A Study on Security and Privacy Practices in Danish Companies

Asmita Dalela*, Saverio Giallorenzo†, Oksana Kulyk*, Jacopo Mauro‡ and Elda Paja*
*IT University of Copenhagen, Denmark
†Università di Bologna, Italy and INRIA, France
‡University of Southern Denmark, Denmark

***Abstract*—Increased levels of digitalization in society expose companies to new security threats, requiring them to establish adequate security and privacy measures. Additionally, the presence of exogenous forces like new regulations, e.g., GDPR and the global COVID-19 pandemic, pose new challenges for companies that should preserve an adequate level of security while having to adapt to change. In this paper, we investigate such challenges through a two-phase study in companies located in Denmark—a country characterized by a high level of digitalization—focusing on software development and tech-related companies. Our results show a number of issues, most notably i) a misalignment between software developers and management when it comes to the implementation of security and privacy measures, ii) difficulties in adapting company practices in light of implementing GDPR compliance, and iii) different views on the need to adapt security measures to cope with the COVID-19 pandemic.**

I. Introduction

The fact that security and privacy are a challenge to companies has long been accepted in research, requiring both technical solutions and a consideration of human and societal factors [29]. Moreover, the ever-growing presence of digital services in people's everyday life and the evolving landscape of security and privacy threats, require companies to adapt to new challenges to avoid severe consequences such as data theft or loss of reputation [28]. Previous studies have shown that the proper implementation of security and privacy processes in companies is often lacking, even for companies employing people with a high level of technical expertise such as software development companies [7], [11], [32], [49], [51]. Security and privacy processes as a subject in need of continuous change and adaptation, however, are less documented.

In this work, we investigate the challenges faced by Danish companies in implementing and keeping up to date security and privacy measures. Since Denmark is a highly digitalized country, it has a high dependency on secure digital solutions that call for a high degree of data protection practices, as well as adequate security measures to be adopted by Danish companies [23]. Our contribution addresses the following research objectives:

- In terms of organizational practices, how are security and privacy integrated, in the product development cycle as well as in terms of general awareness? How are the responsibilities defined and what are the controls (if any) that are implemented?
- In light of GDPR entering into force, how have the companies been dealing with it? Do they incorporate the required measures towards compliance, and what are the challenges they are facing in doing so?
- In light of the COVID-19 pandemic, how have companies adapted to the situation? What are their concerns and challenges given the need to shift to remote work?

Our investigation identifies nuances suggesting that companies lack proper guidelines to support them in adapting to a diversity of emerging challenges. These nuances include a lack of knowledge of proper security and privacy measures and a lack of awareness about security and privacy risks, leading to a situation where the necessary changes such as GDPR compliance measures and remote-work policies are not being fully implemented.

Furthermore, the results show that there is a misalignment between the perception of security issues and responsibilities of senior management, software developers, and people responsible for security and privacy in the company. This presents a barrier to ensuring that the employees have the necessary competencies for implementing the security and privacy measures and that they are given a proper opportunity to do so.

II. Related Work

Previous research on security and privacy challenges in organizations revealed that a source of problems is the difficulty of the employees to comply with the security policies [6], [12], [15], [21], [31], [39]. In particular, these studies have identified several behavioral factors, which influence compliance to security and privacy policies, including the perceived severity of threats, self-efficacy, trust between the employees and the security team, perceived usefulness of the policies, costs of following the policies, the severity of sanctions for non-compliance or social influence perceived norms in one's environment.

In particular, the need for addressing the human factors of security in software development has been highlighted in recent years, e.g., with Green and Smith [30] indicating developers as the "weakest link" and Acar et al. proposing a research agenda for such investigations [2]. Specifically, studies have been conducted to study different aspects of software development,

Network and Distributed Systems Security (NDSS) Symposium 2022
24–28 April 2022, San Diego, CA, USA
ISBN 1-891562-74-6
https://dx.doi.org/10.14722/ndss.2022.23xxx
www.ndss-symposium.org

such as the adoption and usability of specific tools (e.g., static analysis tools [44] and cryptographic APIs [1]), available guidance and support materials [3], organizational processes in software development companies [7], [32], [43], and individual behavior and mental models of security and privacy of software developers [11], [49], [51], [52]. Many of these works have been summarized in a systematic literature review by Tahaei and Vaniea [47]. Overall, these studies reveal a variety of issues, such as the complexity of existing tools and procedures, the lack of security-focused expertise among developers, the lack of reliable guidance, and the prioritization of functional features over security, altogether stressing the importance of establishing a security culture within the company.

Assal and Chaisson [8] investigated security adoption in the software development life cycle from the perspective of the developers, through a quantitative survey design. In their study, they highlight that the issues with security adoption arise due to lack of organizational or process support in integrating security throughout the development cycle. Indeed, they reported that developers are aware of the importance of integrating security in the development cycle and showed themselves self-motivated to apply it. However, they also felt that their peers did not give importance to it, they deem it not their responsibility to implement it, and highlighted that the focus of their organization is towards the development of the functional features. Our paper further enriches the space explored by Assal and Chaisson, including the additional dimensions of the perspectives of senior management and of security and privacy experts.

