JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2020, 1–12
doi: 10.1093/cybsec/tyaa011
Research paper

Research paper

Exploring the security narrative in the work context

Karoline Busse [1,3,*], Jennifer Seifert[2] and Matthew Smith[1,3]

[1]Usable Security and Privacy Group, Rheinische Friedrich-Wilhelms-Universitat Bonn, Bonn, Germany, [2]Faculty of Philosophy, Leibniz Universitat Hannover, Hannover, Germany and [3]Present address: Institut für Informatik IV Endenicher Allee 19a 53115 Bonn, Germany

*Correspondence address: E-mail: kb.usecap@gmail.com

Received 4 February 2019; revised 25 February 2020; accepted 4 February 2019

Abstract

It is a well-known fact that the language of IT security experts differs from that of non-security-related people, leading to a multitude of problems. However, very little work has examined the differences in perception between security experts within a single security department or company. The sociological theory of power relations and organizational uncertainties by Croizer and Friedberg suggests that uncertainties about the narratives used in a department can lead to potentially harmful power relations and dissatisfied employees. We conducted a qualitative interview study within two distinct IT security companies in order to research the impact of diverging security narratives within security departments. Our results show that there is indeed an uncertainty about the term IT security. However, one company we interviewed regarded this uncertainty as highly beneficial for team creativity, communication, and mutual education, while the other, more technical-focused company showed few diversions within the security staff, but a possibly uniting conflict with the company's IT department. Our results suggest that conscious shaping of a zone of uncertainty around the security narrative in the work context can be an important management skill for IT security practitioners. Furthermore, we show that the analysis of language uncertainties provides a powerful approach to studying the motivation of professional security groups.

Key words: usable security and privacy,perception research,organization research,security narrative

Introduction

Human language is never, and can never be, precise [1, 2]. Language works by using symbols that convey different meanings, encompassing words, perceptions, thoughts, and similar. While certain meanings of a word are relatively common and constant, others are open to interpretation and personal association. For example, a "flower" is the seed-bearing part of a plant, consisting of the plant's reproductive organs, typically surrounded by bright petals. However, different people talking about flowers might have different colors or even species in mind: while one person might associate "flower" with a red rose, another might think of a yellow tulip, and a third one might think about the bigger entity with a stalk and leaves. Every symbol features a so-called "fringe" of uncertainty that is open to individual interpretation [1].

While the aforementioned flower example might not seem very impactful, the uncertainty of precision when talking about a concept can lead to conflicts and misunderstandings when it is integral to business. In this article, we look at the term "security" and its narratives and their implication for professional work within the security and privacy context.

The term "security" in the context of Computer Science and Information Technology spans a broad field of associations and meanings. Starting with the spectrum from offensive attack-focused security to responsible and lawful defensive security, the single word is associated with lots of different nuances that coin an individual's view of IT security.

Formal definitions of information security include "preservation of confidentiality, integrity and availability of information" [3],

© The Author(s) 2020. Published by Oxford University Press.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.

Downloaded from https://academic.oup.com/cybersecurity/article/6/1/tyaa011/5920841 by guest on 29 February 2024

"the process of protecting the intellectual property of an organization" [4], and "keep[ing] information in all its locations [...] free from threats" [5].

Over the course of their life, people align themselves on the topic, associate with certain facets and reject others, and granularly form their own personal narrative of IT security and thus their own personal meaning of the word. Education is usually a big influencing factor in experts' narratives, but personal activism or public figures like Edward Snowden (cf. the section "Degree of activism") can also play a significant role in a person's individual picture of security.

Regarding professional contexts, employers in the field of IT security may aim to find employees with a similar narrative to prevent internal conflicts resulting from people meaning different things when talking about the same word (cf. the section "Theoretical background").

Previous research has shown that employee satisfaction in IT security departments is a newly emerging and perspective-widening field in security research [6, 7], extending the human factor in usable security from the individual level to organizational research. We want to further explore the understanding of employee relations and self-fulfillment with our research by looking at language projections of employees' narratives on security.

In this article, we look at similar and diverging security narratives within IT security companies. Corresponding theories from the field of Social Sciences suggest that the personal uncertainty about the definition of IT security leads to interpersonal uncertainties within a department, which can influence power relations and thus may have consequences on employee motivation and satisfaction.

Originally, we formulated our research question around employee satisfaction in IT security departments in relation to security narratives of employees and department heads. During the course of the study however, the research focus shifted toward the effectiveness and work culture of security departments. Therefore we chose to reformulate our research question during the evaluation to better reflect our path throughout the project.

We thus summarize our main research question as:

> How do effectiveness and work culture in IT security departments change in relation to a similar or a different security narrative between employees and department head?

To investigate the effects of language uncertainties around the security narrative in the work context, we design a qualitative study centered around employee and department head interviews. The definition of IT security and the possible problems arising from it are most crucial within departments who actively work on IT security, but also between IT security departments and other parts of the company, such as management or development. This is why we conducted a focused study of two such departments. We focus on extracting employee and department heads' perceptions of and associations with security in order to reconstruct individual narratives and, if possible, a set of shared facets of security that apply to the whole department. Additionally, we investigate actual or potential conflicts around diverging security narratives as perceived by the employees, as well as conflicts emerging from uncertainties around IT security in the respective companies.

We use the methodology of Qualitative Content Analysis [8] to develop a theoretical model and derive evaluation guidelines along this model.

This report presents findings from a series of interviews we conducted at two German companies: a company from the field of IT security and data protection consultancy, and the security branch of a large company for applied research.

Our results show that each company had its own prominent conflict around IT security and its meanings. We confirm that uncertainty around the term IT security exists in security companies and that it shapes company culture and employee satisfaction within the company. Both department heads were aware of diverging narratives. One department head was not only aware of the zone of uncertainty around the term IT security, but – contrary to our theoretical assumptions – viewed it as positive and actively used it to shape company culture and foster growth. This gives important hints that consciously shaping and cultivating a zone of uncertainty can be a powerful tool in managing IT security departments.

The rest of this article is structured as follows: we present an overview on related work in the section "Related work," then outline our theoretical foundation and research question in the section "Theoretical background." The section "Methodology" gives an overview on the methodology we used for conducting and evaluating our interview study and presents the evaluation model we extracted from theory and based our evaluation on. The collected results are presented in the section "Results" and discussed in the section "Discussion." The last section includes "Conclusions and future work."

Related work

Theoretical background

Our theoretical background is heavily grounded in the Social Sciences field of Organizational Sociology [9]. Since most work in the field of Sociology is closely focused on a specific society, we had to focus on literature suitable to our geographical region of research. Croizer and Friedberg published an important piece on Organizational Sociology in 1979 [10]. They focused on the organization's members and their relationship with the system and analyzed the factors power, strategy, and play. For our work, we draw from the part of power plays and how they emerge around organizational uncertainties.

The language imprecision around the security narrative creates a so-called "uncertainty zone"[1] in an IT security-focused department or company [10, p. 47], as we already established that everybody associates slightly different things with the concept (cf. the section "Introduction"). Several actors try to utilize this uncertainty for their own incentives. This is how power relations emerge.

In addition, Croizer and Friedberg state that the so-called "common goals" within a company actually do not exist. Instead, every individual in a company has different priorities of the company's goals and derives their own action from them [11, p. 43–47].

