Assessment on the Status of Cybersecurity in Denmark

Final Report

Dated: 15 December 2020

ITU

SDU

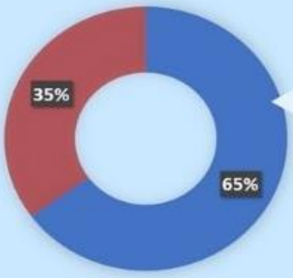
University of Southern Denmark

Assessment on the Status of CyberSecurity in Denmark

Selected statistics and quotes from participants of an exploratory multi-method study (survey and ethnographic interviews) on existing cybersecurity practices in Danish companies

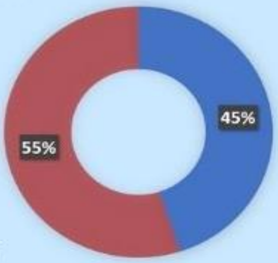
CYBERSECURITY TRAINING

"I was once or twice to some compliance and stuff [cybersecurity training], but my management was not so pleased about [the time investment]"



Know about training opportunities

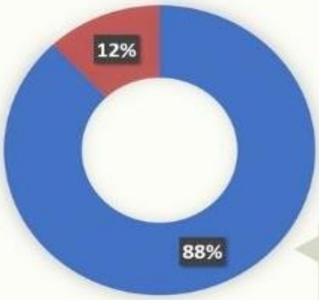
Don't find existing trainings useful



"if you ask any developer... do you have specific training on how to develop software in a secure manner? I think he would say, no"

CYBERSECURITY & PANDEMIC

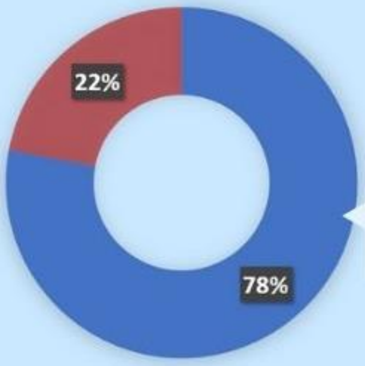
"And in Denmark it is like, we trust people to take their laptop home and we don't expect them to take any company data and stealing..."



No increased concerns due to the pandemic

"The pandemic became a kind of catalyst to accelerate the implementation of some of the security controls that are necessary to manage the risk"

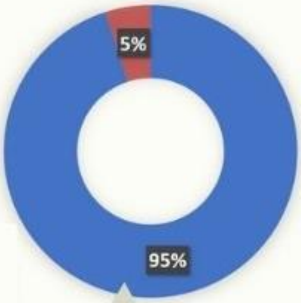
GDPR



Made changes for informing data subjects

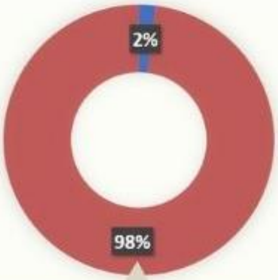
On system changes due to GDPR:
"Maybe something has changed ... basically something like the [usage of the] cookies ..."

SECURITY IN DAILY LIFE



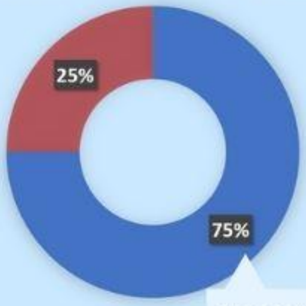
Aware of security policies

"but when you look at your daily work and the requirements...security is always never mentioned. It is something that you kind of have to think through the whole development process [..], if you want to do it right"



Had or saw potential insecure behaviors

SECURITY IN DEVELOPMENT



Usage of Encryption, Testing, and Permission Management

"I don't think agile processes inherently prohibit [security]"

"[security in development] is not really something that the organization ... really encourages. And it's not something they really care about"

The ASCD project has been funded by the Danish Centre for Cybersecurity

Research within the project has been performed by the IT-University of Copenhagen and the University of Southern Denmark

Table of Contents

1 Introduction

To stay competitive in the global market, organizations rely on software which enables them to deliver and maintain an ever-growing set of functionalities in their products. A side-effect of this phenomenon is an increased complexity of the software architecture and team coordination, which heavily impacts on Cybersecurity, i.e., the guarantees that a company can deliver the security and privacy of their applications.

The Assessment on the Status of Cybersecurity in Denmark (ASCD - https://ascd.dk) project aims to study and report on the existing Cybersecurity and privacy protection practices used in Danish organizations (large and small-medium ones), identifying the most important challenges that developers and users in Denmark face in developing secure and privacy-preserving solutions. ASCD is a research project conducted by the IT University of Copenhagen and the University of Southern Denmark and funded by the Danish Centre for Cybersecurity.

While existing studies have been performed to investigate globally the current status of awareness and use of secure and privacy-preserving methods among software development companies (e.g., Status of Software Security [1], Accelerate State of DevOps [2]), researchers have also shown that geographical and cultural aspects tend to play a significant role in determining the security and privacy-related practices and awareness of the population [3]. In the ASCD project we therefore focus on the security and privacy awareness and practices in Danish organizations complementing other existing studies such as "IT-sikkerhed og datahåndtering i danske SMV'er" [4], "Digitaliseringsstyrelsen Og Erhvervsstyrelsen For-Analyse Af Danskernes Informationssikkerhed" [5], "Digital Tryghed – de væsentligste digitale udfordringer for forbrugerne i Danmark" [6], and "Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark" [7] but with the viewpoint of the development of secure software and a mix of quantitative and qualitative approach. In particular, by adopting the explanatory sequential mixed method design approach [8], after performing an initial investigation of the related literature available at https://ascd.dk/results/literature_review.pdf we performed:

- a survey aimed at finding out the extent to which Cybersecurity practices are employed by software development companies located in Denmark, as well as awareness about security and privacy risks, user concerns, and measures to protect against them among the developers;
- a follow-up qualitative study, involving interviews at selected Danish organizations focusing on the investigation of the mental models of security and privacy among the developers [9], as well as identifying challenges they face in adhering to best practices of security and privacy protection and in ensuring trust among their customers.

To the best of our knowledge, this is the first study to conduct a quantitative survey followed by in-depth interviews on the interplay between the COVID-19 pandemic and Cybersecurity (at the time of writing, Denmark is still experiencing the second COVID-19 pandemic wave).

In this document we report on the methodology followed to conduct our study, and the results of our research. In Section 2 we describe the survey methodology and the quantitative results obtained. In Section 3, we detail the interview design process and the qualitative analysis of the transcripts. In Section 4, we discuss the integrated analysis summarizing our finding. We conclude with relevant recommendations emerged from the study, in Section 5.

