

A Mixed-method Study on Security and Privacy Practices in Danish Companies

Asmita Dalela¹, Saverio Giallorenzo², Oksana Kulyk¹, Jacopo Mauro³,
and Elda Paja¹

¹IT University of Copenhagen, Denmark { asmd, okku, elpa }@itu.dk

²Università di Bologna, Italy and INRIA, France saverio.giallorenzo@gmail.com

³University of Southern Denmark, Denmark mauro.jacopo@gmail.com

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 and trust—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.

1 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 [Garfinkel \(2012\)](#). 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 [Fruhlinger \(2020\)](#).

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 [Balebako et al. \(2014\)](#); [Weir et al. \(2020\)](#); [van der Linden et al. \(2019\)](#); [Haney et al. \(2018\)](#); [Assal and Chiasson \(2018\)](#). 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. In our study, we focus on software development and tech-related companies, investigating how they deal with security and privacy: (1) when conducting their day-to-day practices, (2) when required to adapt to new legislation, namely, the introduction to the EU General Data Protection Regulation (GDPR), and (3) when required to adapt to an unforeseen crisis during a rapidly and unpredictably changing situation, namely, the COVID-19 pandemic and the introduced restrictive measures. Our contribution addresses the following research objectives:

- In terms of organizational practices, how are security and privacy integrated? How are the responsibilities defined and what are the controls (if any) that are implemented? How do companies ensure sufficient security and privacy competences among their employees?
- 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 competences for implementing the security and privacy measures and that they are given a proper opportunity to do so.

We also note the occurrence of trust, in terms of social cohesion¹, as a common underlying thread across different themes. While the role of trust in determining security measures is often stressed by previous research in other contexts [Haney and Lutters \(2018\)](#); [Ashenden and Sasse \(2013\)](#), trust is considered to be a distinctive cultural value in Denmark and other Nordic countries [Larsen \(2013\)](#); [Sønderskov and Dinesen \(2014\)](#). Such importance of trust, as a distinguishing characteristic of the Danish society, has been specifically noted in our study, allowing us to elaborate on both positive and negative effects of it on security and privacy.

2 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 [Beautement et al. \(2008\)](#); [Mayer et al. \(2017b\)](#); [Das et al. \(2014\)](#); [Blythe et al. \(2015\)](#); [Ashenden and Sasse \(2013\)](#); [Haney and Lutters \(2018\)](#). 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 [Green and Smith \(2016\)](#) indicating developers as the “weakest link” and Acar et al. proposing a research agenda for such investigations [Acar et al. \(2016\)](#). Specifically, studies have been conducted to study different aspects of software development, such as the adoption and usability of specific tools (e.g., static analysis tools [Smith et al. \(2020\)](#) and cryptographic APIs [Acar et al. \(2017a\)](#)), available guidance and support materials [Acar et al. \(2017b\)](#), organizational processes in software development companies [Haney et al. \(2018\)](#); [Assal and Chiasson \(2018\)](#); [Palombo et al. \(2020\)](#), and individual behavior and mental models of security and privacy of software developers [Balebako et al. \(2014\)](#); [Weir et al. \(2020\)](#); [van der Linden et al. \(2019\)](#); [Xiao et al. \(2014\)](#). Many of these works have been summarized in a systematic literature review by Tahaei and Vaniea [Tahaei and Vaniea \(2019\)](#). 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.

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 [Mori et al. \(2020\)](#), as well as the US and Germany [Mayer et al. \(2017a\)](#)) 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 [Kulyk et al. \(2020\)](#) and participants from Germany, the UK and the US [Coopamootoo \(2020\)](#). Among the studies on these topics, [Volkamer et al. \(2018\)](#) 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

¹ Defined by Larsen [Larsen \(2013\)](#) as “the belief that [citizens] share a moral community, which enables them to trust each other”.

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. [Bada et al. \(2015\)](#), comparing the security awareness campaigns in the UK and Africa and by Al Qahtani et al. [Al Qahtani et al. \(2018\)](#), 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 trust and digitalization in the Danish society and the recent challenges the companies have been confronted with.

3 METHODOLOGY

We dedicate this section to present the mixed-method approach used in this work, detailing its parts: a quantitative survey (Section 3.1) and a subsequent round of interviews (Section 3.2). We conclude the section with a discussion on the ethical considerations of our studies (Section 3.3).

Our mixed-method approach follows a two-phase *sequential explanatory design* [Ivankova et al. \(2006\)](#). As visualized in Figure 1, we conducted a survey to collect data for a first quantitative evaluation ①, and

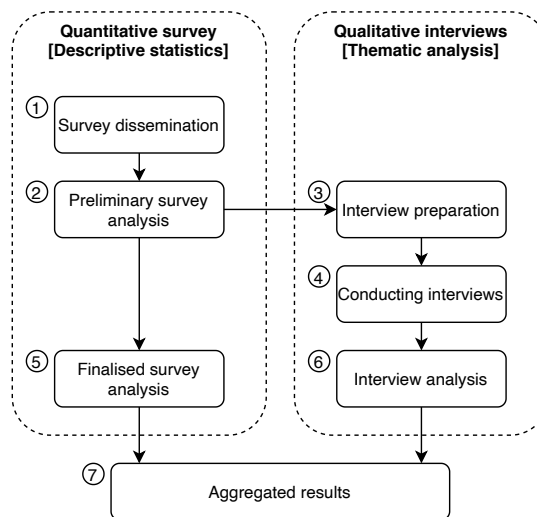


Figure 1. Scheme of the methodology followed in this study.

used the preliminary results collected from the survey ② to inform the interview preparation, namely, the development of the interview guide ③. Then, we conducted ethnographic interviews ④ 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 ⑤ together with the analysis of the interviews ⑥, aggregating findings from both the quantitative and the qualitative part ⑦.