Another research strand has investigated the cultural aspects of security and privacy. As such, studies of leaked passwords from different countries (India, Japan and the UK [41], as well as the US and Germany [38]) reveal the differences in password complexity and chosen words, the most common being culture specific. Other studies have shown the differences in security and privacy risk awareness and behavior comparing for instance participants from Spain, Romania and Germany [35] and participants from Germany, the UK and the US [18]. Among the studies on these topics, [50] is particularly relevant for our work, as it involves another Nordic country. In this work, Volkamer et al. investigate the differences in taking security precautions during ATM usage (e.g., whether people hide their PINs during cash withdrawal) among the participants from Germany, UK and Sweden. The study shows that the participants from Sweden and the UK were less likely to take precautions, suggesting the difference in cultural norms as the reason for these differences. Designing security awareness and education measures in different cultural contexts has been studied by Bada et al. [10], comparing the security awareness campaigns in the UK and Africa and by Al Qahtani et al. [4], replicating the US study on the effectiveness of an awareness campaign in Saudi Arabia and adjusting the campaign contents towards the Saudi cultural context. Both of these studies show that cultural characteristics, such as shared values (e.g., individualism vs. social responsibility) or specific threats that are prevalent in a specific society, are an important factor in shaping these campaigns.

Following the findings from previous research, we look at security as a social issue, considering the dynamics between people in different roles in organizations and the interconnection of the perspectives they have on security and privacy issues, as well as the influences of a broader culture. Our study explores these perspectives in the context of Danish companies, taking into account the high level of digitalization in the Danish society and the recent challenges the companies have been confronted with.

III. Methodology

In our mixed-method two-phase study design, we conducted a survey (Section III.A) to collect data for a first quantitative evaluation, and used the preliminary results collected from the survey to inform the interview preparation, namely, the development of the interview guide [19], [42] . Then, we conducted ethnographic interviews (Section III.B) to gain in-depth qualitative insights over the selected aspects. As the data collection period for the survey overlapped with conducting the interviews, we finalized the analysis of the survey together with the analysis of the interviews, aggregating findings from both the quantitative and the qualitative part. We describe the individual stages of our investigation in more details below, concluding the section with a discussion on the ethical considerations of our studies (Section III.C).

A. Quantitative Survey

The first stage of the study was done as an online survey. The goal of the survey was to obtain initial quantitative insights into security and privacy practices in companies across five areas: i) security management and standards, including challenges in adhering to these standards; ii) the integration of security into the development cycle; iii) the integration of GDPR; iv) general perception of security awareness, security policies, behavior, reporting and available training; v) the impact of pandemic on security. To get a broad perspective on these areas, the survey aimed at eliciting responses from respondents occupying different roles (e.g., management, developers). We describe the survey design, dissemination, and the resulting sample in more detail below.

1) Survey design: The survey consisted of a total of 36 questions, divided across the five areas that were the focus of the investigation. At the beginning of the survey, the participants were asked about their roles in the company, and were encouraged to choose from a predefined list of tasks, viz. management related, IT-security related, privacy/data-protection related, software-development related, IT-administration related and 'other'. The participants in the survey had the option to choose multiple organizational roles, if they considered that the combination of the given roles better described their position. Out of 36 questions, only 8 questions related to the general perception of security awareness, security policies, behavior, reporting and available training were answered by all, while other questions were answered based on the roles selected by the participants. The required time to complete the survey was 10 minutes.[1].

2) Survey dissemination: The survey was implemented as a questionnaire in English hosted on the SurveyXact platform[2] and distributed by providing the link to the survey during the dissemination. To disseminate the survey, we looked at two

[1]The survey questionnaire can be accessed online at https://ascd.dk/results/survey_questions.pdf

[2]https://www.survey-xact.dk.

Role	SMEs	Large companies
Management	38	14
IT-security	24	19
Privacy/data protection	15	8
Software development	18	18
IT administrator	21	11
Other	6	11

TABLE I. PARTICIPANT SELECTIONS FOR EACH ROLE (PARTICIPANTS COULD SELECT MULTIPLE ROLES).

#	Role	Org Size
1	Senior Manager	SME
2	Sec/Priv Expert	SME
3	Senior Manager	SME
4	Developer	SME
5	Senior Manager	SME
6	Developer	SME
7	Developer	Large
8	Senior Manager	Large
9	Sec/Priv Expert	Large
10	Sec/Priv Expert	Large
11	Developer	Large

TABLE II. PROFILES OF THE INTERVIEW PARTICIPANTS.

dimensions: company size and participant roles. For the first dimension, we targeted companies that are based in Denmark.

These companies were from diverse sectors such as software product development, pharmaceuticals, retail, manufacturing, finance, etc., and covered all major sectors. The companies were categorized into two groups: small and medium enterprises (SMEs) ($\leq$ 250 employees) and large ($>$ 250 employees). For the second dimension, eight relevant participant roles were identified as recipients of the survey: CEO, CTO, CISO, DPO, developers, IT administrators, HR, and finance. Irrespective of the size of the company, the survey was sent to its CEO, requesting to disseminate it to the other relevant participants.[3] The survey ran from June to November 2020, and it was promoted in two phases: first in mid-June, and again in early August, to maximize its reach within companies.[4] To maximize the reach-out to the relevant participant roles in diverse companies, five different channels were leveraged for the survey promotion: social media, trade bodies, startup accelerators, the internal network of the authors' universities, and media publications.

3) Survey sample and analysis: Overall, 107 participants completed our survey, of them 47 from large companies and 60 from SMEs. Table I shows the distribution of the participants' roles in the companies. The analysis was done in an exploratory way, preparing the descriptive statistics related to our research objectives and serving as the groundwork for the next study phase.

B. Qualitative Interviews

In this section, we describe how the interviews were planned, their reach-out strategy, and conclude with the methodology used for their analysis.

1) Interview structure planning: The initial insights from the survey were used as a basis to discover the main areas for in-depth investigation during the ethnographic interviews. These interviews consist of a conversation between a researcher (interviewer) and interviewee, where knowledge is constructed in the interaction between them [46].

Interviews took place from September to November 2020, following a preliminary analysis of the survey conducted in August 2020. To adapt to the COVID-19 containment regulation, most interviews were conducted over video calls using Microsoft Teams.

