“GOOD” ORGANIZATIONAL REASONS FOR “BAD” CYBERSECURITY

Ethnographic Study of 30 Danish SMEs

Laura Kocksch & Torben Elgaard Jensen
The Techno-Anthropology Lab (TANTlab)
Department of Culture and Learning

AALBORG UNIVERSITET
ADD Algoritmer, Data & Demokrati

Executive Summary

The Danish Cyber and Information Security Strategy 2022–2024 points to an inadequate level of cybersecurity in Danish small- and medium-sized enterprises (SMEs). However, Erhvervsstyrelsen has repeatedly found it difficult to reach a large and diverse audience of SMEs through traditional channels and information campaigns (Epinion, April 2021 & January 2022). The aim of the present report is to bring new resources to Erhvervsstyrelsen's ongoing information and communication efforts. Based on a comprehensive ethnographic study by Laura Kocksch and Torben Elgaard Jensen from Aalborg University's Techno-Anthropology Lab (TANTlab), this report outlines a series of new insights into the cybersecurity practices, circumstances, and rationalities of Danish SMEs. The study included visits to 30 broadly sampled SMEs, interviews with the key people responsible for cybersecurity in each company, and observations of on-site security practices. The study was carried out by TANTlab as a part of a research collaboration between Erhvervsstyrelsen and Aalborg University (March–December 2022) and presents the largest qualitative enquiry to cybersecurity practices in Denmark to date.

The SMEs' nonstandard organization of cybersecurity creates a challenging communication situation

None of the 30 Danish SMEs had a designated cybersecurity unit or cybersecurity manager. Therefore, the CEOs of these companies have delegated the responsibility for cybersecurity to other people, such as IT managers, accountants, or communication specialists. These nonstandard cybersecurity figures must draw on standard cybersecurity advice and strategies to handle what are often nonstandard problems. This leads to pragmatic dilemmas and sometimes "clumsy solutions," which create a difficult scene for communication and dialogue, one in which standard ideals and norms may conflict with practical necessities and local circumstances.

SMEs' protection practices are significantly shaped by the type of proffesional to whom the responsibilty is assigned

Across the SMEs, different types of professionals are assigned the responsibility for cybersecurity work. Each profession brings different resources and challenges to the job. When *IT managers* are responsible for cybersecurity, they have the benefit of knowing the technical systems of the companies well, but they may face the dilemma of having to criticize the systems they have developed. When *accountants* are responsible for cybersecurity, they have the benefit of close collaboration with the CEO, but they face the challenge that the social-organizational procedures are more readily available to them than technical solutions. When *communication specialists* (sometimes known as compliance managers) are responsible for cybersecurity, they have the benefit of professional communication tools and strategies, but they face the challenge of being less familiar with the ins and outs of the production and administration practices of their companies. *External IT suppliers* also have the difficulty of not knowing the nuts and bolts of the company, as well as being constrained to advisory tasks.

SMEs incorporate local resources and develop local tactics to uphold cybersecurity

The SMEs' practical everyday organization of cybersecurity builds on and incorporates their local long-term social relations, as well as their geographically limited operations and their

small company sites. This allows the companies to handle cybersecurity, sometimes very effectively, by sharing local anecdotes, collective defense strategies, and flexible handling of rules. In this context, breaches of formal cybersecurity rules are not always criticized but rather seen as necessary local adaptation to make things work.

The handling of practical dilemmas show that there are several "good" local reasons for "bad" cybersecurity

The present study has identified several types of dilemmas where the fully adequate cybersecurity solutions are either not available or not compatible with the adequate functioning of the company. The dilemmas include economic-technological dilemmas, such as dependency on legacy technology that is difficult to secure; process-temporal dilemmas, such as the conflict between time-consuming cybersecurity practices (e.g., typing of passwords) and time-critical operations; and social-organizational dilemmas, such as conflicts between company cultures of mutual trust and cybersecurity requirements of sequestering information and access.

The hypothesis that SMEs are simply ignoring cybersecurity issues is not confirmed

Several surveys and interview studies have indicated a worrying lack of basic cybersecurity measures in many SMEs (Erhvervsstyrelsen, 2021). This has led to the suspicion that a substantial number of SMEs may simply take no interest in cybersecurity (Epinion, April 2021). The ethnographic study has not confirmed this suspicion. To the contrary, we have found that all the companies were concerned with cybersecurity, even in cases where they—for a variety of reasons—were not able to live up to the recommended standards of protection. We also found that a basic level of cybersecurity was maintained: all but one company fulfilled the basic IT security recommendations or reported as having critically assessed their cybersecurity situation.

Cybersecurity stakeholders point to several opportunities for improving the dialogue with SMEs

In December 2022, the results of the interview study were presented and discussed at a stakeholder workshop. The stakeholders also played dilemma games and engaged in a collective design challenge developed from the ethnographic material. The stakeholders identified a series of opportunities for improving the dialogue with SMEs. These included the development of new engaging formats (games) and establishing a dialogue with new key actors in and around SMEs (accountants and board members). The stakeholders also emphasized the general need to customize communication and explore new ways to take the full diversity and practical circumstances of SMEs into account.

Implications for the cybersecurity dialogue in the future

The study shows that cybersecurity is neither absent nor ignored by SMEs. Instead, the case is that the SMEs' cybersecurity concerns and practices exist in a form that is not sufficiently recognized and, therefore, generally not in the focus of communication efforts. The current study describes a series of local organizing efforts, types of knowledge, and pragmatic practices that the SMEs have used to handle cybersecurity in a way that makes sense locally.

Awareness of these local efforts and a willingness to explore them further may provide a good starting point for facilitating and improving the dialogue with the SMEs. Specifically, the report recommends the following:

- Involving local cybersecurity figures in cybersecurity campaigns.
- Developing new vocabulary that relates to everyday cybersecurity knowledge.
- Making further efforts to understand "good" local reasons for "bad" cybersecurity practices.
- Facilitating the customization of communication strategies by supplementing the current understanding of segments with a series of additional classifications.
- Staying aware of how moral high grounds and the "shaming" of insufficient cybersecurity measures create obstacles to constructive dialogue.

Table of Contents

Executive summary		**2**
1.	**Project background and aim**	**5**
2.	**The ethnographic study: Methods, scope, and sampling**	**7**
3.	**Local cybersecurity responsibility**	**12**
4.	**Local cybersecurity knowledge**	**17**
5.	**Local cybersecurity practices**	**22**
6.	**Stakeholder workshop**	**27**
7.	**Implications for a cybersecurity dialogue in the future**	**30**
8.	**References in order of appearance**	**33**

1. Project Background and Aim

The present report draws on material collected during a nine-month, multi-sited ethnographic study of 30 SMEs in Denmark. The focus is on the current condition of cybersecurity in SMEs. These companies are seen as a potential target for cyberattacks because of their high level of digitalization, yet they lack formal processes, auditing, and risk assessment.

In August 2021, the Virksomhedsforum for Digital Sikkerhed and Erhvervsstyrelsen's Kontor for cyber- og informationssikkerhed contacted Aalborg University's Techno-Anthropological Laboratory (TANTlab) with the intent of establishing a research collaboration aimed at conducting an in-depth qualitative investigation of the cybersecurity practices of SMEs. The aim was to supplement and potentially challenge existing knowledge of cybersecurity in SMEs by providing real-world observations. The ethnographic method was sought to generate new insights about the people, processes, and practices involved in cybersecurity in SMEs, potentially identifying the shortcomings and drivers for effective cybersecurity mechanisms in SMEs. These insights were then mobilized to suggest improvements to current communication, advice, and dialogue about cybersecurity issues with SMEs.

The present ethnographic study aims for a unique insight into the everyday cybersecurity practices of companies with little to no formal cybersecurity organization. Thus, its scope contributes a novel perspective to the established knowledge about SMEs, largely gained through quantitative inquiries or interview studies. The existing cybersecurity dialogue mostly addresses individual users who are portrayed as lacking knowledge, skills, or resources. The ethnographic approach sheds light on the everyday collective actions of SMEs and incorporates their specific material–technological equipment and physical location. The following research questions guide this approach:

1. *How do SMEs organize cybersecurity responsibilities?*
2. *What types of everyday knowledge do SMEs have of cybersecurity?*
3. *How do SMEs handle cybersecurity issues in everyday practice?*
4. *How can the specific situation of SMEs be taken into account when facilitating future dialogue and communication?*

The current study aims for an enhanced understanding of the unique cybersecurity situation of SMEs, offering alternative ways of targeting SMEs in future communication efforts. Furthermore, it was decided that the ethnographic study would not be limited to evaluating cybersecurity in the SMEs but to investigating the local reasons for lacking or partial security. Companies were not addressed with a specific judgment in mind regarding what cybersecurity should look like in SMEs but rather what was relevant and important to them. By doing so, the aim of the present study was to understand the local situation of SMEs and their specific cybersecurity situation; this situation is characterized by their specific way of organizing cybersecurity, perceiving cybersecurity, and actively engaging in cybersecurity.