3.1 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.

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 1. Number of participant selections for each role (participants could select multiple roles).

3.1.1 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.

The respondents were then shown the questions tailored to the roles they selected so that only 8 out of the 36 questions were presented for each role. Still, the participants were allowed to skip any question they did not want to answer. The full survey questionnaire can be found in Appendix A.

Before launching the survey, two runs of pretest were conducted. The pre-testers included experts in cybersecurity, human-factors research, and software development, from both academia and industry, and all residing outside Denmark. The pretests validated different aspects of the survey, such as the clarity of the questions, its duration, and all the possible role selections with the corresponding questions. The required time to complete the survey was determined to be 10 minutes.

3.1.2 Survey dissemination

The survey was implemented as a questionnaire hosted on the SurveyXact platform² based in Denmark. These companies were from diverse sectors such as software product development, pharmaceuticals, retail, manufacturing, finance. The companies were categorized into two groups: small and medium enterprises (SMEs) (≤ 250 employees) and large (> 250 employees). For the second dimension, eight relevant participant roles were identified to send the survey to: 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, 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.

3.1.3 Survey sample and analysis

Overall, 107 participants completed our survey, of them 47 from large companies and 60 from SMEs. Table 1 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.

3.2 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.

3.2.1 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

²<https://www.survey-xact.dk>, last visited on February 2021

³Note that CEO, CTO, CISO, DPO and HR are acronyms for Chief Executive Officer, Chief Technology Officer, Chief Information Security Officer, Data Protection Officer and Human Resource manager respectively.

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

#	Role	Org Size	Sector
1	Senior Manager	SME	Software products
2	Sec/Priv Expert	SME	Software products
3	Senior Manager	SME	Software products
4	Developer	SME	Software products
5	Senior Manager	SME	Finance
6	Developer	SME	Construction
7	Developer	Large	Services
8	Senior Manager	Large	Services
9	Sec/Priv Expert	Large	Retail/CPG
10	Sec/Priv Expert	Large	Manufacturing
11	Developer	Large	Manufacturing

Table 2. Profiles of the Interview participants.

(interviewer) and interviewee, where knowledge is constructed in the interaction between them [Spradley \(2016\)](#).

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 (Appendix B) with inter-related questions aimed at drawing-out the perspective of the interviewee. They were conducted through semi-structured conversations lasting 1 hour.

3.2.2 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

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 2. The interviews were transcribed and anonymized to keep the opinions and identities of the participants secured.

3.2.3 Interview data analysis

The analysis of individual interviews was conducted using the thematic analysis methodology [Braun and Clarke \(2006\)](#) 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.

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. \(2020\)](#), we iteratively discussed the transcripts to construct the emerging themes and fostered the discussions between the researchers (authors) to build a shared understanding.

3.3 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 [Delamont and Atkinson \(2018\)](#); [Brinkmann and Kvale \(2017\)](#).

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).

We explicitly obtained a consent from the interviewees, ensured a voluntary participation of the people involved, and informed them of their right to withdraw from the study anytime. Before starting the interviews, we clearly stated the goal of our study and data handling procedures.

We also followed the ethical principal of beneficence where we looked that the knowledge gained through conducting this research should outweigh the risk of harm to the participant. Also, the role of researcher was critically reported to the participants at the beginning of our study.

While we asked for some data that might be seen as personal during the survey (e.g., through a number of the questions related to the role, organization-sector, organization-size, contact email for possible follow-up interviews), we explicitly made it clear on the start page of the survey that these questions (with an exception of a question asking about one’s role) were not mandatory to answer, and any information that could be used to identify them would remain confidential. In addition, participants had the option to discontinue the survey at any time, while we emphasized that they could skip questions they preferred not to answer to for whatever reason. Finally, we did not provide any remuneration for our participants.

Since the interviews were conducted during the COVID-19 pandemic, there was a clear recommendation from the government to maintain social distancing and restrict traveling. We provided a choice to our interview participants to conduct the interviews on-premise or over video through MS Teams.

4 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 pandemic⁵.

4.1 General security and privacy integration

Security professionals and managers (47 respondents from SMEs and 25 from large companies⁶) were asked about the general approaches the company takes in measuring cybersecurity readiness. As Figure 2 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).

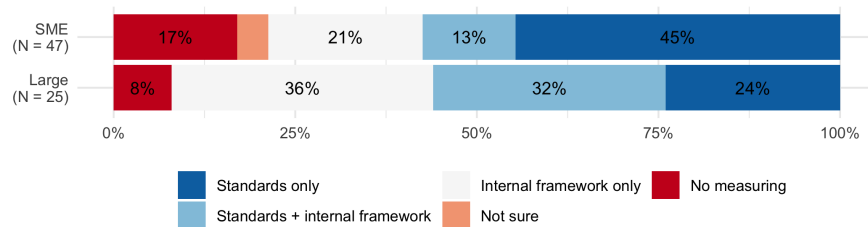


Figure 2. Approaches for measuring security readiness.

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 3, 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.

When asked about experience with security 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

⁵The results on the other key topics are detailed in the full technical report (reference omitted for double-blind reviewing).

⁶Here and everywhere else in this 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.

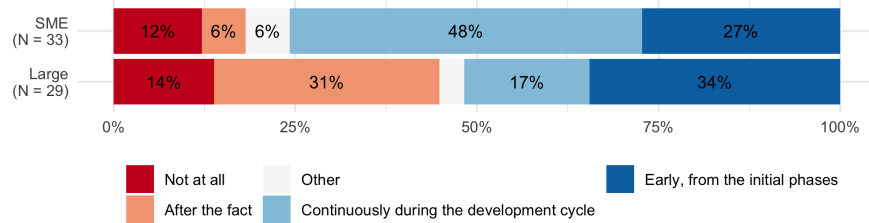


Figure 3. Integration of security into the development cycle.