Our assumption regarding the security narrative is as follows: the more this narrative diverges within a department – or the whole company, if it is centered around IT security – the more do each individual's priorities of the company goals diverge and the more diverge their actions within the department. We therefore derive that a department head – or the whole company – should aim to hire people with a similar mindset regarding security. This would keep the uncertainty zone small and limit the risk for the company from these resulting power relations (see [12, p. 40–42]).

1 *Organisatorische Ungewissheitszone* [10].

Downloaded from https://academic.oup.com/cybersecurity/article/6/1/tyaa011/5920841 by guest on 29 February 2024

In reality, we see many efforts to diversify teams and their perspectives on the work matter such as security [13]. Given that the primary theoretical literature in this case was first published in 1979, we will address the claim of "hiring people with a similar mindset" within the contemporary efforts of diverse recruiting.

Regarding the employees, we assume that a smaller zone of uncertainty may lead to fewer conflicts and a better work environment within a department and thus to a higher department effectiveness. In addition, the relationship between employees and the department head may improve when a similar security narrative shrinks the uncertainty zone and thus the potential for power games [14, p. 150f].

We summarize these theoretical assumptions in our main research question:

> How do effectiveness and work culture in IT security departments change in relation to a similar or a different security narrative between employees and department head?

Mental model and narrative research

The study of people's mental models sheds light on their narratives. Some previous work has explicitly focused on the mental models of security and privacy experts.

Krombolz *et al*. researched end-user and systems administrator models of encryption and especially HTTPS [15]. They conducted an interview study and let participants draw how they imagine encryption works. If was found out that experts' conceptions of encryption relied heavily on technical protocols. In some cases, the administrators relied on the technical terms without really knowing what they stand for, possibly hiding gaps in knowledge. This is an important insight into security professionals' narratives which sheds light on the symbolism of the term "encryption."

Theofanos *et al*. researched the gap between security experts and nonexperts within the US Government [16]. In an interview study with 21 experts and 23 nonexperts, they found out that expert participants have a very strong perception of risk and also base their security narrative on protecting from said risk. Experts further shared a general distrust in everything they encountered online. However, the strategizing around perceived risks helped them manage these risks, so they felt empowered rather than frightened.

In 2014, Posey *et al*. investigated the perception of risk in organizations using an interview study based on the Protection-Motivation Theory [17]. They interviewed security and non-security employees in various organizations and derived a model to identify gaps within risk and security perception between the groups. It turned out that nontechnical employees tend to look toward the outside for threat and risk identification and were concerned about, e.g. hackers or system vulnerabilities, while security workers were aware of inside risks like uneducated coworkers.

Social factors in IT security work

Research around work conditions and employee issues in the field of IT security is a relatively new branch within the field of Usable Security.

Initial efforts in this domain were made by Hawkey *et al*. during the course of the HOT Admin project [18]. While the projects' goals centered on evaluating and improving tools for security practitioners, the researchers also conducted some groundwork about the organizational, technical, and human factors that challenge IT security management, such as different perceptions of risks, or the priority of security within the organization [18].

Chandran *et al*. have researched the phenomenon of burnout in Security Operation Centers [7]. Using methods from anthropological research, the authors sent a graduated student as an employee to a Security Operation Center, where they should observe the environment, and the work and its effect on the people who are employed there. After 6 months, the observations were evaluated with a Grounded Theory approach. As a result, the researchers found a vicious cycle: employees did not feel empowered by their workplace, which resulted in less creative and more repetitive tasks. These unpleasant tasks led to less personal growth which led to a decline in analytic and programming skills. Because the employees' skills lowered over time, their work motivation slowly fell and the cycle continued and eventually produced burnout-like symptoms. The authors concluded that breaking this vicious cycle by introducing more creative tasks and room for individual approaches to security analyst work would lead to motivated, empowered employees. This change may help to combat security analyst burnout [7].

A follow-up from Chandran *et al*. presented in 2016 connected the work issues in Security Operation Centers to the Activity Theory model in order to analyze the working conditions with the overall goal to raise employee satisfaction. So-called "contradictions" were identified and set in connection to the problems found in the first study. Contradictions serve as potential foundations for innovation, so the authors then derived courses of action based on their findings, such as improved tools for reporting incidents that leave more room for creative tasks [19].

Work by Blythe *et al*. researched how employees engage in security actions [6]. Their research focuses around different factors that influence security behaviors within employees and what causes high or low levels of these factors. Another research question focused on the barriers that prevent more security-conscious behavior in employees.

Blythe *et al*. conducted a series of semi-structured interviews combined with the use of Vignettes. Evaluation of the interview data yielded that employee security behavior is influenced by individual knowledge and previous experiences as well as by individual perception of responsibility and the relation between work and personal life. Especially, the researchers found that employees apply different susceptibility levels to online and offline threats, which prior theoretical research did not differentiate. Management behavior and positive reinforcement from the workplace can improve employees' security behavior [6].

Haney *et al*. investigated the development process of cryptographic software within the organizational context and the underlying security mindsets [20]. They conducted an interview study with security developers and found out that there exists a certain "security mindset" in companies that develop cryptographic products. Key aspects of this mindset are the strong commitment to security as a company's "core value" and the perpetuation of security, e.g. with mentoring programs for less experienced coworkers.

In a position paper, Alexander Serebrenik applies Hochschild's concept of emotional labor [21] to the profession of a software engineer. Serebrenik theorizes that software engineers experience emotional labor and presents examples such as Code of Conduct excerpts that define desired tone and discussion policies for community software projects. A methodological plan to further research the phenomenon by various means from neurological analysis to self-rating of previously expressed emotions is laid out [22].

Work by M'manga *et al*. researched how folk models coin security experts' perception of risk. They conducted an interview study with security analysts in three different organizations which was evaluated using Grounded Theory. Four groups of influencing factors were identified: awareness, communication, tool capabilities, and individual capabilities. In addition, five constraints that restrict

Downloaded from https://academic.oup.com/cybersecurity/article/6/1/tyaa011/5920841 by guest on 29 February 2024

decision making were extracted: business processes, data encryption, project management, lack of privileges, and third-party dependencies [23].

Methodology

In order to get as much insight about the motivations and each individual's narrative as possible, we opted for qualitative research. Qualitative studies are designed to be open and adaptive to the interview subject and allow for capturing complexity in habits, emotions, and experiences. Thus, they are well suited for exploring a new field [24], which is the case for our study.

Since we wanted to research power dynamics within security companies, getting a picture on internal relations and dynamics required to interview several security workers within a single organization. Thus, we needed to find companies that would participate by letting us interview several of their security-related employees.

We conducted a series of semi-structured interviews with two companies in the fields of IT security and data protection. In each company, we scheduled five interviews with technical employees and one with the corresponding department head. For further description, we will label the companies as Consulting Company (CC) and Research Company (RC).

The CC is located in the field of corporate and public consultancy for IT security and data protection. The company was founded as a start-up in 2008 and now employs over 20 people, from which about half work on technical topics. Within the company, CC has always promoted democratic structures and low hierarchies, so there is no dedicated department head. Instead, we interviewed one of the CC's CEOs. Given the company's small size, this can be regarded as equivalent to a department head. We conducted the study in the CC in August and September 2016.

