Lacking the Tools and Support to Fix Friction: Results from an Interview Study with Security Managers

Jonas Hielscher, Markus Schöps, Uta Menges, Marco Gutfleisch, Mirko Helbling, and M. Angela Sasse, *Ruhr University Bochum*

https://www.usenix.org/conference/soups2023/presentation/hielscher

This paper is included in the Proceedings of the Nineteenth Symposium on Usable Privacy and Security.

August 7–8, 2023 • Anaheim, CA, USA

978-1-939133-36-6

Open access to the Proceedings of the Nineteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Lacking the Tools and Support to Fix Friction: Results from an Interview Study with Security Managers

Jonas Hielscher, Markus Schöps, Uta Menges, Marco Gutfleisch, Mirko Helbling, and M. Angela Sasse
Human-Centred Security, Ruhr University Bochum

Abstract

Security managers often perceive employees as the key vulnerability in organizations when it comes to security threats, and complain that employees do not follow secure behaviors defined by their security policies and mechanisms. Research has shown, however, that security often interferes with employees primary job function, causing friction and reducing productivity – so when employees circumvent security measures, it is to protect their own productivity, and that of the organization. In this study, we explore to what extent security managers are aware of the friction their security measures cause, if they are aware of usable security methods and tools they could apply to reduce friction, and if they have tried to apply them. We conducted 14 semi-structured interviews with experienced security managers (CISOs and security consultants, with an average 20 years experience) to investigate how security friction is dealt with in organizations. The results of the interviews show security managers are aware that security friction is a significant problem that often reduces productivity and increases the organization's vulnerability. They are also able to identify underlying causes, but are unable to tackle them because the organizations prioritize compliance with relevant external standards, which leaves no place for friction considerations. Given these blockers to reducing security friction in organizations, we identify a number of possible ways forward, such as: including embedding usable security in regulations and norms, developing positive key performance indicators (KPIs) for usable security measures, training security managers, and incorporating usability aspects into the daily processes to ensure security frictionless work routines for everyone.

1 Introduction

Security experts often describe humans as the key vulnerability in organizations [59, 69]: employees who are not aware of security threats, and do not follow prescribed secure behaviors. Usable security research established in the late 90s' [82] showed that in the contexts of employees' work goals and environment, their behavior is completely rational: they are hired, assessed and rewarded for performance on their primary job, so security policies and unusable security mechanisms that get in the way cause friction, and too much friction leads to security being circumvented [13]. Furthermore, friction does not only cost productive time and reduces innovation [47], it also makes organizations more vulnerable.

Even though some research has been done on investigating security tools for employees [19, 26, 29, 63, 91], only a few studies investigated usable security, and consequently also security friction, within real-world organizations [3, 18]. Security in companies cannot be achieved if the context in which employees find themselves is ignored. We therefore want to investigate how usable security and more specifically security friction are handled in organizations. This includes, perceptions of decisions makers, as well as consequences and causes of security friction. Therefore we focus on the following research questions:

Q1: How does organizational security management perceive security friction and deal with it?

Q2: What are the perceived causes of friction in organizations and its impact on the organization and its employees?

We reached out to highly experienced security managers and conducted $n = 14$ semi-structured interviews, 7 with CISOs and 7 with senior security consultants. Each interview focused on capturing their experiences and perceptions of security friction within organizations they worked for. With an average of 20 years of industry experience in large-scale organizations headquartered in a German-speaking region, we have addressed a wide variety of perspectives, measures and decisions made in organizations within the interviews and, consequently, also in our analysis.

Almost all our participants were aware about security friction and its relevance in the context of creating or implementing new security routines and policies. However, they described many cases, where usable security and hence resulting friction is not considered at all. As reasons for this,

they have cited both a lack of resources or strict external, as well as internal regulatory requirements. Additionally, caused friction is almost not measured and the reduction of friction, which might lead to boost in security and an increase in productivity, is not either. The active inclusion of friction in the decision making process and its consequences for productivity and security could be a first step towards more usable security.

To the best of our knowledge we are the first investigating security friction through the lens of security management within real-world contexts – which is also the case because especially CISOs have a busy, high-pressure job, so researchers asking for in-depth interviews face a challenge. Previous work focused either usable security within software engineering [39] or on end-users [55, 56]. Our contributions are the following: (I) we describe possible causes of frictions and the real world impact. (II) We highlight how security friction is perceived by our participants and how this shapes their security decisions within organizations. (III) We discuss open challenges in academia and give recommendations for industry and regulation authorities, how to establish more usable security routines and practices within organizations, e. g., that usable security should become embedded in regulations, norms and the security process [39, 41], that positive key performance indicators (KPIs) should be developed that highlight the (monetary and intellectual) savings that come with usable security measures, that security managers need to be actively trained in usable security, and that usability aspects should become part of procurement processes.

2 Related Work & Background

Here we summarize previous research about security friction in organizations (Section 2.1), as well as with and about security managers (Section 2.2).

2.1 Security Friction

Usable security research has the main goal of reducing the effort to use a secure tool or procedure [34] – explicitly and implicitly – and to increase the adoption rate of such [18]. Time and subjective satisfaction of the users is what needs to be achieved [34, 85]. While usable security studies often focus on understanding the (un)usability or improvement of tools, in our work we took a wider look: we consider *security friction* as a problem created through a multitude of badly written security policies and measures that cost time, effort, and nerves, and are not aligned with employees routines, ultimately leading to reduced productivity [76], shadow security [55] (the implementation of alternative security mechanisms by employees, if they perceive the prescribed as too complicated), or a reduced security level.

Herley [45] points out that security professionals often assume that employees only need to be convinced and persuaded to invest more time and effort in security, implying that employees would misjudge the cost-benefit trade-off, which has been refuted in most cases, for example by the concept of the compliance budget: the lack of adaptation of security and business processes leads to security friction, which, according to Beautement et al. [13], is the key to individual compliance problems. The compliance budget (consciously or unconsciously weighing the costs against the benefits) is further reduced when friction-triggering tasks accumulate or repeat, which can lead to employees no longer adhering to security guidelines. Blythe et al. [15] made it clear that managers in organizations are obliged to ensure that security rules are designed in such a way that they do not hinder the actual work.

In the context of security friction, the concept of *security fatigue* is notable. This phenomenon is described by Furnell [33] as a situation in which users, and thus employees, become tired of dealing with security and associated warnings. Various factors can trigger security fatigue, including the complexity of security tasks, constant confrontation with security measures and more. With regard to security friction, it was observed that employees feel security fatigue due to a state of friction between the fulfillment of security measures and primary job requirements and the resulting conflict [20]. Cram et al. [20] found, for example, that security fatigue can, among other things, lead to employees behaving in a risky manner when using computers in both work and private contexts. Furthermore, security fatigue should be considered as one of the costs users (employees) face when they are inundated with security rules [86].

In a two-fold study with 290 employees, Mayer et al. [62] found that productivity goal setting (KPIs) decreases security compliance – the goal to be productive being in direct conflict with following security policies. Albrechtsen [4], found that users fear a conflict of interest between *functionality and information security*. Molin et al. [67] recognize that CISOs should put personal productivity into consideration when putting security measures into place.

2.2 Security Managers

Some studies in the past looked at security managers, especially on CISOs, and investigated their role descriptions, tasks and backgrounds. While, to the best of our knowledge, no previous study looked at CISOs' perception of security friction, their role and the problems they are facing were part of some evaluations [11]. CISOs can mainly be found in larger organizations, while it is not strictly defined to whom they have to report [2, 27, 83]. Most CISOs have a background in computer science or engineering [28]. However, the required skill set of CISOs also includes *IT security skills* to defend, monitor, and protect [12, 49, 54, 93], *strategic security management and government* [8, 12, 38, 49, 54, 64], *leadership and communication skills* [8, 49, 93], and *security teaching skills* [8, 12, 54, 93].

Independent of their tasks, CISOs are under immense pressure and experience unhealthy levels of stress [70]. 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 [31, 50], their security budgeting decisions in agreement with the management [68], and their perceived role and collaboration in their organization [5, 9, 21–23, 30, 48, 60, 74, 77].

We are not aware of interview or questionnaire studies with a focus on security consultants – with the possibly closest studies being carried out with security advocates [42–44].

3 Method

We performed in-depth, semi-structured interviews with $n = 14$ highly experienced security professionals in highest security management positions to learn about their perception and handling of security friction in their organizations/ the organizations they advice. By combining the perspective of CISOs that drive security decisions from within the organization and security consultants, whose target groups are CISOs and high-level management, we are able to get internal and external perspectives on the topic. Our sample is small – while this specific population is in general rather small –, but they offer unique insights into incentives that drive decisions that create or prevent security friction. The interviews were organized as virtual conversations. They were carried out from April to June 2022. Our method is summarized in Figure 1.

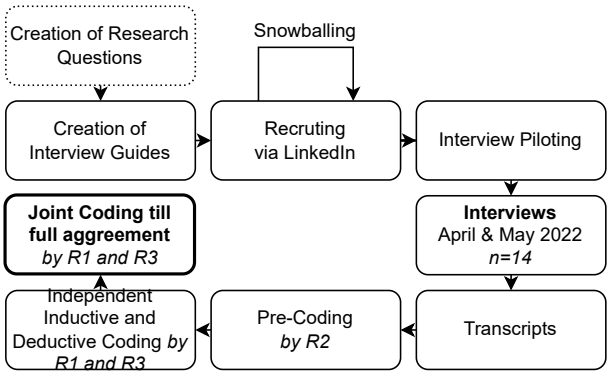

Figure 1: Our methodology.