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.

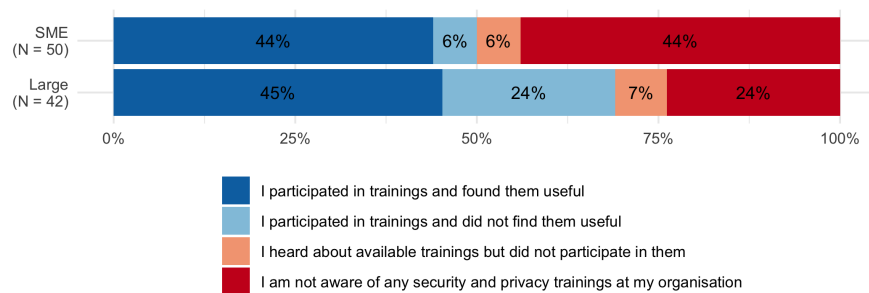


Figure 4. Training attendance and utility perception.

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 responsibility, trust, prioritization and competences.

Responsibility. A common thread in our observations was the delegation of the responsibility to the developers, with senior management assuming that developers know and do all that needs to be done for implementing security for the product development. A senior manager articulated:

“They [software developers] think about it [security] all the time and they are even 10 times more security-aware than I am.”

Such a perspective was reinforced by some of the developers, confirming that the task of implementing security and privacy measures is often placed entirely on them:

“[Security and privacy measures] is not something that they [senior management] really encourage and it’s not something they really care about. It’s something that happens only if the engineers [developers] themselves take care of it.”

Trust. Trust was often mentioned in different contexts, as 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. A senior manager remarked about the high level of trust in his developers.

“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.”

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.”

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.”

Prioritization. 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.

This approach was leading to a tug-of-war between functionality vs security mindset in the development teams. Some developers mentioned that their companies focus more on delivering functionality rather than security as it will decrease their time to market.

“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.”

This often results in developers first working on the business requirements which deliver ‘something’, and apply the security measures on their own, later, resulting in siloed implementations, and a superficial complacency about security, across the company.

Furthermore, the lack of involvement from the senior management was perceived as an issue in allocating resources towards cybersecurity. A developer highlighted

“I don’t get the feeling that management, in general, know a lot about security or really invests time and resources into making this an important thing in our daily engineering.”

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.”

Even in cases when such training was available outside the company, some interviewees felt that participation in these training is generally discouraged and the senior managers want a justification for attending them:

“I was once or twice to some compliance and stuff [security training], but my management was not so pleased about, and you spend the time on things like these is such a big thing.”

This is also reflected in the commentary from some senior managers, wherein they explained their view of generally encouraging developers ‘if’ multiple criteria were satisfied from their perspective. One senior manager commented:

“Generally, yes we would encourage that [providing training] if people came forward, but it has to make sense, you know, where, what is their position, what is the purpose, what is the value to the company if they were to do it.”

Only a few interviewees highlighted 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 development cycle. One of the security experts remarked:

“My ideal scenario, we get a training program that says, here’s the common body of knowledge for agile developers across all of these domains that we support. Here are some training modules, here’s a platform that you can develop on and that will give you coaching as you go, to help you get better at writing secure code. And we want to start a network of champions within the agile squads.”

4.2 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 5 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.

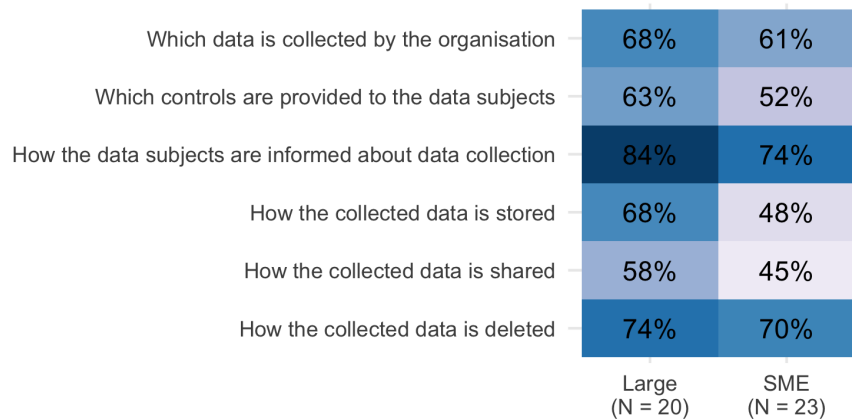


Figure 5. Percentage of respondents reporting changes in how the company handles personal data since the GDPR entry into force.

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

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. A privacy expert stated:

“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.”

Since data collection requires management and compliance, as a result, many companies are avoiding to collect unnecessary data and are trying to erase it from their repositories by using automated or manual procedures. A senior manager remarked:

“Everything that we build from now on, we are aware of these things [GDPR compliance]. We have also put in procedures both manually and automatically that delete or anonymize 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.

“They [data subjects] can ask us to get the data if they want to, we can transfer that out to them, if they want, we do not have any issues with that. Some people have written to us and ask us to erase all the data about them. And we do erase it, but we have some time scheduled to do it because we have some backup that also needs to go.”

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. A senior manager, when asked about the data collection changes in his company, articulated:

“We don’t have anything, I mean, we don’t carry any data.”