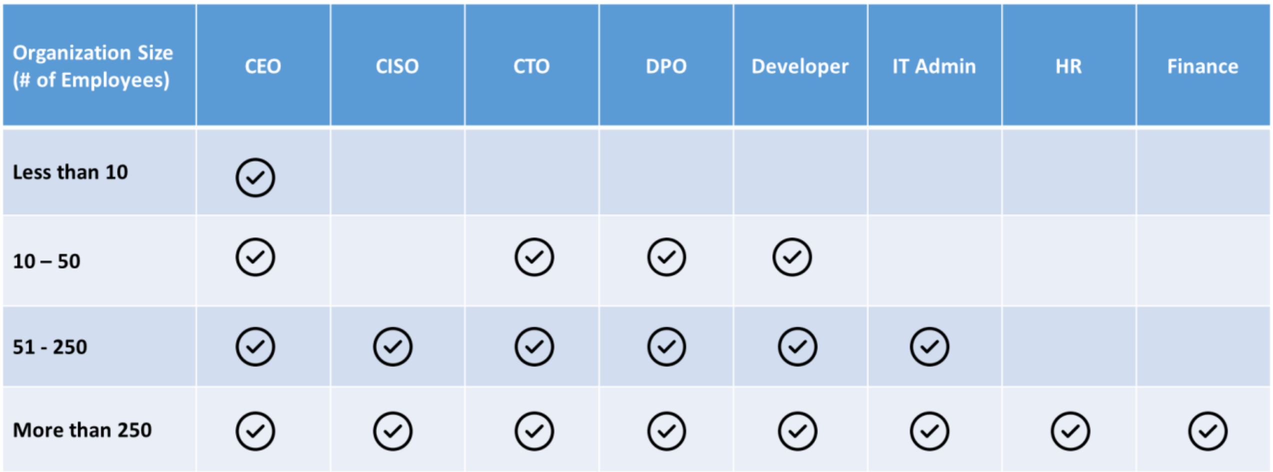
2 Survey

In this section we describe the survey and the results obtained. We start by defining the target group of the survey before presenting its structure. We then conclude by discussing the results obtained.

2.1 Target group

For our survey we targeted all the organizations which operate in Denmark and have presence in Nordics and EU considering diverse sectors going from software development and consultancies to pharma, retail, finance, and manufacturing to better understand the underlying nuances of security and privacy.

The target organizations were initially categorized in four subcategories depending on the size and ranging from micro-organization (with less than 10 employees) to large organizations (with more than 250 employees). In each category of organization around eight relevant stakeholders were identified to send the survey. These eight stakeholders were: CEO, CTO, CISO, DPO, developers, IT admin, HR, Finance.



Organization Size (# of Employees)	CEO	CISO	CTO	DPO	Developer	IT Admin	HR	Finance
Less than 10	✓							
10 – 50	✓		✓	✓	✓			
51 - 250	✓	✓	✓	✓	✓	✓		
More than 250	✓	✓	✓	✓	✓	✓	✓	✓

Figure 1: Stakeholder roles target in relation to company size

Irrespective of the size of the organization, the survey was sent to the CEO of the company, requesting her/him to disseminate to the other relevant stakeholders. Figure 1 depicts the relevant stakeholder in relation to the company size in which we were interested. This mapping was generated by considering the likelihood that companies of different sizes had the targeted stakeholder role in their organization.

In order to maximize the reach-out to the relevant stakeholder roles in the diverse size and industry sectors of the organizations, five different channels were leveraged:

1) Social media,
2) Trade bodies,
3) Startup accelerators,
4) Internal network of the project team members universities,
5) Media publications.

2.2 Survey structure and questions

The aim of the survey was to get initial insights into security- and privacy-related practices in organizations. Namely, we looked at the following topics:

- Security management and standards from the point of view of security experts, IT administration or management, including challenges in adhering to these standards
- The integration of security into development methods, from the point of view of software developers
- The integration of GDPR in organizations, from the point of view of security and privacy experts
- General perception of security awareness, security policies, behavior, reporting and available training, from the point of view of employees in all roles
- Pandemic impact on security, from the point of view of all employees

At the beginning of the questionnaire, the participants were asked about their role in the organization, being able to select among the following list of roles:

- Management related
- IT-security related
- Privacy/data-protection related
- Software-development related
- IT-administration related tasks
- “other” option

The participants were encouraged to select different roles, if they believed their combination described their position and their responsibilities in the organization the best. The questions the participants were shown depended on the role they selected, e.g., questions about the specifics of the software development processes were only shown to the participants who selected software-development related tasks as their role.

We aimed at a survey requiring 15/20 minutes to be completed, discouraging some of the participants. Two runs of pretest were conducted by letting Cybersecurity experts, managers, and non-Cybersecurity experts residing outside Denmark take the survey, to validate the clarity of the questions, its duration, and cover all the possible role selections.

The final survey encompasses 36 questions, among which 8 general questions were asked to all the participants while others were asked based on the roles selected by the participants.

The full questionnaire from the survey is available at https://ascd.dk/results/survey_questions.pdf. The advertisement for the survey was conducted in two phases. An initial one at the end of June 2020 before the holiday season and at the beginning of August at the end of the holiday season.

The data collection started on 19th of June until the beginning of November. The data analysis instead happened in multiple stages, from the mid-August till beginning of December.

2.3 Survey analysis

We consider complete responses, which include answers from a total of 107 participants, of which 47 from large organizations (more than 250 employees) and 60 from small and medium-sized enterprises (SMEs) (250 or less).

We exclude the responses from participants who started filling out the questionnaire but dropped out at some point, not reaching the last questionnaire page (253 participants). We also exclude questions with a small number of responses (<20) from the analysis.

In the following, we provide a broken-down explanation, reporting the distinct figures relative to large and small-medium enterprises in case there were at least 20 responses from each one of these two categories. For questions that had less than 20 responses from participants in either large organizations or SMEs, we report the data in aggregated form.

In the subsections below we describe the results of the survey on each topic outlined in section 2.3, starting from the general description of our sample demographics.

2.3.1 Sample demographic

Table 1 shows the breakdown of the survey participants according to their role in the company. Most of the responses were from participants in management roles, IT-security related roles or software development related roles (the participants could select several roles).

	250 and less (SMEs)	More than 250 (large companies)
Management related tasks	38	14
IT-security related tasks	24	19
Privacy/data protection related tasks	15	8
Software development related tasks	18	18
IT administrator related tasks	21	11
Other	6	11

Table 1: Roles of the participants

Table 2 and Table 3 further summarise the industry sector of respondents' organisations (the respondents were able to choose more than one option), the geographical location of the organisation (the respondents were able to choose more than one option). The participants in a management role were asked about the annual turnover of the organisation, summarised in Table 4.

	250 and less (SMEs)	More than 250 (large companies)
Media & Publishing	0	2
Health care	1	5
Financial services	3	6
Software development	20	8
Entertainment & Music	1	1
Education	4	5
Manufacturing	8	6
Consultancy	19	13
Life Sciences and Pharmaceuticals	2	3
Insurance	2	4
Other	17	17

Table 2: Industry sectors of participants' organizations

	250 and less (SMEs)	More than 250 (large companies)
Denmark	57	44
Other Nordic countries	15	24
Other EU countries (non-Nordic)	14	24
Non-EU countries	6	18

Table 3: Regions in which the participants' organizations have branches

	250 and less (SMEs)	More than 250 (large companies)
500K - 500M	27	2
500M - 1B	1	1
Less than 500k	3	0
More than 1B	1	8
Not sure	3	3

Table 4: Annual turnover of the respondents' organizations (in DKK)

2.3.2 Security management and standards

This subsection describes the results of the survey on the topics of security management, including the allocated Cybersecurity budget, use of security and privacy standards and frameworks, deviations from following the standards, incident response and outsourcing.

2.3.2.1 Cybersecurity budget

Among the respondents who answered the question about their security and privacy budget (management, IT security and privacy/data protection roles, 72 participants in total, 47 from large companies and 25 from SMEs), only 26% of SMEs indicated having a dedicated Cybersecurity budget, compared to 68% in large companies (**Figure 2**).

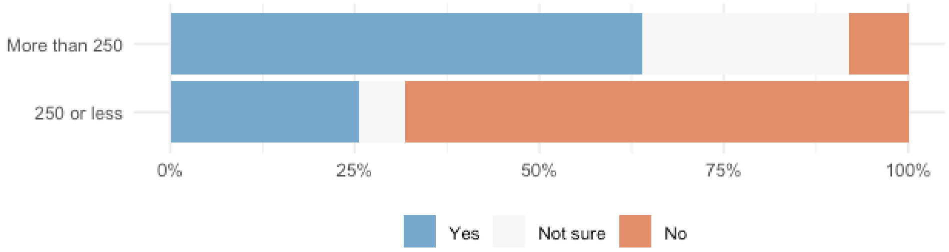


Figure 2: Organizations having an allocated Cybersecurity budget.