After an initial evaluation of the gathered data, we found that some conflicting results regarding the security narrative and the company culture emerged. We wondered if this was related to the small company size of the CC, and thus started the search for other, larger and more traditionally-structured IT security companies to diversify our sample and investigate if observed phenomena would also hold for larger company sizes. Sadly, finding a medium- to large-sized company within the field of IT security that would allow us to conduct our research there turned out very hard, so it took some time to widen the sample.

The RC is the cybersecurity branch of a large semi-public company within the field of applied research. The company is structured in several independent sub-companies that operate individually.

While the company as a whole employs several thousand people, the sub-company which also holds the cybersecurity departments has about 400 employees, further differentiating into several research teams who work more or less independently from each other. We interviewed five employees who work in different but closely related teams on applied research within the field of IT security, as well as the branch head. All interviews in the RC were conducted in December 2018.

In total, we have conducted and evaluated 10 employee and 2 head interviews. The interviews were semi-structured and scheduled for 1 h each. Participants were interviewed one-to-one in a separate room within the company facilities. Before the interview started, participants were informed about anonymity and confidentiality of their contribution as well as the recording of the interview. Participants were required to provide written consent prior to the interview. All participants received a compensation of 15 euros. Employees and CEO roughly received the same questions. All interviews were conducted by the same interviewer. One interview was conducted in English, all others were conducted in German. The interview guide document – English translations of the German questions used in the interview – can be found in Appendix.

Evaluation method

For our evaluation method, we applied Qualitative Content Analysis (QCA), as developed by Mayring [8] and refined by Gläser and Laudel for the application on domain expert interviews [25].

QCA is suited to evaluate qualitative data based on initial research questions and theoretical work (as opposed to Grounded Theory which wants the researchers to be as open minded as possible). However, relying heavily on theoretical pre-assumptions likely introduces informed bias into study design and evaluation [26]. Our solid theoretical foundation and the research question suggest a method that builds on that, so we chose QCA as our evaluation approach.

In QCA, a theoretical model consisting of variables and their presumed relations is constructed from theory and initial assumptions based on the research questions. Each variable contains a definition, indicators from which an evaluation guideline is constructed, a time dimension, and a content dimension. Variables are set in relation to one another, and a model about assumed causality relations is developed. This model is the basis for qualitative evaluation of the interview data.

After all interview data is gathered, the model is revisited and revised based on first impressions of the data. Concrete extraction rules for the interview material are finally derived from the model and documented for further repeatability.

While Mayring's original formalization of QCA demands a test run of the evaluation in which about 40% of the interview material is coded before developing the theoretical model, Gläser and Laudel's extension allows model alteration end extension during the evaluation process [25]. This caters to the usually low number of interviews that can be gathered in domain expert studies.

Information extraction from the text follows the constructed guideline which centers around variable indicators. Passages of the interview are coded and annotated with the extracted content and time dimensions, as well as a cause and an effect, if applicable. Further analysis focuses on these annotations; the source material is only considered as a reference and for documentation.

After extraction is complete, the information is cleaned, restructured if needed, and evaluated with respect to the original model. The goal of the final evaluation step is the extraction of cause-and-effect mechanisms that lead to answering the research question. For a study featuring only a small number of cases, the causal mechanisms for each case are extracted, discrepancies are explained, and the mechanisms are compared in order to eventually answer the research question.

Variables and assumed relations

Based on literature and initial assumptions, we construct the following model about power relations between security workers and their company, on which our evaluation is based on (cf. Fig. 1). Note that all hierarchies, tasks, and such all correspond to IT security work.

Our initial research question "How does the employee satisfaction in IT security departments change in relation to a similar or a different security narrative between employees and department head?" can be broken down into two variables: *Employee*

Downloaded from https://academic.oup.com/cybersecurity/article/6/1/tyaa011/5920841 by guest on 29 February 2024

Satisfaction Within the Company and *Power Struggles Around IT Security*. Power struggles are held between the company and its employees, so we added these two parties to the model and further investigated what tools each party has within this concrete struggle to shape their side.

The company usually sets the *Collective Goals Regarding IT Security*, and, to a large degree, shapes the *Company's Workplace Configuration*, e.g. by choosing open-plan offices or providing certain hardware to its employees. The *Flows of Communication* are an aspect over which both parties have power, so we modeled it as a shared variable.

An employee's narrative of security is shaped by their *Type of Work with IT security*, as well as their *Expertise* within the field. A person's *Own Precision of IT Security* shapes not only their *Satisfaction Within the Company*, but also their *Perceived Distance Towards the Employer*, as it is periodically compared against the company's collective goals. We theorize that *Compliance With Organizational Rules* might be connected to an individual's Degree of Activism, since a political mindset often influences behavior.

When thinking about the variable relations, we consciously did not opt for directional influences, because we wanted to keep an open mind about two-way effects between variables. Connection lines in the model diagram thus only indicate suspected influences between variables, which should aid in forming connections during the study evaluation.

In compliance with the QCA methodology, this model was constructed after surveying the theoretical foundations of our research questions and before conducting any interviews.

Model revisions

During the data gathering and evaluation steps, we noticed that our research question was not well covered by the participants' data. Rather than talking about their personal satisfaction and happiness, the focus was on work culture and effectiveness. We therefore chose to adapt the reserach question as outlined in the section "Introduction."

Furthermore, the model was not precisely fitting the reality we encountered. This is normal within QCA, especially when the theoretical and related work in a field is sufficiently sparse [25]. In the following, we list the revisions that were made during the course of the study and present the final theoretical model in Fig. 2.

After the interviews were conducted, the variable *Activism* was added to the model to reflect the inspiration and motivation from political and activist actors such as Edward Snowden which emerged from the data. We encountered statements about these in a number of cases and theorized that security-centered activism shapes a person's view on the topic.

During the restructuring of the extracted information, it became clear that both the variables *Compliance With Organizational Rules* and *Perceived Distance Towards the Employer* were very closely related to *Power Struggles Around IT Security*, so we decided to merge them.

Furthermore, the variable *Expertise* became a part of *Type of Work With IT Security*, since they were very similar in content.

Results

In this section, we present the findings from our interview study, support them with quotes, and extract the superior conflicts around IT security within both companies, according to our research method. We align the reporting of results by as follows: first, we present an overview on participants' fields of work and expertise, then we continue by expressed activism or association with activists around security, and follow-up with portraying the security narratives we found. We conclude this section by listing the extracted