3.1 Instrument Development

Within the following section we describe the structure of our interview guide and how it was developed. From previous research we can not assume that our participants have a uniform understanding of *usable security* and *security friction*. We therefore centered the interview guide around the organizations' employees in the context of security measures and decisions. Furthermore, within the first part of the interview guide we focused on understanding open challenges and their economic perspective. However, we only deal with these topics in our work if they were directly related to security friction.

Two interview guides were developed for both cohorts with slight differences: the questions for the consultants were asked around the organizations they advise, while the CISOs answered for their own organizations. The interview guides were developed by 4 researchers in multiple iterations over the course of 3 months. Due to the limited literature that focuses on security managers, only some guiding questions could be developed based on it, namely the questions around the relationship between employees and security managers [10, 22, 48]. One week before the first regular interview, we piloted our instrument with a security consultant, who gave feedback about the (I) administration, (II) interview atmosphere, (III) comprehensibility of the questions, and (IV) the content. Slight adjustments were made to the interview guide and the pilot interview was not included in our analysis.

Ultimately, all questions were organized around 8 guiding questions (see Appendix A for the full interview guide): firstly, we asked about the (personal) experience with security in the industry and their education. This was followed by questions about the biggest security challenges. The remaining six questions addressed employees' work routines, friction measurements, primary task conflicts in the organization and negative reactions from employees, as shown in Figure 2.

3.2 Recruitment

Since we aimed for highly experienced participants in management positions (and in larger organizations), we applied the following selection criteria: (I) participants had to be currently working as CISOs or (senior) security consultants, (II) they had to have at least 8 years of experience in the field of security, and (III) they had to either be qualified through an academic degree or relevant professional training (e. g., CISSP, CRISC, CISM) [72]. The recruitment happened in two steps: firstly, participants with according job titles, focused on the largest private and public organizations based in the country of our study, were searched on LinkedIn (33 in total, from which 10 did respond). In a second phase, the participants were asked whether they could provide other interesting interview partners (snowballing), which resulted in the recruiting of another 8 contacts. In the end, 14 interviews took place. We recruited in a German speaking country in Europe. The participants were native German speakers and were interviewed in German. We did not compensate the participants, because we did not feel that any monetary offer we could make would reach the hourly salary of the participants. Instead we offered to share our results.

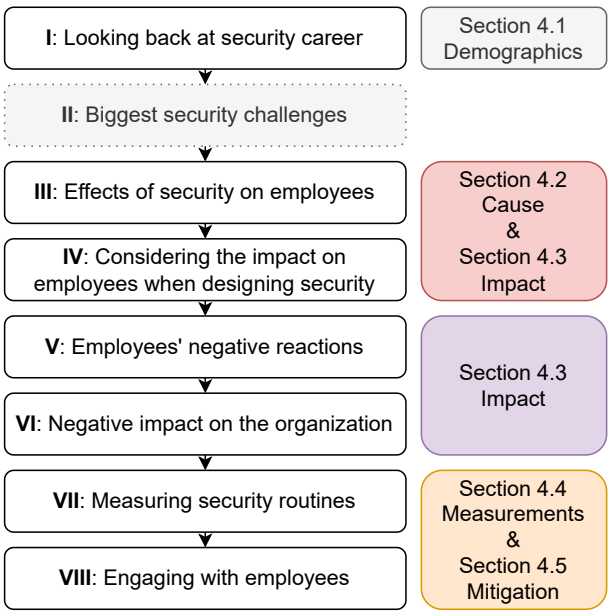

Figure 2: The 8 guiding topics (questions) of our interview guide(s), mapped to results in Sections 4 that mainly (but not exclusively) contain the answers.

3.3 Analysis

We applied Kuckartz' [58] process scheme of content-structuring analysis, combining deductive and inductive coding strategies and a category-based evaluation along main codes. The coding was done with MaxQDA and happened in multiple steps, carried out by three researchers (R1-R3) – all experienced coders – with two more (R4-R5) participating in the final analysis of the data: (I) in a first pre-coding step, R2 coded all 14 interviews to identify potential key topics. (II) Following this, R1 and R3 independently created deductive codebooks based on the interview guide and the research questions. (III) R1 and R3 then coded 5 different interviews (R1 coded 3, R3 coded 2) deductively and inductively. (IV) The codebooks were merged, reduced and superordinate key codes were identified. (V) One interview was deductively coded by both researchers, based on the merged codebook. (VI) We refined the codebook again and coded all remaining 8 interviews in a joint session, **until full agreement was reached**. (VII) In a final step R1,R3,R4 and R5 discussed the results of the coding process and how to present the results, which happened in multiple in-person and virtual meetings.

During all steps, multiple memos were created, guiding the discussion and analysis. Although we did not apply a saturation criteria to our sampling strategy, we experienced saturation during our analysis, as we found a high degree of overlap and repetition within the categories. Since the interviews were done in German, we translated those parts of the transcripts that we cited in the paper into English. The full codebook can be found in the Appendix C.

3.4 Ethics & Data Privacy

Our institution does not have an institutional review board (IRB) nor an ethics review board (ERB) for security research. We followed best practices in human subject research [89] and considered the deanonymization of the participants as the primary threat. We followed European data privacy guidelines (GDPR) and informed the participants about the study procedure and their rights prior to the interviews. All participants gave their agreement. As soon as the transcription of the audio files was completed, we deleted the audio files. We removed personal identifiers like names of individuals, organizations or other terms that might reveal the participants' identity. Furthermore, we kept the participants' country of residence, as well as the company they were working for a secret. We report some demographic data only in a pseudonymized or aggregated form. The community of CISOs is rather small and otherwise the demographic data we report here might reveal their identities.

3.5 Limitations

As with every study with human subjects there are several limitations in this study: all 14 participants were male. This is not only based on the fact that non-male security managers are underrepresented in the country of our study, but also due to the fact that we recruited through snowballing and the participants only suggested other male interview partners – a phenomenon well known as male-only-circles. The participants all present years of experience, with no one being new in this field. While one would expect this of a management position, this might have biased the results towards ignoring recent trends, only perceived by newcomers. Our study was performed in a European country, not all phenomenons might be found in other countries or cultures, e. g., due to different legislation. Given the challenge of getting enough time for an interview, we focused on a region where one of the authors had access to, and the trust of the participants. While they gave us a deep view into the security managers' perceptions of security friction, the results can not be generalized to a greater population.

4 Results

We first provide more details on our study participants (Section 4.1), before presenting our results about the causes of friction (Section 4.2), its impact on employees and the organizations (Section 4.3), how friction is measured (Section 4.4) and mitigated (Section 4.5), and, finally, how our participants perceive usable security (Section 4.6). Statements of CISOs are marked as *Ci1-Ci7*, those of consultants as *Co1-Co7*.

4.1 Demographics

We did ask biographic questions – about the educational background and experience – in the interviews. All 14 participants identified as male. Table 1 shows the most important demographic properties. To keep the participants anonymous, we do not report the exact education or years of experience, but the accumulated numbers in Table 2. The interviews lasted between 23 and 46 minutes, with an average of 34 minutes.

4.2 Causes of Friction

Within the following section, we describe participants' directly or indirectly mentioned causes of friction.

(Regulatory) Security Requirements Eight participants (Ci1, Ci2, Ci4, Ci5, Ci7, Co2, Co3, Co5) stated that following regulatory security requirements cause or can cause security friction: *"If the law makes it mandatory, then you have to do it, even if the employee is not entirely happy with it."* — [Ci2]. Furthermore, Ci2 expressed that there is no *debate* about whether to fulfill regulatory requirements or not. Ci4 explained that audits are so important that there is no room to consider friction: *"We also have our audits and therefore some things we just have to implement."* — [Ci4]. Especially if the focus is only on achieving a security certification, the implementation can suffer and cause friction: *"That leaves ISO27001 again. Because it is the most established. [...] The goal is: 'I want this certification.' And, to put it bluntly, you're almost walking over dead bodies. So now you [the employees] have to do it like this."* — [Co2]. Regulatory requirements, however, do not only come from the outside. Co5, who is working in the defense industry, explained that internal security policies are so strict that he only can support the employees to a certain extent: *"There is an attempt to provide employees with as many aids and assistance as possible. But it certainly cannot be taken into account to the same extent as perhaps in other places."* — [Co5].

New Security Around half of our participants explained that the introduction of new (stronger) security policies causes employees' disapproval: *"And in the worst case employees take this negatively, because something that used to work well then doesn't work anymore."* — [Ci3]; *"And then the bad guys are the security people, because they now demand something that wasn't necessary before, and that is the reason what leads to these backlashes."* — [Ci3]. The security managers view security as an additional expense for the employees in most cases. For example, Ci4 explained that participants have to do a lot more steps, because Multi-Factor Authentication (MFA) was introduced, and it is considered *normal* that participants react negatively, as they have to do more than before. Co1 reported that restrictions are often put in place before workable solutions/ alternatives are implemented: *"Implementing negative measures before you have the positive benefits. So banning messaging tools before you have a tool that is acceptable security-wise. So it doesn't matter now if we use Instagram, WhatsApp, or something. If I ban it for security reasons, then that produces negative reactions."* — [Co1] He added that the friction grew following more restrictions after a public security agency published warnings: *"Until last year, we still had the possibility to receive older office file formats via various channels, because they are still in circulation. [...] this led to an emergency change in the fall, so very quickly stricter restrictions were introduced on various channels."* — [Co1]

Lack of Resources Some participants stated that they did not have sufficient resources (money or time) to consider friction. Ci3 reported that the reduction of friction is possible, but that it comes with a cost: *"It is also relatively often possible to make this comfortable for the employees. The problem is that it costs money. Cheap measures are often taken at the expense of the employees."* — [Ci3]. Furthermore, Ci3 mentioned that if not enough resources are available, *"a lot has to be solved via guidelines or instructions"* — [Ci3]. Co1 also stated that the advantages of low-friction solutions can not (easily) be monetized, in difference to security awareness (trainings): *"If we do awareness, then every employee now has to do an e-learning in, let's say, 30 minutes. 30 minutes at an hourly rate anyway. That time costs. [...] What is charged less are, for example, the improvement possibilities. So let's take implementation of an identity and access management system. Instead of having to manage 20 passwords, for X systems, or so, I only have one password. One central authentication. That effectively gives savings. But you can't monetize that. Or very difficult to monetize."* — [Co1].