2.3.2.2 Use of security and privacy standards

Participants with either a management, IT-security- or privacy/data-protection-related role (72 in total of them 47 in SMEs and 25 in large companies) were asked and have provided an answer about how they measure security readiness in their organisations (see **Figure 3**). Less than 60% of the participants (56% in large and 58% in small-medium enterprises) rely on existing security standards, either exclusively or in combination with internal measurements. A large share of the participants, especially in large companies (36%), reported to use internal measurement methods only, and 21%

of respondents in SMEs and 8% in large companies mentioned that they either do not measure security readiness at all, or are not sure about how they do this.

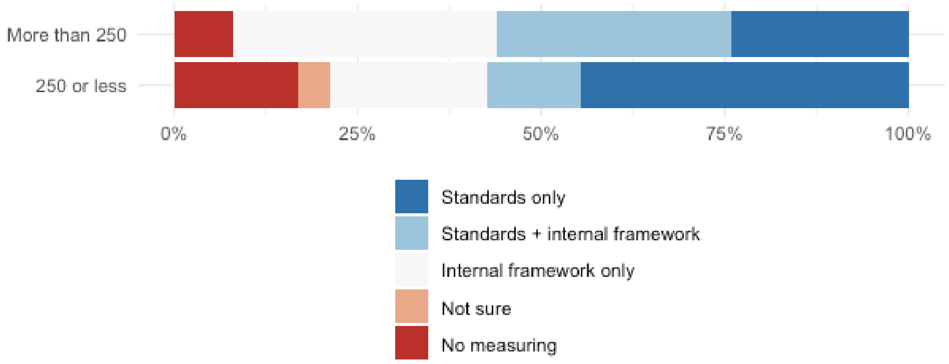


Figure 3: Methods for measuring security readiness.

The respondents in IT-security and privacy/data protection roles who answered to relying on an existing standard (a total of 21 respondents) were asked about the specific standards they used (selecting from a list of provided options, with a possibility to give an open-ended “other” answer). By far, the most mentioned standard was the ISO/IEC 27001 (see Figure 4).

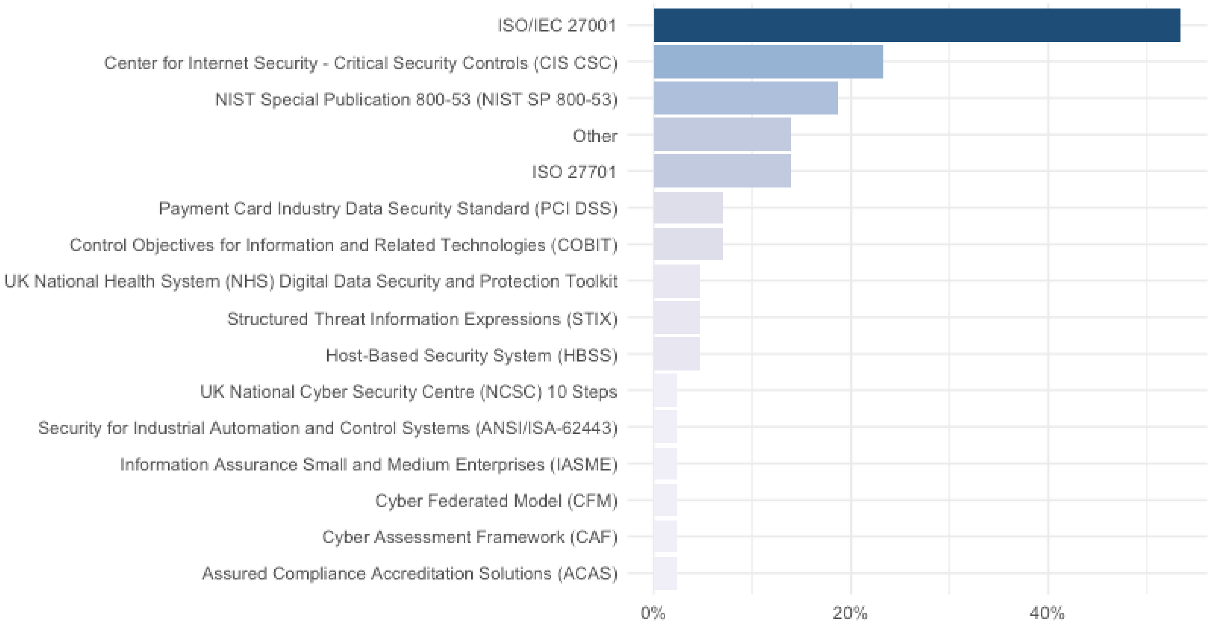


Figure 4: Use of established standards.

Figure 5 shows the distribution of answers from respondents in IT-security and privacy/data protection roles (43 participants, 20 from large companies and 23 from SMEs), when asked about how the security practices are defined in their organisation. The most common answer from the respondents from large organisations was that the practices are defined and improved based on previous experiences with projects (bottom-up), while the most common answer from the respondents from SMEs was that these practices are defined at the company level (top-down).

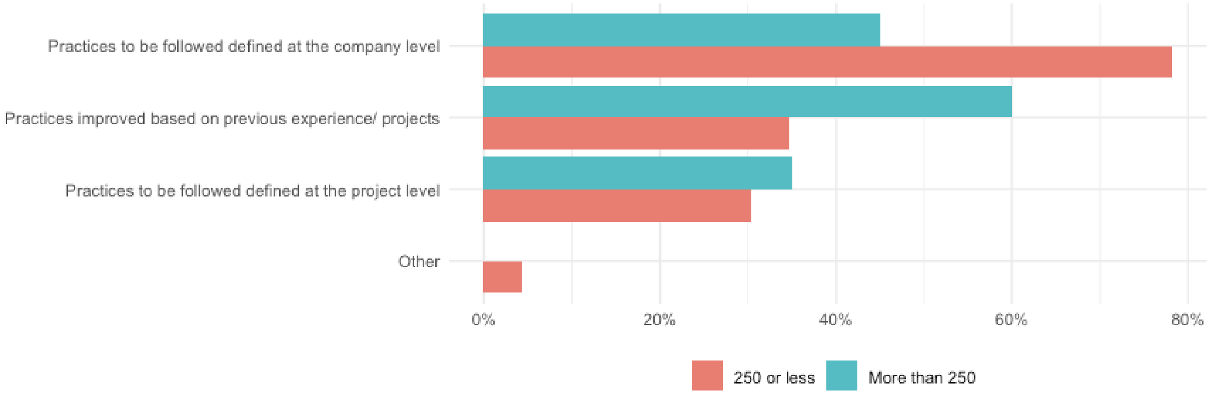


Figure 5: Definition of security procedures.

2.3.2.3 Deviations from standards

When the respondents with either an IT-security or a privacy-data-protection role were asked whether the security methods/standards/frameworks are always followed in all situations, out of the respondents who answered the question (42 participants in total, of them 23 from SMEs and 19 from large organisations), 48% answered negatively, and another 19% were not sure. The most common reasons for deviations (chosen among the provided closed options with a possibility to give an open-ended "other" answer) were the lack of resources, influence from the management, and interference with other workflows in the organisation. (Figure 6).

