the researchers did not have a passive role, but participated in the discussions and delivered scientific content. This may have influenced the outcome, but we were careful at being transparent about those influences in the report of our results. While we co-controlled the agenda of the workshops, open discussions are not like semi-structured-interviews: The CISOs regularly directed the discussions to topics that they found interesting and hence off-topic content was discussed as well. Like with every group where different characters meet, some CISOs engaged proactively in every discussion, while others needed to be be asked to participate by moderators. As a result, the share of the discussions between CISOs may be unequal. This is further amplified by the fact that not all CISOs participated in all workshops. The sample of CISOs is biased in a way that all who participated expressed at least interest in the topic of HCS. Other CISOs that expressed no interest in the workshop series might have a very different perspective on this topic. While the CISOs represent a wide variety of organisations, they were all located

[2]Chatham House Rule: https://www.chathamhouse.org/about-us/chatham-house-rule, accessed October 11, 2022.

in Switzerland and our results might not necessarily speak for other countries and cultures.

4 Workshops

Besides 5 main workshop sessions, so called insight chats, as well as session related feedback interviews were conducted. The first two of the total of five sessions served in particular for exploration. After that, the other three sessions were structured and designed according to the interests and needs of the participants and the corresponding information was made available to them (a community-driven give-and-get approach). An overview of the agendas of the workshops can be found in Appendix B.

Workshop 1 – In Person: The Kick-Off workshop took place in November 2021 in Zurich, 14 CISOs participated. Firstly, a definition of HCS and what HCS includes was discussed. This included concrete examples of usable solutions for corporate environments (e.g., passwordless authentication, low-effort secure data-sharing). The idea of human error and user blaming was challenged [2, 59] and the behaviour model of Fogg [29] was introduced that leads to the conclusion that security must be as simple as possible. The following question guided the participants through a subsequent discussion in two groups: *Where do you think we should be heading to establish a natural security behaviour?*

Workshop Content Feedback: In January 2022 a content team member conducted telephone interviews with 5 CISOs to collect initial content (deeper thoughts about the previously discussed HCS related content) for the second workshop. Results were provided as notes to us; selected statements were taken into the second workshop by the content team member.

Workshop 2 – Virtual: In February 2022, the second workshop took place virtually due to COVID restrictions, 17 CISOs participated. The introductory talk by R1 started with the following opening question: "Do you know how much time your employees spend on security per day?". In the further discourse, R1 clarified the following three myths: 1st myth "Humans are the weakest link", 2nd myth "Security Awareness can change insecure behaviour", 3rd myth: "Humans are the first line of defence" – based on Reason [54].

Insight Chats – Virtual: With the *insight chats* we introduced the idea that the CISOs could discuss HCS topics that were important to them in more depth in small groups or one-on-one with R1. 5 CISOs took that chance and 3 insight chats were conducted virtually in February 2022. Again, researcher 2 and 3 participated to write down notes of this discussions.

Workshop 3 – In Person: The third workshop was held in March 2022 in Zurich, 12 CISOs participated. The topic was *building alliances* with other organisational departments. Therefore, two external speakers (one manager in a marketing department, the other in an HR department) were invited. Firstly, both gave keynotes about their everyday work, followed by group discussions with the CISOs. The CISOs were guided into reflecting how their own requirements could fit with other departments and how a give-and-get relationship could be built in two groups.

Workshop 4 – In Person: The fourth workshop was held in May 2022 in Zurich and the 16 participating CISOs dealt with the topic of leadership: They addressed the question of how managers can devote more time to the topic of human security and how CISOs can gain more of the management's attention with regard to risk communication. A CISO explained his personal situation in his organisation and an external speaker presented insights into his field of enterprise-wide risk management. The CISOs performed risk-analysis with a focus on communicating those in group sessions.

Workshop Content Feedback: After the fourth workshop a member of the content team again interviewed four CISOs via telephone in order to introduce their feedback in the content creation of the last workshop.

Workshop 5 – In Person: The fifth workshop took place in July 2022 in Zurich and 16 CISOs participated. Again, one CISO presented his experience with leadership engagement, before a communication coach talked about engagement with different types of leaders. In groups the CISOs prepared fictive slide-decks for presentations in front of their boards.

5 Results

Here we report the findings from our coding and analysis, based on different key topics that emerged, and relate them to existing work. The CISOs statements are marked with the session they were made at: S1-S5 represent the five workshops, I1-I3 the insight chats. Participant numbers are not included to respect non-attribution conditions.

5.1 Security Awareness & Training

Security awareness and training was the dominant topic that emerged regarding any HCS activity. All CISOs reported that they run **security awareness and training** in some form in their organisation, including in-person lectures, web-based training, video tutorials, posters, or live-hacking sessions. Some CISOs were critical about those efforts, and were looking for new ideas that the researchers and other CISOs might provide. One CISO asked *"How do I make sure that I reach my target group? How can I design regular training so that employees are picked up?"* — [I3].

Several CISOs linked awareness and training activities to a *fire-and-forget* approach, with no clear measurements of success. Some also acknowledged that already overworked employees had a lot of training to complete (not only security), and were missing leadership (middle management) support to make security training mandatory so that it would be recognised and planned for as a workplace duty. Some CISOs were of the view that the *check-box* nature of training was not helpful *"But many [security awareness vendors] just want to*

make money with it. There is then only a tool box off the shelf. So far, we have not found anything adequate." — [I1]

A few CISOs were open about the fact that compliance is the main motivation for why they (or their organisation) enact awareness and training, *"We do security awareness as traditional click-box exercise at the moment, for compliance, but we also do learning-based phishing."* — [I3]. Overall, the consensus among CISOs was that some form of awareness and training is necessary – and that they are responsible for overseeing those activities (in accordance with [33, 39]). At the same time, they were unsure that this would have a positive effect on employees' security behaviour. We asked CISOs whether they tailor the generic awareness and training products they bought for different groups of employees – only one expressed being interested in doing so.

The lack of wider support for awareness activity in organisations was also raised: *"I remember when I started working here a few years ago, there was a big security meeting and the awareness activity was to be introduced. With a lot of effort, five people could be found to help with it – two of whom dropped out after a short time, [...] and in the end one person remained. They do this voluntarily and on top."* — [I2] CISOs complained that middle management and team leaders rarely schedule explicit time for employees to complete awareness and training or attend events – in many of the CISOs' organisations, security awareness is offered but employees are not given time off for it: *"For example, we held a Cyber Security Day at two locations with live hacking and there were many aha moments. [...] but it is very time-consuming and cost-intensive [for the CISO to carry it out]. In addition, it depended on the interest of the employees, because it was a voluntary event. So people could come when they had time."* — [I2]

> CISOs consider security awareness and training activities to be necessary – at the very least for compliance purposes. However, CISOs have not found such activities effective in changing security behaviour, and found it difficult to get support from the rest of the organisation for enabling engagement with those activities.