Interviews were planned by creating an Interview Guide[5] with inter-related questions aimed at drawing-out the perspective of the interviewee. They were conducted through semi-structured conversations lasting 1 hour.

2) Reach-out strategy and interviewee recruitment: We decided to conduct interviews with specific participants chosen across two dimensions: participant role and company size. For the participant role dimension, we aimed at covering different points-of-view of the interviewees on the same issues such as general security and privacy integration, the effect of GDPR, impact of the pandemic on security implementation and others, for triangulating the perspectives, avoiding anecdotal conclusions, and drawing nuanced insights. Three participant roles were covered: senior managers, security experts and people responsible for security and privacy policies in the company, and developers. For the company size dimension, they were segmented into two broad categories: SMEs and large companies. We included companies from a variety of sectors, namely, software products, finance, construction, retail/CPG, services and manufacturing.

The potential participants for the interviews were identified by leveraging different channels such as university networks, LinkedIn, Google, and reaching out and engaging through emails and LinkedIn messages. The profile of the 11 participants can be viewed in Table II. The interviews were audio-recorded, transcribed and anonymized to keep the opinions and identities of the participants secured.

3) Interview data analysis: The analysis of individual interviews was conducted using the thematic analysis methodology [16] to distill a set of key themes across all the ethnographic interviews. Following this methodology, chosen themes were selected when representing some level of patterned response or meaning within the data set and capturing something important about the data.

To strengthen the reliability of the analysis, a single researcher performed the initial thematic analysis, followed by two researchers who met regularly to thoroughly and collaboratively review and edit the themes and to group and interpret the data. Then, to verify the reliability of our analysis, we had a fourth researcher individually analyze 30% of the data.

We took an inductive, open approach while establishing the themes based on the frequently appearing responses rather than aligning the participants' opinion to the preassigned categories. Following Michalec et al. [40], we iteratively discussed the transcripts to construct the emerging themes and fostered the discussions between the researchers (authors) to build a shared understanding.

[3]CEO, CTO, CISO, DPO, and HR are the respective acronyms for Chief Executive Officer, Chief Technology Officer, Chief Information Security Officer, Data Protection Officer, and Human Resource manager.

[4]July is the holiday month in Denmark and thus we did not do any promotional activity during this month.

[5]https://ascd.dk/results/interview_guidelines.pdf

C. Ethical considerations

While our institutions do not have a mandatory Institutional Review Board for studies, we addressed the four considerations related to ethics in such a research, namely, informed consent, confidentiality, consequences and the role of the researcher [17], [22]. While conducting our study, we ensured to apply the ethical principle of confidentiality, so that private data identifying the participants will not be reported. As such, we also followed a set of guidelines when conducting this study, in line with the General Data Protection Regulation (GDPR). As such, we protected the confidentiality of the participants, assuring them that their personal data will not be shared with anyone and that the results will only be reported in anonymized form. We explicitly informed our participants about the purpose of both the survey and the interviews, ensured voluntary participation of the people involved in the studies via informed consent, and informed them of their right to withdraw from the studies anytime. We did not provide any remuneration to our interview and survey participants.

IV. Results

In this section, we discuss the results of both the survey and the interviews. We focus on three key themes that emerged from the analysis of the ethnographic interviews and we assimilate them with the findings from the survey: i) general security and privacy integration, ii) effects of the GDPR, and iii) effects of the COVID-19 pandemic.[6]

A. General security and privacy integration

Security professionals and managers (47 respondents from SMEs and 25 from large companies[7]) were asked about the general approaches the company takes in measuring cybersecurity readiness. As Figure 1 shows, more than half of them (58% and 56% of respondents in large companies and SMEs, respectively) reported relying on established standards either fully or in combination with frameworks developed internally in the company. A relatively small percentage (17% and 8% of respondents in SMEs and large companies respectively) reported not using any kind of measuring approaches at all. Furthermore, respondents from large companies were more likely to report on using internal frameworks, either as the only tool or in combination with established standards (68% compared to 34% respondents from SMEs).

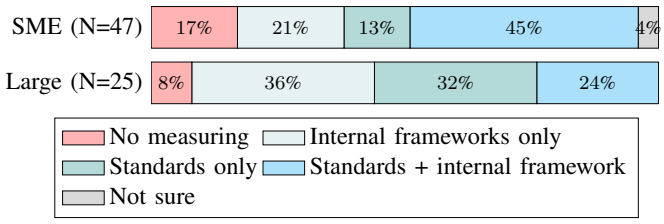

Fig. 1. Approaches for measuring security readiness.

[6]The results on the other key topics are detailed in the full technical report [5].

[7]Here and in the remainder of the section, we provide the number of participants who chose to answer the question. Note that, since the participants could skip any question, the total number of responses for each question can differ.

The software developers who participated in the survey (33 respondents from SMEs and 29 from large companies) were asked about the stage in which security is integrated into the software development cycle. As shown in Figure 2, the majority of the respondents (75% of respondents from SMEs and 51% from large companies) reported security integration either early from the start or continuously during the development. However, almost half of the respondents from large companies (45%) reported integrating security either after the fact, or not at all, in contrast to only 18% of respondents from SMEs.

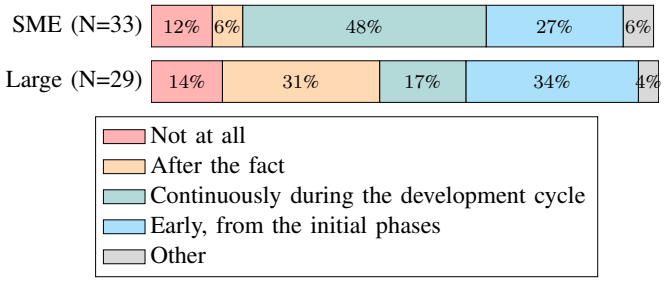

Fig. 2. Integration of security into the development cycle.