Erhvervsstyrelsen's Kontoret for Cyber-og Informationssikkerhed contributed to the recruitment of the companies, offering their expertise in the field of SMES to the researchers. TANTlab conducted the multi-sited ethnography and subsequent analysis. The current study

was aided by TANTlabs' position as research leader for cybersecurity in the 10-year interuniversity research project Algorithms, Data, and Democracy (ADD). The results of the study were discussed at a stakeholder workshop involving the two project partners and the Virksomhedsforum for Digital Sikkerhed, which generated insights beyond the ethnographic material (i.e., how experts in the field assess the current situation of SMEs in Denmark).

The results are presented in the following order: Chapter 3 focuses on RQ1 by exploring in detail how cybersecurity is locally organized and how different organizational tactics benefit or limit effective cybersecurity measures. Chapter 4 provides a comprehensive list of the everyday knowledge repertoires that the SMEs mobilized for cybersecurity, offering insights related to RQ2. Chapter 5 turns to RQ3 and describes the everyday practices and dilemmas that portray SMEs' tactics to encounter cybersecurity with the materials at hand. Chapter 6 outlines the results from the stakeholder workshop. The concluding chapter proposes what can be learned from these insights for a future dialogue with SMEs (Chapter 7).

2. The Ethnographic Study: Methods, Scope, and Sampling

Ethnographic studies of cybersecurity are rare[1]. A multi-sited ethnography on a national scale is unique. Ethnography aims for in-depth—or *thick* descriptions—of places, people, and practices. Its strength lies in the provision of contextual specificity instead of the functional representativeness of the sampling. Ethnography reaches conclusions through moments of saturation: stories and situations that repeat themselves and, thus, can be seen as more than singular occurrences. The large sampling of the present study has additionally enabled analytic comparison, tracing similar and conflicting themes across companies, arriving at conclusions of both contextual relevance—to specific companies—and indicating similarities or frictions.

2.1. Sampling

Table 1: Size of companies

No. of employees	No. in sampling
5–19	5
20–49	9
50–149	10
150–250	6
Total	**30**

Table 2: Distribution across business segment

Business segment (acc. CVR registry)	No. in sampling
Fremstillingsvirksomhed	8
Liberale, videnskabelige og tekniske tjenesteydelser	4
Engroshandel og detailhandel	4
Pengeinstitut-og finansvirksomhed, forsikring	3
Information og kommunikation	2
Administrative tjenesteydelser og hjælpetjenester	2
Landbrug, jagt, skovbrug og fiskeri	1
Bygge-og anlægsvirksomhed	1
Transport og godshåndtering	1
Undervisning	0
Kultur, forlystelser og sport	0
Andre serviceydelser	0
Total	**30**

The current study draws on materials collected from a sampling of 30 SMEs in Denmark, varying in size and business segment (see Tables 1 and 2). The sampling covers all relevant business segments as defined by the segmentation analysis but shows a majority of companies in the "low-involved," "cost-focused," and "gain-oriented" segment (Epinion, April 2021). The recruitment criteria were agreed upon by Erhvervsstyrelsen and TANTlab. The sampling

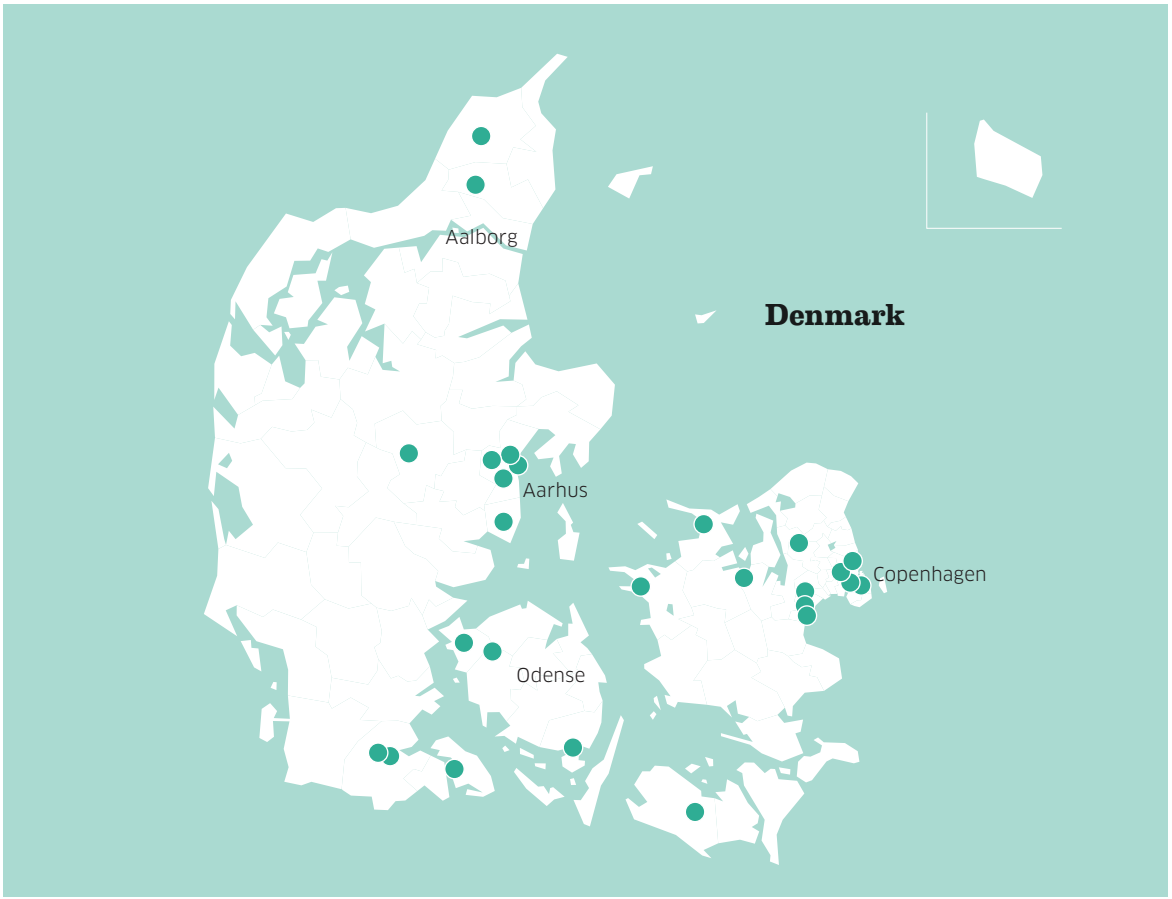
Note 1: Few studies have mobilized ethnographic methods such as participant observation or long-term immersion for cybersecurity, but examples include the following: Kocksch, Laura, Matthias Korn, Andreas Poller, and Susann Wagenknecht. "Caring for IT security: Accountabilities, Moralities, and Oscillations in IT security Practices." Proceedings of the ACM on Human-Computer Interaction 2, no. CSCW (2018): 1-20. Squires, Susan, and Molly Shade. "People, the Weak Link in Cybersecurity: Can Ethnography Bridge the Gap?" In Ethnographic Praxis in Industry Conference Proceedings, vol. 2015, no. 1, pp. 47-57. 2015.

was confined to companies with 9 to 249 employees and included companies that were lone standing, that is, those that were part of larger conglomerates or state-owned (such as critical infrastructures) were excluded. Companies were also chosen to represent a regionally diverse distribution, see Image 1. The diversity of the sampling allowed for a comparison between companies according to their size, business segment and geographic region.

Companies' suitability for the sampling criteria was assessed based on desk research of the CVR registry and phone calls. During the recruitment process, the companies were asked to commit to a physical visit of the ethnographer at the company's facilities, during which at least one interview with the CEOs or someone responsible for cybersecurity was arranged. Companies were encouraged to schedule more than one interview (e.g., one before and one after lunch) to give the ethnographer ample opportunity to tour the company. Recruitment was outsourced to a third party that was not involved in the visits or analysis. Over the course of the study, production companies *("Fremstillingsvirksomhed")* were identified as a particularly intriguing field for cybersecurity because they encountered various nonstandard cybersecurity problems, such as incommensurability between old production machines and the latest security updates. A focus was placed on them in the sampling.

The final recruitment included 51 additional companies that showed initial interest but failed to arrange a date or were asserted to be unsuitable for the recruitment criteria ex-post, and 98 companies refused to partake in the study.

Image 1: Regional Distribution



2.2. Visits and Informants

Visits were conducted between March 2022 and December 2022 with a two-month break during the summer. Each visit included a company tour and a recorded interview with at least one but up to four company representatives. In total, 57 people were interviewed. Table 3 provides an overview of our informant's positions.

Table 3: Positions

Position	No. in sampling
Other Employees	20
CEOs and Owners	19
IT Managers	14
Compliance Managers	4
Total	**57**

During company tours, the informants explained production processes, showed applications on desks or screens, and introduced colleagues whose statements were captured verbatim or paraphrased in the fieldnotes. All the interview participants signed a consent form declaring their rights as research participants and received a reimbursement of 400 DKK in the form of a gift card.

The ethnographer collected various materials from the companies; detailed fieldnotes including drawings and sketches, photographs, audio recordings, screenshots from dashboards, books, and advertisement leaflets. Audio recordings were transcribed, and other materials informed the ethnographic fieldnotes for each of the companies between 1 and 7 pages. The empirical material encompasses 81 pages of ethnographic field notes and 42 hours of audio recordings. As is common for ethnographic studies, the position and relations of the ethnographer to the field are accounted for in interview quotations and fieldnote excerpts, a genre-specific style that we have adopted here by speaking of the informant's interactions with "us" or how "we" experienced a specific setting. In doing so, we refer to the authors of this report.