5.2 Phishing Simulations

In the first workshop and again in the insight chats, R1 challenged CISOs with evidence that phishing simulations have not been shown to be effective in improving employees' ability to detect phishing [43, 56, 66]. The CISOs defended the phishing simulations as key in their work, because they are **the primary tool for measuring employees' security behaviour**: *"There's always a problem with training: we don't know what the learning effect was. With phishing emails, we can see that from KPIs. I'm a fan of that."* — [I3] or *"The miss rate, the fail rate has improved [after a phishing simulation]. The reports are also better. That is what I want."* — [I3] The CISOs use them extensively in their communication with superiors (CIO, board, etc.): *"If I go there today [to the superior] and say we need time, then I don't get it, if I show the phishing simulation numbers, then it works."* — [I3] Not all CISOs reported using phishing simulations yet, but none explicitly stated that they would not like to use it. Only one CISO expressed that the board would not be interested in phishing reports: *"They would never ask me that in a board meeting: What is this phishing mail thing? Can you show me one?"* — [S2]

Some CISOs reported that phishing simulations burden their relationship with employees: *"My organisation did these phishing campaigns and blamed those people. You trained them and you blamed them and now all the people are super confused."* — [S1]. That some organisations have experienced a backlash from employees already has made it into the news and there is research evidence on the negative effects of *sanctions* that are put in place by security managers [16].

Another CISO admitted that phishing simulations are not easy to implement: *"We have really good awareness, but we have a lot of discussions about phishing [with the employees]."* — [S2] One CISO noted that phishing simulations lose their purpose the more often they are conducted, but still believes in their benefits: *"If you've already run a few campaigns, it's already worn out. But I need to know how good my people are, so the phishing simulation helps me a lot."* — [I3] Another CISO agreed, but stated: *"I just want to prevent everyone clicking on everything."* — [I3]

> CISOs see the greatest value in phishing simulations providing numbers (perceived as a direct indicator of behaviour change), which can be used in reports to the board. They nonetheless acknowledged that simulated phishing increases the burden and is disliked by employees.

5.3 Security Friction

CISOs could not agree on whether it was their job to consider the effect of security workload and friction or the primary work of employees. We directly asked the CISOs if they knew the amount of time employees spend, for instance, on authentication every day [62]. The answers ranged from zero to 15 minutes – but most interestingly, some CISOs disliked the question itself: *"Of course, we need to consider this, but I am not quite sure how relevant it is at the end of the day because everybody is asking for a secure environment and it takes some time, of course."* — [S2]. Another CISO stated: *"If the employee doesn't accept that amount of time, he is not aware enough. So, we have to do more awareness so that he understands that [it is necessary to carry out security]"* — [S2]. Most CISOs admitted that they had up to now never thought about how much friction authentication could cause employees. Given that the workload and disruption caused by

authentication is one of the most researched and documented example in usable security research, it is noteworthy that practitioners today have never heard about it.

CISOs were also aware that employees' (business) needs would always outweigh security demands [13]: *"These people are getting paid for numbers and not the security [. . .]."* — [S1] and *"Employees don't care whether the security department denies WhatsApp, their boss doesn't care."* — [S1] However, CISOs from organisations with software developers said multiple times that they did not like to follow their special requirements: *"We have developers who want to install software tools for development, with admin rights. That must be forbidden!"* — [S3]

While some CISOs expressed *"IT-Security needs to be smart and invisible from the employees, needs to be aligned with business."* — [S2], no participants delivered deeper insights into how they would try to achieve this goal. The most extreme statement against the idea to relieve employees from security tasks was *"I think automation is quite dangerous, takes responsibility from the employees."* — [S3]

While some CISOs argued that security solutions must be *usable*, no participant mentioned any measure that could assist employees with their security tasks and hence implement usable security solutions – which might hint towards security managers' struggle to meaningfully consider usable security (as noted elsewhere [52, 55]).

> Many CISOs do not take into account the amount of employee time required for security, because they see security as an unavoidable cost that employees have to bear. This highlights a paradox, as many CISOs also acknowledge that business comes first.

5.4 Basic Concepts of Human Behaviour

In the first session and in the insight chats, multiple CISOs expressed the wish to **learn about psychological concepts**, from the researchers and external speakers. The participating CISOs focused their attention exclusively on techniques that would **help to control human behaviour** [4, 55] (*"Getting a control based on human, I think it is really interesting to look at this human aspect. But I need tools for measuring"* — [S1]) or improve their awareness measures (*"In the workshops I want to learn the best of how to do a human awareness program with the human-centred focus. We know a lot of technology, but there is a lack of knowledge how people act and interact."* — [S1]).

The CISOs were generally open about their lack of knowledge about human behaviour: *"I want to understand the psychology of awareness – there is too little psychological know-how in companies available."* — [S1] After we introduced the concept of (ethical) nudging in security [57], some CISOs said that they already heard about nudging and would like to implement it: *"I wonder where the nudges are that help? That would be really super exciting."* — [I1]. They debated the assertion *human behaviour is largely predictable*: *"human behaviour is really predictable?"* — [S2] with no conclusion: *"Human behaviour is predictable – errors are human. The attackers play with the psyche of people."* — [S1]

> CISOs show interest in learning about *psychological concepts*, especially in instruments for changing employee behaviour. They openly expressed not knowing enough about (the predictability) of human behaviour and having only heard about concepts like nudging.

5.5 Relationship With Management

The relationship with upper management became one of the most important topics in the workshop series. This was not our initial intention, but after the first workshop it became clear that **CISOs talk a lot about what they wish management would do** – even if basic HCS topics such as workload and friction were on the agenda. Management refers to anyone the CISOs directly or indirectly report to (especially CIOs and boards[3]).

Most cases reported by the CISOs cannot be described as a positive relationship, which correlates with recent findings of mistrust between management and CISOs [21]. The CISOs feel that they have a hard time getting their messages through to the board, or perceive a lack of awareness for security among the board members [32]. The CISOs' ideas about how boards function and make decisions also became clear: they agreed that technical details were not relevant for boards, and that they needed the "right language" for them [21]: *"A huge problem is to find the right language for top management. Find the same level as they think to bring this topic into their mindset. Since we achieved this we got more resources and tools."* — [S2] The CISOs used risk-maps, storytelling techniques, incident- and phishing reports on abstract levels or GRC (governance, risk and compliance concerns) reports to bring their messages through.

Most CISOs reported that boards want to spend as little money as possible on security: *"It's about building trust, we want budget and staff. But they [the board] don't really want that, and if we can do it with less budget and staff, then it's better."* — [S5] This contradicts findings from the US, where the majority of CISOs seems to be satisfied with budgeting decisions [48]. In line with the literature, our CISOs thought that they would gain more support and budget after their organisations – or comparable companies – suffered from security incidents [23, 48]: *"Budget usually comes too late – only after a major incident. But then there is understanding"* — [S1] CISOs point out the positive development that IT security is gradually seen as an IT problem, and more as a challenge for

[3] Please note that the term *board* is differently used in Switzerland and could sometimes mean the *Board of Directors* or the *Executive Directors* of the organisation. The CISOs did not distinguish between them.

the whole organisation: *"It was a hard challenge [to convince the management] that IT security belongs to the new normal and to not separate it from the regular business."* — [S2]