When asked about experience with security awareness training (respondents in all roles, overall 50 from SMEs and 42 from large companies), the majority (56% in SMEs and 76% in large companies) reported either participating in or at least being aware of such training in their companies. At the same time, only 50% of the respondents from SMEs participated in such training, and while this percentage was higher in large companies (69%), many of them (24%) did not find the training they attended to be value-adding.

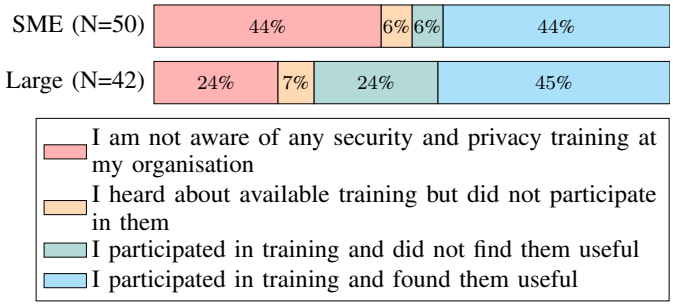

Fig. 3. Training attendance and utility perception.

The analysis of the interviews revealed multiple nuances potentially affecting the organizational practice of security and privacy measures integration in the development cycle, namely, the nuances of trust, developer-manager dynamic and competencies.

a) Trust.: Trust emerged as an important nuance, wherein senior managers trust the developers in their company to have all the necessary knowledge and capabilities to take proper care of security and privacy in the development cycle.

> "On the development side, the people who are working are extremely security-aware [...] I would say, I trust these people. I actually trust them a lot." ([P1], Senior Manager)

Another emerging context was the fact that companies tend to trust their employees to not intentionally engaging in malicious actions towards the company. In particular, one interviewee commented that such prevalence of trust is a cultural characteristic of the Danish society:

> "And I think Denmark as a national culture seems to be very trusting."([P9], Security Expert)

A complementing perspective on trust was also visible with a few senior managers who emphasized that the developers can trust their company enough to come forward with the reporting of security incidents.

> "We're not a company where people are being shot in front of the building, if they come forward and say, 'look, we think we have a problem [security breach] here'. So I'm hoping people will come forward if they do find a breach." ([P3], Senior Manager)

b) Developer-Manager dynamic.: A common perspective among developers was that there was a lack of security prioritization on behalf of senior management. The developers perceive that senior management often focuses more on the roll-out of functionalities, and they do not proactively and meaningfully prioritize the security needs as a part of their business imperatives.

> "So stuff like security, management didn't really want to spend time on or hear about, because that would delay whatever things we were supposed to deliver." ([P7], Developer)

On the contrary, senior management assumes that developers know and do all that needs to be done to implement security during product development. This approach leads to a tug-of-war between functionality vs security mindset in the development teams and often results in developers first working on the business requirements which deliver 'something', and apply the security measures on their own, later. All this results in siloed implementations, and a superficial complacency about security, across the company.

c) Competencies.: When it comes to acquiring competencies necessary for implementing security measures optimally, many interviewees mentioned that there is neither provisioning of general security awareness training nor any developer-specific training, in their companies.

> "And not in this company or the other[company], there was any kind of mentions of security as part of the on-boarding. Then there are no courses or training or anything afterwards." ([P7], Developer)

Even in cases when such training was available outside the company, some interviewees felt that participation in training is generally discouraged and the senior managers want a justification for attending them. Only a few interviewees acknowledged that their companies have a thorough approach to security training, including plans for specific security training for the developers to increase their proficiency level so that they can embed security in the product development.

B. Effects of GDPR

The survey participants who reported being responsible for either security or privacy-related tasks (43 in total) were asked about changes in their company since the GDPR entering into force. Figure 4 shows the percentage of respondents who reported changing some aspects of data sharing, namely, which data is collected, what controls are provided to the data subjects, how the data subjects are informed about the data collection, how the collected data is stored, shared and deleted. The results show that, overall, large companies were more likely to enact changes, and that the data protection aspect most commonly affected by the GDPR was informing the participants (changes reported by 84% and 74% of respondents in large companies and SMEs respectively). On the contrary, almost half of the participants in SMEs did not report any GDPR-related changes with regards to how the data is shared, how it is stored, and which controls are provided to the data subjects.

The analysis of the interviews revealed the following nuances in the state of GDPR compliance.

a) Rethinking data collection.: As the GDPR has changed the data collection and management processes in companies, it has pushed them to be more aware of their collection and retention policies around the different types of data they hold.

> "We have been more aware of what kind of data we get from our customers. We're more aware of when to delete and for how long we need it. Also, we have become more aware of how much we actually need." ([P2], Privacy Expert)

Since data collection requires management and compliance, as a result, many companies are avoiding collecting unnecessary data. Furthermore, in line with the survey data, many interviewees from large companies mentioned that their companies provide control to the data subjects and make sure that they can ask for deletion from their systems. Some interviewees have furthermore expressed the complexities it creates in their systems, making it challenging for them to implement (e.g., to ensure proper data deletion on request from data subjects).

On the other hand, some interviewees mentioned that GDPR has not changed the data collection practices in their companies, either because in their perception, their companies did not store any personal data (e.g., being a business-to-business company), or they have outsourced the handling of their assets, including personal data, to third parties.

b) Guidance.: During the interviews, it became evident that some companies provide guidance to employees on GDPR compliance through portals where employees can read about the GDPR guidelines or can avail consultation from a privacy expert in their companies. However, the employees are still expected to come forward and ask for clarifications themselves if they experienced problems.