2.3. Scope and Interview Tactics

The interview guidelines included questions alluding to the company history and general organizational structure, such as number of departments, regular meetings, and business routines. We expected to evoke histories and organizational forms specific to SMEs. Drawing on this background knowledge, the ethnographer continued to ask about IT systems and relevant data, which resulted in various depictions (sometimes including sketches) of the companies' IT landscapes. In the third step, the topic of cybersecurity was introduced; informants were asked about their own security practices and how they coordinated with others on the topic.

The interview guidelines prompted specific examples and concrete descriptions of recent cases and processes. The ethnographer aimed for descriptions of how certain security fea-

tures were introduced or what concrete actions were taken rather than the perceptions and opinions of the informants. This allowed us to inquire into the practicalities surrounding cybersecurity rather than convictions or beliefs. It was possible through this method to capture various descriptions of practices, even when participant observation of those practices was limited because of the short-term visits.

Furthermore, asking for specific occurrences and practicalities required the participants to portray their daily actions and competent handling, something they were comfortable reporting on, whereas asking outright for cybersecurity might have intimidated them. Asking about their companies and positions helped in recognizing and valuing the informant's experiences and expertise, making it more likely for them to reveal the (perceived) shortcomings in their cybersecurity competence.

The interviews ended with the ethnographer offering informants the opportunity to ask questions, hence creating a moment of reverse interrogation. Five informants asked if the ethnographer was satisfied with their answers. This is a surprising but not uncommon response by study participants expressing the unequal distribution of authority and power in research situations. Another reading of this is that the participants expected the ethnographer to cast judgment over their cybersecurity measures. A few informants actively invited this judgment by requesting the ethnographer's evaluation of their cybersecurity situation. We reflect upon what this means for future communication strategies in chapter 5.

Before each visit, the interview guideline was revised, and additional questions were added based on the company's online research. Impressions of the homepages of companies and possible security questions were noted in the ethnographic field notes.

2.4. Analysis

Ethnographic field studies and analyses are based on a type of logic that is often summarized using the terms recursive, iterative, and abductive; essentially, the analytical themes and results are developed through a series of steps, where the researchers gradually clarify the analysis by systematically using previous rounds of data collection and analysis to generate new questions and new perspectives on the topic under study. In the present study, the iterative analysis was organized into the following steps:

1. In March 2022, project planning meetings were held between TANTlab (Laura Kocksch and Torben Elgaard Jensen) and Erhvervsstyrelsen (Eva Roland and Ellen Bech Lund). In these meetings, the participants from Erhvervsstyrelsen presented established knowledge about SMEs, drawing attention to a series of recent surveys. Through this, the research collaborators generated a shared understanding of how the new study might supplement existing knowledge. The process of organizing the 30 site visits was set into motion.

2. The ethnographer who conducted the site visits (Laura Kocksch) wrote reflexive ethnographic field notes immediately after each visit, thus generating the first attempt to identify analytical themes.

3. The two techno-anthropology student assistants who transcribed the interviews were asked to jot down their immediate thoughts on the key themes in the interviews.

4. Based on the transcriptions and field notes, the authors of the present report (Laura Kocksch and Torben Elgaard Jensen) discussed and decided upon a series of preliminary themes and key insights.

5. The preliminary analysis was discussed and further developed with a selection of colleagues at TANTlab.

6. In September 2022, a "touch base meeting" was held between the authors and their collaborators in Erhvervsstyrelsen. This led to further development of the themes and a clearer sense of how the study might contribute to current thinking about SMEs.

7. In dialogue with Erhvervsstyrelsen, the authors used selected parts of the ethnographic material to develop three dilemma games and a design challenge (how to customize cybersecurity information for different audiences).

8. In December 2022, the preliminary results, the dilemma games, and the design challenge were presented at a stakeholder workshop. The workshop, jointly organized by Erhvervsstyrelsen and TANTlab, included people from public authorities, employer organizations, trade unions, and private industry. The participants were invited to discuss how the insights from the study might improve future advice and dialogue about cybersecurity in SMEs.

9. Finally, all the materials and discussions generated in the previous steps were used as the basis for the present report. An early draft of the report was discussed with Erhvervsstyrelsen in December 2022. The process of writing the report constituted yet another occasion to analyze and reflect upon the material.

3. Local Cybersecurity Responsibility

Organizing cybersecurity responsibility in SMEs is distinctly characterized by the absence of designated cybersecurity departments or hand-picked specialists. During the visits, we asked the CEOs and employees to point us to their local *cybersecurity figures,* that is, people with whom the CEO consults or has put in charge of cybersecurity questions. In practice, those local cybersecurity advisors were scattered across the company and sometimes coexisted with formal cybersecurity organizing.

Table 3 lists the positions of the informants in the companies. Among the residual category of *other employees,* we found nondescript security advisors, such as those with whom one brainstorms with to assert if a strange-looking email could be a phishing attempt. In the following, we describe the key types of cybersecurity figures and their relations in the company that we found. The descriptions offer some ethnographic details to give the reader a nuanced impression of the figures and their circumstances.

3.1. IT Managers

Fourteen SMEs pointed us to their full-time IT managers as central figures for cybersecurity competence in the company. Although not very surprising, this indicates that cybersecurity is perceived as, first and foremost, a technical concern, making IT managers the obvious respondents.

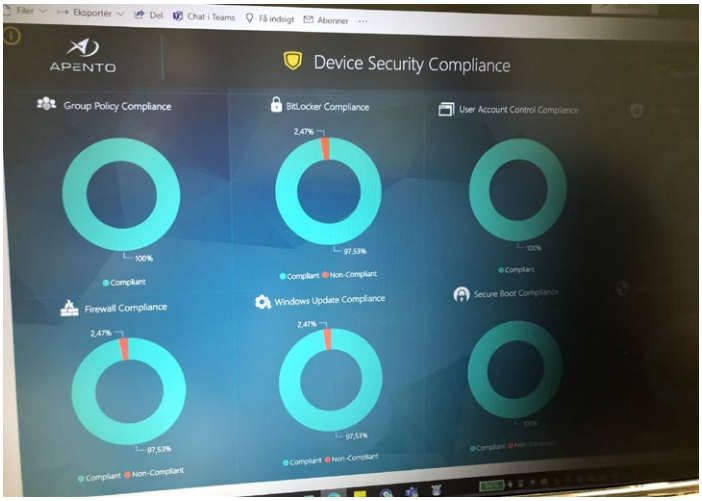
The IT managers were well-known figures in the company and respected by their colleagues. Most IT managers shared offices with administrative staff and often took on several everyday tasks:

"I'm a bit all around," Fredrik, the IT manager of a vegetable farm, explained.
Another specified, *"For the last 30 years, I have been doing, you know, economic systems, EPR, consulting, and programming. […] and of course, the computers, all IT-related: printers, copiers, AV equipment […] some economy, too. Logistics […] I have some human resource functions: work time registration, information service, information screens we have all around. And there's lots of calls for small and large problems."* (Christian, IT Manager of an Electronics Producer)

From their "allrounder" position, IT managers were knowledgeable advisors on all IT issues, while they also knew various local adaptations and were capable of making locally suitable IT recommendations. For example, Thomas, the IT manager of a small insurance brokerage, had various relations to people in the company and, therefore, was capable of explaining why a security measure he had recently introduced was not yet implemented by everyone. While we studied the monitoring tool in Image 2 on his office screen, he said:

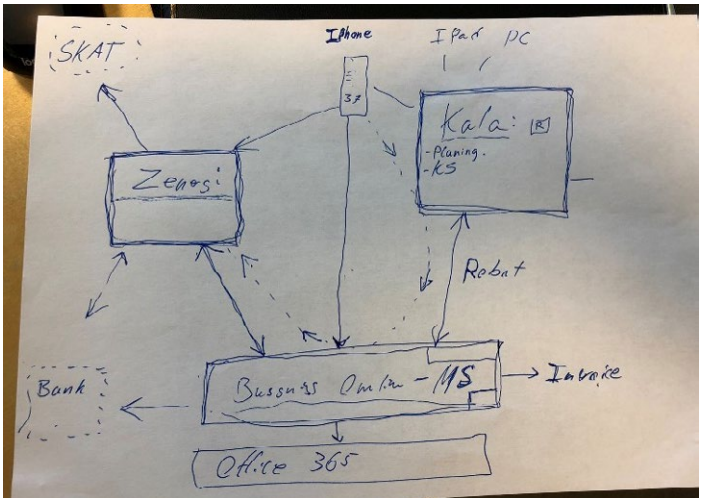
I know them [the missing 2.47% indicated by the small red section of the donut]. She was sick, and he has this one program that always acts out if we change something. We just introduced [the Bitlocker] last week. This is pretty good.

Image 2: Security Monitoring Tool



Thomas' relations were essential to organizing cybersecurity in the SME. He told us about a special program that he was aware of that was essential in one department but always required additional tweaking when he introduced company-wide security updates. He also knew that someone was out sick and missed the update day. Thomas was not only knowledgeable but also accessible: he had various phone numbers on a slip attached to his desk, his door was kept open while we talked, and we were disrupted by visitors several times. Thomas and other IT managers were pivotal to their companies because they not only knew individual IT systems by heart, but they also possessed specific knowledge of people's machines, absences, and local IT troubles.