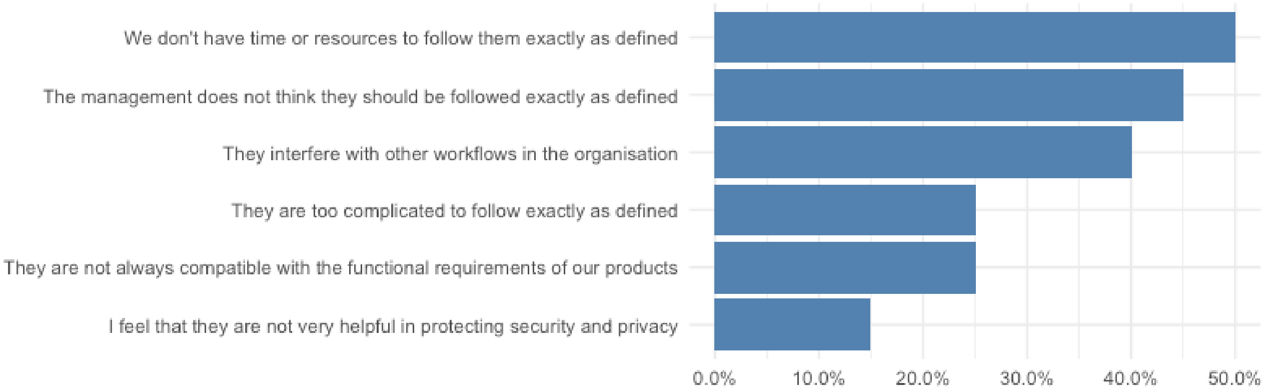


Figure 6: Reasons for deviating from standards and procedures.

2.3.2.4 Incident response

The responses provided by participants with IT-security and IT-administration roles (51 participants in total, of them 28 from SMEs and 23 from large companies) are summarised in Figure 7. The responses show that a variety of data is collected in case of Cybersecurity incidents in SMEs as well as in large companies, with the latter collecting more extensive data on the incidents.

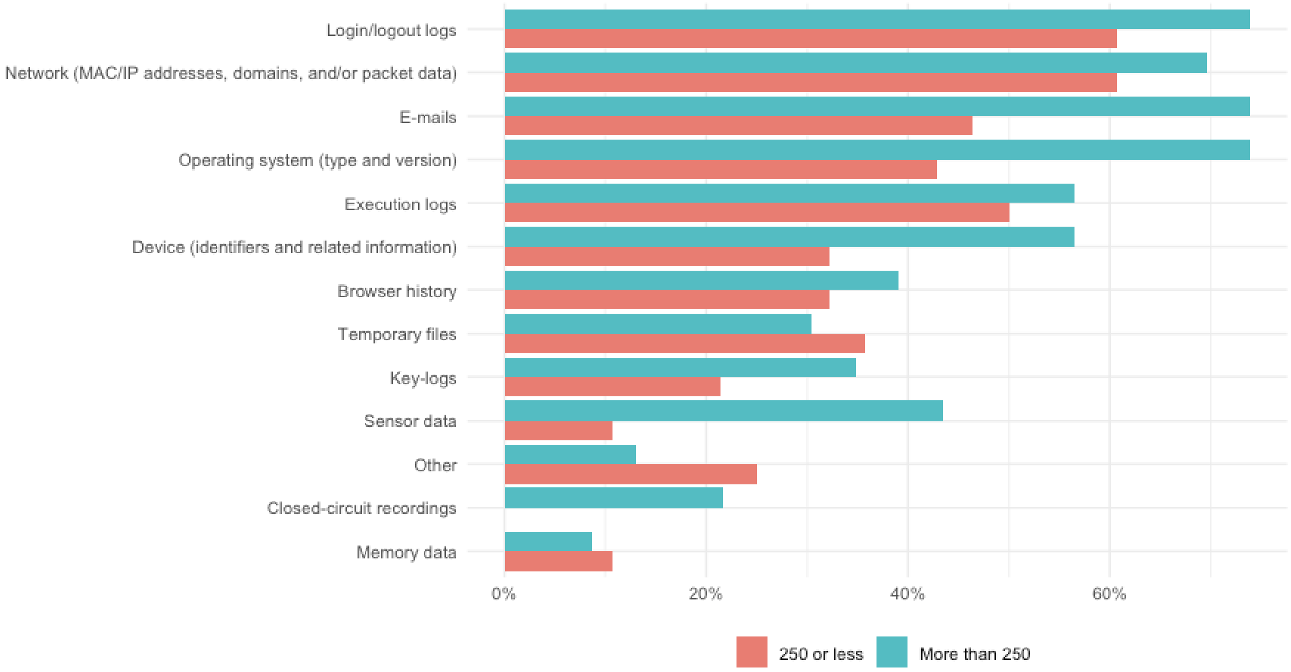


Figure 7: Data collected from security incidents.

2.3.2.5 Outsourcing

When asked about the extent to which their organisations outsource their IT systems, most of the respondents with IT-security, IT-administration or management roles (78 in total, 50 from SMEs and 28 from large organisations) mentioned outsourcing at least to some extent, see Figure 8. Nonetheless, a large share of respondents reported that they handled IT security internally (38% in SMEs and 61% in large organisations).

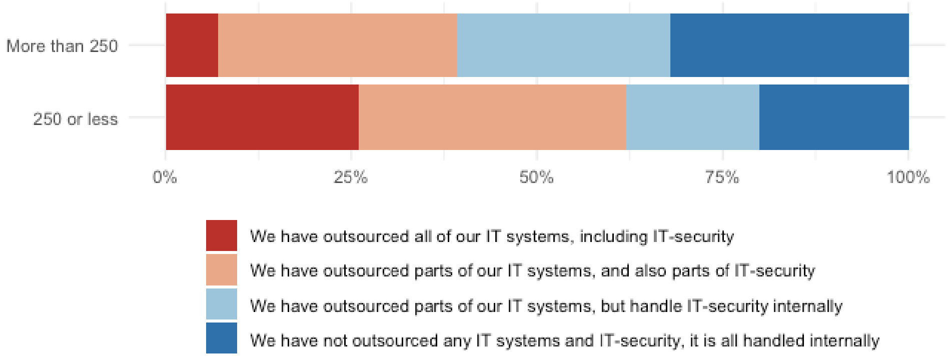


Figure 8: Outsourcing.

2.3.3 Development methods

The participants who entered software-development related tasks as their role in the organisation (36 participants, 18 from large as well as small-medium enterprises), were asked questions about the development process followed in the company. Namely, when asked about the development methods, the most common response was using an iterative development method (Figure 9). When asked about release frequency (Figure 10), the most common answer was more than a month.

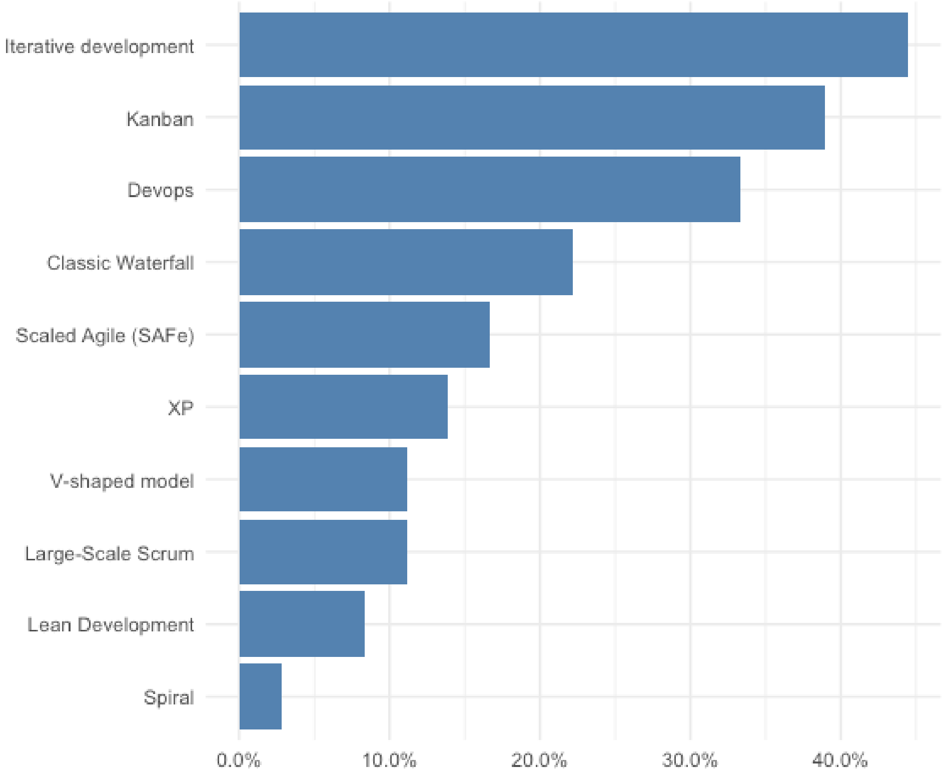


Figure 9: Software development process.