At least four CISOs expressed sentiments similar to paternalism towards the board. Examples ranged from the goal to make the board members more aware of security (e.g., one CISO directly asked the researchers: *"I'd be interested to know how you get management to look in the mirror and take a more self-critical look at the risks as well?"* — [S4]), the will to *raise them the right way* (*"You have to educate everyone, for all [security] processes. You also have to educate the management board."* — [S3]) to wanting to even bend the CEO to the security rules: *"At the awareness level, I want people to understand why they can't use it [a software prohibited by the compliance rules]. Everyone has to follow the same rules, including the CEO."* — [I2] Another CISO described the relationship with the CEO as: *"In the private company I work for, my boss [the CEO] sees me as his bodyguard."* — [S2]

Some CISOs felt that *"the management is not aware of their responsibility. They think they are secure, but no, they are responsible."* — [I1] However, here the experiences diverge and other CISOs saw a positive development: *"The problem is the tolerance for non-compliance at the top, but this tolerance is probably dropping."* — [S2]

> The CISOs reported diverse relationships with their management, but most have some form of communication issue (unavailability, misunderstanding, paternalism towards the board). Getting buy-in from top management is still something CISOs wish for, as they would like to receive more resources and also from management a higher awareness as well as a view of IT security as a challenge for the whole organisation.

5.6 Relationship with Employees

Even though researchers introduced not blaming the user as the key HCS principle in the first workshop [2, 47, 59], CISOs continued to use the phrase of employees as the *"weakest link"* in all subsequent workshops: (*"People are and remain the central factor. It's not the technology, all it takes is one employee who doesn't follow the regulations and standards."* — [S1]). In terms of how **CISOs (want to) communicate with employees**, different ideas, approaches, and wishes were raised. One CISO stated that it was important for them to talk to the employees in order to figure out and understand their business needs. Another participant admitted that *"The problem might be that we are talking too technically"* — [S1].

It was also discussed frequently whether a top-down, bottom-up or peer-to-peer communication approach would be more appropriate, and to what extent the storytelling approach could or should be followed: *"we have to convince them and start the community but not from up to down but from peer-to-peer, simplify the whole cybersecurity process"* — [S1] Regarding a possible appropriate form and setting of communication, one CISO shared the following experience: *"They appreciate one-to-one sessions, even if they don't have time."* — [S1] However, multiple CISOs responded to this idea with the concern that this would not be possible in larger organisations: *"The pure size of an organisation [number of employees] is a problem and hard to tackle, the reach is really important, my idea instead of direct talks: webinars."* — [S1] CISOs believed that communication and collaboration with employees could be a way forward. We introduced the idea of security champions [14, 15] (representative employees in different teams that would have direct connection to the security department or CISO) as a possible model. This was received more positively, and CISOs reported that in-house software development teams had implemented such a concept: *"There should be a security champion in every agile team. We train the champions and they always have a contact person in the second line (security coaches)."* — [S3]

The idea that employees should have a specific contact person in the security department was brought up by the participants independent of the security champions approach: at least some CISOs mentioned that employees should have a personal contact in the security department, to encourage reporting of possible security breaches: *"Do you [employees] know your security person? Or do you need any further information?"* — [S1] In a group discussion, CISOs described how they perceived their own role and related tasks in working with employees: they agreed that *"[The] CISO should be in a challenger role [. . .]: One should talk to employees about their concerns, and the CISO should have a 'How can I help you?' attitude."* — [S1]

> The image of employees, the attitude towards their security behaviour and the way of communicating with them varies among CISOs. Different ideas, approaches, challenges (e.g. regarding the size of the organisation, their role as CISO) and needs regarding communication with employees became clear. Approaches to collaboration were discussed partly positively, partly doubtfully.

5.7 Relationships Within the Organisation

The Content Team actively brought the topic of alliances with other departments into the discussion, starting at the third workshop. The topic was not raised by the CISOs themselves, but because they expressed so many problems in the communication with upper management, the content team felt that they should explore **possible solutions: building alliances with other departments (horizontal rather than vertical)** [7, 8] and deliver joint messages to the board. Relationships with the communication, sales, legal, marketing, and HR departments were discussed.

Some CISOs were eager to report that they had touchpoints

with other departments, but a collaboration of equals as outlined in *security dialogues* [7] – where CISOs try to understand the needs of others before adapting and pushing their own ideas – was not part of the discourse. CISOs who talked about their relationships with other parts of the organisation were most proud of having proactively forewarned them of security policy changes, so they are not overwhelmed when it happens: *"We have alliances, I mean stakeholder management. We have done a stakeholder analysis: We looked at who we need to pick up and inform, etc."* — [S5] Two CISOs saw marketing and sales as powerful allies, since they could help to market their IT security (which they considered excellent) internally and externally.

After one participant said in a group discussion that they liked to sanction employees who do not comply, another CISO disagreed and highlighted the role of the HR department in improving their relationship with employees: *"But then I would not have a reporting system anymore [no employee would report incidents anymore], so you have to do it with caution. And with HR, and also with Care Gate.*[4]*"* — [S3] Even though the topic of the third workshop was *Building Alliances*, one CISO's first thought of collaboration with other departments was: *"If increased risks are identified, I go to the departments as CISO and try to solve that there."* — [S3] – which is a traditional paternalistic policing approach. One CISO noted that building alliances only worked in larger organisations: *"The CISO is lucky if he has resources like marketing in the company."* — [S3] A more positive report came by another CISO: *"At the hospital [where this CISO works], I bring stories to the communication department, then they get them into the internal newspaper."* — [S3] One CISO saw the importance of collaboration with other departments primarily because their organisational structure demanded it: *"There are still a lot of meetings where there are a lot of people who have something to do with security (they all represent different departments) so collaboration is important."* — [S5]

> The CISOs realise that they have to meet the needs of a growing number of different departments. Building understanding of the needs of the other departments and building alliances happens with constraints, as their tasks and associated resources do not scale to meet the need.

5.8 Simple Solutions

Throughout all workshops, the CISOs wanted **check-lists** from the different speakers for solving **HCS and security relationship tasks**, e.g., *"For me personally, my responsibility is to make people feel aware about security. This is really annoying. What would help me is a paper or something, which says how it should be done."* — [S1] or *"Nudges for Information Security: An implementation guide would be helpful here."* — [S1]

[4] Online provider of psychological support.

Our results show up another perspective of previous findings, as we have observed that CISOs seem to view security as a *craft* where things *just need to get done* [21]. In smaller group discussions, the CISOs would regularly fall back to discussing technical security challenges, and the moderators had to bring the discussions back to the workshop topic.

The CISOs were interested, but sceptical of examples of HCS solutions from other organisational contexts, because they perceived them as not transferable. Especially the size of the organisations was something the CISOs saw as a hurdle for the discussed solutions, e.g., to get in contact with more employees: *"The difficulty is getting the new employees on board. This varies greatly depending on the size and the company."* — [S3] or *"With 14,000 employees, you're not going to be able to manage that [getting feedback from the employees]."* — [I2] The CISOs also repeated that *"HCS really depends on culture."* — [S2]

> CISOs would like to see checklists to guide them in influencing the behaviour of others. They see solutions that would involve direct interaction with employees as a challenge.

6 Discussion

We discuss our findings relative to our research questions, and infer lessons for practice (6.1) and research (6.2).