Image 3: Schematic drawing of IT systems



A key strength of IT managers as cybersecurity figures was their well-developed knowledge of the plethora of different IT systems that could be found in almost every SME. The example of the erratic machine in Thomas' company was exemplary of the patchy IT landscapes IT managers have to wrestle with: tools and systems were locally diverse and only partially under cen-

tralized control. The schema in Image 3 illustrates the compartmentalization of systems in a subterranean construction company. Although some company-wide systems were in place, such as Microsoft Office 365, there were additional services that connected daily scheduling ("Business Operations") with invoicing ("Kala") and book-keeping ("Zenergi"). Peter, the CEO, voiced that, although they took care of the correct translations between the programs, a full integration has not taken place.

One reason for this compartmentalization was that IT suppliers rarely build tailored systems for small companies that are just among their many customers. Although we also encountered exceptions where IT vendors did provide specialized systems, one system usually did not provide every specialized function necessary for the SMEs. This kept IT solutions in SME in a permanently fragile state where the systems from different sources had to be made interoperable. As Oscar, the IT manager in Peter's company, pointed out, "We've had a lot of problems to make connections between the programs, but I think, we are almost there. It's working now … There are still some problems, but we work around that, and it works, so." This reflects what security measures can be installed in a patchy landscape, something that knowledgeable IT managers can determine when they know how the system is held together.

The IT managers in SMEs have become essential because they were capable of adopting off-the-shelf IT systems to companies' needs and integrating them with the existing systems. Several of the IT managers had previously been employed as service providers from software vendors or were self-employed before the companies hired them full time. The SMEs had tailored IT solutions that added SME-specific tools or allowed communication between different tools, such as older enterprise resource planning tools (ERPs) and newer online payment systems.

All the IT managers attested to the fact that they knew local IT solutions by heart or had tweaked software with their own coding. They had long been advocates for IT systems and were eager to maintain it to the best of their ability. This turned cybersecurity issues into a matter of personal pride, where they tried to secure existing systems or had to consider discontinuing their systems for external services (that could provide better security, they assumed).

Thus, the IT managers were critical local figures for organizing cybersecurity. They made constant judgments about what a good technical solution should be capable of in relation to its local applicability, its role in the local patchwork of systems and its security. In this way, the IT managers were managers of "good" local reasons for sometimes half-baked security measures when individual PCs were left out of the update or older software was maintained as a part of a patchy landscape of IT systems.

3.2. Accountants

The second most common local cybersecurity expert we were pointed to was accountants. This came as a surprise to us, but it speaks directly to the way SMEs grapple with cybersecurity as an everyday problem. The accountants were full-time employees who had a background in book-keeping or economics. In our sample, the accountants had been in the company for 15+ years and often acted as "right-hand" to the CEO or owner. Physically speaking, their desk was in the adjoining office with the CEO or owner, or they were located in the same office

area. Physical proximity was important, especially in production companies where administration areas and production areas were clearly separated. In three cases, the accountant and CEO were interviewed together. In one of those cases, at a logistics company in Zealand, the accountant, Sine, had prepared a neat list of IT security features for the visit and explained why the IT supplier had recommended these features. Although she was competent and well-informed, reporting on security felt unusual for her and having the list at her disposal made her as a momentary expert. The CEO kindly referred several times to her competencies, and Sine responded by shyly smiling. Regarding the security competence of accountants, we conclude from this encounter, that Sine draws on experience from case-to-case negotiations with IT suppliers and employees instead of in-depth technical knowledge. exchanges with IT suppliers and employees. For example, the accountant at a construction company near Aarhus was called by the IT provider to confirm changes in access policies or the installation of new programs to the virtual machines. She knew well what everyone needed without having much technical knowledge of the matter.

Furthermore, the accountant's knowledge drew on their economic expertise: with the accountant's command over financial expenses and procurement, they were the natural coordinators for IT purchases, but the fact that their security knowledge was not technically but business oriented was potentially crucial when addressing them as the one responsible for IT. In all the conversations with the accountants, we discovered they possessed an excellent overview of the company's IT systems and valuable data because they were directly involved in the most essential handling of payments and invoices, but also processed data from time-logging applications.

Some of the accountants' work was not confined to book-keeping tasks; instead, they were considered the social heart and soul of the company, who would hang Christmas decorations and tidy up after commoners' breakfast. Cybersecurity tasks then fell into their competencies as general caretakers of the office, who knew everyone well and could estimate the proper level of cybersecurity for them. Those accountants could make competent decisions about who would be overwhelmed with a sophisticated security mechanism and should be approached more carefully.

Accountants were worried about the cybersecurity situation of the companies and directly engaged in how cybersecurity was practiced. Their inclination was not to focus on sophisticated technical solutions but rather on socio-organizational measures such as knowing and responding to other's competencies.

3.3. Compliance Specialists

Four companies had recently hired full-time cybersecurity experts who were tasked with improving compliance with GDPR regulations and cybersecurity best practices. The compliance specialists conducted standardization procedures and conducted trainings and campaigns, such as simulated phishing. The compliance specialists had a background in communications, PR, or law but did not undergo extensive technical training or in-depth introductions to the company.

Although the compliance specialists possessed the latest cybersecurity knowledge and devel-

oped state-of-the-art campaigns, they expressed frustration about being limited to communication strategies and tools and lacked more substantial tools, such as the rights to reallocate resources or shift teams or physical arrangements.

Aleks, the compliance manager of a wastewater plant, noticed that, although he had introduced a user-friendly issue reporting system and invested in rigorous testing, he still felt disconnected from the company. As an example, he recollected a recent phishing campaign he had conducted in which one employee had exposed his artificial phishing emails on a common notice board. He had to ask that employee to take down his notice and remembered his frustration to explain why these tests needed to be done without disclosure. Although he found himself in a position of being fully supported by the board of directors and getting considerable visibility from local news, employees reacted defiantly to his attempts.

An account of this was a blue-collar worker who greeted him with a hint of sarcasm when he showed us around in the company. Aleks later reflected that the worker was among those that he had publicly singled out as having fallen for the phishing campaign. Now, Aleks had a strategy to improve his rapport with the workers: he organized a weekly consulting hour in the canteen during lunch times where everyone was encouraged to reach out to him. Aleks perceived his role as taking cybersecurity training elsewhere one step further by "following up" and being "available for questions."

Quite in opposition to what we heard from the IT managers and accountants who saw cybersecurity as a collective achievement or were engaged with "good" organizational and historical reasons for "bad" cybersecurity, compliance specialists evoked people's personality traits and socio-psychological explanations for lacking compliance, for example, "Women above 50 who have been working the same job for the last 20 years" or "People who are insecure about IT." During one of his trainings, Aleks even discovered that a few employees were functionally illiterate (or dyslexic) and could not understand training language at all. This was an additional hurdle to achieving cybersecurity compliance that Aleks was currently wrestling with.

Although employing a full-time cybersecurity compliance specialist is an effective organizational strategy in SMEs, they often find themselves in delicate debates of practical competencies and practicability. Although the compliance specialists saw their most impact in developing sophisticated communication campaigns because "the weak link is always the employee" (Aleks), they also attested to their difficult role being "the only one responsible" for cybersecurity and that they saw their work as a "fight against windmills" (Aleks). In contrast to the cybersecurity figures we identified above; compliance specialists were not yet seen as trusted advisors whom one consulted with in everyday practice.

3.4. IT Suppliers

Three companies suggested that we should contact their IT suppliers with inquiries about cybersecurity. The low number surprised us. We found that, although all our SMEs had outsourced parts of their IT landscape or at least carried service agreements with IT vendors, most still responded to our request to interview someone who was responsible for cybersecurity within the company. Although this can easily be an artifact of our recruitment process, we also conclude that SMEs had local (internal) ways of organizing cybersecurity.

The relationship between SMEs and IT suppliers was characterized by their patchy IT landscape with various partially connected systems and little to no customized solutions. This had two effects: First, it reiterated the need for local IT managers to communicate customization requirements. Second, SMEs had a high turnaround of IT suppliers. Two reported that they were currently in the process of changing IT suppliers. Their main reasons were better offers or because they felt that their company size had outgrown their IT supplier's service. Two informants articulated that it needed some calibration between the IT supplier and the SME; if the supplier was too big, an SME like theirs with around 100 employees would disappear from their radar and would never be granted any customization requests. If the supplier was too small, however, it may not be capable of providing the services needed, even for a top-priority customer.

Half of the SMEs reported that they factored in a sound personal rapport with the IT supplier in their purchasing decisions. Although some saw their IT suppliers as long-term friends or as trusted neighbors (in two cases, we were told the IT supplier sits "just next door"), others had a very contentious relationship with them. Two companies felt that their IT supplier had not delivered what they were promised, and one company was sued by the IT supplier over a dispute on contractual obligations.

Cybersecurity figures

Responsibility for cybersecurity in SMEs is characterized by vagueness and fuzziness in stark contrast to companies where formal organizational procedures are in place. We identified local cybersecurity figures that take on distributed and various tasks of advice giving, making local technical adaptations or rolling out updates. IT managers and accountants operate with intricate knowledge of the IT system, maintain good relations with the CEO and employees, or oversee spending and income. On the contrary, both external IT suppliers and compliance specialists were in a difficult position as local cybersecurity figures because they lacked an understanding of and ability to anchor cybersecurity in the routine practices of the organization. This speaks to a need to not only train IT managers and accountants in cybersecurity, but possibly also train IT suppliers and compliance specialists in ways to understand the companies better.