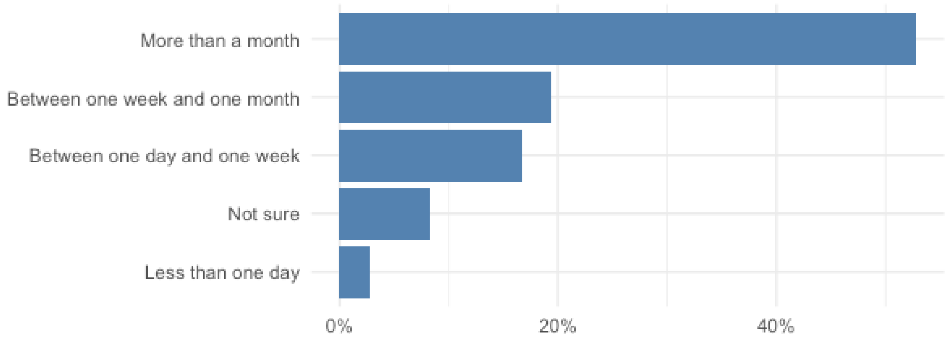


Figure 10: Frequency of releases.

2.3.4 Integration of security

The participants with either IT-security or software-development tasks (62 participants in total, of them 33 from SMEs and 29 from large companies) were asked about the points of integration of security practices into the development cycle. Most of them (76% of respondents from SMEs and 52% from large companies) answered that their organisations integrate security from the initial phases of the project or continuously during the development cycle. A large share of respondents from larger companies (31%), however, reported integrating security after the fact, and 13% of all the respondents (12% from SMEs and 14% from large companies) mentioned that their companies do not integrate security into the development cycle at all.

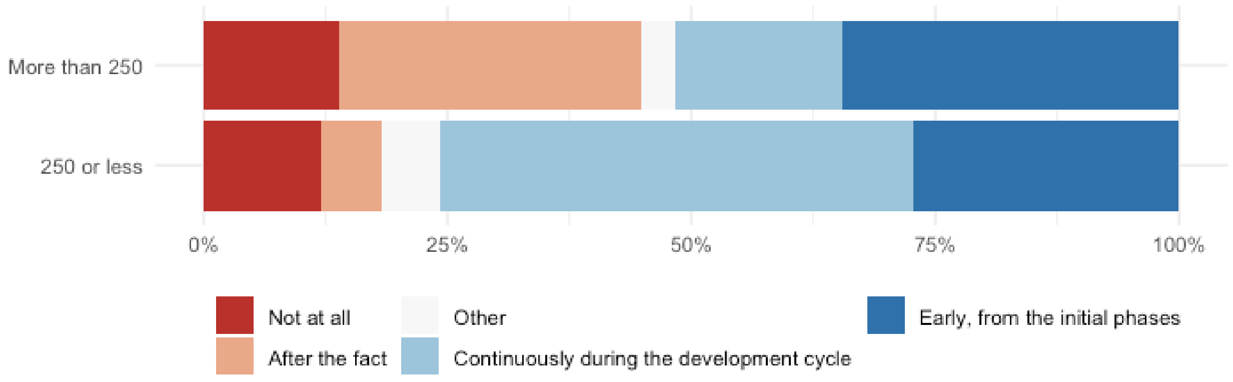


Figure 11: Integration of security into development cycle.

2.3.5 Usage of specific tools and techniques

Participants with either software-development, IT-security, privacy/data-protection or IT-administration tasks (72 respondents in total, of them 38 from SMEs and 34 from large companies) were asked a series of questions on which tools and procedures are used for ensuring software reliability, security and privacy. Figure 12 shows the percentage of respondents answering that a corresponding tool was used in their company, and Figure 13 shows the percentage of respondents answering that the tool is not used (excluding participants who did not provide any answer about a tool). A third available option was "Don't know", to accommodate participants whose tasks might not involve using a particular procedure, but they might assume that the procedure is performed by someone else in their organisation.

According to their answers, the most widely used techniques and procedures in both large and small-medium companies are permission management, testing and encryption. Using circuit breakers, load balancers and network isolation, penetration testing, intrusion detection, and simulation was more widespread in large companies. While more respondents from small-medium companies indicated that they used anonymisation and pseudonymisation of data compared to responses from large companies, the share of participants who indicated that these techniques were not used was roughly similar in both large and small-medium companies. This could possibly indicate that participants from large companies were not personally aware to which extent these techniques are applied within the organisation, as they were within the responsibility of another team/department.

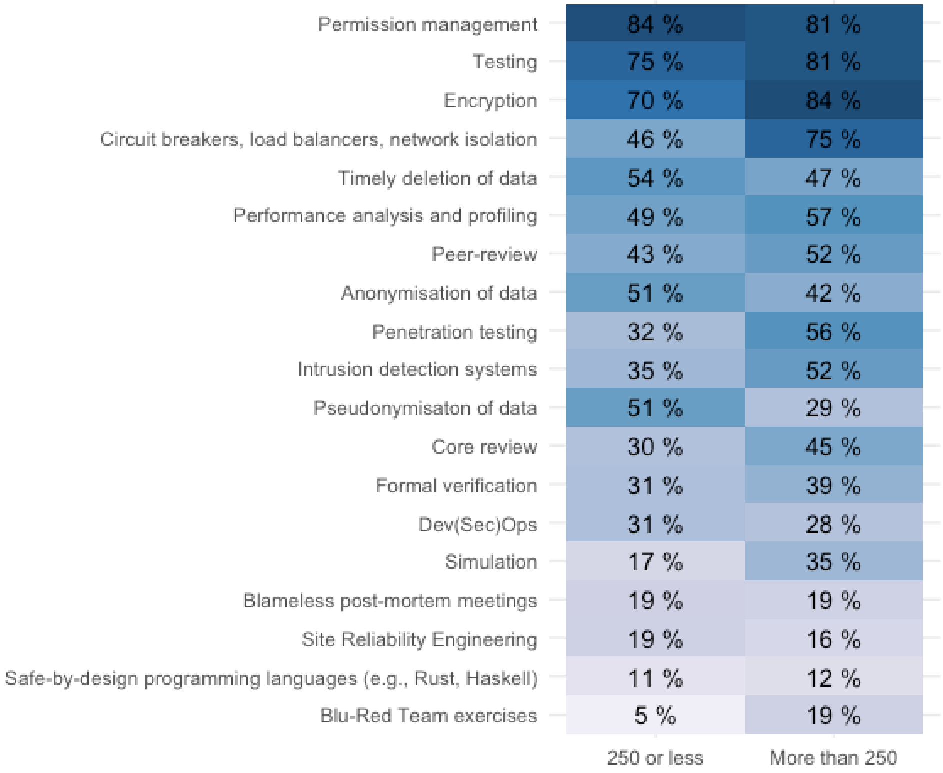


Figure 12: Percentage of participants answering that a particular tool/procedure is used.