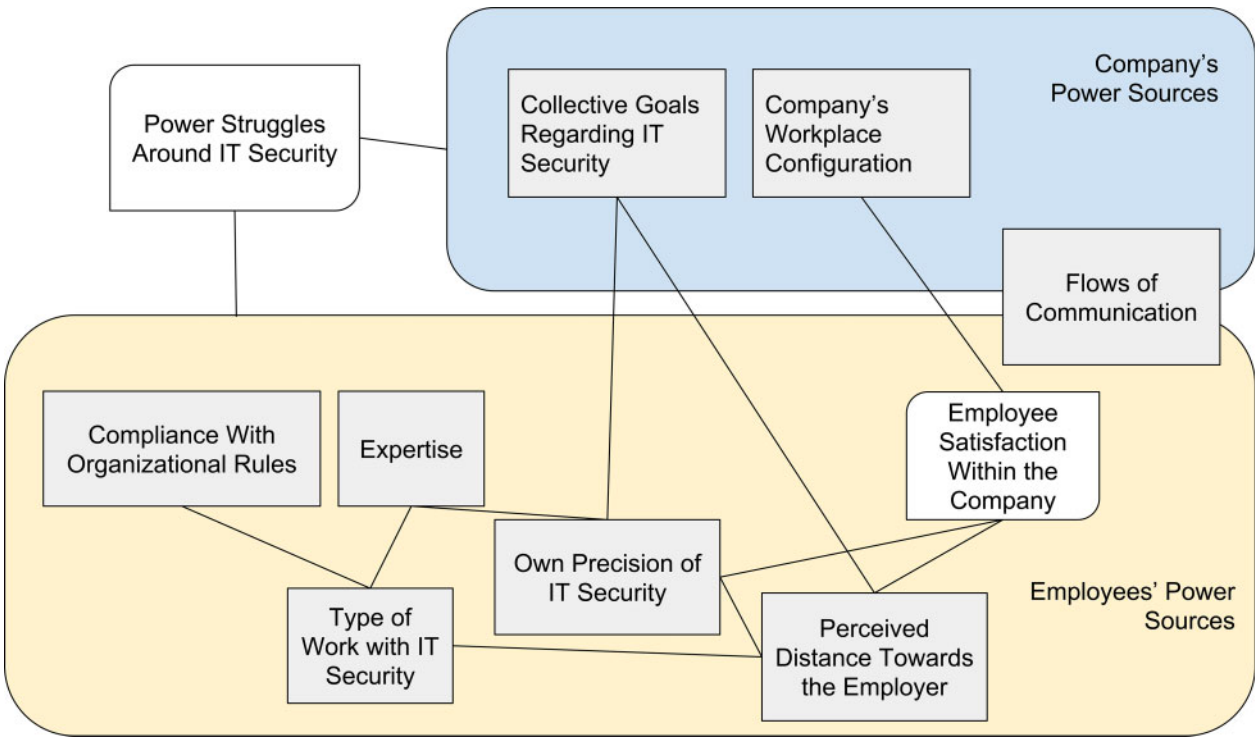

Figure 1. The evaluation model after conducting the interviews, depicting all variables used for evaluation. Variables corresponding to one party (company or employee) are grouped accordingly, and variables with two rounded corners are directly derived from the research question.

Downloaded from https://academic.oup.com/cybersecurity/article/6/1/tyaa011/5920841 by guest on 29 February 2024

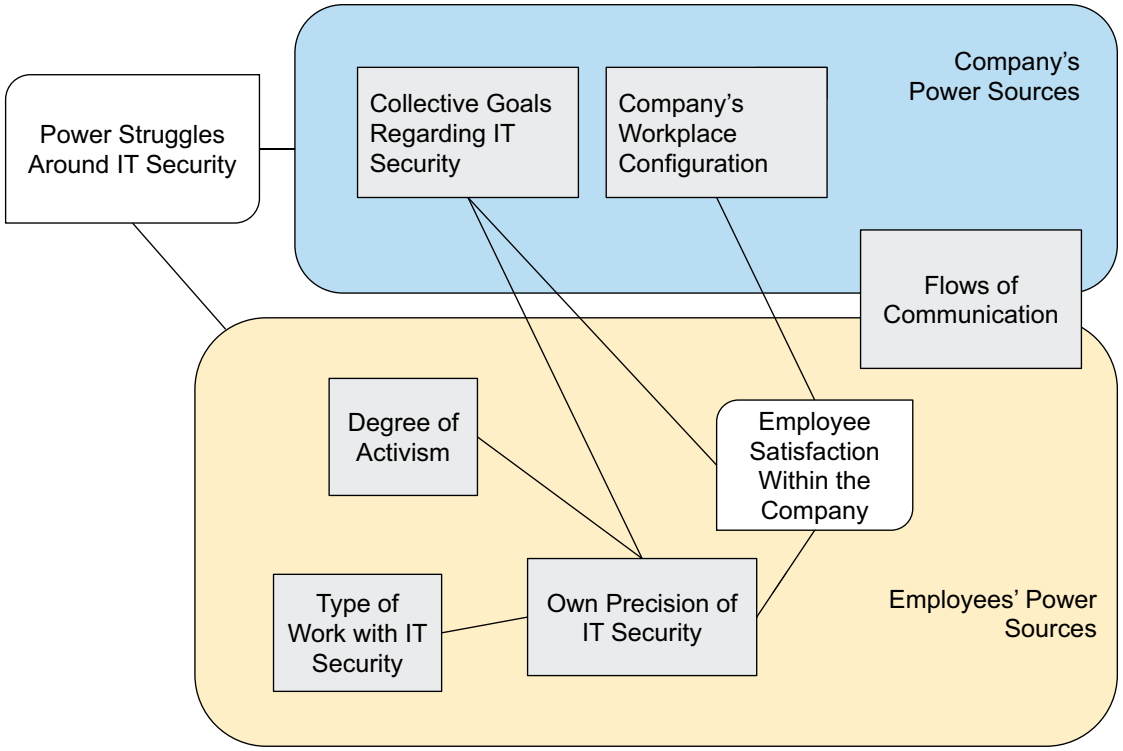

Figure 2. The final evaluation model. In comparison to our first model, the variable *Degree of Activism* was introduced, the variable *Expertise* was merged with *Type of Work with IT Security,* and the variables *Compliance With Organizational Rules* and *Perceived Distance Towards the Employer* were merged with *Power Struggles Around IT Security.*

conflicts for each employee and the overarching struggle within each company.

As mentioned in the section "Methodology," our recruiting requirement was getting a sample of security workers from single companies that ideall stem from a single, security-related team within each company. We were able to sample two companies, each with five employees and one department head.

We thus interviewed 12 employees in total, out of which 10 were male and 2 were female. This gender ratio is in line with the overall employment situation in tech in Germany [27]. Since both companies have very few women among their security-related staff, we chose not to identify them in order to protect their privacy. All participants will be further addressed with the singular they pronoun.

While we did not specifically ask for personal backgrounds, it became clear that one participant was educated outside of Germany and that their native language was not German. We cannot say how representative this is, since we sadly did not find statistics on ethnic representation in the German tech sector. One participant reported during the course of the interview that they had studied Sociology for 5 years, which might have influenced their answers to our questions.

All participants in the CC were on a permanent contract. This is a company-wide regulation and should not be considered special. In our sample from the RC, all participants but the head were on limited contracts. Employment time in the respective companies varied between 10 months and 8 years. For an overview on all participants, see Table 1.

All participants were asked for informed consent through a separate consent form that was also explained to them by the interviewer. At the time of the interviews, our department did not have a formalized ethics review process. Instead, we aligned the consent statement and procedure along German data privacy law and EU-GDPR, which enforce strict handling of identifying information. Participant *R1* declined the recording of the interview, thus, we can only report paraphrased quotes. All other participants consented to a recording. The recordings were transcribed and deleted afterward as communicated by the consent process. All but one interview were conducted in German (the other was conducted in English), the participant quotes in this report are thus translated from the original transcript.

Fields of work and expertise

The CC is operating in the field of data protection and privacy consulting, so four employees as well as CD reported that consulting, teaching, or auditing is part of their daily work. C2 and C4 reported systems administration as their only or as part of their tasks at work.