> "From a product development point of view, there is no clear guidelines or no clear standard that our products can or cannot do this [...] I should say always it is the initiative of R&D to go to legal and say, we have this idea of doing this or that, what should we be aware of?" ([P11], Developer)

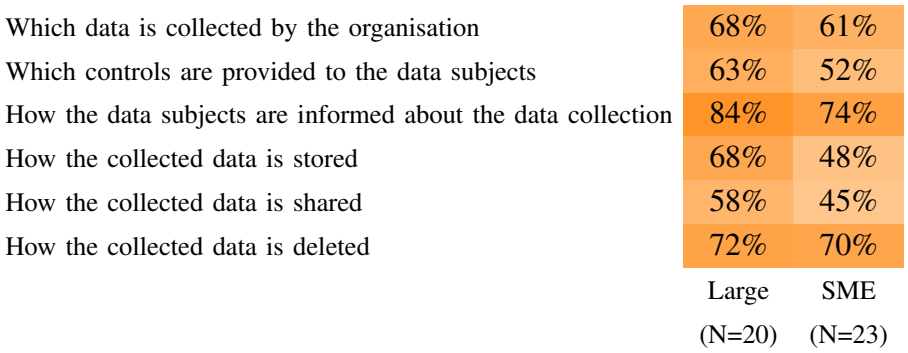

Fig. 4. Percentage of respondents reporting changes in how the company handles personal data since the GDPR entry into force.

At the same time, some interviewees commented about the lack of support for GDPR-related matters in their companies.

> "I don't think we have a person responsible for security and privacy and GDPR and all the stuff that actually sits down and ensures that all this is in order" ([P7], Developer)

c) Burden on resources.: It was evident in the interviews, that GDPR compliance requires a significant amount of time, money and expertise, and the lack of such resources or unwillingness to use them towards prioritizing security and privacy could be a barrier in ensuring compliance.

> "A number of our smaller competitors have it very difficult now because they find it very difficult to live up to the demands put upon them. We are a little larger than many of them, and perhaps had a little more resources, both time, money, and intellectual resources as well to make sure we did comply." ([P3], Senior Manager)

C. Effects of Pandemic

The survey results have shown that a vast majority of the participants had experience with remote work during the pandemic, with 38% of respondents from large companies and 47% from SMEs already working remotely even before the pandemic (Figure 5).

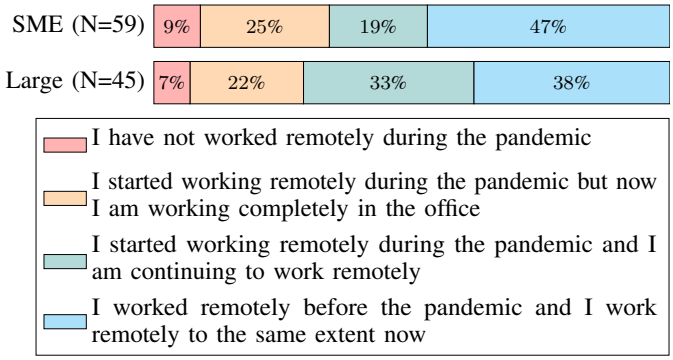

Fig. 5. Remote work experience before and during the pandemic.

The responses furthermore show that the majority of the respondents (85% of all the participants who answered the question) did not find the security and privacy policies introduced for remote work challenging. (Figure 6). Only a small percentage of respondents in both large companies (11%) and SMEs (13%) reported having increased concerns because of the pandemic and the remote work that followed (Figure 7).

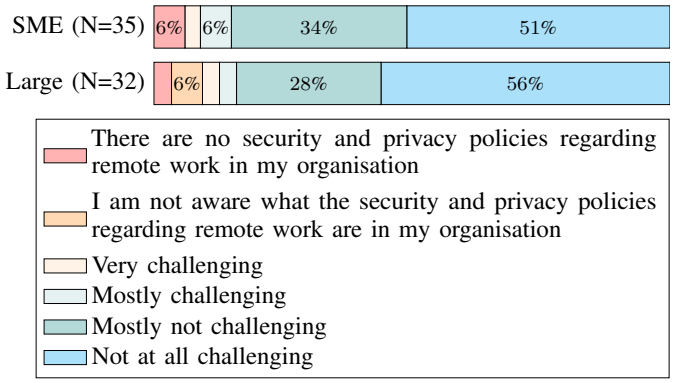

Fig. 6. Experience with remote work policies among the survey participants.

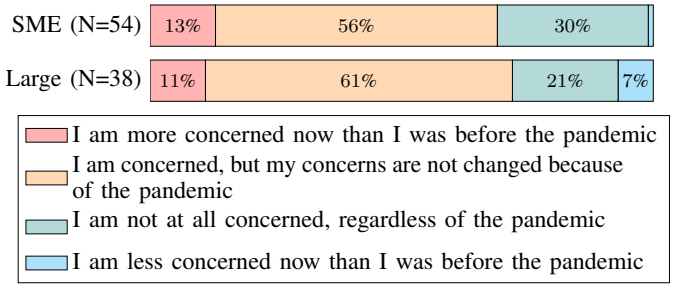

Fig. 7. Pandemic-related security and privacy concerns among the survey participants.

The analysis of the interviews revealed the following nuances in the perspectives of the interviewees, on the influence of the pandemic.

a) Relying on pre-pandemic processes.: It was evident from our interviews that the pandemic has not changed the way of working, including security management, in many companies. They are relying on their pre-pandemic practices of facilitating remote work and are not envisioning the potential repercussions of ignoring security threats. Some interviewees mentioned that the infrastructure in their company had already been accustomed to remote work prior to the pandemic, e.g., by leveraging cloud

and SaaS solutions, and they feel confident that the security measures are taken care of by the cloud and SaaS providers and these measures provide sufficient security.