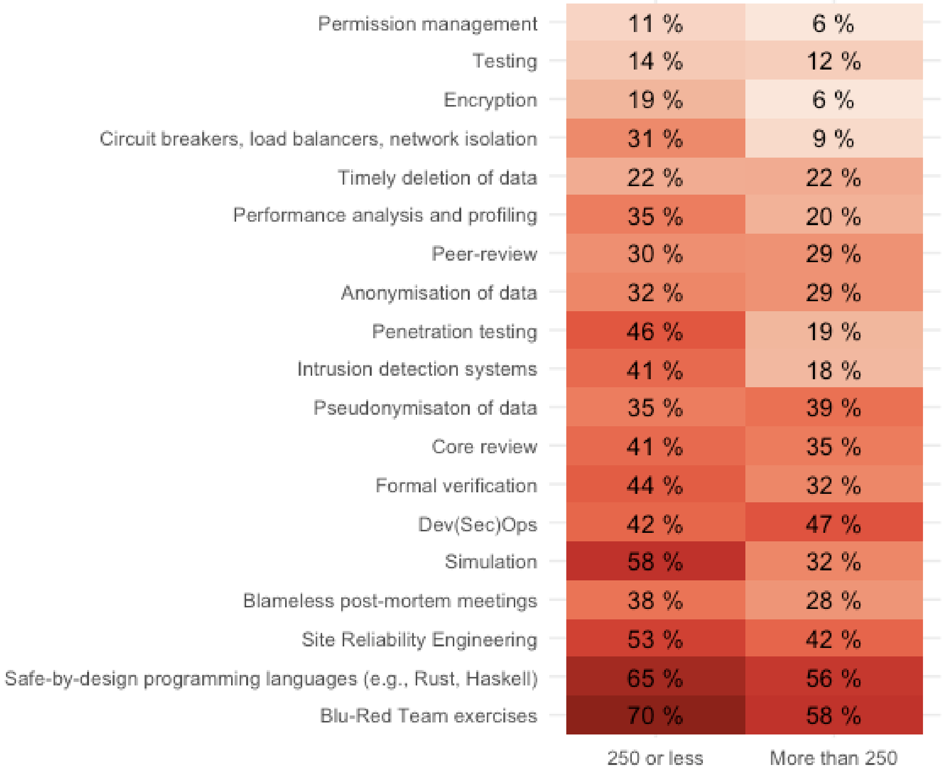


Figure 13: Percentage of participants answering that a particular tool/procedure is not used

2.3.6 Deviations from security procedures

Respondents who entered software development related tasks but not IT-security or privacy/data-protection tasks were asked whether the procedures meant to ensure security, privacy and reliability are followed in all situations. Of the 20 participants who provided an answer to this question, 8 answered negatively and another 4 reported that they were not sure. Of the participants who provided a response to the question about the reasons for such deviations, the most mentioned answer was lack of time and interference with the functionality of the product (mentioned by 5 participants each).

2.3.7 GDPR

The respondents who entered either IT-security or privacy/data-protection as their role (a total of 42 respondents, of them 22 from SMEs and 20 from large companies) were asked a series of questions on whether there have been changes to their company policies with regards to different data protection aspects (namely, which data is collected, which controls are provided to data subjects, how the data subjects are informed about data collection, how the collected data is stored and how it is shared. Figure 14 and Figure 15 summarise the percentages of participants who answered "yes" and "no" to these questions correspondingly[1] (omitting the participants who did not provide an answer for a specific aspect). The answers show that GDPR changed the ways data is processed at most of the companies, although these changes have been less pronounced in smaller companies, especially with regards to policies on storing and sharing data, and on providing controls to data subjects.

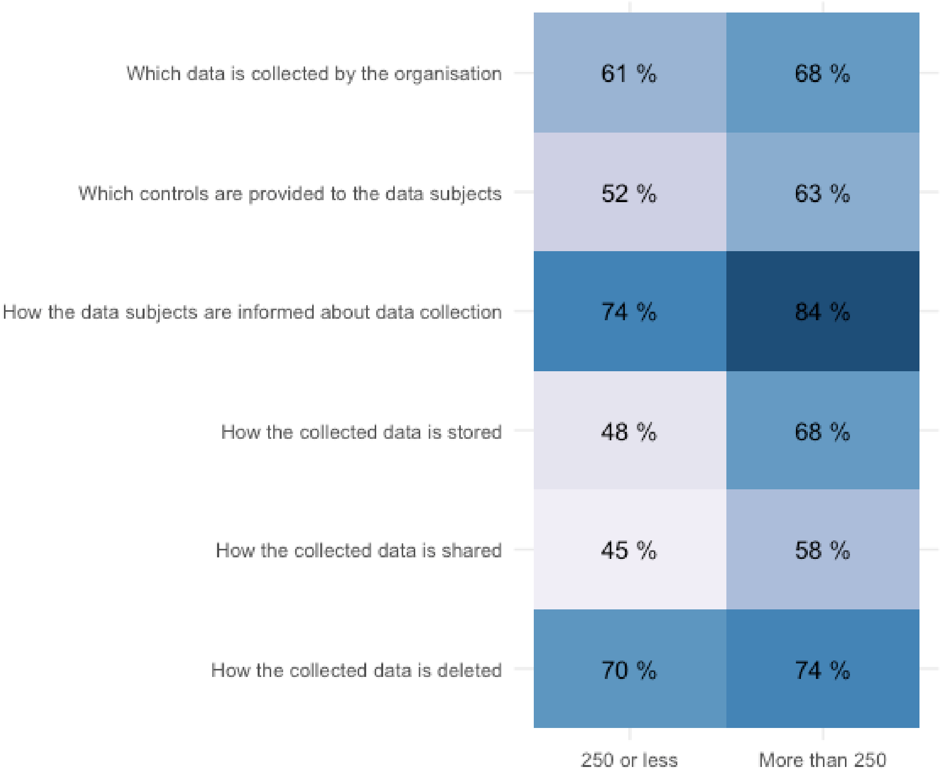


Figure 14: Percentage of participants answering that a particular aspect of data protection has changed since the arrival of GDPR.