In the RC, employees were all working on technical topics like malware analysis, reverse engineering, or forensics. Several participants reported teaching or student coaching as part of their duties, since the company cooperates closely with nearby universities. All participants in the RC we interviewed were university educated. Some did not mention their study subject, but whenever they did, it was Computer Science.[2]

Educational backgrounds in the CC were more diverse. C1 extensively reported about their studies and a lecture by a company's

2 The German subject of *Informatik* might be slightly different than what an international audience understands as Computer Science, since it often is closer to Engineering than to Science.

Downloaded from https://academic.oup.com/cybersecurity/article/6/1/tyaa011/5920841 by guest on 29 February 2024

Table 1. Participant overview

Participant	Contract	Employed for	Field of work
C1	Permanent	2 years	Security & Privacy Consulting
C2	Permanent	1.5 years	Systems Administration
C3	Permanent	2 years	Technical Privacy Consulting
C4	Permanent	10 months	Administration, Security Auditing
C5	Permanent	6 months	Security Auditing, Training
CD	Permanent	8 years	CEO
R1	No answer	4 years	Malware Analysis
R2	Limited	4 years	Risk Research & Assessment
R3	Limited	2.5 years	Security Auditing
R4	Limited	4 years	Reverse Engineering
R5	Limited	2 years	Forensics, Database Reconstruction
RD	Permanent	8 years	Company Branch Lead

Notes: C in participant pseudonym refers to the "Consulting Company," an R refers to the "Research Company." Employment time recorded at point of interview. Participants with a D alias are department or company heads.

Chief Information Security Officer (CISO) on security management that greatly influenced them and their security narrative. C3 reported to have studied a non-security-related field before, but did not mention the exact topic. C5 reported to having studied Sociology for 5 years before switching to Computer Science. CD was a PhD student in Chip Design before founding the company.

For a summary of all participant's fields of work at the time of the interview, see Table 1.

Degree of activism

Security is often a very political field, since it closely connects to privacy and thus to basic human rights.

Our participants mentioned Edward Snowden, the Free, Libre, and Open Source Software Movement (FLOSS), and the German "Chaos Computer Club" (CCC) [28], a grassroots political hacker association with large impact on national IT and security politics, as their influences. Several participants also mentioned the importance of citizen rights in the context of security, especially the German right of informational self-determination [29].

In the CC, all participants mentioned some degree of political or activist influence on their narrative. C1 and CD showed a strong consciousness for citizen rights, especially in regards to privacy and self-determination about their data.

> There is this nice civil right, the right of informational self-determination [. . .], and *I* believe that you can apply this down to very concrete levels like requirements engineering within the software development process. (C1)

Participants C2 and C4 talked about hacker culture and hacker images. For C2, watching recorded talks of the annual CCC congresses [30] was a turning point in shaping their narrative about "hackers," and thus about security.

> That kind of opened my eyes back then, that even normal, or "normal", or good-willed people tear things apart to see how they work. And that exploits or other things that can be used to attack systems, are rather a byproduct from this curiosity about understanding things. (C2)

Edward Snowden was a prominent figure and source of inspiration for many participants (R2, R5, C2, C5). Participant C5 was so moved by Snowden's revelations about large-scale government spying that they decided to switch majors in their Computer Science Master, from computer graphics to security. C3 mentioned strong influence by the Echelon scandal in 2001 in the course of which was revealed that a group of governments eavesdropped on wireless communication, which is similar in nature.

Security narrative

Traits and features our participants commonly associated with security are network security, encryption, data protection and privacy, malware, and a general consciousness about security. Table 2 differentiates these further into categories, namely core attributes of security (confidentiality, integrity, protection), management facets, technical facets, influences, and metaphors. While employees within the RC center their associations around technical facets, the associations among the CC employees are more heterogeneous. They often use metaphors such as security being a "toy" to illustrate their narrative. Furthermore, connections to "hacker culture" were only made among the participants from the CC, as was laid out in the section "Degree of activism." On the other hand, the technical facet of "firmware and IoT" was only associated within the RC, which might reflect the daily work topics.

When asked about what coined their personal picture of security, most participants mentioned education in security or a related field. However, especially in the CC, some people reported being heavily influenced by data breach scandals, such as the Echelon scandal in 2001 or the Snowden revelations in 2013.

Some participants report a general frustration or a pessimistic view on security in general. For example, R1 states that there is either "bad, very bad, or okay-ish security."

In the following, we portray the security narratives we found in each company.

The CC

Company head CD reports that their picture of security developed during their PhD studies in Electrical Engineering, when it became clear to them that security always needs to be considered, regardless of field of work. They see security as a process accompanying the whole product life cycle in IT.

Among the employees in the CC, we noticed that those employees who reported to mainly work in technical areas of security (namely C2 and C4, cf. Table 1), had a narrative that was very focused around the tools they mainly use. For example, C2 answered the following when asked about their associations with the term IT security:

Downloaded from https://academic.oup.com/cybersecurity/article/6/1/tyaa011/5920841 by guest on 29 February 2024

Table 2. Study participants' individual associations with the term "IT Security"

	C1	C2	C3	C4	C5	CD	R1	R2	R3	R4	R5	RD
Confidentiality	•		•							•		•
Integrity	•		•						•			•
Protection	•	•	•	•	•		•		•	•	•	•
Risk (Management)	•		•					•	•		•	
Management/Processes/ Communication	•					•						•
Laws/Regulations	•		•		•							•
Human Factors				•		•				•	•	•
Securing Processes/Apps/Communication	•		•		•	•	•	•	•	•		
Malware/Virus Protection		•					•		•	•	•	•
Cryptography	•		•		•		•	•	•			
Compromised Systems		•		•				•		•	•	
Firmware/IoT								•	•			
Tools		•										
News		•									•	
NSA/Snowden		•			•			•			•	
Hacker Culture		•	•									
Hacker Cliche		•	•									•
Toy	•		•	•	•							
Buzzwords		•	•			•					•	
Good vs. Evil		•			•					•		

Note: IT Security is grouped into core attributes, management facets, technical facets, influences, and metaphors.

> In the recent time [I think] mostly about cryptoviruses, and what has happened in the news. And yes, methods how you can counter them, good virus protection and so on, but also the NSA scandals, now that new parts of the software library have been leaked. That the Cisco routers are, again, still insecure. So yeah, the Heise[3] news connected to these examples. (C2)

C4 fell victim to a hacking attack on a self-hosted game server and subsequently started to become interested in securing their own as well as hacking other people's servers.

On the contrary, the CC employees who mainly worked in consultancy and training expressed a very differentiated narrative, distinguishing between terminologies such as data protection, data security, and information security.

> And recently we had a discussion about data protection, and then there was another term, data security, that somehow competes with IT security and you have to consider, what is the difference? Or is it the same, yes? And then there is the term of information security where again the question is, is this different from IT security? (C1)

Following this statement, C1 proceeded to differentiate the terms they mentioned further.

Employee statements in the CC acknowledge that there is no unified narrative within the company:

> One could start with the fiction of a unified opinion in here regarding IT security, but there is none. And I think the only common thing we have here, is that it is something good, something we should have. (C3)

CD confirms this, further adding that there are frequent discussions about the concept of security which lead to frustration among the employees. They are aware of the tension and explicitly acknowledge the existence of a conflict around the security narrative, but consider it as a source of active knowledge exchange and, eventually, fruitful discussion.