All 30 CISOs participated in the workshops because they were interested in HCS, and they all reported that the consideration of humans (employees) was part of their daily responsibility [39, 68]: They run security awareness and training, phishing simulations and report human-related measurements to their superiors. They attended the workshop because they had experienced problems in the course of those activities, and were seeking advice on how they could improve. Some CISOs hoped to understand human behaviour better, so that they could adapt their measures and messages. The researchers challenged participants' general belief that there were simple check-list-like ways of changing human behaviour, and introduced key principles from HCS research [2, 7, 35] and basic psychology [29] to make the organisation secure while maintaining employee productivity [12, 13, 34].

What our results show is that CISOs want to implement HCS. We also found that they do not sufficiently engage, analyse or craft bespoke solutions for their organisation. The reasons for this, which emerge from both our research and previous publications, are e.g., lack of board support or friction with other departments. They want ready-made solutions, and buy standard security awareness and training packages and phishing simulations (largely because it is the measure that provides numbers). Some of the participating CISOs have indicated that they see employees either as a vulnerability, or as people who should actively and enthusiastically participate in the defence of the organisation. With the exception of the

human firewall, CISOs did not describe employees as their partners or as their customers – their interest in *psychological concepts* is primarily because they want *to change the behaviour of unpredictable humans*.

In order for employees to develop secure routines [35], they would have to be actively supported and security would have to be made as easy as possible. Some participating CISOs believe that security is already easy enough for employees to manage. We would like to point out that while CISOs are able to simplify policies and configurations for employees and provide them with better guidance, simplifying security technologies is the domain of technology vendors.

A multitude of usable security studies investigate how controls can be designed to reduce the effort users need to spend to be secure (e.g., [13]) – and some of this research is backed by key industry players. So we left wondering why CISOs seem to not have realised yet that security that causes friction in their organisations is a problem. This finds its strongest expression in one CISO stating that it does not matter how much time employees spend on authentication tasks – because security is important, employees should do whatever it takes. Of course, CISOs are employed to make others see that security is important – so the mere suggestion that there might be considerations beside security (such as friction) for some contradicts the job description. As in other studies with CISOs [21], we found our CISOs to be somewhat detached from the organisation and its day-to-day business, and seeing their key relationships – with the employees and management – as adversarial rather than cooperative [4, 8, 55].

Since we conducted this activity with CISOs as action research, this accommodated the participating CISOs moving the discussions away from the HCS topics we introduced, to their relationship with the management and search for ways of influencing employee behaviour. One interpretation of our results is that the CISOs rationalise and deflect the responsibility for change either to the management (e.g., *they are responsible for errors if a breach happens*, *they do not personally commit to security*, *they do not make resources available before a breach happens*), or to the employees (e.g, *they are a security vulnerability and do not listen to our advice* or *they are the first layer of defence*). It should be noted that CISOs hereby retain their responsibilities within their job description. In order to expect them to take on the responsibility, they would also have to have the power (which they do not have) to do something in relation to that responsibility. However, we find that most CISOs (I) are aware of their lack of power [8, 55] (e.g., they cannot force employees to attend security training), (II) reach limits (e.g., not enough time is available to consult employees), (III) are perceived as IT-guys by other members of the organisations (e.g., are part of the IT and their budget is within the IT budget) and (IV) lack understanding by their superiors (e.g., superiors firstly care about the security strategies of competitors rather than security initiatives of the CISOs) – and hence blaming them for this situation would not be appropriate [55].

Dysfunctional Relationship With the Board What the CISOs told about their interaction with management suggest that the oft-cited *top-level buy-in* might be a myth. The CISOs relationship with the board is transactional, not collaborative, even though the CISOs themselves wish for more. Academic researchers and policy-makers assume that organisational leaders engage and provide support [8, 37]. Management colludes with the tunnel perspective, focusing on compliance and measurements to show they are doing something, and not realising how decisions about IT investment and procurement, for instance, affect the security posture of the organisation, and the security workload for employees. This problem is not new and not unique to security but rather common in many compliance-related topics, like sustainability, harassment-prevention or occupational safety: Responsibilities are shifted down in the hierarchy, but without active management support. What CISOs need from management is not necessarily more money, but for leadership to find relevant capability and capacity in the other parts of the organisation that can work with CISOs. The current status is part of a growing trend to try and solve problems in organisational structures and processes with training[5] rather than eliminating the root causes and initiate necessary changes. Here, more research that brings together board members and CISOs is required to identify the blockers – so far, the focus lies on the side of security and little is known in the security community about what drives top-management security decisions.

The Misconception of HCS in Organisations Arguably one sign of progress over the past 20 years is that CISOs and organisations are now aware of the *human factor of security*. That they run awareness, security training and phishing simulations might suggest that usable security makes an impact in practice. However, our participating CISOs use these measures in a way that is centred around the circumstances of their role, in a way which does not naturally enable human-centred security around meeting the needs of employees. Phishing simulations were originally designed to reduce the number of successful phishing attacks, but CISOs mostly use the numbers to link training (simulated emails) with action (click rates), which result in metrics that can be articulated to management. Over-reliance on this single measure to indicate how well the organisation is managing *human risk* is dangerous.

On the surface, the security awareness and training products the organisations use may close security knowledge gaps, but what is also important for the CISOs, is to use them to be compliant and to make a case for the importance of security, even if it causes friction. Important concepts of usable security and the compliance budget [13], contradict the view of the

[5] Better management, not endless training, will solve our corporate ills: https://www.ft.com/content/9d706def-2b70-42cf-9adb-099f7cd0c72b, accessed October 11, 2022.

CISOs who describe security friction as unavoidable. Some CISOs acknowledge that business needs come first, but either had not considered to track security workload until attending the workshops, or refused to do so, let alone consider ways of reducing the burden on employees. Two challenges arise from this: (I) measuring workload across technologies in complex organisational settings, and (II) ensuring that organisations can readily renew their security technologies to bring in more usable solutions (e.g., more advanced email filters to reduce the need for employees to manually check emails for threats). In summary, CISOs want to change employee behaviour, but respect that business comes first, while they are not measuring friction, but need something to measure behaviour, for which they use click-rates from phishing simulations.

6.1 Lessons for Industry

Little Effort Is Too Much Effort Even if the ambition of security management would be to demand as little effort as possible for security from the employees, Demjaha et al. [24] posit that secure behaviour provisions also assume that the employees, as decision-makers, have the resources to undertake training, education, etc. However, employees in an organisation are busy doing their paid work. This leads to the conclusion that any additional time spent on security-related behaviour should be negotiated for the employees, not by the employees. Demjaha et al. made it clear that the goal is not to dictate security-related behaviour to employees; rather, employees should be supported to not have to use their limited resources to compensate for gaps in security provisioning.

Lack of Power We found that our participants lack power (e.g., they cannot demand employee time, and can apparently only set up voluntary events, as in Section 5.1), which aligns with previous findings [8, 55]. The lack of empowerment of CISOs creates negative externalities for employees – because the CISOs are not empowered to make training a mandatory workplace activity, employees appear at fault for not over-extending to make the CISOs' under-powered efforts succeed.