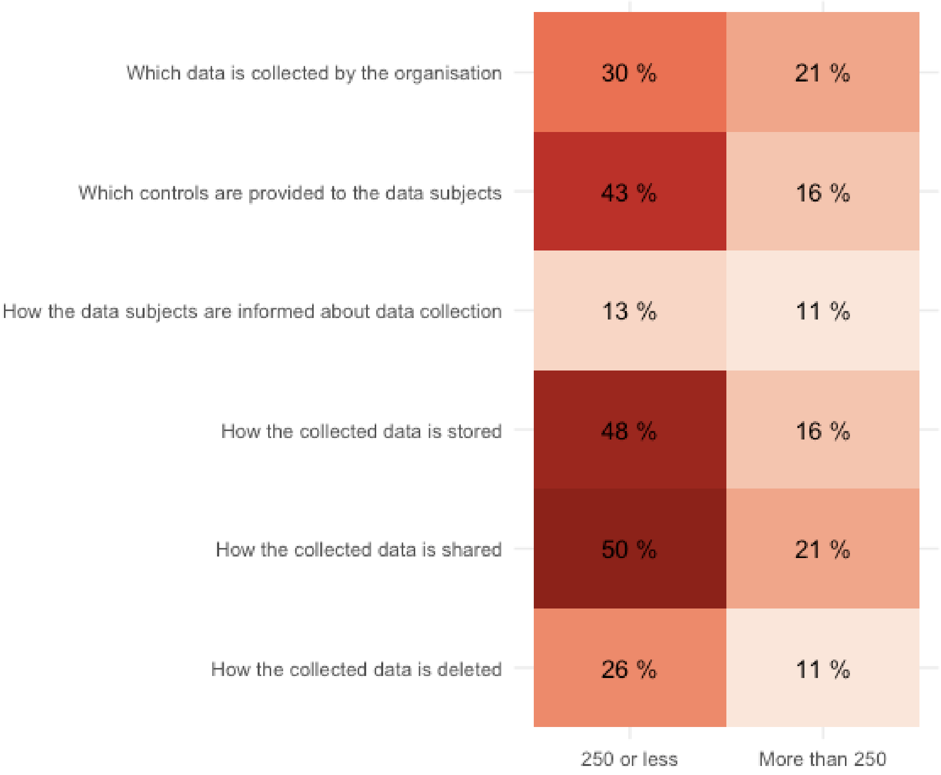


Figure 15: Percentage of participants answering that a particular aspect of data protection has not changed since the arrival of GDPR.

Further questions detailing the data protection policies in companies were asked to participants who chose privacy/data-protection tasks as their role in the company. Out of 21 participants who answered these questions[2], most reported having collected either sensitive (11 participants) or non-sensitive (5 participants) personal data. When asked about controls over their data provided to data subjects, half of the respondents (11) answered that their organisation provides an option to get an overview of data collected about a person and request deletion of such data, 11 mentioned that they allow the participants to request deletion of their data, 9 answered enabling the data subjects to correct data collected from them, and 8 answered that they provide the data subjects with an option to decide which data they want to share. Two participants furthermore chose the “other” option, specifying that they provide the data subjects with all the rights according to GDPR or other laws.

2.3.8 General security and privacy policies, behaviours, attitudes

This subsection details the general awareness and behaviours regarding security and privacy in the organisation, including awareness about assets that might become a target of a cyberattack, knowledge and perception of security policies in the organization, awareness and participation in security trainings, knowledge on whom to contact in case of a Cybersecurity incident and occurrences of insecure behaviours in the organization (e.g., using weak passwords).

2.3.8.1 Awareness of sensitive assets

Figure 16 depicts the number of respondents from either large or small-medium companies, mentioning that a particular asset could be suspectable to a cyber-attack. The responses did not differ much for most of the assets, with most respondents in both large and small-medium companies identifying as the main attackable assets: the IT infrastructure, costumers’ and suppliers’ data, and the company's website. A notable exception is the perception of employees' data, which was considered suspectable to a cyber-attack by most respondents in large companies (64%), but only by 50% of the respondents in SMEs.

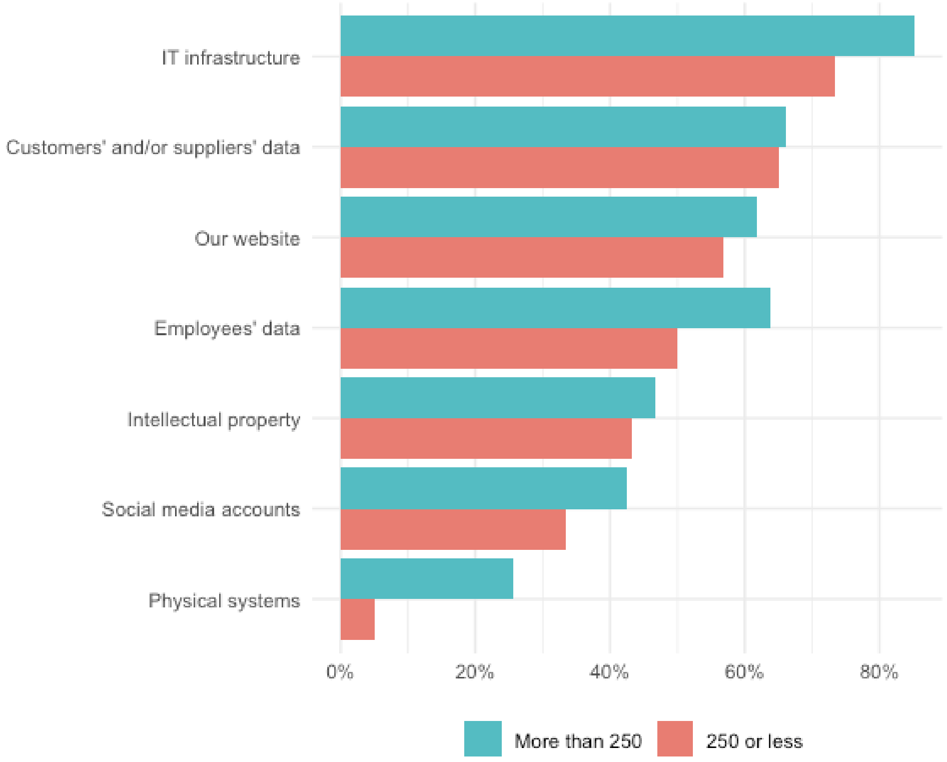


Figure 16: Percentage of participants stating that a particular asset can be a target for cyberattacks.

2.3.8.2 Company policies and training

Among the participants who responded to a question about their familiarity with security and privacy policies[1] that their organisation wants them to follow (92 participants, 54 from SMEs and 38 from larger companies), less than half of respondents from large companies (45%) said being familiar with all of the policies that they are supposed to follow in the company, with this percentage being higher among respondents in SMEs (61%), see Figure 17. At the same time, only a small minority of the participants in both large and small-medium organisations (5%) mentioned being not familiar with either most or all the policies.

[1] The questions about familiarity, challenges and helpfulness with security policies were asked to the participants who selected at least one role other than security/privacy expert, 94 participants in total

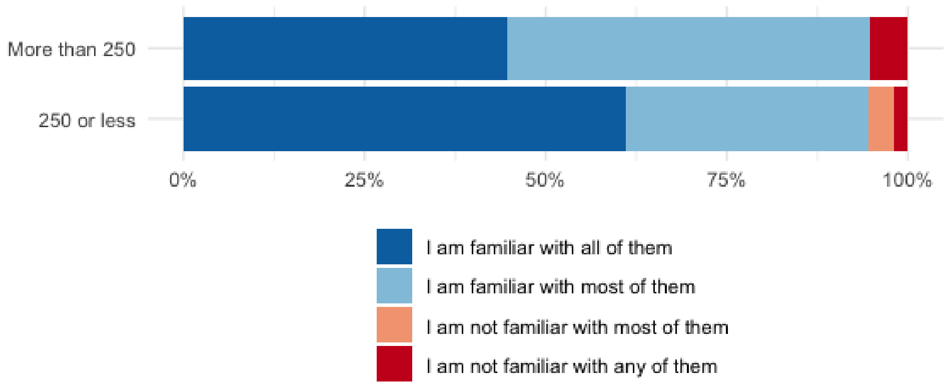


Figure 17: Familiarity with the security and privacy policies of the organization.