> And stemming from the fact that there are many different opinions around here, the discussion is never finished. Read: We wouldn't pose and say "We really know stuff about IT security and exactly *this* is how it works". This will never happen. It is inherent to the system, sometimes gets on your nerves and I even understand that, but I regard this as a very important part. It is part of the company and I think this is the way how security can work best, by constant questioning. (CD) (emphasis in original)

The RC

Branch head RD's security narrative is closely aligned to the different levels of confidentiality that play a big part in the company's procedures. RD expresses strong consciousness about what type of information needs what level of protection and also applies this mental model to their daily life.

> For myself, I am very consequent on that matter. In contrast to many others, I regard it as noncritical to consciously send unencrypted emails, so I differentiate in my mind between what is deserving protection and what is not deserving protection. When we make an appointment, it is by my strongest belief not deserving much protection. But when we'd exchange on how I evaluate certain people [. . .], it would be a totally different thing. (RD)

In addition, CD mentioned Sun Tzu, the ancient Chinese military strategist as an inspiration for their security strategies. This is the only mention of an authoritarian figure across all interviews.

> The ancient strategist Sun Tzu has said on that: "Who defends equally in all areas, has no structured defense at all". And those who protect the canteen's menu the same level as they protect

3 A major German tech news outlet, https://heise.de.

Downloaded from https://academic.oup.com/cybersecurity/article/6/1/tyaa011/5920841 by guest on 29 February 2024

> their most important technical design drawings where the company's competitive advantages are stored, they haven't properly set up their security. (CD)

Employees in the RC feel very close to their team leaders, but report struggles with the company's IT department.

> But then there are days where you file a request for an IP clearing, which is a port clearance on a firewall, and then it takes time until it's done, and then it has only been done for two or three parts but not in the other parts, because some person had the opinion that you wouldn't need that, but you actually needed that. But then nobody notifies you, and then you start debugging your own stuff until you eventually find out using *iptrace* or the like that you actually weren't the cause of the error, but the firewall rules were, and well, on such days you're really cursing it. (R5)

Two employees in the RC mention that some contracts the company acquires come from the military. While R3 sees the potential of a personal moral conflict for others, they report that they personally would have no problem with working on military projects. In contrast, R2 would not feel comfortable in such a situation, but they are sure that their team leader would respect their worries and would not assign them such a project.

R3 assumes that the narrative varies significantly by team. R5 confirms this by stating that they have a very similar mindset with their team leader. RD assumes that the mindset within the company greatly diverges ("We have 450 employees and likely 570 opinions on the topic"), but assumes that most will have a similar narrative to them.

Conflicts

After extracting information according to our variables, the next step was to identify a high-level conflict around IT Security for each participant. Subsequently, these conflicts were grouped by company and then used to extract the company's conflict around the security narrative. An overview is provided by Tables 3 and 4.

Within the CC, two employees expressed internal conflicts about their own narrative of security. A strong personal interest in the topic contrasts with the realities that the participants face in their daily work life.

> I think the only potential conflict for me is that I work in a field in which I am personally interested. And you just can't do some things the way you personally regard them as right. And what *I* perceive as right for *myself*, does not necessarily have to be right for a company. (C3) (emphasis in original)

Participants from the CC also expressed awareness about diverging narratives within the company.

C1 refined this statement from C3 about the "fiction of a unified opinion" (cf. the section "Security narrative") further, explaining that:

> I think the dangerous thing is, that there is no explicit consensus. There is something implicit, that as developed within people's minds from conversations and the like. But this doesn't sync, and at some point you have the feeling that you don't need to talk about it any more. (C1)

Participant C5 feels tension stemming from unresolved conflicts around the security narrative within the company.

> There is a lot of beating around the bush. Nobody speaks plain text. And this beating around the bush is such a hindrance, because nobody communicates their point of view clearly. Even when it should come to a conflict, we could resolve it. Even if it seems insurmountable, resolving conflicts os possible. (C5)

The CC's head adds that the security narrative is a frequent subject of discussion among the employees. CD consciously uses their power within the organization to keep this zone of uncertainty around the term security open.

> Within the *Consulting Company*, the differences at this point are somewhat embraced. That leads to frequent discussions, to frequent discrepancies, to disagreements. But this doesn't really harm the company, quite the contrary. (CD)

Discussions about the security narrative are frequent and lead to frustration and fatigue, but also to development and mutual education within the company (see also the section "Security narrative").

> Yes, there are frequent discussions, and my opinion [...] is of course questioned too, and discussed every now and then, sure.

Table 3. Summary of conflicts within the CC

C1	Own idealism and attention to detail clash with the necessity to offer realistic services. This leads to frustration.
C2	No conflict, self-image as a "good hacker", narrative focuses around tools.
C3	Fun and intellectual challenge with security, but frustration with the business, also within the company.
C4	Administrator restricts the company-given flexibility by not offering certain tools.
C5	Inhibited communication culture within the company because of uncertainties. Wishes for clarifying conflicts.
CD	Conscious uncertainty around the narrative, therefore frequent discussions and fatigue among employees, but also education and advancement.

Table 4. Summary of conflicts within the RC

R1	No conflicts within the company. General frustration with quality of and consciousness about security.
R2	Security regulations imposed by the parent company hinder research work, active circumvention of these regulations with help of team lead.
R3	Only structural conflicts within the company. Personal conflict with consequently applying security knowledge in daily life.
R4	No conflicts within the company because of very similar narrative.
R5	Security regulations imposed by the parent company hinder research work, active circumvention of these regulations with help of team lead.
RD	Handling confidential information requires special considerations regarding security which are not well realized by employees and lead to conflicts. Active circumvention of the regulations is tolerated.

Downloaded from https://academic.oup.com/cybersecurity/article/6/1/tyaa011/5920841 by guest on 29 February 2024

> But as I said, I regard this as desirable. It might not be perceived this way by everyone, but I see this as a pleasant thing. (CD)

Participant C5 shares another view on the issue. Since they are relatively new in the company (6 months at time of interview, cf. Table 1), they welcome any coworkers who would share their opinion on security and privacy with them.

> Sure, first and foremost it is a conflict, but for *me*, as a relative newbie in the field, I really appreciate any input that I can get. I think about it, I process it somehow. And if I assume that someone wouldn't regard IT security as important as I do, but instead something else, then I am open to their point of view and accepting it. I don't think that my opinion is the non plus ultra. (C5) (emphasis in original)

The most prevalent conflict within the RC is the struggle around security guidelines. The company works with classified data and therefore special considerations on infrastructure and protection need to be made. At one point in the interview, RD expressed that these rules often do not align with employee mental models and thus lead to misunderstandings:

> We are in the process of advancing in the separation of networks I mentioned. This comes with a lot of uncertainty from the employees, and often it happens that the questions that are asked from the security point of view [...] are answered in a way that lead to a high level of security. For example, when someone says "Yes, I always work with classified data and always need to access it", that would lead to cutting off the access to Google because the page can not be made available within the high-security network. And that leads to frustration. (RD)

There are security guidelines for the whole company which also apply to the branch working on security. These guidelines regularly clash with active and experimental security research which is conducted in the RC.