This is to say that, rather than giving CISOs more authority to 'demand' more employee time, what is first required is to have a joined-up relationship with the rest of the organisation, to have agreement on ring-fencing the time they currently request alongside other workplace tasks, and have any time negotiated and committed for security agreed with the rest of the organisation [24]. This would have a number of consequences: (I) CISOs would need to quantify the time they need, thereby incentivising measuring the workload, and also, (II) by engaging more directly in negotiating time for employees to do training and security tasks, this acts as a 'brake' to moderate the amount of time that can be asked for security. Currently, there is a toxic mix of no measure of time mixed with an expectation of full compliance with what are, in practice, non-mandatory security demands.

What Can Money Buy You? If a CISO had sufficient financial resources, what type of awareness and security training could they buy? Can one get more videos, more posters, more quizzes for more money? Or could one get custom-made training, tailored to the organisational structures, policies, roles, knowledge levels and environments? Only one CISO reported that their training is customised to the employees. While two other CISOs reported that it is at least possible to buy customised training, we are not to sure about this: A short analysis of the publicly available product information of 38 leading security awareness vendors [3] shows that at most five offer some form of customisation – but in all cases only based on different knowledge levels or job roles.

Silos & Isolated Communities Our results suggest that the CISOs are not often working (exchanging) with other departments in their organisations, but rather only work with their team members and the management above them – something well known in organisational theory as *Silo Effect* [63, 65]. As the CISOs acknowledge that IT security is not uniquely about IT anymore, but rather a task for the whole organisation and the board [32, 44], every security strategy has its limits as long as other departments are not engaged in a give-and-get process. The CISOs also reported that their managers would look at the *best practices* of competitors to make their security budget decisions. The CISOs themselves naturally follow best practices, academic concepts did not reach them [21] and so the CISOs end up implementing awareness and training, without being incentivised to be able to balance the pros and cons for their own organisations. CISOs and other security practitioners need to break those silos, start working with other departments, listen to them, accept contradicting ideas and also meet in circles and conferences that are not only built around the topic of security. Otherwise, inward-looking security best practices will further self-amplify and cause damage to the productivity and security of organisations.

Another part of the solution could be to recognise that much of the work done by CISOs naturally involves many levels and functions in a business (see Section 5.5). For instance, multi-stakeholder (board) **risk committees** already exist, yet our participants argued that it was up to them to fight a case for being included – they were being kept in a silo as much as they were willing to remain in a silo. Signalling that good security requires collaboration with others in the organisation would change the perspective of the role.

6.2 Lessons for Researchers

Bringing the Water to the Horse Our results show that usable security and human-centred security are of great interest to practitioners, but key concepts are misinterpreted. Our method bridges the gap between producing research and it reaching the practitioners who would benefit from it. What we uncover in doing so is 'patchwork' adoption of HCS prin-

ciples, sometimes with negative side-effects (a known phenomena in behaviour change interventions [50] and security specifically [17]). The format we introduced in this paper – where we not only collected data, but also brought research knowledge to a large group of security leaders – was only partially successful. We conclude that explaining the principles – leading the horse to water – was not enough to sustainable change the CISOs mindset. CISOs do not think scientifically (it is not part of their role and own biographies), they need concrete tools for engaging with employees [55] and coaching while applying them in their own context – bring the water to the horse and show how to drink it. We, the researchers, need to actively engage with the practitioners.

A Shift to Evidence-Based Security We assumed that CISOs would have interest in learning the principles of HCS, and how to apply them. However, this was only partly true and the CISOs redirected the sessions to different topics. The reason could be that it is not part of the traditional CISO worldview and requires a new skill set, as outlined by [7], and because organisations do not provide them with the relevant expertise, such as usability, as diagnosed by [55].

What was perhaps even more surprising to the researchers was the little interest in a evidence-based approach assessing the cost and benefit of the security measures they introduced, and that the CISOs pushed back when evidence to the contrary – such as [43] on the effects of simulated phishing – was presented to them. They were mostly interested in measurements they could present to answer questions from superiors, satisfy compliance requirements, or argue for more budget. Having listened over many hours, we attribute this in large parts to the fact that CISOs are overworked and worn down by feeling misunderstood and underappreciated by employees and management alike. Measurements that would help them improve security over time, or long-term planning to improve technology and processes, is not what they are interested in. They exhibit signs of being in a *tunnelling state* [53], just focusing on the tasks they know from their community of practice, and what they think management wants, instead of applying *evidence-based security*, like physicians do these days with *evidence-based medicine* [58].

Reflection on the Community Method As we hoped, the input from the CISOs shaped the content of the workshops (especially the focus on problems in the relationship with management), and we got many surprising insights that we reported here. In every group setting, some participants are very active, while others only offer their thoughts when asked directly in smaller group sessions. Capturing who said what is not always possible, meaning we could not relate every statement to a concrete participant, or capture how many CISOs agreed or disagreed with a particular statement. The CISOs who participated in the private insight chats were more open there than in the workshops (e.g. admitted that they only do awareness training for compliance reasons). In the course of the workshops, we could see changes on different levels: On the one hand, these resulted from the content-related and organisational framework conditions. The open structure of the first two sessions led to open discussions and many contributions from the CISOs, which was reduced in the subsequent sessions (which is reflected in our results). On the other hand, we were able to determine that the fluctuation initially observed decreased, a process-oriented concretisation of the common goal led to fewer critical voices (presumably also due to the active involvement of the CISOs) and the trust of the CISOs in each other and in the content team grew – reflected in an increasing disclosure of personal experiences as well as opposing opinions. In summary, we believe our method is valuable for (I) adaptive, (II) long-lasting, (III) give-and-get research with (IV) an exclusive (harder to reach) population.

7 Conclusion

This is the first longitudinal study of a community of $n = 30$ CISOs discussing how they interact with employees and management in their organisation. We found that CISOs are interested in HCS, but ultimately entirely dependent on what security vendors offer and their peer community sees as *best practice* – i.e., they can only implement awareness and security training and phishing simulations and wish for methods to get control over employees, rather than acknowledging human constraints and employee requirements. The CISOs shift responsibilities towards the management and employees, with the root cause being a lack of power to enforce HCS measures. While we suggest that CISOs could, for example, be positioned in multi-stakeholder risk committees to reduce this problem, we believe that (more) research into the perspective of board members and top-management on security is necessary, for example by bringing CISOs and board members together in a similar workshop setting.

Acknowledgements

We would like to thank the members of the Content Team and all participating CISOs. Thanks to the five anonymous reviewers and especially our shepherd for their detailed feedback. We would like to thank Maximilian Golla, Christina Eckel, Jennifer Friedauer, Leona Lassak and Markus Schöps for their technical help and proofreading. 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] ABRAHAM, C., CHATTERJEE, D., AND SIMS, R. R. Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons 62*, 4 (2019), 539–548.

[2] ADAMS, A., AND SASSE, M. A. Users are not the enemy. *Communications of the ACM 42*, 12 (1999), 40–46.

[3] ADDISCOTT, R., AND CLAUDE, M. Market Guide for Security Awareness Computer-Based Training.

[4] ALBRECHTSEN, E., AND HOVDEN, J. The information security digital divide between information security managers and users. *Computers & Security 28*, 6 (2009), 476–490.