4. Local Cybersecurity Knowledge

SMEs are rarely subject to formal security auditing that would be part of a risk assessment or licensing process. Consequently, knowledge about the status of cybersecurity in SMEs drew on informal sources and materials.

Twelve companies arranged regular cybersecurity awareness trainings. When consulting with those who led training courses in the companies, it was reported that, although people participated in online courses, not many voiced questions and training sessions were often perceived as boring or a "necessary evil." Being interested in the way SMEs mobilized local knowledge for cybersecurity, we became attentive to how SMEs portrayed cybersecurity in their everyday work. For example, we discovered that collective events such as regular breakfast or lunch breaks were important avenues through which cybersecurity information was shared. This was true as well for short moments of inquiry with colleagues: "Did you get this strange mail, too?" one informant played back a recent situation where she assured a suspected phishing attempt with her colleague. "In the office, we talk about it," a CEO pointed out, "but not so much in the factory," she admitted. However, as the statement "Nothing is written down [for cybersecurity]" indicates, the SMEs relied on local moments and informal rules where and when to converse about cybersecurity. Although some companies did possess formal documentation for cybersecurity, such as paragraphs in employee handbooks on how to handle company laptops, what public Wi-Fi to avoid, and how to handle passwords, all companies attested to informal records and collective anecdotes about cybersecurity.

We list six distinct forms of everyday knowledge that the SMEs used to assess their cybersecurity.

4.1. Anecdotal knowledge

Providing anecdotes was a widely used method to encapsulate and convey past incidences or hearsay from other companies, friends, or family. These stories were repeatedly told by informants in the same company, which made them imperative to shaping collective cybersecurity understanding. Examples included the following:

A company here in [a town north of Aalborg] was hacked, right over there," he pointed with his finger toward the window, "they lost a lot of money. That made us aware."

Others recollected, "I can tell you a funny story that happened to us. ..." This was followed by the explanation of a mistake made by the bank that had turned a private into a business account. Although some of these anecdotes were only remotely related to cybersecurity, they contributed to how companies sensed their risks.

4.2. Firsthand experiential knowledge

In some circumstances, the informants had firsthand experiences that they interpreted as evidence that a particular system was secure (or not).

We see that it is secure [...] It was not possible for me to put a new program in and download so-

mething to the platform. […] [Nobody] can get a fun idea and do something. (Rikke, accountant of a construction company near Aarhus)

Others took their daily struggles with passwords as an indicator that guessing passwords was not easy. In addition, when first asking about cybersecurity, most companies associated the term with external attacks, while they did not have much to say about password rules and backups. When prompted to talk about internal access control, however, a plethora of practices and tactics were revealed. The informants were competent in telling who had access to what and what they had experienced firsthand to not have access to, for example, payrolls. We read this to mean that access control is often not included in the imagination of cybersecurity, even though the informants had good experiences with it.

4.3. Knowledge derived from a sense of normal temporal flows

When the informants talked about more or less secure systems or arrangements, they often used their sense of the normal flow of events in the company as a source of reasoning.

In one case, the CEO of a logistics company was well aware that a particular system was, in principle, quite insecure: the company had an office building where a large number of chauffeurs were dropping by during the day to use PC stations to print documentation. The PCs were unprotected by passwords. However, the CEO was also aware that there would normally always be people in the office building. Therefore, he reasoned that—in light of the normal flow of events—the system was secure enough or less of a hassle than managing individual passwords for all chauffeurs. As he put it, "We can't have it that every chauffeur has their own log in and password, because that would be a mess."

In several other cases, the informants made connections between cybersecurity and the seasons. Generally, the companies reported having received more spear-phishing and CEO-fraud emails during the summer months when employees were on holiday and consulting with a desk neighbor was not possible. Several companies scheduled information campaigns on phishing briefly before summer break.

To others, the change of seasons also meant a change of regular work tasks; construction companies shifted their work from outdoor construction to cleaning up storage spaces, snowplowing, or delivering Christmas trees. During the off-season, the numbers of employees plummeted, for example, in vegetable cultivation and packing (because fewer harvesters, drivers, and farmers are needed). The winter months served as an occasion to tidy up storage spaces and sift through databases to delete obsolete or potential GDPR-related items.

The latter was not confined to "off-season" times for other companies. A head-hunting consultancy maintained a regular schedule with a designated calendar entry to remind Ida, a higher manager, to delete client data from their centralized database. She described the process as highly manual, setting a search frame (up to one year, according to the consent agreement), reading through names, activating fields, and deleting. This tedious labor was necessary because there may be some cases that would require additional research and could result in keeping certain information when they were not GDPR relevant, as Ida described in her actions.

Making momentary exceptions could also mean "breaking GDPR a bit" as the GDPR officer of a printing company admitted when explaining his case-to-case deletion practice. A tool helped him identify data, but his sound knowledge of local tasks allowed him to make reasonable choices about what data may be kept a few more months to ensure processes can be maintained. He never used the "delete all button," he assured us.

4.4. Knowledge about cybersecurity based on projections of the physical or organizational environment

In contemporary discussions about cybersecurity, it is common to use terms and phenomena from the physical world to speak of IT security. Metaphors drawn from warfare ("cyberattack"), crime ("break-in"), biology ("virus"), inferior food quality ("spam"), or construction ("firewall") are thus widely used to explain and make sense of cybersecurity. In addition to these common tropes, we observed that SMEs often used features of their immediate physical or organizational environment as a resource for thinking about cybersecurity.

In one case, a company carefully maintained a boundary between a building with special hygiene requirements where food was packaged and a regular office building without special restrictions. Following the physical layout of the company, people in the company tended to think of cybersecurity as a matter of maintaining clearly separated boundaries between systems.

In another case—a law firm—the workplace was structured around a shared file system, which had been physical in the past but was now digitized. The lawyers were keenly aware that files should, under no circumstance, be shared with someone outside the firm. However, at the same time, the lawyers considered it a matter of professional ethos and courtesy that lawyers would never think of prying into other lawyers' physical offices and drawers. Therefore, it was considered safe to share offices and information systems. Following these professional experiences, the lawyers tended to think of risks as always originating from the outside, while it would be considered unnecessary or even a potential collegial insult to sequester information within the company.

The projection of the physical features of the company onto the reasoning about cybersecurity—or vice versa—was also evident in several companies where administration areas were perceived as trusted while production areas were perceived as more insecure. For example, at an industrial painting shop, the office area was confined to a few desks in the basement of a former residential house, while the production was in the newly built industrial hall next door. A kitchen area connected the two. Only designated personnel performed transition tasks between the administration area and the shop floor, such as carrying paper orders to the production and writing them on a whiteboard. The administration staff had acquired confidence in each other's secrecy and trustworthiness. The computers were updated and under collective surveillance. The production area, however, had other rules: the production workers were given limited access to the databases, most computers were outdated because they had to transfer data to older painting machines, and the computers stayed disconnected from the internet. As long as administration and production were disconnected—thus the shop floor disconnected from the internet—the risk was considered tolerable.

As indicated by these examples, SMEs' knowledge of cybersecurity had a *spatial-physical dimension* worth taking into account. Features of the environment were drawn upon when the informants reasoned about what was secure or not.

4.5. Knowledge based on associations with geographical Locality

As another physical association, the informants referred to their geographical location as an indicator for cybersecurity. Pelle, the IT manager of a family-owned hotel in Northern Zealand, explained, "A hotel in Copenhagen or Aarhus might get attacked, but not us out here."

Our view out the window was scenic () and the fieldnotes resonated with this sense of an idyllic countryside: during a visit to a town in Djursland, the fieldnotes suggested, *"The world seems still in order our here."* This expression was motivated by the sighting of a poster announcing *"Landluft"* (in German) — *"country air,"* both a praise to the air quality outside the city and a slogan attesting to peacefulness and conviviality typical of the countryside. Although we shared the sense of harmony and serenity in the countryside, it did not resonate with the locations of the companies that reported having been the victims of a successful cyberattack. We find it hard to conclude that cyberattacks are generally geographically distributed and suggest further research.

What was important to our informants, however, was that the Danish work culture of flat hierarchies and few formal rules was a contributing factor to how well they resisted cybersecurity attacks. Informal organizing was seen as an effective measure against cyberattacks because "We talk about everything" and "We are not fooled here."

Image 4: Scenic view

Collective security strategies, such as informing each other on phishing emails or reassuring banking transfers, worked well precisely because colleagues were together in one small geographical location. As a result, this protection by proximity was disrupted when they were not in the same place as usual:

Image 5: Companies that were attacked

[It] is not easy when you get a text message from your boss, who says, "Oh, I'm in a meeting, will you please go and buy this for me?" And Jonas is normally in a place in the country, but that day, he was in the middle of the city. So he was in a place where it was natural [...] to go down there and buy this. (Rikke, explaining the circumstances of a fraud attack)

Not all agreed that the Danish work culture would account for more security perse: Different regions in Denmark were assigned as having different work cultures, so some were more susceptible to cyberattacks than others: "People work harder out here," the compliance specialist of a utilities company in Northern Zealand asserted while we walked through a fierce wind looking at different pools of water. We had led the conversation by talking about all the different regions this study had made us visit, and he indicated his comparison was mainly between people in Copenhagen (like us) and the rest. He insinuated that Copenhageners may be at risk because they lack conscientiousness.