Procedural complexities. During the interview, it became evident that many companies are facing different procedural challenges while handling the data as per the GDPR. A privacy expert articulated:

”[Data collection] has changed because now we must not have the data for a long time. And therefore we have to do a lot of things in a technical way to erase and all the things that we don’t need anymore... And therefore we have erased a lot of them and made some tools to eliminate all the unneeded data. So fewer data. Yes, but more specific and targeted to what we need in the business.”

Since GDPR is stringent on the specificities of the data types that a company can hold, its retention period, data deletion after a certain period, and other controls exposed to the data subjects, some interviewees expressed the complexities it creates in their systems, making it challenging for them to implement.

“[Regarding] the amount of data, we have changed a lot. We actually have a lot of de-validation or deletion tools that make sure that all this data is continuously deleted from our systems [...] and also those tools are very difficult, well [we], make sure that they are up to date and keep working and that they don’t delete anything they should not delete.”

Guidance. During the interviews, some interviewees mentioned that their companies provide clear instructions to employees on GDPR compliance. They have portals where employees can read about the necessary measures to be taken when they are enabling GDPR in their work process.

“We have a ‘Blackboard’ [a portal] in the company. And then on [that] Blackboard, we have a specific area which is dealing with the GDPR and there are information papers for all the people and they can go in and see what do they need to look at and to know about.”

Some companies also facilitate the opportunity to avail the consultation from a privacy expert in case the employee has doubts around the implementation process.

“We have an internal ticket handling system where people can forward their GDPR related issues or security breaches, and other things to the GDPR group. And people use that to ask questions.”

Still, the employees were expected to come forward and ask for clarifications themselves if they experienced problems. A developer articulated:

“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?”

At the same time, some interviewees talked about the lack of support for GDPR-related matters in their companies. One developer stated:

“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”

Some mentioned that there is a general lack of clear frameworks for the implementation of GDPR. It is difficult for their companies to comprehend and implement GDPR, as their companies are small in size and are operating without the support of a dedicated legal department. A senior manager:

“We felt that the guidelines were either very, very strict or very, very open to interpretation. So like everyone else, we were thinking, how do we approach this?”

Burden on resources. It was evident in the interviews, that GDPR compliance requires a significant amount of time, money and expertise. A senior manager commented that smaller companies without such resources would not be able to properly ensure 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.”

Furthermore, some of the changes that were implemented for compliance reasons, such as the requirement to provide cookie notice on the company’s website were perceived to be annoying and time-consuming rather than useful.

“We have to wait a few weeks actually to get the texts ready and to make sure that the lawyers could see, what we were doing was correct. And all this kind of stuff annoys me a bit. ”

4.3 Effects of Pandemic

The survey results have shown that a vast majority of the participants had experience with remote work during the pandemic. As shown in Figure 6, a large part of them (38% of respondents from large companies and 47% from SMEs) were already working remotely even before the pandemic.

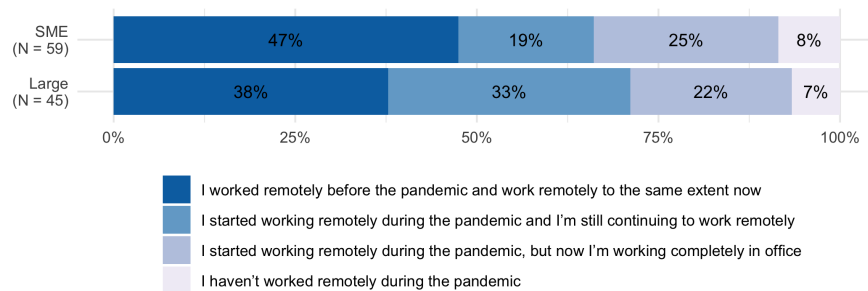


Figure 6. Remote work experience before and during the pandemic among the survey participants.

The responses furthermore show that the majority of the respondents (85% of all the participants who answered the question) did not experience issues with the security and privacy policies introduced for remote work, finding these policies either not challenging at all or mostly not challenging (Figure 7).

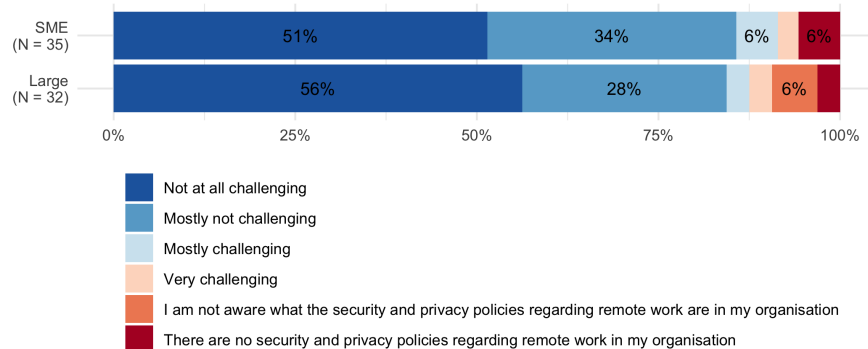


Figure 7. Experience with remote work policies among the survey participants.

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 8).

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

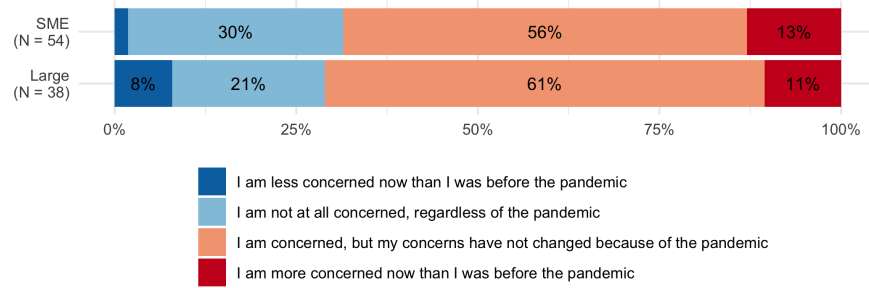


Figure 8. Pandemic-related security and privacy concerns among the survey participants.