[5] ANDERSON, A. B., AHMAD, A., AND CHANG, S. Competencies of cybersecurity leaders: A review and research agenda. *ICIS 2022 Proceedings* (2022).

[6] ARMBRUSTER, G., WHITTINGTON, J., AND ENDICOTT-POPOVSKY, B. Strategic Communications Planning for a CISO: Strength in Weak Ties. In *Journal of The Colloquium for Information Systems Security Education* (2014), vol. 2, p. 10.

[7] ASHENDEN, D., AND LAWRENCE, D. Security Dialogues: Building Better Relationships between Security and Business. *IEEE Security & Privacy 14*, 3 (2016), 82–87.

[8] ASHENDEN, D., AND SASSE, A. CISOs and organisational culture: Their own worst enemy? *Computers & Security 39* (2013), 396–405.

[9] BARBOUR, R. S. Checklists for improving rigour in qualitative research: a case of the tail wagging the dog? *Bmj 322*, 7294 (2001), 1115–1117.

[10] BARTSCH, M. Woher nehmen, wenn nicht stehlen – oder wo haben Sie Ihren CISO her? (German). In *Cybersecurity Best Practices*, M. Bartsch and S. Frey, Eds. Springer Fachmedien Wiesbaden, Wiesbaden, 2018, pp. 261–269.

[11] BAUM, F., MACDOUGALL, C., AND SMITH, D. Participatory action research. *Journal of epidemiology and community health 60*, 10 (2006), 854.

[12] BEAUTEMENT, A., BECKER, I., PARKIN, S., KROL, K., AND SASSE, A. Productive security: A scalable methodology for analysing employee security behaviours. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (2016), pp. 253–270.

[13] BEAUTEMENT, A., SASSE, M. A., AND WONHAM, M. The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms* (New York, 2008), A. Keromytis, A. Somayaji, C. W. Probst, and M. Bishop, Eds., Association for Computing Machinery, p. 47.

[14] BECKER, I., PARKIN, S., AND SASSE, M. A. Finding security champions in blends of organisational culture. *Proc. USEC 11* (2017).

[15] BERIS, O., BEAUTEMENT, A., AND SASSE, M. A. 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* (2015), pp. 73–84.

[16] BLYTHE, J. M., GRAY, A., AND COLLINS, E. Human cyber risk management by security awareness professionals: Carrots or sticks to drive behaviour change? In *International Conference on Human-Computer Interaction* (2020), Springer, pp. 76–91.

[17] CHUA, Y. T., PARKIN, S., EDWARDS, M., OLIVEIRA, D., SCHIFFNER, S., TYSON, G., AND HUTCHINGS, A. Identifying unintended harms of cybersecurity countermeasures. In *2019 APWG Symposium on Electronic Crime Research (eCrime)* (2019), IEEE, pp. 1–15.

[18] COLES-KEMP, L., AND ASHENDEN, A. Community-centric engagement: lessons learned from privacy awareness intervention design. In *The 26th BCS Conference on Human Computer Interaction 26* (2012), pp. 1–4.

[19] COLES-KEMP, L., ASHENDEN, D., AND O'HARA, K. Why should i? cybersecurity, the security of the state and the insecurity of the citizen. *Politics and Governance 6*, 2 (2018), 41–48.

[20] DA SILVA, J. Cyber security and the Leviathan. *Computers & Security 116* (2022), 102674.

[21] DA SILVA, J., AND JENSEN, R. B. 'cyber security is a dark art': The ciso as soothsayer. *arXiv preprint arXiv:2202.12755* (2022).

[22] DEATH, D. *The CISO Role within US Federal Government Contracting Organizations: A Delphi Study*. PhD thesis, Capella University, 2021.

[23] DEMJAHA, A., CAULFIELD, T., ANGELA SASSE, M., AND PYM, D. 2 Fast 2 Secure: A Case Study of Post-Breach Security Changes. In *Proceedings of EuroS&PW 2019, IEEE European Symposium on Security and Privacy Workshop* (2019), IEEE, pp. 192–201.

[24] DEMJAHA, A., PARKIN, S., PYM, D., GROSS, T., AND VIGANÒ, L. The boundedly rational employee: Security economics for behaviour intervention support in organizations. *J. Comput. Secur. 30*, 3 (jan 2022), 435–464.

[25] ERASTUS KARANJA. The role of the chief information security officer in the management of IT security. *Inf. Comput. Secur. 25* (2017), 300–329.

[26] ERASTUS KARANJA, AND MARK A. ROSSO. The Chief Information Security Officer: An Exploratory Study. *Journal of International Technology and Information Management 26* (2017), 23–47.

[27] FITZGERALD, T., AND KRAUSE, M. *CISO leadership: Essential principles for success*. CRC Press, 2007.

[28] FLYNN WOLF, ADAM J. AVIV, AND RAVI KUBER. Security Obstacles and Motivations for Small Businesses from a CISO's Perspective. In *30th USENIX Security Symposium (USENIX Security 21)* (2021), USENIX Association, pp. 1199–1216.

[29] FOGG, B. J. *Tiny habits: The small changes that change everything*. Eamon Dolan Books, 2019.

[30] FORD, A., AL-NEMRAT, A., ALI GHORASHI, S., AND DAVIDSON, J. Impact of CISO Appointment Announcements on the Market Value of Firms. *International Conference on Cyber Warfare and Security 17*, 1 (2022), 375–384.

[31] FORTUNE BUSINESS INSIGHTS. Cyber Security Market Size 2021-2029.

[32] GALE, M., BONGIOVANNI, I., AND SLAPNICAR, S. Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. *Computers & Security 121* (2022), 102840.

[33] GOODYEAR, M., GOERDEL, H. T., PORTILLO, S., AND WILLIAMS, L. Cybersecurity Management In the States: The Emerging Role of Chief Information Security Officers. *SSRN Electronic Journal* (2010).

[34] HERLEY, C. 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* (2009), pp. 133–144.

[35] HIELSCHER, J., KLUGE, A., MENGES, U., AND SASSE, M. A. "Taking out the Trash": Why Security Behavior Change requires Intentional Forgetting. In *New Security Paradigms Workshop* (New York, NY, USA, 2021), ACM, pp. 108–122.

[36] HOOPER, V., AND MCKISSACK, J. The emerging role of the CISO. *Business Horizons 59*, 6 (2016), 585–591.

[37] HU, Q., DINEV, T., HART, P., AND COOKE, D. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences 43*, 4 (2012), 615–660.

[38] HUAMAN, N., VON SKARCZINSKI, B., STRANSKY, C., WERMKE, D., ACAR, Y., DREISSIGACKER, A., AND FAHL, S. A Large-Scale interview study on information security in and attacks against small and medium-sized enterprises. In *30th USENIX Security Symposium (USENIX Security 21)* (Aug. 2021), USENIX Association, pp. 1235–1252.

[39] JULIA H ALLEN, GREGORY CRABB, PAMELA CURTIS, BRENDAN FITZPATRICK, NADER MEHRAVARI, AND DAVID TOBAR. Structuring the Chief Information Security Officer Organization.