> "Everything is cloud even the most sensitive part of the business, because then you know, that you have professionals handling those things. [...] I don't even have to be on a VPN tunnel or something like that. I can work just on my computer." ([P8], senior Manager)

b) Trust.: Several interviewees mentioned that since remote work has been an integral part of their company before the pandemic, there has been an inherent trust in the employees for not misusing the company devices or documents. A developer remarked, once again hinting at the role of trust in the Danish society:

> "In Denmark it's like, we trust people to take their laptop home and we don't expect them to take any company data and stealing, of course" ([P7], Developer)

V. Discussion

As presented in Section IV, particularly prominent was the mention of (i) *trust*, which could also be perceived as a cultural characteristic of the demographics in our sample, and its relation with the perceived *responsibility* regarding security and privacy in the organization, and the emerging nuances of (ii) *lack of awareness* of security and privacy risks as well as *knowledge* about the appropriate countermeasures. We elaborate on these below.

Trust and responsibility Trust appeared as a recurring nuance in many of the themes after analyzing the data from the ethnographic interviews. Moreover, some of the participants explicitly connected such trust to Danish cultural values. Such prevalence of trust, in terms of social cohesion (cf. Section I), might therefore be a reflection of a broader cultural trait of the Danish society (and possibly, more broadly, of Nordic countries), where people in the society are more likely to trust each other, including their superiors or employees at their workplace [37], [45]. Future research is therefore required to understand the prevalence of trust in the context of cybersecurity in Danish companies and both its positive and negative effects.

Lack of awareness Lack of awareness and concern about security and privacy risks has manifested in different contexts in our study. One example is the lack of concerns of additional risks connected to the pandemic and the remote work. Such attitudes might result from seeing remote work as something that has been already been established before the COVID-19 restrictions, with Denmark being a highly digitalized society [23], and our survey results showing the prevalence of remote work before the pandemic. At the same time, with the scale of remote work dramatically increasing within the last year (and alternatives such as part-time physical presence in offices often unfeasible), experts both in Denmark and internationally claim an increased level of cyber-attacks and privacy issues [20], [33], and surveys in other countries indeed show a high level of concerns among the population regarding cybersecurity during the pandemic [9]. It, therefore, remains an open question, to which extent the lack of concerns among our study participants represent the actual risks their companies face.

A further related issue was lack of familiarity with the GDPR compliance, manifesting such as lack of awareness regarding the data that is subject to the GDPR regulations, lack of familiarity with procedural requirements related to the GDPR among both developers and managers, and the general perception of the existing GDPR guidelines as too vague. Such results might not be surprising, given previously voiced concerns over diverse issues of defining and implementing GDPR compliance [36], yet these results show that several years after its entry into force, GDPR is still perceived as a significant challenge, and highlighting once again the need for better guidance.

Generally, our results show a lack of knowledge about available security and privacy protection measures, also manifesting in comments from developers about unavailability of training to enhance their security and privacy skill-set. On the other hand, providing more security education measures raises significant challenges with ensuring the effectiveness of such measures, such as their known problems of failing to engage the participants or providing them with skills they can successfully apply outside of the training context [10]. Indeed, as also shown by the results of our survey, a large share of participants did not find the training they attended to be useful. Furthermore in absence of clear management support and prioritization of security—the issue furthermore revealed in our study—the developers would have no incentive or desire to attend the training.

Limitations of our study During our study, a sample was created to represent different sectors and sizes of organizations, and cover different participant' roles. Although the sample includes a range of participant roles, sectors, and size of organizations, the insights derived from the analysis might not necessarily generalize to any of those variables. In particular, while we aimed for gender balance and reached out to other possible gender participants during the interviews, only male participants gave us their time-wise availability to conduct the interviews during the two months reserved for that. Including more diverse perspectives on security and privacy would therefore be an important direction of future work.

VI. Conclusion

We conclude this paper by summarizing the main challenges that emerged from our study. In particular, we deem these challenges likely to play key roles in the social and economic norms of the more and more digitalized societies that will emerge from the aftermaths of the pandemic.

Accounting for change is the first and overarching topic of our investigation. Our results show that there is a need to develop guidelines and roadmaps that are not just designed to tackle a particular issue such as new legislation or the most recent crisis, but also are adaptable enough to be applied continuously to account for a variety of future changes. These roadmaps, for example, could result in guidelines for the companies in shaping their security training, ensuring regular updates and adaptations of their contents, as well as ongoing two-way collaborations between companies, researchers and

public institutions. Specifically, in the context of software development, such an accounting for change could be facilitated by methodologies such as Dev(Sec)Ops [14], [34] and Site Reliability Engineering [13], that already embrace change and security in their core process. While the interest in this kind of methodologies [27] has been increasing, more studies will be needed to understand how change could be integrated, especially for SMEs and for the more general picture in the digitalized society.

When investigating the adoption of the GDPR, we found that companies adopted a patchwork approach for handling the implementation of compliance measures to a sufficient extent, but many are still struggling with its adoption. A more *structured approach towards new regulations* is therefore needed for the forthcoming implementation of standards and regulations, e.g., via a creation of a task force constituted by the relevant stakeholders and lightweight conformity-assessment methods for basic security assurance [25].

Our results furthermore confirm and corroborate existing and well-know challenges like *raising competences*. As previous research shows, awareness, while being an important first step towards improving security and privacy, is not sufficient, unless people are both provided with skills to cope with threats and are confident that they are capable of applying them [24].

Our study shows a need for accessible training for developers and managers alike. To make the training relevant for the attendees, the security education measures should be tailored towards specific contexts, taking into account the general background and the needs of the developers that are about to participate, also ensuring that the participants would be able to easily translate the contents of the training into their daily tasks. While the offer of test labs, cyber-ranges, documentation, and best practices has increased in the last two years, both on-premises and with cloud offerings [26], particular attention must be given to check their effectiveness for training staff, simulating attacks, and testing multiple defense strategies.