4.6. Cybersecurity knowledge woven into the Narrative of the company

The final register of cybersecurity was to make it part of stories about the past or future of the company. This was why Palle, the head of development at a software company, reflected on introducing stricter access permissions for his developers: So far, everyone had the same permissions to make changes in the software code (after a quality control, i.e., code review). However, now, as the company was expanding, they may grow out of this trust-based system.

For others, their history was part of possessing what we term *legacy security.* An industrial printing company in Djursland had a safe room and locked basement to store SIM cards they glued to printed letters. When the SIM cards were first shipped, they were often prepaid, making them very valuable and, thus, in need of high-protection mechanisms. However, today, SIM cards are less often prepaid, "and generally, less are shipped," the manager explained to us. The company still maintained the safe room and still had employees trained in handling the SIM cards with great caution. "But, [they] technically do not need it anymore." Nevertheless, they hoped that security could make a sales argument for future customers.

The construction company near Aarhus reported having migrated some security procedures from their former employer. The company emerged out of a Swedish company's cutback of production in Denmark, and most employees had worked together in the Swedish company. The security protocols perdured during the transition, for example, a four-eye review of banking transfers. Taking into account company histories and current transitions was essential to the SMEs when illustrating what security tactics they had or planned to pursue in the future. Cybersecurity was not a *new* topic to them but rather something they related closely to the history and narrative of their company.

Cybersecurity knowledge in SME's

We have identified six types of everyday knowledge relevant to cybersecurity in SMEs. Instead of seeing the competencies of SMEs as insufficient or in need of correction, the types of cybersecurity knowledge displayed here suggest unexplored repertoires that can be utilized for dialogue and interventions in the future.

5. Local Cybersecurity Practices

The SMEs showed distinct organizational measures, such as unofficial figures and local forms of knowledge about cybersecurity. During the visits, we also observed the specific everyday practices SMEs had created to handle cybersecurity issues. Many of the SMEs in our sampling had made competent decisions about what security mechanisms (not) to deploy, how and when. Instead of rolling out standard cybersecurity mechanisms, the SMEs grappled with the limited resources and materials at hand, facing intricate dilemmas, which resulted in improvised and apparently clumsy solutions.

5.1. Handling Practical Dilemmas

In the following, we describe three hybrid dilemmas derived from three distinct cases. We chose these three cases because they depict the various practical negotiations that the SMEs had to engage in. All of them have one thing in common: simply rolling out "better" security would significantly impair "good"—efficient, necessary, or delicate—local practices. Although the dilemmas can be read as barriers to "good" security, we try to also understand them as local compromise and competent tinkering in real-world situations. In practice, the SMEs did not strive toward definite solutions but attempted to make things slightly better or worse in often improvised arrangements.

5.1.1. ECONOMIC-TECHNOLOGICAL DILEMMA

In an ideal scenario, all the SMEs would continually update their technological systems, including the cybersecurity measures that protect them. In reality, the SMEs did not have the resources to keep everything updated so had to make priorities. Furthermore, as time goes by and specific technologies become "legacy technologies," it may become increasingly expensive to turn away from legacy technologies, especially when such technologies have closely fitted to market demands and the competencies of the employees. Thus, companies may find themselves trapped in technological path dependencies that become problematic from a cybersecurity perspective.

We encountered one company that found itself in such an economic-technological dilemma, and it is instructive to see how the company handled the challenges.

The SME had an old printer that was purpose-built for printing the letters onto which sim cards are attached before being sent by mail. At the time of the visit, the SME was responsible for sending out more than half of all Danish SIM cards for a major Danish telecommunications company, which made up a significant revenue stream for the SME. However, the cybersecurity of the printer was a growing concern for the company. When the truck-sized printer was installed, it was hooked up to a Windows NT machine that would receive its input data from a floppy disk sent by the Telecom. In 2003, the Telecom began sending the data through a file server; therefore, the SME had to invent a kind of bridge: they installed an XP machine that could receive data from the fileserver and connected it to the NT machine.

This setup is still in operation. The problem, however, is that it is now impossible to get security updates for the XP machine from 2003. The situation is even more complex because

the Windows NT machine still writes floppy disks (see Image 6) for a neighboring printer that is fully disconnected from the internet.

Image 6: Photo of essential storage technology

The company has handled this dilemma with an insulation strategy; they have made sure that the XP machine is not online and that it is only used for the purpose of receiving data from the Telecom, and they have, so far, managed to avoid cybersecurity threats to the printer. A few years back, there was a major virus attack on the company. At the time, they were pleased to discover that the XP machine had not been infected. For the time being, the SME has managed to attain a reasonable degree of security while avoiding the insurmountable cost of replacing a key piece of legacy technology.

5.1.2. PROCESS-TEMPORAL DILEMMA

The security practices that SME employees carry out must be integrated into the daily workflow and practical circumstances of work. One very common challenge is the type of workflow where working at a computer only happens intermittently. In these workflows, the employees leave and return to the computer over and over again during the day. The computer is, therefore, often left out of sight, and when returning to the computer, standard protocols demand that the employees have to log in again. Therefore, SMEs must find ways to balance the access security issue with the need to move quickly and efficiently between the different moments in a workflow.

One example of handling this dilemma was described to us by a SME employee who repaired heavy machinery, both in a garage and by driving out to customers. He worked with a laptop in the administration office, which he shared with various colleagues. He also had a smart-

phone app to document his work outside the company. The employee and his colleagues have agreed to use each other's accounts because, otherwise, they would have to log in and out repeatedly during the day to track finished tasks and work hours per order. This solution solved two issues at once: First, when work tasks were completed by two or more employees, they could easily track the same hours and reference the same tasks for everyone. Second, as the employee reported, his hands would often be greasy from working with cogs and chains or cold and stiff from being outside a lot.

What is noteworthy about the practical arrangement of this SME is the pragmatic balancing of risk and efficiency. The company decided to run the risk of using the same account and password because there will be a significant benefit to the efficiency of the workflow and the daily operations of the company. At the same time, however, the risk of sharing an account was mitigated by some of the practical circumstances of the company: there were always people around the administration office, and when employees worked outside the garage, they used an app on a phone.

5.1.3. SOCIAL-ORGANIZATIONAL DILEMMA

The general advice to SMEs is to map out their most valuable assets to realistically assess what kinds of protection mechanisms are required. This approach is premised on the idea that certain things rather than others are of high value and that this high value should be explicitly recognized and acted upon. However, such an approach appeared to run counter to those company cultures that saw themselves as "easy going," equality oriented, and reluctant to single out specific parts of the business operation as more valuable than others. An observation we repeatedly made was that the SMEs did not speak of their IT systems as particularly valuable or worth protecting. Some were confused why we would even include them in our study because they felt there was nothing interesting to see at their companies when it came to cybersecurity.

For some, IT was not imperative to pursuing their business; as the IT manager of a vegetable farm contended when explaining that IT systems provide monitoring and task management, "Everything goes on without IT." Vegetables still grow and can be packaged at need.

For others, assessing IT assets was not only irrelevant to their core business, but they were reluctant to "brag" (IT manager at a law firm) about their success. Many informants would much rather refer to personal pride and community vigor than portraying their companies as extraordinarily prosperous or competitive. This "Jantelov[2]" attitude worked against the idea of identifying distinctive assets or producing oneself as being of significance to a hacker . Being driven by an attempt to be "like others" (IT manager of a financial institute), the SMEs downplayed their uniqueness and exceptionality. We experienced this as both an excuse to not purchase cybersecurity controls and also as adhering to a commitment to the common good over personal aspirations.

Note 2: Jantelov, or the "Law of Jante," refers to a disdainful attitude to one's achievements assigned to people in Northern Europe: https://nordics.info/show/artikel/jantelov

This was paired with a commitment to flat hierarchies and doing cybersecurity "the Danish way" (CEO at a construction company), which included that employees would openly communicate about problems that occurred in a process. "My employees tell me early on," the CEO contended, suggesting this would be a special trait of Danish companies. In turn, he was afraid that more formal rules might tamper with the bond he had created with his employees because they might fear being judged by him if they disregarded something that was written down. Urging SMEs to be more assertive about their qualities by listing and publicly stating their assets conflicted with some of their essential organizational commitments, such as modest self-presentation and maintaining flat hierarchies.

The SMEs encountered this dilemma by turning their regular flat hierarchies into cybersecurity protection mechanisms, for example, by forming strong trusting relationships that allowed for effective defenses against external cyberattacks.

The dilemma in this section between singling out unique assets and sharing responsibility and modesty has pointed to several local good reasons for nonstandard cybersecurity. The SMEs negotiated what "good" cybersecurity looks like by inventing solutions that were relatable to their specific situation and company cultures.

5.2. Flexible handling of rules

It is often assumed that the existence of company rules for cybersecurity will somehow ensure that the practice will be conducted in a particular way. At the same time, however, it is common knowledge that rules are always interpreted and sometimes bent. In the case of the studied SMEs, there tended to be fewer rules compared with larger and more hierarchical organizations. In the following, through a couple of examples, we portray how the SMEs incorporated rules into their everyday practices while leaving open a significant space for exceptions and adjustment of their courses of action.