[40] KIRLAPPOS, I., PARKIN, S., AND SASSE, M. A. "Shadow security" as a tool for the learning organization. *ACM SIGCAS Computers and Society 45*, 1 (2015), 29–37.

[41] KIRLAPPOS, I., AND SASSE, M. A. Fixing security together: Leveraging trust relationships to improve security in organizations. In *USEC15* (2015), Internet Society.

[42] KUCKARTZ, U. *Qualitative inhaltsanalyse (German)*. Beltz Juventa, 2012.

[43] LAIN, D., KOSTIAINEN, K., AND ČAPKUN, S. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)* (2022), pp. 842–859.

[44] LOWRY, M. R., VANCE, A., AND VANCE, M. D. Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity. *SANS* (2021).

[45] MAYNARD, S. B., ONIBERE, M., AND AHMAD, A. Defining the Strategic Role of the Chief Information Security Officer. *Pacific Asia Journal of the Association for Information Systems* (2018), 61–86.

[46] MCDONALD, N., SCHOENEBECK, S., AND FORTE, A. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proceedings of the ACM on Human-Computer Interaction 3*, CSCW (2019), 1–23.

[47] MENGES, U., HIELSCHER, J., BUCKMANN, A., KLUGE, A., SASSE, M. A., AND VERRET, I. Why IT Security Needs Therapy. In *Computer Security. ESORICS 2021 International Workshops*, vol. 13106 of *Lecture Notes in Computer Science*. Springer International Publishing, Cham, 2022, pp. 335–356.

[48] MOORE, T., DYNES, S., AND CHANG, F. R. Identifying how firms manage cybersecurity investment. *Available: Southern Methodist University. 32* (2015).

[49] NOBLES, C. Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *HOLISTICA–Journal of Business and Public Administration 13*, 1 (2022), 49–72.

[50] OSMAN, M., MCLACHLAN, S., FENTON, N., NEIL, M., LÖFSTEDT, R., AND MEDER, B. Learning from behavioural changes that fail. *Trends in Cognitive Sciences 24*, 12 (2020), 969–980.

[51] PARKIN, S., ARNELL, S., AND WARD, J. Change that respects business expertise: Stories as prompts for a conversation about organisation security. In *New Security Paradigms Workshop* (New York, NY, USA, 2021), NSPW '21, Association for Computing Machinery, p. 28–42.

[52] PARKIN, S., VAN MOORSEL, A., INGLESANT, P., AND SASSE, M. A. A stealth approach to usable security: Helping it security managers to identify workable security solutions. In *Proceedings of the 2010 New Security Paradigms Workshop* (New York, NY, USA, 2010), NSPW '10, Association for Computing Machinery, p. 33–50.

[53] RATNER, R. K., ZHU, M., SHAH, A. K., SHAFIR, E., MULLAINATHAN, S., THOMPSON, D. V., AND GRISKEVICIUS, V. Why having so little means so much: scarcity shapes consumer decision making. *Advances in Consumer Research 42* (2014), 230.

[54] REASON, J. *Human error*. Cambridge university press, 1990.

[55] REINFELDER, L., LANDWIRTH, R., AND BENENSON, Z. Security Managers Are Not The Enemy Either. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19* (New York, New York, USA, 2019), S. A. Brewster, G. Fitzpatrick, A. L. Cox, and V. Kostakos, Eds., ACM Press, pp. 1–7.

[56] REINHEIMER, B., ALDAG, L., MAYER, P., MOSSANO, M., DUEZGUEN, R., LOFTHOUSE, B., VON LANDESBERGER, T., AND VOLKAMER, M. An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (2020), pp. 259–284.

[57] RENAUD, K., AND ZIMMERMANN, V. Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies 120* (2018), 22–35.

[58] SACKETT, D. L. Evidence-based medicine. In *Seminars in perinatology* (1997), vol. 21, Elsevier, pp. 3–5.

[59] SASSE, M. A., BROSTOFF, S., AND WEIRICH, D. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal 19*, 3 (2001), 122–131.

[60] SHAYO, C., AND LIN, F. An exploration of the evolving reporting organizational structure for the chief information security officer (ciso) function. *Journal of Computer Science 7*, 1 (2019), 1–20.

[61] SLUPSKA, J., DAWSON DUCKWORTH, S. D., MA, L., AND NEFF, G. Participatory threat modelling: Exploring paths to reconfigure cybersecurity. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2021), CHI EA '21, Association for Computing Machinery.

[62] STEVES, M., CHISNELL, D., SASSE, A., KROL, K., THEOFANOS, M., AND WALD, H. Report: Authentication Diary Study, 2014.

[63] TETT, G. *Silo Effect, the: Why Putting Everything in its Place isn't Such a Bright Idea*. Little, Brown Book Group, London, 2015.

[64] ULRICH, P. S., TIMMERMANN, A., AND FRANK, V. Organizational aspects of cybersecurity in German family firms – Do opportunities or risks predominate? *Organizational Cybersecurity Journal: Practice, Process and People ahead-of-print*, ahead-of-print (2021).

[65] VATANPOUR, H., KHORRAMNIA, A., AND FORUTAN, N. Silo effect a prominence factor to decrease efficiency of pharmaceutical industry. *Iranian journal of pharmaceutical research: IJPR 12*, Suppl (2013), 207.

[66] VOLKAMER, M., SASSE, M. A., AND BOEHM, F. Analysing Simulated Phishing Campaigns for Staff. In *Computer Security* (Cham, 2020), I. Boureanu, C. C. Dragan, M. Manulis, T. Giannetsos, C. Dadoyan, P. Gouvas, R. A. Hallman, S. Li, V. Chang, F. Pallas, J. Pohle, and A. Sasse, Eds., Springer International Publishing, pp. 312–328.

[67] WHITTEN, A., AND TYGAR, J. D. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX security symposium* (1999), vol. 348, pp. 169–184.

[68] WHITTEN, D. The chief information security officer: An analysis of the skills required for success. *Journal of Computer Information Systems 48*, 3 (2008), 15–19.

[69] ZURKO, M. E., AND SIMON, R. T. User-centered security. In *Proceedings of the 1996 workshop on New security paradigms* (1996), pp. 27–33.

[70] ZWILLING, M. Trends and Challenges Regarding Cyber Risk Mitigation by CISOs—A Systematic Literature and Experts' Opinion Review Based on Text Analytics. *Sustainability 14*, 3 (2022), 1311.

A Insight Chats Interview Guide

View on Human Error

1. What do you think about human error in the context of IT security?
2. What do you see as the *weakness* of employees in the context of IT security?
3. What do you think employees need to learn (when and how) about IT security?
4. Do you assume that employees are aware of the risks related to IT security?

Information Sources

1. Where do you get your information about security and especially human-centred security from?
2. Do you have any particular sources?
3. What are you guided by? (public security agencies, other CISOs, security magazines, conferences, research articles, twitter, etc.) In case there is an answer: which exactly [name of the venue]?

Security Communication and Productive Security

1. Who are the people you are regularly working with in your jobs? (IT guys, management/ board, CIO, regular employees, other security experts, security vendors, security consultants)
2. How would you describe your relationship with other employees?
3. How often do you have contact with other employees? (in which setting, if any, does this contact take place? by phone, via e-mail, in person, etc.)
4. How do you think employees would describe this relationship?
5. What do you know about the employees' work tasks?
6. How would you describe your relationship with your boss and to whom do you report?
7. When you design security policies, do you consider how they might affect employees in their working routines in the end?