Another aspect, emphasized also by previous research [24] is the need of the *managerial involvement*. In our study, we have witnessed that security and privacy measures are often perceived as a cost and therefore not properly prioritized. For the establishment of a proper security culture in the company, the involvement of management in the security decisions should be increased, ideally with senior management leading the company's security and privacy measures by their example and establishing a dedicated budget for security. While not all managers are expected to become security and privacy experts, they should have a basic awareness of security risks to drive the prioritization of security. They should also make sure that the developers feel incentivized to both implement the security measures they know of and also to improve their competences, e.g. by attending training, participating in conferences, and other educational opportunities.

Based on the mismatch between the perception of responsibilities with regards to security and privacy tasks we witnessed, we would recommend to managers also to foster as much as possible a *transparent communication*. The expectations of both management and developers with regards to security and privacy responsibilities should be clearly communicated and agreed upon. Furthermore, efficient communication should be ensured for people seeking support with security and privacy-related task, so that they know whom they should turn to, be it *security champions* [48] in their teams or a specifically assigned person of contact that handles security and privacy issues in the company.

Finally, we would like to conclude by emphasizing the *role of culture* in security and privacy. Our study shows an effect of cultural contexts, such as the prevalence of trust in the companies towards external partners or employees, as a reflection of the importance of trust in general in Danish society. Further research into ways to support companies in their security and privacy practices while considering these cultural influences, including future studies with cross-cultural comparisons, might provide interesting insights.

REFERENCES

[1] Y. Acar, M. Backes, S. Fahl, S. Garfinkel, D. Kim, M. L. Mazurek, and C. Stransky, "Comparing the usability of cryptographic apis," in *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 154–171.

[2] Y. Acar, S. Fahl, and M. L. Mazurek, "You are not your developer, either: A research agenda for usable security and privacy research beyond end users," in *2016 IEEE Cybersecurity Development*, 2016, pp. 3–8.

[3] Y. Acar, C. Stransky, D. Wermke, C. Weir, M. L. Mazurek, and S. Fahl, "Developers need support, too: A survey of security advice for software developers," in *2017 IEEE Cybersecurity Development*, 2017, pp. 22–26.

[4] E. Al Qahtani, M. Shehab, and A. Aljohani, "The effectiveness of fear appeals in increasing smartphone locking behavior among saudi arabians," in *Fourteenth Symposium on Usable Privacy and Security 2018)*, 2018, pp. 31–46.

[5] ASCD Project Team, "ASCD Project Report," https://ascd.dk/results/report.pdf, 2020.

[6] D. Ashenden and A. Sasse, "Cisos and organisational culture: Their own worst enemy?" *Computers & Security*, vol. 39, pp. 396–405, 2013.

[7] H. Assal and S. Chiasson, "Security in the software development lifecycle," in *14th Symposium on Usable Privacy and Security*, 2018, pp. 281–296.

[8] ——, "Think secure from the beginning: Survey with software developers," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 2019, p. 289.

[9] AT&T-Communications, "Survey suggests the behaviour of remote workers is adding extra cybersecurity risk to their employers' business," 2021. [Online]. Available: https://www.prnewswire.com/news-releases/survey-suggests-the-behaviour-of-remote-workers-is-adding-extra-cybersecurity-risk-to-their-employers-business-301252707.html

[10] M. Bada, A. M. Sasse, and J. R. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" in *International Conference on Cyber Security for Sustainable Society*, 2015.

[11] R. Balebako, A. Marsh, J. Lin, J. I. Hong, and L. F. Cranor, "The privacy and security behaviors of smartphone app developers," 2014.

[12] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *Proc. of the 2008 New Security Paradigms Workshop*, 2008, pp. 47–58.

[13] B. Beyer, C. Jones, J. Petoff, and N. R. Murphy, *Site Reliability Engineering: How Google Runs Production Systems*, 1st ed. O'Reilly Media, Inc., 2016.

[14] J. Bird, *DevOpsSec: Securing Software Through Continuous Delivery*. O'Reilly Media, Incorporated, 2016. [Online]. Available: https://books.google.dk/books?id=5v25AQAACAAJ

[15] J. M. Blythe, L. Coventry, and L. Little, "Unpacking security policy compliance: The motivators and barriers of employees' security behaviors," in *Proceedings of the 11th Symposium on Usable Privacy and Security*, 2015, pp. 103–104.

[16] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[17] S. Brinkmann and S. Kvale, *The SAGE Handbook of Qualitative Research in Psychology*. Sage, 2017.

[18] K. P. Coopamootoo, "Dis-empowerment online: An investigation of privacy-sharing perceptions and method preferences," in *International Conference on Financial Cryptography and Data Security*. Springer, 2020, pp. 71–83.

[19] J. W. Creswell, "Mixed-method research: Introduction and application," in *Handbook of educational policy*. Elsevier, 1999, pp. 455–472.

[20] Danish Centre for Cybersecurity (CFCS), "Cyber criminals rearm in the shadow of the pandemic," https://cfcs.dk/en/cybertruslen/threat-assessments/cyber-criminals-rearm-in-the-shadow-of-the-pandemic/, 2020.

[21] S. Das, T. Hyun-Jin Kim, L. A. Dabbish, and J. I. Hong, "The effect of social influence on security sensitivity," in *Proceedings of the 10th Symposium on Usable Privacy and Security*, 2014, pp. 143–144.

[22] S. Delamont and P. Atkinson, *The sage handbook of qualitative research ethics*. Sage, 2018.

[23] S. R. Department, "Country-level digital competitiveness rankings worldwide as of 2021," https://www.statista.com/statistics/1042743/worldwide-digital-competitiveness-rankings-by-country/, 2021.