The following observation came from a young technician who was setting up the automatic detection of unusual data traffic:

"This is unusual traffic to a certain IP address," the technician told us while pointing his cursor at an orange-red bar on his screen. Someone in the company was uploading or downloading unusual amounts of data to an unknown or suspicious URLs, but he was not alarmed. "We look at it, but these few I had last week already." If they come up regularly, he would create a rule for the monitoring system to disregard them as "regular irregular behavior," he said, smirking while acknowledging the oxymoron. He showed me another tool that depicted where the data traffic were going. "This is an image-exchange tool. They [the financial brokers] use it to get photos for their reports. Nothing to worry about." Although this entry was harmless, he has not created a rule yet to disregard it entirely, and I wanted to know why. "Sometimes, we let them in because they might turn dangerous eventually, and we'd rather keep an eye on them."

The episode above portrays the work of a security operator at a financial institute. The company had very strong rules for cybersecurity monitoring, and the young technician was one of two employees hired to oversee full-time traffic and firewall responses.

On a daily basis, the technicians had to decide if a new type of data traffic was "regular irregular" or "irregular irregular," which would require him to flag it and could result in the URL being blocked. However, there was a third option, as he explained: keeping the warning on his screen and reviewing it again later. The technician's work reiterates the importance of understanding local practice (here, how brokers prepare a financial report) to perform relevant security decisions, but more than this, it also showed the need for competent weighing and tinkering with what was deemed regular and irregular. Cybersecurity rules in SMEs are not simply created and adhered to or subverted, but they also rely on grappling with ambiguity, being temporarily bent, or subjected to re-negotiation. The technician kept the rule unset because he wanted to be able to react if the source of data changed or if even more data were suddenly transferred. He stayed alert by keeping the rule unsettled.

Image 7: Instruction signs

Instead of seeing this as "bad" implementation of a security rule because it did not formally prohibit or allow the traffic to the side, his actions speak to how cybersecurity rules can be willingly kept ambiguous. Cybersecurity oscillates in the companies: within practices, it can be adjusted, partially avoided, but not decommissioned entirely.

Another example of the flexible handling of rules was encountered during a visit to the packing area of an online fashion retailer. The IT manager raised our attention to two slips of paper taped to the wall next to a PC station used to print labels for the packages (see Image 7): "This is some IT security right here! [he points] We don't want the other packers except for Susan to be in the webshipper program. Hence, it shouldn't be left open like this." He used his hand to operate the computer mouse and showed the program in question being left open—against instructions on the sign. His attempted to underscore the essential instructions with a highlighter on the paper that have so far been resisted. Our conversation did not stay un-

noticed, and he reassured a nearby packer that Susan had been here just a moment ago. The rules of the paper were not entirely forgone, though: Spotify plays in the background, and the second rule was breached that required only a few homepages be opened on this terminal. "Spotify is ok," Jesper smirked. The rules of the paper were momentarily circumvented by this exception.

As evidenced by our two examples and by similar observations in other companies, rules can be handled flexibly. Sometimes, the rules are temporarily subverted, despite the fact that CEOs and cybersecurity figures were fully aware of it. Instead of concluding a lack of perseverance of rule and rule-makers, we interpret this as an indication that rules must be put into practice, although this often means adapting them momentarily. Jesper attested to the unease that resulted from this breach of his rules: "Don't judge!" he pleaded to us.

Everyday cybersecurity practices

In everyday practices, cybersecurity is constantly reshifted and rearticulated depending on intricate pragmatic realities. By pointing to three different types of dilemmas, we have emphasized that a simple addition of competencies or resources does not easily solve a SME's complex situations. Rather, we propose understanding cybersecurity work as a constant process of adjusting, calibrating, and reassuring existing processes, practices, and flows. This section has highlighted, more than the previous ones that something was at stake and at conflict in the companies when urging them to introduce more security. A more profound understanding of " good" local reasons for " bad" cybersecurity can serve as significant resource for communication and dialogue.

6. Stakeholder Workshop

As we mentioned in the "Analysis" section, one of the final activities in the project was to present the results of the study to a group of stakeholders and facilitate their engagement with the material. Below, we describe the facilitation methods and devices we used at the workshop, summarizing the stakeholders' conclusions about possible ways to improve the future dialogue about cybersecurity.

The stakeholder workshop was a full-day event held on Aalborg University's Copenhagen campus on December 20, 2022. The workshop was jointly organized by Erhvervsstyrelsen and TANTlab. The 20 participants represented public authorities, employer organizations, trade unions, private enterprises, and Aalborg University.

The workshop began with a presentation of the results of the ethnographic study and a Q&A session, in which the participants had ample opportunity to elicit additional information from the ethnographer and comment on specific examples. Following this, the stakeholders were invited to play two dilemma games and engage with a design challenge.

6.1. Dilemma games

Based on the ethnographic material, we developed two specific dilemmas in which the SMEs might find themselves. The first dilemma described a situation in which a newly employed compliance manager was running into trouble with people in the company who saw his efforts and campaigns as overzealous and obstructive to the company's operation. The second dilemma described a situation in which a company found itself to be dependent on a legacy technology that became increasingly difficult to secure.

The workshop participants were given vivid one-page descriptions of each dilemma and were divided into groups. Each group was placed at a table with a game board and four stacks of "resource cards"' that the participants might incorporate into their solution of the dilemma. The types of resources were color-coded on playing cards, suggesting *technical changes* (e.g., update firewall), *management & reorganization* (e.g., allocate more resources to X), *involvement of people* (e.g., Internal IT), or *knowledge gathering* (e.g., arrange a coffee meeting with Y). The participants were also given empty cards of each color and generic cards to add resources that they found more appropriate.

The participants played each game for 45 minutes before presenting their suggested solution to the other teams (Image 8 shows the game play). Notably, no team considered there to be an easy solution to any of the two dilemmas, confirming that cybersecurity practices in SMEs are convoluted. All teams were also inclined to create additional resources, such as conducting a risk assessment (a knowledge gathering resource), involving a consultant (a people resource), or enforcing a new password rule (a technical change).

The first dilemma about the overeager security compliance manager caused one team to carefully balance organizational measures with technological measures; for example, a new password rule can only be implemented if the compliance manager had coffee with the HR

department first. One participant acknowledged that his (technical) competence alone was insufficient in this case.

The second dilemma about a piece of legacy technology was tackled by one group by doing nothing—a "solution" that surprised us. The team reasoned that the technology would soon lose its relevance to the company anyway, and thus, investing resources may not be advisable.

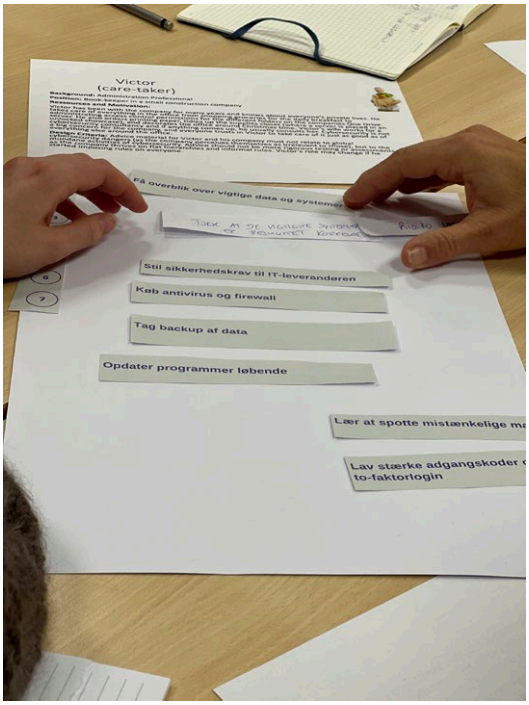
The dilemma games fulfilled their purpose of facilitating a discussion of the ethnographic material during the short-dated workshop and engendering an insider's perspective on the SMEs' real-world challenges. Playing the games urged participants to explore different means of tackling cybersecurity issues and debating their appropriateness. The participants contributed their own anecdotes to this process, making decisions about what to prioritize and what consequences fictional actions could have.

Image 8: Board game tables

6.2. Design challenge

The design challenge was also organized as a group exercise. Drawing on our ethnographic encounters with different people or "figures" in the SMEs, we developed a series of idealized personas. We then asked the workshop participants to choose one persona and image that they were to tailor-make cybersecurity advice to that persona. Specifically, we asked the participants to look at the Sikkerdigital.dk homepage and discuss how the advice offered might be redesigned to suit the needs of a particular persona. Image 9 shows the participants finding a new way of ordering and displaying the seven pieces of advice given on Sikkerdigital.dk.

Image 9: Design challenge



6.3. Stakeholders' ideas for improved dialogues on cybersecurity

The workshop ended with a joint discussion about possible ways to facilitate and improve dialogue with SMEs about cybersecurity issues. The stakeholders identified the following opportunities:

Engaging formats: The stakeholders suggested that the game formats deployed at the workshop be further developed and used to drive and facilitate dialogue with SMEs. These formats included the following:

- Dilemma games based on ethnographic observations of actual dilemmas and local circumstances.
- Design challenges based on realistic personas.