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. A senior manager stated:

“We see that is okay to be working from home. We were also doing it before the pandemic. So for us, it was just a matter of scaling up for some of our systems to be able to accommodate the number of people working from home that was increasing dramatically.”

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.

“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.”

Increased security. A few interviewees mention that their companies have implemented some changes to their security policies, such as mandating VPN usage when accessing the company data or forbidding the use of personal devices for work purposes. A security expert commented:

“I think our biggest line of defense is the VPN planning [which] includes a firewall. So the corporate PC on the local network is isolated from the local event and you can only connect by the VPN.”

A security expert commented on the pandemic’s role in bringing awareness to cybersecurity in general, mentioning that it served as a catalyst for implementing some of the security controls that would otherwise take more time.

“The pandemic has accelerated our deployment of some security technologies that might otherwise have taken longer to deploy. So I think it’s actually, in some ways benefited us and that we’ve now got some more improved remote access solutions and an improved level of security for remote workers than we would have done otherwise.”

Working from home is more secure. Another perspective that arose from interviews was the notion that working from home had in some aspects fewer security issues, due to limited physical access to company devices and sensitive documents.

“I would say I’m more afraid [when] I’m actually working at the office and leaving my laptop there. When the cleaning personnel comes in or some other guests are in [there] they could physically do something to my laptop. I think that’s a bigger risk to manage [than] leaving the laptop at home.”

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 [...] it’s not like anyone is keeping eyes on you or something like that.”

5 DISCUSSION

In this section, we reflect on our findings, identifying recurrent nuances throughout the different themes investigated in our studies, as well as discuss the limitations of our work.

5.1 Recurrent nuances

As presented in Section 4, particularly prominent was the mention of (i) *trust*, which could also be perceived as a cultural characteristic of the demographics in our sample, and the emerging nuances of (ii) *lack of awareness* of security and privacy risks, as well as (iii) *lack of knowledge* about the appropriate countermeasures. We elaborate on these below.

5.1.1 Trust

Trust appeared as a recurring nuance in many of the themes after analyzing the data from the ethnographic interviews. When it comes to enabling security and privacy in the development cycle, senior managers in many organizations often choose to “trust” the developers adopting a “let developers handle it” mindset, assuming that the developers know all that needs to be done. Another occurrence of trust as an emerging nuance was apparent while evaluating the GDPR influence. Senior managers trust the developers in their organizations to be compliant with the GDPR while developing a new product or working on versioning an existing one. They feel that in case the developers find it challenging, they will come forward and ask for help—an approach that becomes a challenge if the developers themselves do not recognize their need for support, do not know whom exactly they could ask for such support or are otherwise reluctant to admit that they are struggling. Similarly, trust appeared as an integral part of the pandemic theme, where it was evident that Danish organizations trust their employees with their network security at home and feel assured that the employees are taking good care of the company’s data and the physical devices.

As the findings from the interviews suggest, such prevalence of trust, in terms of social cohesion (cf. Section 1), might 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 [Larsen \(2013\)](#); [Sønderskov and Dinesen \(2014\)](#). Such trust can have positive implications on the application of security and privacy measures. For example, employees’ trust in the security team reduces the risk of not accepting or fighting against security policies and regulations—an issue that has been identified in previous studies in other cultural contexts [Ashenden and Sasse \(2013\)](#); [Haney and Lutters \(2018\)](#). Furthermore, in cases where employees tend to trust their superiors and colleagues well enough to ask for help or report problems without fear of repercussions, issues in security and privacy measures are more likely to be identified and remedied promptly, provided that such transparent communication takes place. At the same time, trust that is misplaced can hurt security, especially without sufficient controls and accountability measures. Such an approach to security and privacy could lead to the compartmentalization of the implementation of security and privacy measures, potentially leading to a situation in which everyone feels that security and privacy measures are implemented regularly, whereas, in reality, it is left to developers to incorporate as they see fit.

5.1.2 Lack of awareness

Lack of awareness and concern about security and privacy risks has manifested in different contexts in our study. Most notably, our investigation has shown that the pandemic did not lead to a significant increase in concerns or changes in security and privacy-related workflows, despite experts, both in Denmark and internationally, claiming an increased level of cyber-attacks and privacy issues [Danish Centre for Cybersecurity \(CFCS\) \(2020\)](#); [INTERPOL \(2020\)](#). Many of the participants in both interviews and surveys showed no concerns with security, saying that it creates no additional risks for them, as compared

to the situation before the pandemic. For some interviewees, usage of cloud and cloud-based solutions was enough to ensure security for their landscape.

The lack of awareness has furthermore manifested in the discussion of changes to data protection policies required for GDPR compliance. As such, especially on the senior management level, many were not aware of what can potentially constitute personal data, and therefore subject to the GDPR. They were oblivious to the risk of non-compliance, which in turn creates a self-feeding circle in which the lack of awareness gets perpetuated across senior managers and developers.

The insufficient awareness or concern could easily correlate with the under-prioritization of security and privacy measures in the company, which has also shown by our studies (e.g., no defined budget for security, prioritize feature development over security). As such, the participants mentioned the perception of security needs as a distraction from the “real” business requirements and feeling that the senior management does not have it on their agenda, hindering regular updates of cybersecurity measures and eventually sacrificing security and privacy to cost optimization over the long period.