> Many of my colleagues do reverse engineering of viruses for example, and conduct dynamic analyses of viruses. First, they can't do that on a Microsoft Windows. They can't work with a running antivirus, because of course there are viruses on their computers, that's the point of their work! Often, there are no company-level strategies for this, it only leads to friction on all levels. (R5)

There are conflicts both in complying with the security guidelines as well as applying the confidentiality rules. Team leaders support their employees in actively circumventing and working around these restrictions, so that they can accomplish the tasks they are assigned to. RD knows about these rule breaks and tolerates them silently, but not without remorse.

> There are workarounds which touch critical areas and where I have to ask myself if I really want to know it. Usually, I don't. But of course, in a position of responsibility such as mine, I have to ask myself then, "How much control do we need, how many decisions do we really need to execute, and where can one sometimes look away?" (RD)

RD thus abstains from using their power within the zone of conflict.

Discussion

We see frequent discussions about the "fringe" in the CC. CD regards them as fruitful because their employees already have a very defined mental model, but they acknowledge the emotional burden in the form of frustration and fatigue (cf. the section "Security narrative"). CD uses their power within the organization to keep the uncertainty zone around the company definition of security consciously open, as they believe that it would benefit the company, and eventually, its employees, too.

It was striking that individual security narratives were more precise among participants who worked in consulting, especially within the CC (cf. the section Security narrative"). The more technical participants C2 and C4 mainly aligned their narrative on technical terms and tools as well as activist motifs. The other employees expressed more layered narratives of security, encompassing (business) processes and different perspectives. This indicates that power struggles and dynamics might be more present in companies where security experts talk about security as part of their professions and pose a hypothesis for further investigation within the security consulting sector.

It was striking and even surprising based on our theoretical research (cf. the section "Theoretical background") that CD was very aware of diverging security narratives within their company, the uncertainty zone they opened, and the effects of frequent discussions about this. Moreover, they regarded the power struggles as a benevolent effect, because they lead to mutual education and the exchange of knowledge and news around IT security. The sharing of resources and information in this scenario would be a suitable starting point for further research into the influence of news, scientific findings – CD explicitly mentioned being confronted with research papers – and stories, as it has already been researched that these different types are used to convey different types of information when shared [31]. On the other hand, the question about to what degree language uncertainties are or can be used as a tool for staying up to date with security and privacy-related topics poses itself in this context.

The awareness of the narrative within a company and careful employee steering around the associated uncertainty zone could be an important "soft skill" for management positions. It remains open as to how targeted uncertainty zones can be cultivated by department or company heads. CD reports that there is no top-down definition of what security means for the company, and that they explicitly foster different opinions (cf. the section "Conflicts"), but we do not yet know what other effects might play a role in cultivating uncertainty, so follow-up work in that direction is needed.

In comparison, we found employees in the CC to be idealistic people, in part motivated by activism, and to bring very defined models of security into the company. Why this was the case was sadly outside of our study scope.

Within the RC, the internal conflict of working on military projects was visible. One participant reported such a conflict for themselves, and another participant was not affected personally, but stated that their colleagues might have this conflict (cf. the section "Security narrative"). It is important for department and company heads to carefully consider this conflict of interest among their employees, as such a strong, unresolved internal conflict can lead to employees leaving the company. However, the RC has developed a strategy for this potential of conflict, as it only tasks employees with military projects who explicitly want to (cf. the section "Security narrative").

Downloaded from https://academic.oup.com/cybersecurity/article/6/1/tyaa011/5920841 by guest on 29 February 2024

The most prevalent conflict within the RC was the struggle around security guidelines. Participants from the RC have mentioned that they are supported by their team leaders in coping with this conflict, so allying against a "common enemy" within the company might boost an employee's bonding with their employer.

RD knows about the guideline circumventions and rule breaks and tolerates them silently, but not without remorse. They thus abstain from using their power within the zone of conflict, leaving it to the employees and the IT department. This might be because they do not want to lose their employees, since they mentioned that the biggest constraint for their branch is acquiring good personnel.

> The challenge is doing the most meaningful things with the available personnel. So there are only limits in acquiring new employees, content-wise, this is the land of opportunities. (RD)

To fully capture the conflict on security regulations in the RC, additional interviews with members of the company's IT department would be necessary.

Limitations

This work is not free from limitations, which we will report in the following.

This study features a rather small sample size, which limits the generalization of our results. This stems from the recruiting difficulties we had, as it turned out to be very hard to get into companies for an interview study. Where other researchers could draw from their institutional background (e.g. Haney *et al.* [32]), we as university researchers had no such background but only a few ties to local industry from which we could draw.

In addition, the participants we interviewed came from a very narrow sociocultural window. All but one were white, there were only 17% non-males in our sample, and we consciously only chose one single sociocultural area to recruit from, in order to not introduce additional effects because of culturally different work or interpersonal habits.

It was not our goal to get a large, representative overview on the security narrative, but instead go down deep into one special culture. Thus, follow-up work to extend our findings to other cultural contexts would be greatly appreciated and might be used to identify further, culture-specific influences on power struggles around the security narrative.

Conclusions and future work

In this work, we investigated the narrative of the term IT security within two companies working in or closely related to security. By looking at individual definitions of the term "security," we showed that different narratives exist within a company and that the level of detail might relate to an employee's task within the company. In our case, the people working in consulting and training had very precise narratives, technical employees such as systems administrators in comparison had a coarse narrative, centered around tools and protocols.

This provides new insights into the human factor and social dynamics between security workers, those who create or shape the creation of security and privacy practice. It is thus a contribution to deeper understanding of social and power dynamics within the context of Usable Security and Privacy.

When addressing our initial research question, "How do effectiveness and work culture in IT security departments change in relation to a similar or a different security narrative between employees and department head?," we can give an answer for each company we studied.

In the RC, the employees working on security research had narratives focused around the technology they work with and reported no internal conflicts about the narrative, but struggled with the company's IT regulations. For example, malware research was jeopardized by mandatory antivirus software. Employees and whole teams have established workarounds and set up a second "shadow infrastructure" to arrange with this. The company head is aware of such workarounds but sees them with remorse.

In the CC, our theory of uncertainty zones around the definition of security was confirmed. The company has no top-down regulation of what security is, and employees often discuss and clash on that topic. However, in contrast to our initial assumption, the company's head was aware and actively fostered this culture by leaving the uncertainty zone around the security narrative consciously open. The diversity of narratives had a small negative impact on employee satisfaction, but profited the company as a whole. This indicates that uncertainty around IT security might not be inherently bad for company climate, although we see a clear tradeoff with employee frustration and fatigue.

Shaping (or not shaping) the security narrative might thus be a new tool for managers in IT security to precisely foster their department's intellectual growth. A narrative can function as a bonding tool within the department and can create a clear distinction toward other departments. Cultivating collective uncertainty around it can lead to increased interpersonal exchange and mutual education around the topic.

Regarding research, this work shows – in its own, limited scope (cf. the section "Limitations") – that the analysis of language uncertainties can be a powerful indicator of company climate and motivation within professional security departments. This opens up new possibilities for security perception research in professional communities as well.