Old and Poorly Designed Security Two participants (Ci3,Ci7) described that old products, routines or services slowed down the implementation of modern (more usable) security structures or mechanisms: *"it will probably go on for some time until virtually all the legacy that we have built up over the last thirty years is somehow no longer there [...]"* — [Ci3]. But also bad designed awareness campaigns, or poorly planned security initiatives might cause friction and reactance: *"Poorly designed security measures or poorly designed awareness campaigns always lead to resistance at the beginning."* — [Co1].

Short Summary: Our participants perceive regulations and norms as a major cause of friction – as they do not believe that these leave room for taking employee demands into account. They also report that the introduction of new security policies and measures create friction.

Table 1: Demographic information of our participants. *Experience* is the experience in the field of information security in years. *Origin* describes the first touch points the participants had with information security. *Usab.* (Usability Importance) shows the participants answers to the question: "How important do you rate the issue on scale from 1 (not important) to 10 (very important) that security measures can be integrated into the work routines of employees?". Some participants decided to answer outside the scale with 11. *Size* is the number of employees of the organizations the CISOs are working for. *Dur.* is the duration of the interviews in minutes.

P	Sector	Education	Experience	Origin	Usab.	Size	Dur.
			CISOs				
Ci1	Public Sector	Certificates	20-25	Security Revision, Consulting	9	>30,000	25
Ci2	Finance	Master/ Diploma	20-25	Consulting	10	?	27
Ci3	Transportation	Master/ Diploma	10-14	Technical IT Security (Firewalls, etc.)	10	>30,000	31
Ci4	Finance	Vocational Training	>25	Mainframe IT	11	1,200	56
Ci5	Insurance	Master/ Diploma	>25	Organizational Security	7-8	4,500	43
Ci6	Construction	Master/ Diploma	22-25	Cryptography	10	3,500	22
Ci7	Banking	Master/ Diploma	20-25	Technical IT Security	10	900	32
			Consultants				
Co1	Consulting	Master/ Diploma	>25	Security Revision, Consulting	11		34
Co2	Consulting	Master/ Diploma	20-25	Penetration Testing	11		37
Co3	Consulting	Master/ Diploma	10-14	Technical IT Security	7-8		23
Co4	Consulting	Master/ Diploma	15-19	IT Administrator	10		46
Co5	Defense	Certificates	5-9	Project Consulting	9-10		27
Co6	Consulting	Certificates	N/A	Business Continuity Consulting	10		30
Co7	Consulting	Certificates	10-14	Politics Advisor	8		40

4.3 Impact of Friction

The security managers described the negative effect of security friction on employees, and the organization as such, which we elaborate in this section.

Circumventing Security Eight security managers (Ci1,Ci2,Ci5-Ci7,Co2-Co4) described that, in order to avoid friction between their primary task and the organization's security measures, the employees would seek for opportunities to circumvent the organizational security measures. Often it is about saving time to complete work tasks faster (and more comfortably), e. g., in regard to the handling of data: *"[...] that you send things home because it's so wonderfully convenient. Or that there is an instruction that data must be sent by web transfer, but you still send it unencrypted by e-mail because it's just faster."* — [Ci1]. The danger that was explicitly pointed out was that security measures can increase security to a certain extent, but that this could also have the opposite effect: if the employees are dissatisfied or feel disturbed by the security measures, it can happen that the security is circumvented, which creates new risks (*"The measures are circumvented. The security instructions are not followed. This creates new risks."* — [Ci6]). Another interviewee made it clear that reactions that express the experience of friction must be dealt with appropriately; and that it is precisely these *negative* reactions that are highly relevant. Especially regarding incomprehensible and impractical measures, there would be reactance and defensive reactions and ways of circumventing them. Furthermore, it was discussed that practical resistance and circumvention possibilities get around and are thus quickly spread.

Negative Reactions Triggered by Friction The interviews reveal a variety of possible reactions of employees to security measures that generate friction. As concrete examples, two interviewees (Ci2, Ci3) mentioned the development of *shitstorms* – an accumulation of incomprehension, frustration, displeasure, etc. – in response to new, changed and poorly implemented measures that can *escalate*, especially when several people in the team feel affected. In addition to possible resignations of employees, Co4 described the following form of employee reaction: *"[...] making a fist in your pocket sometimes and just up to refusing to work or just doing the exact opposite"* — [Co4]. Declining motivation or anger, triggered by a feeling of being overwhelmed, are also described as reactions. According to Ci3, negative feedback would be received especially if the security department had gone too far.

Restricting and Work-Impeding Security The respondents mainly described that friction for employees is that their work becomes *more difficult* due to security measures. This means that processes take longer and are more cumbersome, and that goals are achieved more slowly. Security measures are perceived as creating friction when restrictions are the result: *"You can no longer do everything as an employee. You are no longer available and so on. In other words, increased security typically leads to restrictions in the first phase, which*

are perceived negatively" — [Co1]. Other examples of restrictions are the prohibited exchange via cloud platforms or the use of flash drives. Examples of tedious and work-inhibiting processes are requirements for long passwords, frequent entry of a second factor or a screen time-out after five minutes.

Some of the interviewees clearly stated that employees want to do their main work (*primary task*) [37], also because they are measured by their achievement of goals and productivity. Security (*secondary task* [25,82]) means the investment of time that is lacking elsewhere. Ci4 gave the example of a nurse who might have such conflicts: *"Explain to a nurse, and I certainly have a very high level of understanding that she has to lock the screen of the departmental PC [...] And has to unlock it again when she comes back to the PC. The argument that they hear that can cost lives. Because it costs time. Yes, but it can also cost lives or at least have a bad impact on lives if someone wrong has access to the data."* — [Ci4].

Endangering Economic Efficiency Also (partly potential) economic effects were described in connection with friction through security measures. An increasing fluctuation rate of the employees due to emerging frustration about that processes are too slow, hinder work or block the achievement of defined project goals, was mentioned as an example. The output that employees could provide and the organization's revenue that depends on it can be negatively affected by friction-triggering security measures, such as the multiple entry of passwords. Employees may be discouraged from performing the associated work tasks regularly or need more breaks. Co7 has been clear about this: *"[...] we are shooting ourselves in the foot if we make employees there dissatisfied and also negatively influence the profitability of an organization"* — [Co7]

Short Summary: The security managers described various effects triggered by friction, such as the circumvention of security measures, which can lead to new risks, or the deterioration of the quality of relationships between employees and the security department. Resignation, frustration and decreasing motivation were described as reactions of the employees, which in turn can negatively influence the economic efficiency of the organization.

4.4 Friction & Routine Measurements

Importance of Friction Measurements In general, all security managers (except Co4) did provide ideas about how to measure security friction or get insights into employees routines. Even though most managers describe friction measurements as being important, some (Ci2,Ci6,Ci7, Co1,Co3,Co5-Co7) mentioned that it is often not followed through in the organization (*"In my experience, far too little. You do something, you can check it off. Okay, we've now implemented another heuristic spam filter. Check it off. And then the job is done. You don't ask, has it gotten better now?"* — [Co1]), or that measurements have little impact on the implementation of measures (Co1,Co2,Co5): *"Of course there is the possibility to give feedback. But I think that usually it has little influence, because it's just the guidelines and has to be adapted that way."* — [Co5].

The most frequently mentioned measurement method was to simply talk with and listen to employees (Ci1-Ci2,Ci4-Ci7,Co1-Co3,Co5-Co7). Other examples were target group analyses (Ci1,Co1,Co3), surveys (Ci5,Co3) or technical measurements (Ci5-Ci7,Co1). These types of measurements were not all viewed positively: two managers mentioned the advantage of technical measurements compared to surveys (Ci6,Ci7), with one relying strongly on these measurements *"[...] many people are in the home office, okay? so you don't actually have to start a survey. We have very clear key figures from the systems."* — [Ci7] One manager described using technical methods to measure friction by monitoring employees' rule breaks *"I see on the one hand, yes, issues when people have trouble implementing something because it doesn't work or because it's difficult or something. And I can also detect rule violations and so on in a technical way."* — [Ci6] One manager directly stated the necessity of measuring before implementing security mechanisms (*"Before I instruct or regulate anything, I first have to understand what people are doing so that I can evaluate whether what I am proposing makes any sense at all and fits in with it."* — [Ci1]) following that the consequence of not doing so might lead to the non-acceptance of employees: *"[...] and if you don't do exactly that, then you won't have any understanding from your employees."* — [Ci1]. On different occasions managers (Ci4,Ci7,Co1,Co6) mentioned the importance of considering employees' wishes, even if it meant hearing negative reactions *"A negative reaction means that someone dared to react and these reactions are particularly important."* — [Ci7]

Obtaining Direct Feedback Some managers (Ci3,Ci7) mentioned a kind of "distance" to the employees, which resulted in only superficial measurements of friction: *"We also like it when comments come in unfiltered. That's what I said at the beginning, because it's very hierarchical, you sometimes don't feel the pulse of the employees."* — [Ci3]. Other managers (Ci4,Ci5,Co1,Co2,Co6) mentioned the importance of being close to employees to get an accurate view of whether the implementation of security measures worked and if they were accepted: *"You see, the only thing that helps there is proximity to the base. You have to somehow manage to get feedback from the employees as to whether the measures can be implemented, whether the measures are credible."* — [Co6], sometimes highlighting casual situations as the best way of getting feedback: *"[...] as a security officer, I have to get out among the people. And talk to them. At company meetings, company events. Departmental events. Lunch. Whatever."* — [Co1]. Another manager highlighted empathy as a necessary character trait of the person measuring: *"He*

has the right methods, but he may not have the right empathy. He doesn't have the understanding of the process. He doesn't have the understanding of the interplay, the interlocking on the human side, but also on the technical side. And that's the thing that it takes for the measures to be accepted." — [Ci4].