5.1.3 Lack of knowledge

Lack of knowledge on the appropriate security and privacy measures appeared as a ubiquitous nuance across multiple themes. As such, the developers commented on the unavailability of training to enhance their security and privacy skill-set, which is even more troubling in case the senior management feels that it is the responsibility of the developers to handle the security and privacy tasks on their own. Such a lack of necessary knowledge was also mentioned with regards to the GDPR compliance, with employees in many companies not being familiar with the procedural requirements to receive clarification on GDPR. Similarly, the existing GDPR guidelines were perceived to be too vague, highlighting once again the need for better guidance.

While providing more security education measures, including training, might seem like a solution, there are also significant challenges with ensuring the effectiveness of such measures, such as their known problems of failing to engage the participants or provide them with knowledge and skills they can successfully apply outside of the training context [Bada et al. \(2015\)](#). 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, even if good training were available, in absence of clear management support and prioritization of security, the developers would have no incentive or desire to attend the training nor to acquire the needed knowledge otherwise.

5.2 Limitations

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 coding 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.

Another challenge we experienced was the pandemic restrictions, which forced all the interviews to be conducted over video via MS-Teams rather than on-premise with the interviewees. The restriction over travel and in-person interactions might have affected the outcome of the interviews (e.g., missing non-verbal communication clues due to the shortcoming of online interviews versus face-to-face ones).

6 CONCLUSIONS

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 [Bird \(2016\)](#); [Kim et al. \(2016\)](#) and Site Reliability Engineering [Beyer et al. \(2016\)](#), that already embrace change and security in their core process. While the interest in this kind of methodologies [Forsgren et al. \(2018\)](#) 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 [European Union Agency for Cybersecurity \(ENISA\) \(2019b\)](#).

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 [European Union Agency for Cybersecurity \(ENISA\) \(2019a\)](#). 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 [European Union Agency for Cybersecurity \(ENISA\) \(2020\)](#), 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 [European Union Agency for Cybersecurity \(ENISA\) \(2019a\)](#) 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* [Thomas et al. \(2018\)](#) 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

- Acar, Y., Backes, M., Fahl, S., Garfinkel, S., Kim, D., Mazurek, M. L., and Stransky, C. (2017a). Comparing the usability of cryptographic apis. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 154–171.
- Acar, Y., Fahl, S., and Mazurek, M. L. (2016). You are not your developer, either: A research agenda for usable security and privacy research beyond end users. In *2016 IEEE Cybersecurity Development (SecDev)*, pages 3–8.