[24] ENISA, "Cybersecurity culture guidelines: Behavioural aspects of cybersecurity," https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity, 2019.

[25] ——, "Enisa advancing software security in the eu," https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework, 2019.

[26] ——, "ENISA Threat Landscape - The year in review," https://www.enisa.europa.eu/publications/year-in-review, 2020.

[27] N. Forsgren, J. Humble, and G. Kim, *Accelerate: The Science of Lean Software and DevOps Building and Scaling High Performing Technology Organizations*, 1st ed. IT Revolution Press, 2018.

[28] J. Fruhlinger, "Equifax data breach faq," https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html, 2020.

[29] S. L. Garfinkel, "The cybersecurity risk," *Communications of the ACM*, vol. 55, no. 6, pp. 29–32, 2012.

[30] M. Green and M. Smith, "Developers are not the enemy!: The need for usable security apis," *IEEE Security Privacy*, vol. 14, no. 5, pp. 40–46, 2016.

[31] J. M. Haney and W. G. Lutters, ""it's scary...it's confusing...it's dull": How cybersecurity advocates overcome negative perceptions of security," in *Proceedings of the 14th Symposium on Usable Privacy and Security*, 2018, pp. 411–412.

[32] J. M. Haney, M. Theofanos, Y. Acar, and S. S. Prettyman, ""we make it a big deal in the company": Security mindsets in organizations that develop cryptographic products," in *14th Symposium on Usable Privacy and Security*, 2018, pp. 357–373.

[33] INTERPOL, "Interpol report shows alarming rate of cyberattacks during covid-19," https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19, 2020.

[34] G. Kim, P. Debois, J. Willis, and J. Humble, *The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations*. IT Revolution Press, 2016.

[35] O. Kulyk, B. Reinheimer, L. Aldag, P. Mayer, N. Gerber, and M. Volkamer, "Security and privacy awareness in smart environments – a cross-country investigation," in *Financial Cryptography and Data Security Workshop on Usable Security (AsiaUSEC), February 14, 2020 Sabah, Malaysia*. Springer, 2020.

[36] M. Kutyłowski, A. Lauks-Dutka, and M. Yung, "Gdpr–challenges for reconciling legal rules with technical reality," in *European Symposium on Research in Computer Security*. Springer, 2020, pp. 736–755.

[37] C. A. Larsen, *The rise and fall of social cohesion: The construction and de-construction of social trust in the US, UK, Sweden and Denmark*. Oxford University Press, 2013, vol. 1.

[38] P. Mayer, J. Kirchner, and M. Volkamer, "A second look at password composition policies in the wild: Comparing samples from 2010 and 2016," in *Thirteenth Symposium on Usable Privacy and Security 2017)*, 2017, pp. 13–28.

[39] P. Mayer, A. Kunz, and M. Volkamer, "Reliable behavioural factors in the information security context," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1–10.

[40] O. Michalec, D. van der Linden, S. Milyaeva, and A. Rashid, "Industry responses to the european directive on security of network and information systems (nis): Understanding policy implementation practices across critical infrastructures," in *16th Symposium on Usable Privacy and Security*, 2020, pp. 301–317.

[41] K. Mori, T. Watanabe, Y. Zhou, A. A. Hasegawa, M. Akiyama, and T. Mori, "Comparative analysis of three language spheres: Are linguistic and cultural differences reflected in password selection habits?" *IEICE Transactions on Information and Systems*, vol. 103, no. 7, pp. 1541–1555, 2020.

[42] J. M. Morse, *Mixed method design: Principles and procedures*. Routledge, 2016.

[43] H. Palombo, A. Z. Tabari, D. Lende, J. Ligatti, and X. Ou, "An ethnographic understanding of software (in) security and a co-creation model to improve secure software development," in *16th Symposium on Usable Privacy and Security*, 2020, pp. 205–220.

[44] J. Smith, L. N. Q. Do, and E. Murphy-Hill, "Why can't johnny fix vulnerabilities: A usability evaluation of static analysis tools for security," in *16th Symposium on Usable Privacy and Security*, 2020, pp. 221–238.

[45] K. M. Sønderskov and P. T. Dinesen, "Danish exceptionalism: Explaining the unique increase in social trust over the past 30 years," *European Sociological Review*, vol. 30, no. 6, pp. 782–795, 2014.

[46] J. P. Spradley, *The ethnographic interview*. Waveland Press, 2016.

[47] M. Tahaei and K. Vaniea, "A survey on developer-centred security," in *2019 IEEE European Symposium on Security and Privacy Workshops*, 2019, pp. 129–138.

[48] T. W. Thomas, M. Tabassum, B. Chu, and H. Lipford, "Security during application development: An application security expert perspective," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–12.

[49] D. van der Linden, I. Hadar, M. Edwards, and A. Rashid, "Data, data, everywhere: quantifying software developers' privacy attitudes," in *Int. Workshop on Socio-Technical Aspects in Security and Trust*, 2019.

[50] M. Volkamer, A. Gutmann, K. Renaud, P. Gerber, and P. Mayer, "Replication study: A cross-country field observation study of real world {PIN} usage at atms and in various electronic payment scenarios," in *Fourteenth Symposium on Usable Privacy and Security 2018)*, 2018, pp. 1–11.

[51] C. Weir, B. Hermann, and S. Fahl, "From needs to actions to secure apps? the effect of requirements and developer practices on app security," in *29th Security Symposium ({USENIX} 20)*, 2020, pp. 289–305.

[52] S. Xiao, J. Witschey, and E. Murphy-Hill, "Social influences on secure development tool adoption: Why security tools spread," in *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 2014, p. 1095–1106.