Short Summary: Most security managers are aware of the importance of friction measurements and employees' feedback, often citing casual talks as the best way of doing so. Still, this is not followed through and measurements are described as having no impact on security decisions.

4.5 Friction Mitigation Strategies

Different mitigation strategies – to reduce friction – were named by the security managers. However, we found that the majority of participants did not consider such reduction before (the interview) and did not name concrete examples where they applied strategies that would eliminate the causes of friction.

Awareness Will Solve Friction By far the most frequently presented mitigation strategy (named by 12/14 managers) was the idea to explain the importance of security and why restrictions are necessary to employees so that they will accept them and stop complaining. Some security managers insisted that a pro-active and open communication with the employees is key to raise their understanding: *"Security is [...] perceived as somewhere, maybe an obstacle or something. So we're aware of that, and we try to maintain a positive image, i.e. that people can approach us at any time. But security has priority, of course."* — [Ci7]. The majority of managers combined their suggestions with a form of excuse: they would not be in the position of bending rules and norms and hence can not do anything to reduce the friction: *"So the supreme law and regulation, what does it say? If the law requires it, then you have to do it, even if the employee is not entirely happy with it."* — [Ci1]. Others stated that, especially in their industries, the employees need to understand why security is so strict and causes problems: *"I think that's also primarily a mental attitude that has to take place that we're in a company that doesn't function like we do at home, because we're operating in very sensitive areas."* — [Ci2]. Some gave concrete examples where they would use explanations to solve the problem: *"But at best, if an employee is dissatisfied that a longer password than before suddenly has to be entered, then you simply have to communicate that."* — [Co7].

Develop Security Together Five security managers (Ci1,Ci2,Ci3,Co4,Co5) in some form or another expressed the idea to adapt security in collaboration with the employees. This ranges from implementing actively gathered feedback to the inclusion of the employees in the security requirement engineering process: *"And consequently, via data classification and categorization and protection needs analysis, it is then clear how much and where protective measures must be applied that then just together with the users, must also be balanced."* — [Co4].

Change Security Four security managers (Ci2,Ci3,Co1,Co3) were open to changing security/ lowering the level of security to reduce friction. Co3, for example, explained that security policies must be bent if the job requires it: *"[...] need to get changed, if that is too restrictive, or incompatible with the field of activity. Just as a sales person is often on the road, probably needs flash drives to work and exchange data. And to forbid him to do so would probably be bad."* — [Co3] Co1 explained that, over time, it is possible to consolidate security policies which would also reduce friction: *"[...] products have been standardized, harmonized, guidelines have also been slimmed down. And so on. So, if security is at a high level. Then it effectively becomes easier for the employees. And not more difficult."* — [Co1]

Others Only one manager said that he would help employees to practically train the security procedures to reduce friction, in that case with the unsolved usability problem of e-mail encryption [78, 84, 92]: *"A typical example is sending confidential information by e-mail [...] what exactly does he have to do? What is the button in the e-mail program where I activate the encryption? How can I see that it's all working? Things like that."* — [Ci1] Another idea was to offer secure alternative software to replace those that employees are used to, but are banned for security reasons. Co1 was convinced that all messengers are the same, and that it would be easy to introduce a secure messenger as an alternative for a more insecure but popular one (like WhatsApp): *"If I offer a messenger that allows end-to-end encryption and allows confidentiality in the relationship. Then there's no negative reaction because now I might have to switch from product A to product B. But I can communicate."* — [Co1]

Short Summary: Most security managers propose mitigation strategies that rather hide the friction but do not solve it – namely the idea to convince the employees that restrictions and friction are necessary in the name of security.

4.6 Usable Security

The managers hinted at an understanding of usable security. While the term *usable security* was not used by any manager, *usability* was mentioned 5 times by 4 managers (Ci1,Co3,Co5,Co7) and the term *user friendly* 8 times by 4 managers (Ci3,Ci6,Co4,Co7), e. g.,: *"Legitimate is certainly the desire for usability that you do something securely, but*

not so complicated that it takes away a significant amount of work time that it's understandable that the employee has a sense of security in what they're doing that they're doing it right." — [Ci1]

The managers mentioned software and mechanisms that could make security usable, namely password managers, Single Sign-On (SSO), biometric authentication and MFA codes on mobile devices, e. g.,: *"And basically the subject of single sign-on. If I want or have to log on to different platforms because I need different tools, different applications, different services, but can largely cover this with SSO that's an increased security feature. But at the same time an improvement in user-friendliness."* — [Co7]. However, while multiple mechanisms were named by the participants, they always talked about them in abstract forms, never mentioning that they had introduced such themselves in their organizations. The only exception was Co3 who gave an example about how he implemented a usability concept: *"I found that the screen timeout is set to something like two hours and the settings are not up to security standards at all. [...] The people who work on these systems sometimes wear gloves, there are three or four screens around this machine and that would definitely not be usable or compatible with today's standard rules if the screen saver came on every 15 minutes without anything being pressed."* — [Co3]

Invisible Security The idea to make security invisible to the employees – a concept that the usable security community can not agree upon to date [24] – was brought up by some managers: *"So in the best case, not at all. So if we, let's stay with the example of user authentication, if that goes by very gently, so that we don't virtually burden the the employee with security, but rather check that in the background."* — [Ci3] or *"Before disk encryption was introduced, you had to find a tool. Find a solution. Which makes this very transparent in the background, without employees noticing or feeling it. You switch it on and at some point, over the next few hours or days, it will be encrypted in the background. Such a security measure is accepted. Because it doesn't affect users, hinder them."* — [Co1]

Problematic Understanding of Usable Security Ci6 showed quite a controversial understanding of usable security. Employees told him that a security mechanism does not work on mobile devices and instead of improving the UI/UX, he reacted with restrictions. When he reported the following he was fully certain that his reaction was appropriate and he wanted to show that usability is something he is addressing: *"For example, I have repeatedly received the feedback: On small screens like on smartphones, you don't necessarily see the details you need to see to identify phishing emails, so I was able to recommend that you generally shouldn't open links on mobile phones if you're not sure what you're looking at."* — [Ci6] In another example, Co7 and Ci4 reported that, especially software developer would demand local administrator privileges on their machines, with both not questioning that this might be a legitimate request, but denying them with a reference to the danger that they fear comes with it.

Short Summary: A few participants were aware that usability of security mechanisms is important and can name examples, like SSO, with only one manager reporting how he implemented those concepts.

5 Discussion

In the following we discuss our findings with regard to our research questions. The majority of security managers stated that security friction was indeed a problem (especially since it can lead to negative reactions from employees that might escalate through the hierarchies). They could easily name cases where friction occurred (e. g., when they restricted access to certain programs) and some also showed understanding about concepts of usability (e. g., when they suggested that password managers or SSO would reduce the password load). However, those considerations played little to no role when they designed security policies, purchased new security products or implemented new security measures. They were able to explain friction, but could rarely name examples of how they mitigated it in their organizations – beyond suppressing friction symptoms by appeasing upset employees. While they reported knowing how to measure friction and got insights into employees demands – mainly through personal talks – they did not do so in practice, or the measurement results did not change the outcome.

Here, the lack of diversity in the security sector – also reflected in the male security leaders we recruited exclusively – becomes an obvious challenge. Within Kocksch et al.'s [57] approach to security as a discipline of care, it is assumed that such a caring approach is characterized by refraining from blaming and attributing responsibility, and instead viewing security as a collaborative and collective achievement [25]. One of our assumptions about why participants could not put usability into practice is that caring work is often feminized (and made invisible) [61] and thus is not taken into account by the male-dominated industry, by which we do not mean to promote that "women" should be declared solely responsible for security [57].

In the academic community, it was established more than a decade ago that small security demands can have a large financial impact [45, 46, 74]. Our results suggest that this knowledge still did not find its way to security (management) practice yet. However, we can not blame the security managers [77]: they are paid to make organizations secure, they have to report numbers to the business leadership that show how investments reduce security risks. The costs of security friction and their reduction is not part of those numbers, not written in norms and regulations they try to implement and

is not part of a security professional's training curriculum. Basic usability and economics concepts need to become part of that curriculum – security professionals don't have time to read research papers in usable security. In the rest of this discussion we will recapitulate some of our findings in more depth, before we derive recommendations (Section 5.1).