- Acar, Y., Stransky, C., Wermke, D., Weir, C., Mazurek, M. L., and Fahl, S. (2017b). Developers need support, too: A survey of security advice for software developers. In *2017 IEEE Cybersecurity Development (SecDev)*, pages 22–26.
- Al Qahtani, E., Shehab, M., and Aljohani, A. (2018). The effectiveness of fear appeals in increasing smartphone locking behavior among saudi arabians. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pages 31–46.
- Ashenden, D. and Sasse, A. (2013). Cisos and organisational culture: Their own worst enemy? *Computers & Security*, 39:396–405.
- Assal, H. and Chiasson, S. (2018). Security in the software development lifecycle. In *14th Symposium on Usable Privacy and Security*, pages 281–296.
- Bada, M., Sasse, A. M., and Nurse, J. R. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? In *International Conference on Cyber Security for Sustainable Society*.
- Balebako, R., Marsh, A., Lin, J., Hong, J. I., and Cranor, L. F. (2014). The privacy and security behaviors of smartphone app developers.
- Beautement, A., Sasse, M. A., and Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. In *Proc. of the 2008 New Security Paradigms Workshop*, pages 47–58.
- Beyer, B., Jones, C., Petoff, J., and Murphy, N. R. (2016). *Site Reliability Engineering: How Google Runs Production Systems*. O’Reilly Media, Inc., 1st edition.
- Bird, J. (2016). *DevOpsSec: Securing Software Through Continuous Delivery*. O’Reilly Media, Incorporated.
- Blythe, J. M., Coventry, L., and Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees’ security behaviors. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS 2015)*, pages 103–104.
- Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101.
- Brinkmann, S. and Kvale, S. (2017). *The SAGE Handbook of Qualitative Research in Psychology*. Sage.
- Coopamootoo, K. P. (2020). Dis-empowerment online: An investigation of privacy-sharing perceptions and method preferences. In *International Conference on Financial Cryptography and Data Security*, pages 71–83. Springer.
- Danish Centre for Cybersecurity (CFCS) (2020). 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/>. (accessed: February 2021).
- Das, S., Hyun-Jin Kim, T., Dabbish, L. A., and Hong, J. I. (2014). The effect of social influence on security sensitivity. In *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS 2014)*, pages 143–144.
- Delamont, S. and Atkinson, P. (2018). *The sage handbook of qualitative research ethics*. Sage.
- European Union Agency for Cybersecurity (ENISA) (2019a). Cybersecurity culture guidelines: Behavioural aspects of cybersecurity. <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity>. (accessed: February 2021).
- European Union Agency for Cybersecurity (ENISA) (2019b). Enisa advancing software security in the eu. <https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework>. (accessed: February 2021).
- European Union Agency for Cybersecurity (ENISA) (2020). Enisa threat landscape - the year in review. <https://www.enisa.europa.eu/publications/year-in-review>. (accessed: February 2021).
- Forsgren, N., Humble, J., and Kim, G. (2018). *Accelerate: The Science of Lean Software and DevOps Building and Scaling High Performing Technology Organizations*. IT Revolution Press, 1st edition.
- Fruhlinger, J. (2020). Equifax data breach faq. <https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html>. (accessed: February 2021).
- Garfinkel, S. L. (2012). The cybersecurity risk. *Communications of the ACM*, 55(6):29–32.
- Green, M. and Smith, M. (2016). Developers are not the enemy!: The need for usable security apis. *IEEE Security Privacy*, 14(5):40–46.
- Haney, J. M. and Lutters, W. G. (2018). ”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 (SOUPS 2018)*, pages 411–412.
- Haney, J. M., Theofanos, M., Acar, Y., and Prettyman, S. S. (2018). ” 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*, pages 357–373.
- INTERPOL (2020). 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>. (accessed: February 2021).
- Ivankova, N. V., Creswell, J. W., and Stick, S. L. (2006). Using mixed-methods sequential explanatory design: From theory to practice. *Field methods*, 18(1):3–20.
- Kim, G., Debois, P., Willis, J., and Humble, J. (2016). *The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations*. IT Revolution Press.
- Kulyk, O., Reinheimer, B., Aldag, L., Mayer, P., Gerber, N., and Volkamer, M. (2020). 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.
- Larsen, C. A. (2013). *The rise and fall of social cohesion: The construction and de-construction of social trust in the US, UK, Sweden and Denmark*, volume 1. Oxford University Press.
- Mayer, P., Kirchner, J., and Volkamer, M. (2017a). A second look at password composition policies in the wild: Comparing samples from 2010 and 2016. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 13–28.
- Mayer, P., Kunz, A., and Volkamer, M. (2017b). Reliable behavioural factors in the information security context. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, pages 1–10.
- Michalec, O., van der Linden, D., Milyaeva, S., and Rashid, A. (2020). 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*, pages 301–317. (accessed: February 2021).
- Mori, K., Watanabe, T., Zhou, Y., Hasegawa, A. A., Akiyama, M., and Mori, T. (2020). Comparative analysis of three language spheres: Are linguistic and cultural differences reflected in password selection habits? *IEICE Transactions on Information and Systems*, 103(7):1541–1555.
- Palombo, H., Tabari, A. Z., Lende, D., Ligatti, J., and Ou, X. (2020). 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*, pages 205–220.
- Smith, J., Do, L. N. Q., and Murphy-Hill, E. (2020). Why can’t johnny fix vulnerabilities: A usability evaluation of static analysis tools for security. In *16th Symposium on Usable Privacy and Security*, pages 221–238.
- Sønderskov, K. M. and Dinesen, P. T. (2014). Danish exceptionalism: Explaining the unique increase in social trust over the past 30 years. *European Sociological Review*, 30(6):782–795.
- Spradley, J. P. (2016). *The ethnographic interview*. Waveland Press.
- Tahaei, M. and Vaniea, K. (2019). A survey on developer-centred security. In *2019 IEEE European Symposium on Security and Privacy Workshops*, pages 129–138.
- Thomas, T. W., Tabassum, M., Chu, B., and Lipford, H. (2018). Security during application development: An application security expert perspective. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–12.
- van der Linden, D., Hadar, I., Edwards, M., and Rashid, A. (2019). Data, data, everywhere: quantifying software developers’ privacy attitudes. In *Int. Workshop on Socio-Technical Aspects in Security and Trust (STAST)*.
- Volkamer, M., Gutmann, A., Renaud, K., Gerber, P., and Mayer, P. (2018). 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 ({SOUPS} 2018)*, pages 1–11.
- Weir, C., Hermann, B., and Fahl, S. (2020). From needs to actions to secure apps? the effect of requirements and developer practices on app security. In *29th Security Symposium ({USENIX} 20)*, pages 289–305.

Xiao, S., Witschey, J., and Murphy-Hill, E. (2014). 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*, page 1095–1106.

A SURVEY QUESTIONNAIRE

We present the questions of the survey. For space reasons, we are reporting only those questions in this questionnaire that are directly relevant to the research questions presented in this paper. The full questionnaire is available online (reference omitted for double-blind reviewing).

Survey questions

1. What are your responsibilities in your organization? *all, multiple choice, mandatory*

- IT security related tasks
- Privacy/data protection related tasks
- Software development related tasks
- Management related tasks
- IT administrator related tasks
- Others, please specify

2. Which industry/ sector is your organization in? *all, multiple selection, optional*

- Media & Publishing
- Health care
- Financial services
- Software development
- Entertainment & Music
- Education
- Manufacturing
- Consultancy
- Other, please specify

3. Do you have a yearly budget allocated for Security & Privacy needs? *all, single choice*

- Yes
- No

4. If YES, what percentage of your IT budget does it constitute? *all, single choice*

- less than 1%
- 1%-3%
- 3%-5%
- More than 5%
- We don't have a defined security budget

- Not sure
5. How do you measure your cyber-security and privacy readiness? *Management, Sec, Priv, multiple choice, optional*
- We rely on the IT solutions derived from established security and privacy standards
 - Internal method/framework/procedure
 - We do not have any measure
6. If you rely on established standards to measure your cyber-security and privacy readiness, which ones do you use? *Sec, Priv, multiple choice, optional*
- ISO/IEC 27001
 - ISO 27701
 - Center for Internet Security - Critical Security Controls (CIS CSC)
 - Control Objectives for Information and Related Technologies (COBIT)
 - Security for Industrial Automation and Control Systems (ANSI/ISA-62443)
 - NIST Special Publication 800-53 (NIST SP 800-53)
 - Payment Card Industry Data Security Standard (PCI DSS)
 - UK National Cyber Security Centre (NCSC) 10 Steps
 - UK National Health System (NHS) Digital Data Security and Protection Toolkit
 - Cyber Assessment Framework (CAF)
 - Information Assurance Small and Medium Enterprises (IASME)
 - Host-Based Security System (HBSS)
 - Structured Threat Information Expressions (STIX)
 - Assured Compliance Accreditation Solutions (ACAS)
 - Cyber Federated Model (CFM)
 - Other, please specify
7. Has anything in the security and privacy practices of your organization changed since the introduction of the GDPR regarding the following aspects? *Each of the subsections have yes, no & not sure options.*
SecPriv, optional
- Which data is collected by the organization
 - How the data subjects are informed about data collection
 - How the collected data is stored
 - How the collected data is shared
 - How the collected data is deleted
 - Which controls are provided to the data subject