B Workshop Agenda

Workshop 1

1. Introduction of the workshop, the organisers and the participants; in plenary by CISOs and Content Team
2. Establishing an agenda on HCS/ comic showing "human error"; as keynote and discussion by researcher 1 and CISOs
3. How to establish a natural security behaviour?; as group sessions by CISOs and Content Team
4. Aims of the workshop; in plenary by CISOs and Content Team

Workshop 2

1. "Do you know much time your employees spend on security?"; as keynote and discussion by researcher 1 and CISOs
2. Busting three security myths; as keynote by researcher 1
3. Daily challenges and hurdles; in plenary by 2 CISOs and Content Team
4. HCS definition; as group sessions by CISOs and Content Team

Workshop 3

1. Clarification HCS definition; as keynote by researcher 1
2. Experiences with alliances in the organisational context; as field report and discussion by one CISO
3. Alliances with the HR and marketing departments; as group sessions by CISOs, speaker from HR, speaker from marketing, Content Team
4. Classification and complementation of the findings; in plenary by researcher 1

Workshop 4

1. Management attention/ risk communication; as keynote and discussion by one CISO
2. Human factor in risk management/ risk assessment in organisations; as keynote and discussion, risk expert and CISOs
3. Carrying out a risk analysis; as group sessions with the Bow-Tie method by CISOs and Content Team

Workshop 5

1. Carrying out a risk analysis; as keynote and discussion by one CISO
2. People's risk perception and risk behaviour; as keynote and discussion by a professor of psychology and CISOs
3. Creation of 8 slides containing a story about the risk to be reported; as group sessions by CISOs and Content Team

C Code Book

Table 2: Our code book with main categories (bold) – 1/2.

Code	Description	Example Quote
Measurement	-	
Metrics	Statements on the use of metrics, KPIs or other measurability methods	*I am a fan of transparency and for that I need metrics. We are in the process of defining such metrics, what do we spend X amount on? [...] (P4)*
KPIs for management	Reported links between KPI use and management	*Figures/KPI are expected in practice. (PX)*
Security Friction	-	
Security Effort	Statements that refer to the (time) effort that employees have to spend on security	*If it is an aware user and it is still too much, then we have to look if we have too restrictive policies. (P10)*
Usable Security	Participants describe explicitly or implicitly what they understand by usable security and its implementation	*In general, you should look to get away from passwords. (P18)*
Conflicting Goals	Participants describe conflicts that employees experience in the interaction between security measures and their work tasks	*An example: The developer says that IT security is important, but that he needs a different tool. (P7)*
Relationship with Employees	-	
Communication with Employees	Reported experiences and problems regarding the possibilities of communicating about security with employees	*[...] the problem might be that we are talking too technical. (PX)*
Sanctioning	Statements that show the mindset and the handling of sanctioning possibilities with regard to the security behaviour of employees	*I want people to comply because they think it's good. I don't want people to behave safely so that they don't get terminated. (PX)*
Blaming	Statements from participants in which they hold employees responsible for security gaps and possible incidents	*Human is the weakest link, you need just one user to break the system. (P14)*
Positive Security	Statements indicating the extent to which concepts of positive security and thus non-prohibitive security are taken into account by participants	*"Are you sure that..." is much more effective than "You must not do that either". (P5)*
HCS and Psychology	-	
Human-Centred Security	Statements that are indicative of participants' attitudes and understandings of HCS	*Now we are back to technology. The technology has to influence the employees. Staff prefer to take the path of least resistance. (P7)*
Psychology	Experiences and expectations related to psychological constructs and models	*I wonder where the nudges are that help. That would be really super exciting. (P18)*
Incomparability	-	
Old vs. young People	Reported perceived differences between different age groups of employees related to the use and handling of security measures	*The third challenge are the different people (old, young...). Young people need more freedom, nudges, and flexibility. The challenge is to address the different mindsets. (PX)*
Organisations are different	Experiences that relate to the extent to which company size has an influence on the feasibility and success of security	*With 3,000 people, I can't catch everything. The people who work in development, controlling, who move a lot of money. That's where things have to work better. (P5)*
Awareness	-	
Training	Statements that refer to the training methods regarding security	*Customised training depending on user knowledge is expensive. (P13)*

Table 3: Our code book with main categories (bold) – 1/2.

Code	Description	Example Quote
Phishing Simulations	Reported experiences, attitudes and implementation practices explicitly related to the use of phishing simulations	*There is always a problem with training: we don't know what the learning effect was. With phishing emails, we can see that through KPIs. I am a fan of that. (P6)*
Awareness	Any statements from the participants that relate to awareness and corresponding mechanisms regarding security in the organisation	*We have models where it works, i.e. occupational safety, etc., because it works everywhere. That might also help security, perhaps in a slightly different way. It's always just the issue of awareness. (P7)*
Organisational Details		
Incidents and Near Misses	Participants expressed their experiences and ways of dealing with security incidents or near-incidents	*One example is reporting security incidents. I really do have things on my desk sometimes that you think are obvious. (P18)*
Compliance, Laws and Regulations	Statements that refer to which security rules are in place, how these are communicated and how the companies deal with non-compliance with established rules regarding security	*[...] Moreover, it is a company that does not dare to pronounce rules. Moreover, the rules are often softly formulated. (P7)*
Understanding Risks	Concrete examples and statements relating to the handling and assessment of security risks	*The risk we are talking about here is initially invisible and intangible. (PX)*
Responsibility	Reported experiences and attitudes on how organisations deal with taking responsibility for security incidents and risks	*You can hand over responsibility. If the awareness is not there, then no one cares. You think "it will fit". [...] (PX)*
Resources	Statements that refer to the resources that are made available to employees and CISOs in organisations for security and the effects of this (non-)provision	*The CISO is lucky if he has resources like marketing in the company. (PX)*
Financial Aspects	Participants describe which financial resources they are provided with for security and to what extent this has an impact on their work and the implementation of security in the organisation	*Budget usually comes too late - only after a major incident. BUT then there is understanding. (P14)*
Organisational Structure	Participants report on organisational structures and the impact these organisational structures have on the work of CISOs and the implementation of security measures	*[...] More often, it is only about organisational issues. For us, the security rule maker and the implementer must not be the same person. [...] (P6)*
Alliances	Participants report how they (do not) cooperate with other departments regarding security and what impact this alliance building has on their work	*I talked to internal communications the other day, would like to use only one channel, they would like to use multiple channels (newsletters, videos, etc. (P4)*
Role and Task of the CISO	Statements in which the CISOs describe how they themselves perceive their role and related tasks as CISO in the company and how these roles and tasks are seen by the employees	*[...] I am the personal phishing filter. People send me the mails. [...] (P5)*
Relationship with Management	Reported experiences on the relationship between CISOs and management and the (lack of) management support in organisations regarding security and related impacts	*A huge problem is to find the right language for Top-Management. Find the same level as they think to bring this topic into their mindset. Since we achieved this we got more resources and tools. (P14)*