No Measurements = No Insights The results show that most of the interviewed security managers (CISOs and consultants) are aware of the importance of measuring friction, and that considering the other demands employees have to meet was essential for security measures to work. This recognition of human aspects of IT security contrasts other findings [77] that showed that security managers see users in a negative way. Many managers (mostly consultants) described that friction measurements were often a "one and done" solution in organizations, with no real follow-up to see long term effects. Their preferred way of measuring friction, casual talks by the coffee machine, might play into this: even though the gathering of real world experiences is recommendable, the lack of planning and structure might impair an effective, long term measurement of friction. Friction, therefore, might remain in the organization without security managers knowing about it.

Perception From what we gathered in the present study, security managers hold employees' needs and wishes in high regard, citing them as paramount for the effectiveness of security measures. Security managers, naturally, care a lot about the security in the organization, but seem to rely too much on official security regulations and guidelines. These rules are perceived, not only as a practical aid for making decisions about security, but also as an excuse if the implemented measures are not accepted. This may lead to security managers seeing themselves as more of communicators of rules instead of solution-finders. Similarly, in earlier work, CISOs have been shown to appear as "interpreters" of security [22].

Considering the view that security managers have of themselves, as communicators of rules, it is no wonder that their preferred method for mitigating friction is raising the awareness of employees. If employees are dissatisfied with security measures, regulations are brought up as a sort of "knockout argument" to mitigate non-compliance. And to mitigate friction in general, security managers want employees to know about these rules and why they need to be followed.

For the security managers, friction is something which is often seen as inevitable when implementing new security measures, and when it appears, employees are predicted to circumvent them. Negative reactions by the employees are then seen as logical and even important, even though the solution for this then seems to be reiterating the necessity of these measures.

Causes Regulatory security requirements were one of the main causes of friction according to most of the security managers. The compliance of these regulations was often seen as "above" the wishes of employees, leading to unhappiness and friction. The root cause of this security managers' view may lay in their relationship with the regulating institutions: because of a lack of time and an abundance of stress [70], managers need to, in some way or other, trust these institutions and their regulations and guidelines, assuming that a lot of thoughts must have been put into them [81]. When these are seen as perfect, internal security policies are seemingly also adapted to this strictness, leading to a constant balancing of regulation and employees' wishes, with regulation coming out as the winner. A similar case seems to apply to certifications: to get these, as seen by security managers, important certifications, employees are "walked over". This lack of consideration might be caused by a complex and expensive certification process [51], which needs a lot of resources and, in turn, prioritizes this over the employees.

What only a few security managers described as a cause was *bad IT*: security mechanisms that are just badly designed and hindering *security hygiene* – which is described as a necessary prerequisite for all further measures, such as increasing employees' understanding [47, 80]. The foregoing of useful security in favor of cheap products and mechanisms, sometimes referred to as "security debt" [73], slows down the implementation of usable security measures in the organizations. The cause of this is, possibly, a lack of resources for security in the investigated companies, which some security managers also mentioned. As the results show, this not only applies to technical factors or training- and awareness programs for the employees, but also to the measurements of friction: measurements are often done casually, or quickly, without following through in a structured way. This lack of "success"-measurement makes it impossible to get a clear view of the friction caused by security measures. And the reasoning for this, a lack of resources, is probably a dangerous misconception, which might result in a "slippery slope" into even more investments in the future: if friction measurements are neglected, inappropriate security measures can secretly pile up friction in the organization, increasing the cost of achieving compliance even further because of the need for more measurements or, worse, constant monitoring of employees [13].

Impact Our analysis revealed that participants consider friction in security as a source of risk. Although security can be increased through certain measures, the sword of Damocles can also hang over the security of the organization: in the case of the perception of friction, the employees tend to circumvent the required measures or change to a shadow security behavior [55, 56], where they try to keep the security level high, but following their own rules. This finding suggests that security managers are at least aware of the friction between

the actual work tasks and security measures. A deterioration in the quality of the relationship between security staff and employees was also described by security managers as a possible consequence of the perceived friction, which echoes the findings of Menges et al. [66]. Other negative impacts such as decreasing motivation, frustration and anger were also described. Overall, employees would feel disturbed by security in the performance of their actual work tasks and feel restricted in their freedom and productivity. These reactions of employees can have negative consequences for the economic efficiency of an organization: discouragement to carry out security-related tasks, increasing fluctuation rates, etc.

The impacts we identified are not only known in the context of security, but also in the area of safety research. For example, the challenge of *work-safety tension* has already been studied by some researchers [65, 88, 90]. As Brostoff & Sasse [17] have already made clear, there are differences between safety and security, but these two domains share, for example, the fact that they are secondary goals for employees, while they have to complete their primary tasks. Safety research has shown that when employees are in tension between work tasks and safety, they tend to prefer the productive path that requires unsafe behavior, which means that such a conflict of goals always leads to a violation of safety-related rules [16]. However, safety research, as the much older discipline, has managed to translate their findings into organizational practice. There, for example, environments have to be changed to reduce the impact on employees, and only if this is not possible the employees need to be warned or actively act. Something that did not find its way in security practice yet (see also Section 5.1).

Mitigation Our participants primarily tried to mitigate friction by raising awareness: explaining the importance of security to employees, in the hope that they would accept friction is unavoidable and stop complaining (see Section 4.5). This may work, up to a point, in cases where employees were unaware or severely underestimated a risk and the communication is convincing – but not if employees' compliance budget [13] is exhausted. Behavioral science has clearly shown that trying to increase motivation to adopt a new behavior when effort is high works only in the short-term, followed by a motivational crash [32], and the study by Poller et al. [75] documented a real-world case of a security intervention creating huge enthusiasm for secure development practice, followed by 'slipping back' into old insecure routines [80]. Instead of focusing on reducing or removing friction, security managers refer to security standards and regulation as their touchstone, which they also use to deflect employees' demands for lower-effort security. Some of our participants were aware of this being a problem and at least consider changing the rules to incorporate the needs of employees. Some participants claimed that they would like to (personally) *talk* to employees, since this can be a first step towards building a relationship [10, 66]. However, they mostly want to talk about risks and try to convince employees to just accept the friction, rather than addressing on the root causes, and adapt security to employees' needs and routines. One participant explained that he wanted employees to understand that complex passwords were necessary, and did not even consider the many usable alternatives available, such as password managers and passwordless authentication solutions [6, 79].

5.1 Recommendations for Industry

Here we derive recommendations for industry with the goal to strengthen the position of usable security in security (management) practice. Measurements of friction were seen as important by many of our participant, but they currently do not see a viable route for reducing or removing it. They seemed to consider it their job – and their job alone – to make security work. This 'lone security hero' perspective means they are afraid to ask for help [21]: the organization of resources for reducing friction, or a helping hand from colleagues running business processes and other organizational functions. And whilst they appreciated casual conversations with employees, they saw them as receivers of security knowledge and directives, not as partners in developing usable security. They need to change their perspective and build relationships, and also take a systematic approach to obtain feedback from employees, identifying friction hotspots, and engaging employees to co-design security, and engage in constantly learning. From an organizational perspective, to facilitate the communication and decision-making about friction, the currently hidden costs need to be tracked and made explicit to organizational leadership. If the possible losses [45] of neglecting security friction are made clear, decision-makers are incentivized to invest in the mitigation of it.

Usable Security Training Security managers like security certificates. Among our participants, the majority earned common certificates like CISM, CISSP or CISA (this was not only true for those managers we selected because of the criteria of having certificates, but also for those we selected because of their academic degree). Those trainings do not solely focus on technical security measures, but also on *softer* topics like secure operations, organizational risk management or secure software development. This is a perfect place to also include topics of usable security, e. g., as part of the software development life cycle [39] or in the risk-cost calculations they learn about. While efforts are made to include usable security topics into (traditionally technology-heavy) academic information security programs [35], they come too late to reach security professionals that are already in the industry for years or decades, like our participants. Certificates, that need to be renewed every few years can help to fill the usable security knowledge gap.

Usable Security Norms We find that regulations and norms prevent the implementation of usable security principles and the reduction of security friction – at least the security managers use those as an excuse for not considering such. And indeed: while ISO27001 (and its implementation guideline ISO27004) and BSI Basic Protection [36] demand password policies, security awareness training, phishing simulations, restrictions on local machines, etc., they do not consider the friction that those measures cause and the costs they raise. One could argue that the sole purpose of these norms is to set security standards, but we argue that the underlying goal is to reduce the (financial) impact of attacks on the organizations. This, however, includes a balance between risk and investments and security friction covertly raises the costs of investments – so they need to be included in these calculations. Norms are a good starting point, as previous authors already proposed for software development standards [39, 41].

Positive KPIs If usable security principles are correctly applied they reduce costs. While some positive effects are rather hard to measure (e. g., the reduction of mental workload) others are easier to measure, e. g., biometric authentication reduces the time employees have to spend on authentication tasks [71], as does SSO [53]. Technical logs, observations and surveys can be the basis for measurements. Subsequently, those can be used in KPIs and reports to the management to showcase the impact of usable security considerations and to make a clear statement for further improvement. The possible fatal security consequences of low usability, which many studies show [40, 78, 87], as well as the economic benefit from reducing the aforementioned different costs should be presented to the management in a clear way to accentuate the importance of usable security. As long as the security managers themselves do not see the necessity of such, the vendors of the products themselves should implement the measurements and report the usability advantages – they could even advertise their products through those numbers.