8. What is your experience with security and privacy awareness training at your company *all, single choice, optional*
- I participated in training and found them useful
 - I participated in training and did not find them useful
 - I heard about available training but did not participate in them
 - I am not aware of any security and privacy training at my organization
 - Prefer not to answer
9. When do you integrate security/privacy into your development practices? *Sec, Dev, single choice, optional*
- Early, from the initial phases
 - Continuously during the development cycle
 - After the fact
 - Not at all
 - Other, please specify
10. Are the methods/practices /standards for security and privacy protection in the development processes, always followed in all the situations? *Developer, Not Sec, Not priv, optional, single choice*
- Yes
 - No
 - Not sure
11. If NO, why? *Developer, Not Sec, Not priv, optional, single choice*
- They are not always compatible with the functional requirements of our products
 - I don't believe that they are helpful in protecting security and privacy
 - They interfere with other workflows of my tasks and responsibilities
 - They are too complicated to follow exactly as defined
 - We don't have time or resources to follow them exactly as defined
 - The management does not think they should be followed exactly as defined
 - Other, please specify
12. To what extent has pandemic affected your working style, in particular remote working? *all, single choice, optional*
- I worked remotely before the pandemic and work remotely to the same extent now
 - I started working remotely during the pandemic, but now I'm working completely in office
 - I started working remotely during the pandemic and I'm still continuing to work remotely
 - I haven't worked remotely during the pandemic

13. If you started working remotely during the pandemic, how challenging do you find it to comply to the security and privacy policies of your organization regarding remote work? *all NOT Sec & NOT Priv, single choice, optional*

- Not at all challenging
- Mostly not challenging
- Mostly challenging
- Very challenging
- There are no security and privacy policies regarding remote work in my organization
- I am not aware of the security and privacy policies regarding remote work in my organization

14. How did your concerns regarding security and privacy in your organizations change because of the pandemic? *all NOT Sec & NOT Priv, single choice, optional*

- I am more concerned now than I was before the pandemic
- I am concerned, but my concerns have not changed because of the pandemic
- I am less concerned now than I was before the pandemic
- I am not at all concerned, regardless of the pandemic

B INTERVIEW GUIDE

In this section, we present the Interview Guide that we used for the ethnographic interviews in our study.

Opening questions *Purpose: To make the participant comfortable with the situation and present him/herself.*

1. To begin with, please start by telling me about yourself?
 - What's your role
 - Day-to-Day life at work
 - How long have you been working in this role and organization?
2. Do you think about security and privacy in your regular work?
 - Is yes: How often and for what?
 - If no: Why not?
3. What is most important to you when it comes to security and privacy? (e.g. specific aspects of technology, business needs and constraints, etc.)
4. How do you incorporate security and privacy in your daily work life?
5. Looking 2–3 years into the future, how would you expect the security and privacy needs to evolve?

Questions to explore perceptions, motivation, perceived responsibility (outsourcing), and stress

Purpose: To encourage the participant to share his/her perspective and realities of motivation and stress related to security usage in work life. Also, understanding the perceived responsibility of security and privacy when it is outsourced.

1. Do people in your organization feel that security and privacy are important?
2. Do you feel that there are risks that are mitigated by security and privacy?
3. How are security and privacy practices handled in your organization? (Outsourcing/SaaS/Insurance)
4. Do people face challenges when it comes to security and privacy(Implementing/ daily usage/ operations/ etc.)
5. Are there enough measures taken by your company to mitigate security and privacy problems?
 - If yes: please describe
 - If no: Why not?
6. What do you think can be done to improve the situation?

Questions to explore low adoption of continuous Sec adoption in the Development cycle

Purpose: To understand the factors that inhibit the developers to do continuous integration of security in development cycles.

1. When do you typically implement security and privacy in your development cycle?
2. In your organization, do you have clear guidelines on precisely what methods and processes should be adopted to incorporate security in the development cycle? Could you broadly describe the methods and processes?
3. Do you personally believe that your development cycles are including security considerations to the extent that they should?
4. Do you get sufficient resources and training to enable this?
5. Do you follow Agile methodology in your development cycle? If so, do you think that Agile processes inhibit the developers to do continuous integration of security in development cycles?
6. Is management buy-in a contributing factor for this inhibition? According to you what role can management play in encouraging the adoption of security and privacy inclusion in development cycles?

Questions to explore on GDPR influence *Purpose: To encourage the participant to share their perspective on the influence of GDPR on the data collection.*

1. How has data collection behavior in your organization changed after GDPR?
 - What all has changed? Could you provide some examples?
2. When is the data-collection management planning done? Is it done early in the stage with proactive planning or post fact 'fixing'?
3. How do people in your organization feel about giving controls to data-subjects?
 - Do you have a well-defined approach for providing controls to data-subject?

Questions to explore the impact of Pandemic *Purpose: To understand the security concerns of the participants due to higher remote working in Pandemic*

1. How are people working in your organization? Are they more often in the office or prefer to work remotely?
2. How do people feel about security adoption in your organization, while they are working more remotely?
3. Has your organization crafted security policies to cover such a large-scale and sustained remote working condition?
4. What all changes have been done in the security setup by your organization? Can you describe some of them?