As for future work, one could continue the general direction which the results from the CC have outlined. The narratives among the consulting employees were very well defined and the impacts of different narratives were prominent in their daily work life. Thinking the field of consulting further, the narratives of "opinion shapers" and communication multipliers such as blogs or news outlets could be investigated.

When considering the other direction outlined by our findings within the RC, a field of future research could be the uncertainty zone around IT security between security departments and other employees in nontechnical companies with a high focus on security, such as banks.

Acknowledgements

The authors would like to thank the following people for help and support during this project: Jens Bergmann, Julie M. Haney, Maximilian Häring, Yasemin Acar and Mary Theofanos, the anonymous reviewers, and all participants of our study.

Conflict of interest statement. None declared.

References

1. Russell B. Vagueness, 1923.
2. Wittgenstein L. *Philosophische Untersuchungen Kritisch-genetische Edition*. Suhrkamp: Berlin, 2001.

Downloaded from https://academic.oup.com/cybersecurity/article/6/1/tyaa011/5920841 by guest on 29 February 2024

3. I. O. for Standardization. *Information Technology; Security Techniques; Information Security Management Guidelines for Telecommunications Organizations Based on ISO/IEC 27002*. International Organization for Standardization, 2009.
4. Pipkin DL. *Information Security: Protecting the Global Enterprise*. Upper Saddle River, N.J.: Prentice Hall PTR, 2000.
5. Cherdantseva Y, Hilton J. Information security and information assurance: discussion about the meaning. In: Irene MP and Fernando A (eds) *Organizational, Legal, and Technological Dimensions of Information System Administration*, Hershey, Pennsylvania, USA: IGI Global, p. 167, 2013.
6. Blythe JMCoventry LLittle L. Unpacking security policy compliance: the motivators and barriers of employees' security behaviors. In: *Symposium on Usable Privacy and Security*, pp. 103–22. USENIX Association, 2015.
7. Chandran SOu XBardas AG, *et al*. A human capital model for mitigating security analyst burnout. In: *Symposium on Usable Privacy and Security*, pp. 347–59, Ottawa, Canada: USENIX Association, 2015.
8. Mayring P. *Qualitative Inhaltsanalyse, 12th edn*, Beltz, 2012.
9. Scott WR. *Institutions and Organizations: Ideas and Interests*. Thousand Oaks, California, USA: Sage, 2008.
10. Croizer MFriedberg E. *Die Zwänge kollektiven Handelns. über Macht und Organisation*. Königstein/Ts: Athenäum-Verlag, 1979.
11. Seidel C. Ungewissheit, Vielfalt, Mehrdeutigkeit – Eine Heuristik unsicherer Umwelten. In: *Organisation und Unsicherheit*. Wiesbaden: Springer VS, 2015.
12. Kühl S. *Organisation - Eine sehr kurze Einführung*. Wiesbaden: VS Verlag für Sozialwissenschaften, 2011.
13. Belbin RM. *Management Teams, 3rd edn*. Bingley: Emerald Group Publishing Limited, 2010.
14. Becke G. Die Entdeckung des Informellen im Organisationswandel. Zum Potenzial kommunikativer Forschungsmethoden. In: Victoria von G. and Sylvia MW (ed.), *Formalität Und Informalität in Organisationen*. Wiesbaden: Springer VS, 2015, 145–168.
15. Krombholz KBusse KPfeffer K, *et al*. "if https were secure, i wouldn't need 2fa" - end user and administrator mental models of https. In: *S&P 2019*, 2019.
16. Theofanos MStanton BFurman S, *et al*. Be prepared: how US government experts think about cybersecurity. In: *USEC Workshop*, Internet Society, 2017.
17. Posey CRoberts TLLowry PB, *et al*. Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Inform Manage* 2014;**51**:551–67.
18. Hawkey KBotta DWerlinger R, *et al*. Human, organizational, and technological factors of it security. In: *CHI '08 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '08, pp. 3639–44. New York, NY: ACM, 2008.
19. Sundaramurthy SCMcHugh JOu X, *et al*. Turning contradictions into innovations or: how we learned to stop whining and improve security operations. In: *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pp. 237–51. Denver, CO: USENIX Association, 2016.
20. Haney JMTheofanos MAcar Y, *et al*. "we make it a big deal in the company": security mindsets in organizations that develop cryptographic products. In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pp. 357–73. Baltimore, MD: USENIX Association, 2018.
21. Hochschild AR. *The Managed Heart: Commercialization of Human Feeling*. The University of California Press: Berkeley, 1991.
22. Serebrenik A. Emotional labor of software engineers. In: Demeyer SParsai ALaghari G *et al*. (eds), *BENEVOL 2017: BElgian-NEtherlands Software eVOLution Symposium, 4–5 December 2017, pp. 1–6*. Antwerp, Belgium: CEUR-WS.org, 2017.
23. M'manga AFaily SMcAlaney J, *et al*. Folk risk analysis: factors influencing security analysts' interpretation of risk. In: *Proc. of the 13th Symposium on Usable Privacy and Security, ser. SOUPS*, USENIX Association, volume 17, 2017.
24. Creswell JWPoth CN. *Qualitative Inquiry and Research Design: Choosing among Five Approaches, 4th edn*. Thousand Oaks, California, USA: Sage, 2017.
25. Gläser JLaudel G. *Experteninterviews und qualitative Inhaltsanalyse*. Wiesbaden: VS Verlag für Sozialwissenschaften, 2010.
26. Hsieh H-FShannon SE. Three approaches to qualitative content analysis. *Qual Health Res* 2005;**15**:1277–88.
27. GmbH. H. Frauen in der IT-Branche 2018, 2018. https://www.honeypot.io/de/women-in-tech-2018/ (1 June 2019, date last accessed).
28. Chaos Computer Club e. V. Chaos Computer Club. https://www.ccc.de/en/home (29 January 2019, date last accessed).
29. Kodde C. Germany's 'right to be forgotten' - between the freedom of expression and the right to informational self-determination. *International Review of Law, Computers & Technology* 2016;**30**:17–31.
30. Chaos Computer Club e. V. Browse Videos by Category: Congress. https://media.ccc.de/b/congress (https://www.ccc.de/en/home (29 January 2019, date last accessed).
31. Rader EWash R. Identifying patterns in informal sources of security information. *J Cybersecur* 2015;**1**:121–144.
32. Haney JMGarfinkel SLTheofanos MF. Organizational practices in cryptographic development and testing. In: *2017 IEEE Conference on Communications and Network Security (CNS)*, IEEE, pp. 1–9, 2017.

Appendix

The interview guideline

In this section, the English translation of the German interview script is provided. Please note that the briefing statement and consent form are not included.

1. First, we'd like to know some general information about you. For how long have you been working in this company resp. this department?
2. Are you on a temporary or a permanent contract?
3. What are your tasks here?
4. There have been some restructuring measurements within the company. How did you experience these? Are you content with your labour situation?
5. Thank you. Now, we would like to talk to you about the topic of IT Security in general. What are you thinking of when you hear the term?
6. What do you personally connect to the term IT Security?
7. Did the term always have this meaning to you?
8. How do you think your employer regards the term IT Security?
9. Do you see any potential of conflicts between these two notions?
10. If you could change one thing about your current work situation, what would it be?

Downloaded from https://academic.oup.com/cybersecurity/article/6/1/tyaa011/5920841 by guest on 29 February 2024