Security Champions Security managers rightly highlighted the need to measure friction by being "close" to employees and talking with them directly. Still, many security managers (mostly consultants) described that this was often not followed through in the organization. The implementation of the so-called *security champions* – employees who not necessarily have a background in security and who are intrinsically motivated to improve the security in their teams [1, 7, 52], and who have regular contact with the security teams – could help bridging the gap between employees and security managers, allowing this role, which would represent various employees, to be an economic contact point of friction-measurement. Security champions can also help by being "bottom-up" agents [14], who question security policies that may be too strict for employees to follow.

Learning from Safety For the implementation of feasible security measures and for mitigating security friction, organizations and security managers could use the knowledge and recommendations already gained from safety research, for example: McGonagle & Keth [65] suggest monitoring the level of tension (*friction*) in the context of safety (*security*). By this they mean the explicit monitoring of the tension perceived by employees that interferes or conflicts with the effective completion of their actual tasks. They also propose a participatory approach in which employees have the opportunity to communicate those specific aspects of their work that prevent them from doing their job safely (securely). Furthermore, they should be involved in the development of effective and efficient solutions, based on the idea that they are experts of their own work.

6 Conclusion

In this paper we reported how ($n = 14$) security managers perceive security friction in organizations. While they deem friction as a problem, they have no working strategies on how to mitigate it, rely on appeasing enraged employees, and do not consider such in their own work when creating policies and implementing measures. We conclude that security managers lack the necessary support to consider friction, namely the appropriate training, KPIs that make a case for usable security, and norms that demand it. The security industry knows and talks about usable security, and focuses on what steps they take in practice to make it happen. Identifying and dealing with security friction is an essential first step towards making security usable, but we find the managers do not identify and tackle it. For usable security research this means considering how we make our knowledge and tools more accessible to this particular user group. Our study aimed at evaluating how usable security works in organizational practice. More similar studies, especially working with those that are responsible for security – the security and business managers – are necessary to increase the impact that usable security research can have towards organizational practice. Further work can also be built around the evaluation of our suggestions for industry, e. g., positive usability KPIs in organizations. The security managers in our study all worked for rather big organizations. Further studies should also study security management in small enterprises.

Acknowledgments

We would like to thank all managers who took part in our study. Thanks to the four anonymous reviewers for their helpful feedback. Thanks to Julian Becker for his help with the literature review. Thanks to Steve Ehleringer, Maximilian Golla, Stefan Horstmann, and Konstantin Fischer for their support and proof-reading. The work was supported by

the PhD School "SecHuman – Security for Humans in Cyberspace" by the federal state of NRW, Germany and partly also by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972.

References

[1] Hege Aalvik. Towards an effective security champions program. Master's thesis, NTNU, 2022.

[2] Chon Abraham, Dave Chatterjee, and Ronald R. Sims. Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, 62(4):539–548, 2019.

[3] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[4] Eirik Albrechtsen. A qualitative study of users' view on information security. *Computers & Security*, 26(4):276–289, 2007.

[5] Eirik Albrechtsen and Jan Hovden. The information security digital divide between information security managers and users. *Computers & Security*, 28(6):476–490, 2009.

[6] Nora Alkaldi and Karen Renaud. Why Do People Adopt, or Reject, Smartphone Password Managers? In Karen Renaud and Melanie Volkamer, editors, *Proceedings 1st European Workshop on Usable Security*, Reston, VA, 2016. Internet Society.

[7] Moneer Alshaikh and Blair Adamson. From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, 25(5):829–841, 2021.

[8] Ashley Baines Anderson, Atif Ahmad, and Shanton Chang. Competencies of cybersecurity leaders: A review and research agenda. *ICIS 2022 Proceedings*, 2022.

[9] Ginger Armbruster, Jan Whittington, and Barbara Endicott-Popovsky. Strategic Communications Planning for a CISO: Strength in Weak Ties. In *Journal of The Colloquium for Information Systems Security Education*, volume 2, page 10, 2014.

[10] Debi Ashenden and Darren Lawrence. Security Dialogues: Building Better Relationships between Security and Business. *IEEE Security & Privacy*, 14(3):82–87, 2016.

[11] Debi Ashenden and Angela Sasse. CISOs and organisational culture: Their own worst enemy? *Computers & Security*, 39:396–405, 2013.

[12] Michael Bartsch. Woher nehmen, wenn nicht stehlen – oder wo haben Sie Ihren CISO her? (German). In Michael Bartsch and Stefanie Frey, editors, *Cybersecurity Best Practices*, pages 261–269. Springer Fachmedien Wiesbaden, Wiesbaden, 2018.

[13] Adam Beautement, M Angela Sasse, and Mike Wonham. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop*, pages 47–58, 2008.

[14] Ingolf Becker, Simon Parkin, and M Angela Sasse. Finding security champions in blends of organisational culture. *Proc. USEC*, 11, 2017.

[15] Jim Blythe, Ross Koppel, and Sean W Smith. Circumvention of security: Good users do bad things. *IEEE Security & Privacy*, 11(5):80–83, 2013.

[16] Sebastian Brandhorst and Annette Kluge. When the tension is rising: a simulation-based study on the effects of safety incentive programs and behavior-based safety management. *Safety*, 7(1):9, 2021.

[17] Sacha Brostoff and M Angela Sasse. Safe and sound: a safety-critical approach to security. In *Proceedings of the 2001 workshop on New security paradigms*, pages 41–50, 2001.

[18] Deanna D Caputo, Shari Lawrence Pfleeger, M Angela Sasse, Paul Ammann, Jeff Offutt, and Lin Deng. Barriers to usable security? three organizational case studies. *IEEE Security & Privacy*, 14(5):22–32, 2016.

[19] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "it's not actually that horrible": Exploring adoption of two-factor authentication at a university. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–11, New York, NY, USA, 2018. Association for Computing Machinery.

[20] W Alec Cram, Jeffrey G Proudfoot, and John D'Arcy. When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, 31(4):521–549, 2021.

[21] Joseph Da Silva. Cyber security and the Leviathan. *Computers & Security*, 116:102674, 2022.

[22] Joseph Da Silva and Rikke Bjerg Jensen. 'cyber security is a dark art': The ciso as soothsayer. *arXiv preprint arXiv:2202.12755*, 2022.

[23] Darren Death. *The CISO Role within US Federal Government Contracting Organizations: A Delphi Study*. PhD thesis, Capella University, 2021.

[24] Verena Distler, Marie-Laure Zollinger, Carine Lallemand, Peter B. Roenne, Peter Y. A. Ryan, and Vincent Koenig. Security - visible, yet unseen? In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–13, New York, NY, USA, 2019. Association for Computing Machinery.

[25] Paul Dourish, Rebecca E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8:391–401, 2004.

[26] Jonathan Dutson, Danny Allen, Dennis Eggett, and Kent Seamons. Don't punish all of us: Measuring user attitudes about two-factor authentication. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 119–128, New York, 2019. IEEE.

[27] Erastus Karanja. The role of the chief information security officer in the management of IT security. *Inf. Comput. Secur.*, 25:300–329, 2017.

[28] Erastus Karanja and Mark A. Rosso. The Chief Information Security Officer: An Exploratory Study. *Journal of International Technology and Information Management*, 26:23–47, 2017.

[29] Florian M Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. " you still use the password after all"—exploring fido2 security keys in a small company. In *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*, pages 19–35, 2020.

[30] Todd Fitzgerald and Micki Krause. *CISO leadership: Essential principles for success*. CRC Press, 2007.

[31] 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)*, pages 1199–1216. USENIX Association, 2021.

[32] Brian J Fogg. *Tiny habits: The small changes that change everything*. Eamon Dolan Books, 2019.

[33] Steven Furnell. Security fatigue. *Encyclopedia of Cryptography, Security and Privacy*, pages 1–5, 2019.

[34] Simson Garfinkel and Heather Richter Lipford. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust*, 5(2):1–124, 2014.

[35] Binto George, Martha Klems, and Anna Valeva. A method for incorporating usable security into computer security courses. In *Proceeding of the 44th ACM Technical Symposium on Computer Science Education*, SIGCSE '13, page 681–686, New York, NY, USA, 2013. Association for Computing Machinery.

[36] German Federal Office for Information Security. IT-Grundschutz-Compendium. Standard, BSI – German Federal Office for Information Security, Bonn, DE, 2022.

[37] Brain Glass, Graeme Jenkinson, Yuqi Liu, M Angela Sasse, and Frank Stajano. The usability canary in the security coal mine: A cognitive framework for evaluation and design of usable authentication solutions. *arXiv preprint arXiv:1607.03417*, 2016.

[38] Marilu Goodyear, Holly T. Goerdel, Shannon Portillo, and Linda Williams. Cybersecurity Management In the States: The Emerging Role of Chief Information Security Officers. *SSRN Electronic Journal*, 2010.

[39] Marco Gutfleisch, Jan H. Klemmer, Niklas Busch, Yasemin Acar, M. Angela Sasse, and Sascha Fahl. How does usable security (not) end up in software products? results from a qualitative interview study. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 893–910, New York, 2022. IEEE.

[40] Marco Gutfleisch, Maximilian Peiffer, Selim Erk, and Martina Angela Sasse. Microsoft office macro warnings: A design comedy of errors with tragic security consequences. In *Proceedings of the 2021 European Symposium on Usable Security*, pages 9–22, 2021.

[41] Marco Gutfleisch, Markus Schöps, Jonas Hielscher, Mary Cheney, Sibel Sayin, Nathalie Schuhmacher, Ali Mohamad, and M. Angela Sasse. Caring about iot-security – an interview study in the healthcare sector. In *Proceedings of the 2022 European Symposium on Usable Security*, EuroUSEC '22, page 202–215, New York, NY, USA, 2022. Association for Computing Machinery.