New collaborators: The workshop participants identified key actors in the SMEs who have not yet been the center of attention for cybersecurity advice and dialogue:

- Accountants who assume the role of cybersecurity are responsible in many smaller firms.
- Board members who were increasingly concerned with cybersecurity as a part of SME's risk management.

New approach and understanding: The stakeholders pointed to a general need to customize communication and take the wide diversity of SMEs into account.

7. Implications for a Cyber-security Dialogue in the Future

In this section, we deduce some concrete implications for a future dialogue with SMEs. This does not include technical specificities or answers what the best companies in our study were but instead adopts a more general perspective. That is, how can the results of our study be utilized to create a meaningful communication strategy with SMEs in the future.

Involving local cybersecurity figures in cybersecurity campaigns

The informal way of appointing responsibility for cybersecurity in SMEs has traditionally been seen as a disadvantage. Our study has suggested a different take: cybersecurity responsibility lies in the hands of local experts—those who already possess extraordinary knowledge of the companies and are capable of making competent decisions about the local applicability of cybersecurity measures. We see this *fuzziness* as a prerequisite for successful cybersecurity campaigns in SMEs. When cybersecurity competence became formalized (e.g., at the hands of compliance specialists), this caused local defiance and skepticism.

For a future cybersecurity dialogue, this entails involving local experts in defining "good" local cybersecurity measures. CEOs and employees had no trouble pointing us to locally relevant cybersecurity figures, and we suggest that this situated knowledge is valuable to future dialogues with SMEs.

New vocabulary is needed to relate to everyday cybersecurity knowledge

To SMEs, their companies resembled a local community; thus, cybersecurity was perceived as a collective task entangled with the company location and history. So far, most cybersecurity advice was individualized and targeted subjective knowledge and skills rather than collective practice and processes.

The vocabulary that derived from risk assessment and thread analysis failed to consider the concrete practical dilemmas SMEs encountered. The SMEs portrayed their cybersecurity actions not as responding to urgency and alarm, but as a here-and-now practicality they already grappled with every day. The SMEs were not assumed to be secure to begin with. Furthermore, we discovered several ways in which the SMEs' physical arrangements affected what was considered secure (or not), for example, by creating trusted areas through physical barriers or serving as blueprint for how SMEs differentiate their IT.

Despite the initial skepticism toward the ethnographer and their perceived evaluation by her, many informants expressed gratitude and feeling understood during and in the aftermath of the visits. Some informants noted that nobody had asked about cybersecurity "in that way," suggesting that, if advice becomes more asking than telling, it might meet fertile ground. Instead of perceiving cybersecurity awareness as a state of mind, and something who people "have or not" (industrial production CEO), we suggest a dialogue that aims at how companies grapple with cybersecurity as a practical achievement, or put differently, something that is done in action.

In facilitating future cybersecurity dialogue, we recommend the following:

- Evoking collective and narrative knowledge of cybersecurity.
- Shifting attention to SMEs' physical circumstances.
- Supporting SMEs' ongoing material struggles rather than attempting to shock them into action while assuming that they are so far naïve to the issue.

Understand "good" practical reasons for "bad" cybersecurity

We emphasize the real-world difficulties of SMEs that emerge from economic-technological, process-temporal, and socio-organizational dilemmas. This implies that, even if the SMEs had unlimited resources and full compliance by their employees, they would still be caught up in specific practical challenges. Understanding the negotiation of cybersecurity rules allowed us to see SMEs' cybersecurity efforts as ongoing and contentious rather than absolute fixes.

For the future cybersecurity dialogue, this suggests equipping SMEs with the necessary tools to achieve locally good cybersecurity, train local cybersecurity figures capable of making competent, albeit uneasy, local decisions, and sustain security-relevant local arrangements. Instead of introducing cybersecurity as an entirely new requirement, we found solid organizational measures, knowledge, and practices to build on in SMEs. A substantial part of this was mobilizing existing efforts, even if they were improvised and inconclusive. However, general advice will always have limited reach, which is why we suggest different strategies for categorizing SMEs in the following. This can serve as a basis for targeted communication strategies.

SMEs are heterogeneous; hence, communication tactics should be customized

SMEs represent a diverse set of companies. Communication attempts ought to respond to this heterogeneity. Thus far, communication efforts have targeted SMEs by discerning their size and business segment. However, in our sampling, size has served as an unreliable indicator: bigger companies did not automatically have "better" security, though security may be more formalized at the hands of single cybersecurity figures. In addition, although companies were small in their number of employees, they may be world leading or "critical." For example, one of the companies of our sampling packed and shipped 50% of all SIM cards in Denmark, another one was internationally recognized for special pumps, and a third one produced an essential item to a world-renown Danish brand.

Targeting advice at companies of certain *business segments* has proved a successful tactic. Certain business segments in our sampling were under certification pressure because of their clients or line of business (e.g., software development in the health sector, vegetable packing, home care services, etc.). Others translated professional ethics into cybersecurity, such as lawyers and artists who were committed to intellectual property rights. We have supplemented the findings of previous studies aiming at the segmentation of SMEs (Epinion, April 2022) by explaining some of the findings in more detail. The proficient cybersecurity of IT-savvy companies, for example, can be explained by the contribution of long-term IT experts involved in both the IT system and local idiosyncrasies.

In this report, we have alluded to another way of differentiating between the SMEs without explicating it: *location*. We have presented a geographic map of the distribution of companies

in Figure 1 and referred to the location of companies when citing informants or drawing on field notes. We have done so to satisfy calls for specificity in ethnography, but what if we took it as a classifier to make a statement about cybersecurity in SMEs? This suggests that there could be different practices in Denmark than in any other country or that SMEs in Aarhus do things fundamentally different from SMEs in Copenhagen or SMEs in Zealand are different from Jutland.

Another classification emerged from our material: *history*. We could start by classifying and targeting communication material to SMEs according to their history; for example, have they grown out of other companies, or are they newly found? Are they a long family tradition with great pride or a company thriving in anonymity? What are the types of events that SMEs have experienced collectively? This classifier makes prevalent those issues of legacy technology but also treasures collective learning and overcoming moments of precarity. It may allow us to involve considerations of what is worth preserving and what is not. In addition, with the questions of legacy technology comes the questions of the "legacy competencies" of those who are experts of a technological system that may be becoming outdated (or, to the contrary, are trusted sources of local cybersecurity knowledge). With the classifier of history, we might turn the scales upside down from when we assess cybersecurity according to size, business segment, or location.

Other classifiers for SMEs have emerged from our material: the *IT landscape, physical arrangements, assurance culture,* etc.). These allow not only SME-specific communication of cybersecurity issues, but they also drill down into the ominous group of SMEs in more detail. In this report, we have provided some grounded categories of how cybersecurity differs within SMEs. This prompts further questions of what to inquire about when assessing the cybersecurity maturity of companies in the future. Instead of assessing security according to standard categories by asking, "How many security tests are conducted? How complex are user passwords?" we might start asking the following: How much do employees talk about security? Where is the company located? Who works where and with whom? How well do people know each other? How can physical means be changed to create cybersecurity reminders?

Moral high grounds have a negative effect on SMEs

We have encountered several occurrences where casting judgment about good or bad cybersecurity was either difficult for our informants or where they felt judged by the ethnographer. During conversations about particularly painful cybersecurity decisions (such as the dilemmas), the conversation turned awkward, and informants appeared to suddenly speak to the ethnographer as a representative of formal cybersecurity expertise. They asked her to "not judge" and ensured they knew they "could do better," or they outright asked for an evaluation of the cybersecurity measures taken ("How are we doing?" "Maybe you can help us?").

We take this as a sign of discomfort that the informants sensed with the topic of cybersecurity. Although most had at least considered cybersecurity features and made competent decisions, they felt audited by an ethnographer, sometimes unfolding their troubles in front of her or attempting to hide them. One informant admitted she had tidied up her computer before the visit; another one was quick to rip a Post-It note with a password off her computer when the ethnographer showed up. In both cases, practical reasons were explained as to why having

a messy desktop and having a password posted to the computer are sometimes necessary, albeit "bad" practices.

The experienced judgment by cybersecurity officials seeded initial mistrust in the visits, which were expressed in the beginning, for example: "Can this have any negative effects for us?" one informant interrogated the ethnographer right away and requested full assurance that data would be anonymized. Echoing their anxiety of being exposed to authorities, several informants assured them they "could get better," but when asked why they had not done so, practical reasons and dilemmas were revealed that showed extensive consideration. Instead of a lack of awareness of cybersecurity, we encountered competent informants who were intimidated to explain to a researcher their situation because they had been scared off by generalist cybersecurity instructions. The informants did not lack awareness of cybersecurity but rather possessed uncomfortable knowledge of the practical realities of cybersecurity in their company. This was knowledge that they felt was not asked for in general cybersecurity campaigns.

8. References in order of appearance

The Danish Government, December 2021. The Danish Cyber and Information Security Strategy 2022–2024.

Epinion, April 2021. Segmenteringsanalyse af små og mellemstore virksomheder. Report.

Erhvervsstyrelsen, September 2021. Digital Sikkerhed i Danske SMV'er 2021. Report.

Epinion, January 2022. Kendskabsanalyse 2021. Report.


AALBORG
UNIVERSITET


ADD
Algoritmer, Data
& Demokrati