[42] Julie M. Haney and Wayne G. Lutters. The work of cybersecurity advocates. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '17, page 1663–1670, New York, NY, USA, 2017. Association for Computing Machinery.

[43] Julie M Haney and Wayne G Lutters. " it's scary... it's confusing... it's dull": How cybersecurity advocates overcome negative perceptions of security. In *SOUPS@ USENIX Security Symposium*, pages 411–425, Berkeley, 2018. USENIX.

[44] Julie M. Haney and Wayne G. Lutters. Cybersecurity Advocates: Discovering the Characteristics and Skills of an Emergent Role. *Information and Computer Security*, 29(3), 2021.

[45] Cormac Herley. 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*, pages 133–144, 2009.

[46] Cormac Herley. More is not the answer. *IEEE Security & Privacy*, 12(1):14–19, 2013.

[47] Jonas Hielscher, Annette Kluge, Uta Menges, and M. Angela Sasse. "taking out the trash": Why security behavior change requires intentional forgetting. In *New Security Paradigms Workshop*, NSPW '21, page 108–122, New York, NY, USA, 2022. Association for Computing Machinery.

[48] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M. Angela Sasse. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *32st USENIX Security Symposium (USENIX Security 23)*, Boston, MA, August 2023. USENIX Association.

[49] Val Hooper and Jeremy McKissack. The emerging role of the CISO. *Business Horizons*, 59(6):585–591, 2016.

[50] Nicolas Huaman, Bennet von Skarczinski, Christian Stransky, Dominik Wermke, Yasemin Acar, Arne Dreißigacker, and Sascha Fahl. 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)*, pages 1235–1252. USENIX Association, August 2021.

[51] Mike Hulshof and Maya Daneva. Benefits and challenges in information security certification–a systematic literature review. In *Business Modeling and Software Design: 11th International Symposium, BMSD 2021, Sofia, Bulgaria, July 5–7, 2021, Proceedings 11*, pages 154–169. Springer, 2021.

[52] Martin Gilje Jaatun and Daniela Soares Cruzes. Care and feeding of your security champion. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pages 1–7, New York, 2021. IEEE, IEEE.

[53] Neely James, Shruti Marwaha, Stacie Brough, and Thomas T John. Impact of single sign-on adoption in an assessment triage unit: A hospital's journey to higher efficiency. *JONA: The Journal of Nursing Administration*, 50(3):159–164, 2020.

[54] Julia H Allen, Gregory Crabb, Pamela Curtis, Brendan Fitzpatrick, Nader Mehravari, and David Tobar. Structuring the Chief Information Security Officer Organization.

[55] Iacovos Kirlappos, Simon Parkin, and M. Angela Sasse. "Shadow security" as a tool for the learning organization. *ACM SIGCAS Computers and Society*, 45(1):29–37, 2015.

[56] Iacovos Kirlappos, Simon Parkin, and M. Angela Sasse. Learning from "Shadow Security": Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security. In Matthew Smith and David Wagner, editors, *Proceedings 2014 Workshop on Usable Security*, Reston, VA, February 23, 2014. Internet Society.

[57] Laura Kocksch, Matthias Korn, Andreas Poller, and Susann Wagenknecht. Caring for IT Security. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–20, 2018.

[58] Udo Kuckartz. *Qualitative inhaltsanalyse (German)*. Beltz Juventa, 2012.

[59] Benedikt Lebek, Jörg Uffen, Michael H. Breitner, Markus Neumann, and Bernd Hohler. Employees' information security awareness and behavior: A literature review. In *2013 46th Hawaii International Conference on System Sciences*, pages 2978–2987, New York, 2013. IEEE.

[60] Michelle R. Lowry, Anthony Vance, and Marshall D. Vance. Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity. *SANS*, 2021.

[61] Aryn Martin, Natasha Myers, and Ana Viseu. The politics of care in technoscience. *Social studies of science*, 45(5):625–641, 2015.

[62] Peter Mayer, Nina Gerber, Ronja McDermott, Melanie Volkamer, and Joachim Vogt. Productivity vs security: mitigating conflicting goals in organizations. *Information & Computer Security*, 2017.

[63] Peter Mayer, Collins W. Munyendo, Michelle L. Mazurek, and Adam J. Aviv. Why users (don't) use password managers at a large educational institution. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1849–1866, Boston, MA, August 2022. USENIX Association.

[64] Sean B. Maynard, Mazino Onibere, and Atif Ahmad. Defining the Strategic Role of the Chief Information Security Officer. *Pacific Asia Journal of the Association for Information Systems*, pages 61–86, 2018.

[65] Alyssa K McGonagle and Lisa M Kath. Work-safety tension, perceived risk, and worker injuries: A meso-mediational model. *Journal of safety research*, 41(6):475–479, 2010.

[66] Uta Menges, Jonas Hielscher, Annalina Buckmann, Annette Kluge, M. Angela Sasse, and Imogen Verret. Why IT Security Needs Therapy. In *Computer Security. ESORICS 2021 International Workshops*, volume 13106 of *Lecture Notes in Computer Science*, pages 335–356. Springer International Publishing, Cham, 2022.

[67] Eric Molin, Kirsten Meeuwisse, Wolter Pieters, and Caspar Chorus. Secure or usable computers? Revealing employees' perceptions and trade-offs by means of a discrete choice experiment. *Computers & Security*, 77:65–78, 2018.

[68] Tyler Moore, Scott Dynes, and Frederick R. Chang. Identifying how firms manage cybersecurity investment. *Available: Southern Methodist University.*, 32, 2015.

[69] Tabisa Ncubukezi. Human errors: A cybersecurity concern and the weakest link to small businesses. In *Proceedings of the 17th International Conference on Information Warfare and Security*, page 395, 2022.

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

[71] MO Oloyede, AO Adedoyin, and KS Adewole. Fingerprint biometric authentication for enhancing staff attendance system. *International Journal of Applied Information Systems*, 2013.

[72] Jon Oltsik, Candy Alexander, and CISSP CISM. The life and times of cybersecurity professionals. *ESG and ISSA: Research Report*, 2017.

[73] Simon Parkin, Simon Arnell, and Jeremy Ward. Change that respects business expertise: Stories as prompts for a conversation about organisation security. In *New Security Paradigms Workshop*, NSPW '21, page 28–42, New York, NY, USA, 2021. Association for Computing Machinery.

[74] Simon Parkin, Aad van Moorsel, Philip Inglesant, and M. Angela Sasse. A stealth approach to usable security: Helping it security managers to identify workable security solutions. In *Proceedings of the 2010 New Security Paradigms Workshop*, NSPW '10, page 33–50, New York, NY, USA, 2010. Association for Computing Machinery.

[75] Andreas Poller, Laura Kocksch, Sven Türpe, Felix Anand Epp, and Katharina Kinder-Kurlanda. Can security become a routine? a study of organizational change in an agile software development group. In *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*, pages 2489–2503, 2017.

[76] Gerald V Post and Albert Kagan. Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, 26(3):229–237, 2007.

[77] Lena Reinfelder, Robert Landwirth, and Zinaida Benenson. Security Managers Are Not The Enemy Either. In Stephen A. Brewster, Geraldine Fitzpatrick, Anna L. Cox, and Vassilis Kostakos, editors, *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, pages 1–7, New York, New York, USA, 2019. ACM Press.

[78] Scott Ruoti, Jeff Andersen, Daniel Zappala, and Kent Seamons. Why johnny still, still can't encrypt: Evaluating the usability of a modern pgp client. *arXiv preprint arXiv:1510.08555*, 2015.

[79] Scott Ruoti, Brent Roberts, and Kent Seamons. Authentication melee: A usability analysis of seven web authentication systems. In *Proceedings of the 24th International Conference on World Wide Web*, WWW '15, page 916–926, Republic and Canton of Geneva, CHE, 2015. International World Wide Web Conferences Steering Committee.

[80] Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. Rebooting it security awareness – how organisations can encourage and sustain secure behaviours. In *European Symposium on Research in Computer Security*, pages 1–18, Berlin, 09 2022. Springer, Springer.

[81] M Angela Sasse, Matthew Smith, Cormac Herley, Heather Lipford, and Kami Vaniea. Debunking security-usability tradeoff myths. *IEEE Security & Privacy*, 14(5):33–39, 2016.

[82] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, 19(3):122–131, 2001.

[83] Conrad Shayo and Frank Lin. An exploration of the evolving reporting organizational structure for the chief information security officer (ciso) function. *Journal of Computer Science*, 7(1):1–20, 2019.

[84] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. Why johnny still can't encrypt: evaluating the usability of email encryption software. In *Symposium on usable privacy and security*, pages 3–4. ACM, 2006.

[85] Ben Shneiderman, Catherine Plaisant, Maxine S Cohen, Steven Jacobs, Niklas Elmqvist, and Nicholas Diakopoulos. *Designing the user interface: strategies for effective human-computer interaction*. Pearson, 2016.

[86] Brian Stanton, Mary F Theofanos, Sandra Spickard Prettyman, and Susanne Furman. Security fatigue. *It Professional*, 18(5):26–32, 2016.

[87] Christian Stransky, Oliver Wiese, Volker Roth, Yasemin Acar, and Sascha Fahl. 27 years and 81 million opportunities later: Investigating the use of email encryption for an entire university. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 860–875. IEEE, 2022.

[88] Chris B Stride, Nick Turner, M Sandy Hershcovis, Tara C Reich, Chris W Clegg, and Philippa Murphy. Negative safety events as correlates of work-safety tension. *Safety science*, 53:45–50, 2013.

[89] U.S. Department of Homeland Security. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, August 2012. https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/, as of June 2, 2023.

[90] Benjamin M Walsh, Alyssa K McGonagle, Timothy Bauerle, and Tarya Bardwell. Safety stressors: Deviant reactions to work-safety tension. *Occupational Health Science*, 4:63–81, 2020.

[91] Jake Weidman and Jens Grossklags. I like it, but i hate it: Employee perceptions towards an institutional transition to byod second-factor authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference*, ACSAC '17, page 212–224, New York, NY, USA, 2017. Association for Computing Machinery.

[92] Alma Whitten and J Doug Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX security symposium*, volume 348, pages 169–184, 1999.

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

A Interview Guide

The following interview guide is the one developed for the CISOs. The interview guide for consultants differs in how the questions are asked for *the organizations they advise*, rather than their own organizations.

1. **Looking back on your career, how and when did you first come into contact with cybersecurity?**
   (a) What were the most important turning points in your professional career so far (describe them briefly)?
   (b) What experience or training do you currently have in cybersecurity?
   (c) In what time and based on what training and/or experience were you able to acquire the greatest part of your knowledge in the field of cybersecurity?
2. **What are currently the biggest structural and/or organizational challenges you are facing in the context of cybersecurity?**
   (a) Describe briefly and compactly the form of organization in which you are embedded?
   (b) Which organizational interfaces are currently causing you the most challenges?
   (c) How do you determine whether and how your environment (management, board of directors, etc.) is sufficiently 'aware' of cybersecurity issues?
   (d) On the basis of which circumstances is the budget for cybersecurity decided?
   (e) Which activities take up most of your attention?
3. **The application of security measures (technical, organizational or administrative) usually leads to an increase in the security maturity of an organization. What effects can such measures have on employees in your organization?**
   (a) Do you try to get feedback from employees after applying new measures?
   (b) Can you give some examples of this?
   (c) How are security measures generally perceived by your employees?
4. **In everyday work, there are often business interests versus security interests to be balanced. When developing and applying security measures, do you think about the concrete effects (individual consequences) on the individual employees affected?**
   (a) How do you decide whether business interests or employee interests take precedence over security interests?
   (b) Based on which metrics, methods or techniques do you balance the respective interests?

(c) In your opinion, which personal interests of employees are legitimate and must be taken into account? Which are not?

(d) Do you know of any examples where cybersecurity measures have been adapted or even improved based on feedback from employees (briefly describe them)?

5. **It can happen that employees do not dare to show negative reactions or do not know who to turn to with their criticism. What negative experiences do you think these employees would report?**

   (a) How would you describe the relationship between security and restriction (Can there be security without 'sacrifice'?)?

   (b) What do you do to keep the corresponding negative reactions as low as possible?

   (c) How do you react to negative reactions?

   (d) In your view, are such negative reactions legitimate?

6. **Can an accumulation of negative staff reactions become a problem for organizations?**

   (a) What can be the consequences for an organization if these negative reactions are not taken ito account?

   (b) Have you ever had to deal with staff reactions that were escalated (carried over the reporting line)?

   (c) What could be the triggers for such escalations?

7. **How do you find out whether the security measures can be implemented during the employees' work routines or not (process adaptability, etc.)?**

   (a) To what extent do you make an effort to understand employees' work routines?

   (b) How do you ensure that security measures can be applied by employees?

8. **How do you engage with employees' work routines?**

   (a) Which means and methods do you prefer to understand the work routines of your employees?

   (b) How important do you rate the issue on scale from 1 (not important) to 10 (very important) that security measures can be integrated into the work routines of employees?

B Accumulated Demographic Data

Table 2: Accumulated demographic data of our participants.

Gender			#	%
Male			14	*100%*
Highest (Security) Education				
Master/ Diploma Computer Science			3	*21%*
Master/ Diploma (Information) Security			3	*21%*
Vocational Training			1	*7%*
Security Certificates			4	*30%*
Other Master/ Diploma			3	*21%*
Experience in Security				
Max	38	*Average*	19.8	
Min	8	*Median*	20	
Sum	258			

C Code Book

Table 3: The code book (1/2). *Occ.*: the number of occurrences of the code in all documents.

Code	Description	Example Quote	Occ.
(Perceived) Causes of Friction	Where does friction come from? The hard hand of the participant, from norms, from management, from security itself.	*If poorly designed security measures or poorly designed awareness campaigns always lead to resistance at the beginning.*	15
ISO Norms and Regulations	All the audit and norm problems that the participants report with regards to their security strategy.	*On the one hand, we have clear regulatory requirements. That means we have to implement them and can have relatively little consideration for the people themselves.*	22
Additional Security	The participant explains that his organization needs additional security measures that the employees need to implement or follow that cause or might cause friction.	*And the bad guys are the security people, because they now demand something that wasn't necessary before, and that leads to these backlashes.*	7
Impact of Friction	(Negative) consequences of security friction on all stakeholders and the organization itself. This includes all types of negative reactions of employees and others.	*Or, even worse, is hidden. If the security measure is deactivated without those responsible realizing it.*	11
Negative Reactions	The employees dislike the friction caused by security/ they actively react negative.	*Unsightly case: An Employee, IT manager, who showed up at the workplace with a shotgun. This is a kind of escalation. Not in the way, probably, that you expected now. [...] It had to do with the fact that freedoms, in quotation marks, were restricted by standardization and harmonization.*	23
Primary vs. Secondary Task Conflict	The security task clashes with the primary task of the employees.	*And at first glance, a longer password or multiple passwords can look very banal, because, okay, then you enter one more password. But that can prevent an employee from doing the work at all, or perhaps from doing it less often or less regularly. Or he gets upset, needs additional breaks. That all has an impact.*	17
Economic Impact	Impact on the productivity, revenue, etc. of an organization through security.	*Because every organization has to generate output somehow. Or let's take the private sector: organizations have to generate revenue. And any aspect that has even the slightest negative impact on an employee's daily business, let's say, instead of single sign-on, the password has to be entered every time. That reduces the output that the employee can provide.*	10
Shadow Security/ Circumventing Security	Friction will cause circumventing security policies and measures.	*If no platform is offered for secure data exchange, then an employee has a legitimate interest. And it is precisely then that he will turn to any private means he knows, e-mail or any other cloud services, Dropbox, etc., simply for lack of an alternative that is not available.*	11
(Perceived) Solutions for Friction	The participant explains how security friction can or should be reduced in his opinion (this includes hard measures like taking security tasks away, but also soft measures like "just explaining friction to employees so that they understand and accept it").	*You simply have to find a sensible balance between what you allow and what you ban, because you can't ban everything. Instead, you have to weigh up how bad this is, what I am supposed to judge? And do I have to ban it or not?*	10

Table 4: The code book (2/2). *Occ.*: the number of occurrences of the code in all documents.

Code	Description	Example Quote	Occ.
Awareness and Communication Will Solve Friction	Awareness and/or communication with the employees will lead to an understanding of security friction.	*Security is not, so is always perceived as somewhere, yes, maybe an obstacle or something. So we're aware of that, and we try to maintain a positive image, i.e. that people can approach us at any time. But security has priority, of course.*	39
Develop Security Together	Employees and business units can co-define how security should work.	*As a matter of principle, we try to develop the solutions together with IT and pick up the teams from the business side early on.*	9
Change Security to Reduce Friction	Security is reduced or changed in order to reduce the friction experienced by the employees.	*and it may well be that there is a legitimate interest, and then we can also reconsider the solution.*	10
Measurements and Observations	Measurements that the participants or other stakeholders take to understand, learn or quantify security friction (including usable security, time effort) and working routines (that might be affected by security measures) of employees.	-	-
Methods	With which methods is the security friction measured?	*I ask questions. I go and ask people, "How's that working out for you now?"*	55
No Measurements	Security friction is not measured.	*I hardly ever observe that, that feedback is collected. No, I hardly ever observe that.*	9
Active Communication	Actively talking about security measures and friction with the employees.	*We also like it when comments come in unfiltered. That's what I said at the beginning, because it's very hierarchical, you sometimes don't feel the pulse of the employees.*	3
Usable Security	Definitions, status quo descriptions, technical measures, attitudes about usable security. E.g., to say that "security needs to be user friendly", or that "security is not compatible with usability", or that "longer passwords are unusable".	*And basically the issue of single sign-on. If I want to or have to log on to different platforms because I need different tools, different applications, different services, but I can largely cover this with single sign-on, that's an increased security feature. But at the same time, it also improves user-friendliness.*	34
Invisible Security	Security is good if it is not visible to the employees.	*So in the best case, not at all. So if we, let's stay with the example of user authentication et cetera, if that's possible, if that goes by very gently, so that we don't virtually burden the entire security with the, the employee, but rather check that quasi in the background.*	4
Hard Hand/Restrictions	The participant restricts (or wants to restrict) what employees can do and/ or pushes for a law-and-order policy.	*That's why I have to clarify restrictions somehow, you are not allowed to attach this file to an e-mail, whether you understand it or not, that's just the way it is. And if I specify something like that, then I have to think about exactly when I specify it, how I can either technically enforce it so that it is not possible. Or, on the other hand, how can I monitor people who don't comply so that I can draw their attention to it or, in the worst case, impose sanctions on them?*	9