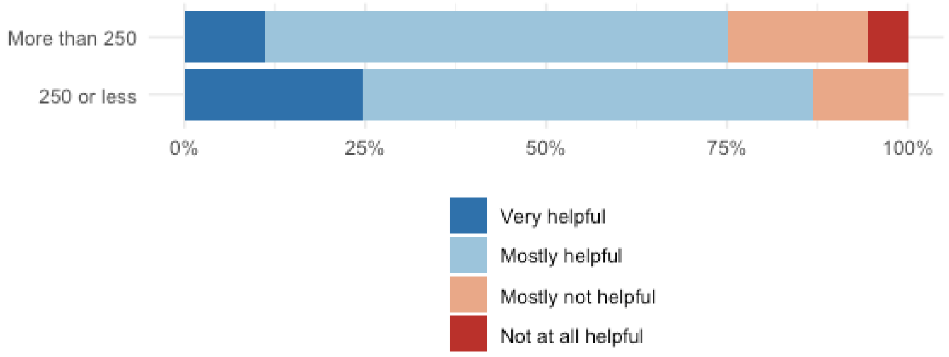


Figure 18: Perceived helpfulness of the security and privacy policies.

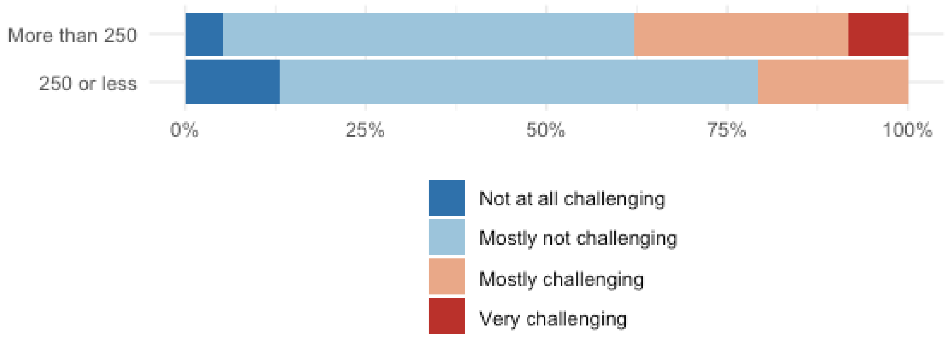


Figure 19: Finding the security and privacy policies challenging.

The majority of people in both large and small-medium companies found the policies either mostly or very helpful (out of 89 participants who answered the question, of them 53 from SMEs and 36 from large organizations), see Figure 18, and either mostly not challenging or not at all challenging (out of 90 participants who answered the question, of them 53 from SMEs and 37 from large organizations), see Figure 19. Yet, a large percentage of them struggles with the policies, considering them mostly unhelpful/not at all helpful (25% of respondents in large companies) or mostly/very challenging (38% of respondents in large companies). Interestingly, these percentages are lower in small-medium companies (13% and 21% correspondingly).

2.3.8.3 Training

Less than half of participants in both large and small-medium companies participated in trainings and found them useful (out of 92 participants who answered the question, of them 50 from SMEs and 42 from large organizations). A lot of people, especially in SMEs (44%), are not aware of any trainings in the companies. Moreover, 31% of respondents in large companies and 12% respondents in SMEs stated that they either did not participate in the trainings or participated but did not find them useful.

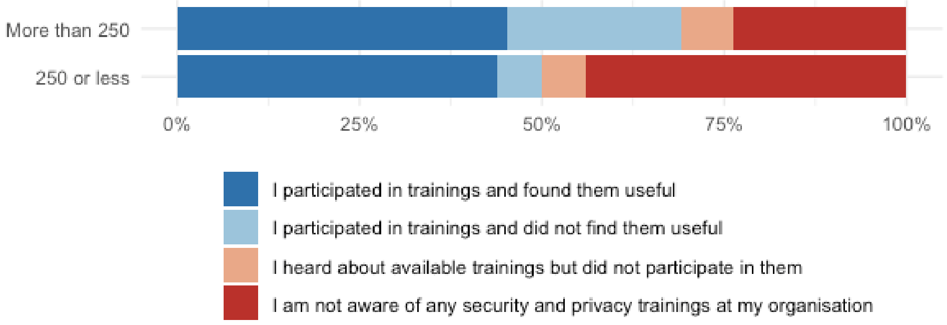


Figure 20: Awareness and participation in security trainings

2.3.8.4 *Incident reporting*

Out of the respondents who provided an answer to the question on whether they know how to report a security incident[2] (80 respondents, 53 from SMEs and 36 from large companies), most highlighted that they knew how to report a security incident. However, there is a slightly higher percentage among SMEs (17%) that either did not know or were not sure how to report incidents.

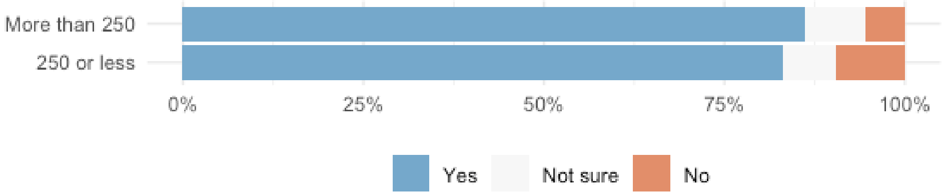


Figure 21: knowledge about incident reporting

2.3.8.5 *Potentially insecure behaviours*

When asked about different types of behaviours that create vulnerabilities in terms of security, almost everyone (98% of people who completed the survey) indicated that they practiced or observed at least one of the behaviours that create vulnerabilities in terms of security listed in the survey. Figure 22 depicts the percentage of participants mentioning each type of behaviours that create vulnerabilities, grouped related to authentication with passwords, potential misuse of IT infrastructure, and behaviours that put one at risk of social engineering attacks. The most commonly mentioned behaviours were password reuse (mentioned by 77% of participants), downloading programs without authorisation of the IT department (62%), and using non-secure passwords (55%).

[2] The question was asked to the participants who selected at least one role other than security or privacy-related tasks, 94 participants in total.

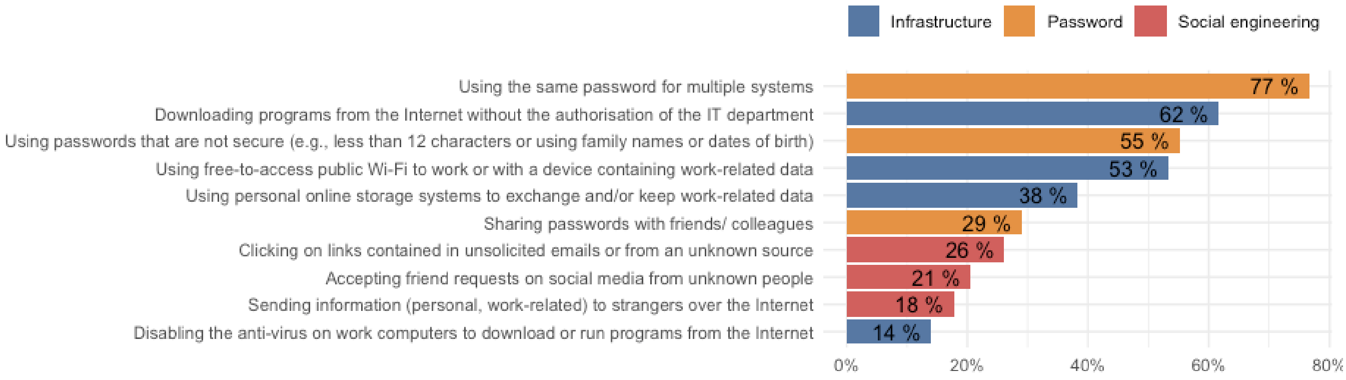


Figure 22: Potentially insecure behaviors

2.3.9 Pandemic impact

While a large number of participants in the survey (out of 92 participants who provided a response for that question, of them 54 from SMEs and 38 from large organisations) answered being concerned about security and privacy, only 12% of them were more concerned as the result of the ongoing COVID-19 pandemic[3]. Another 4% mentioned being less concerned than before the pandemic, and for the vast majority, the pandemic had no effect on their level of concerns.

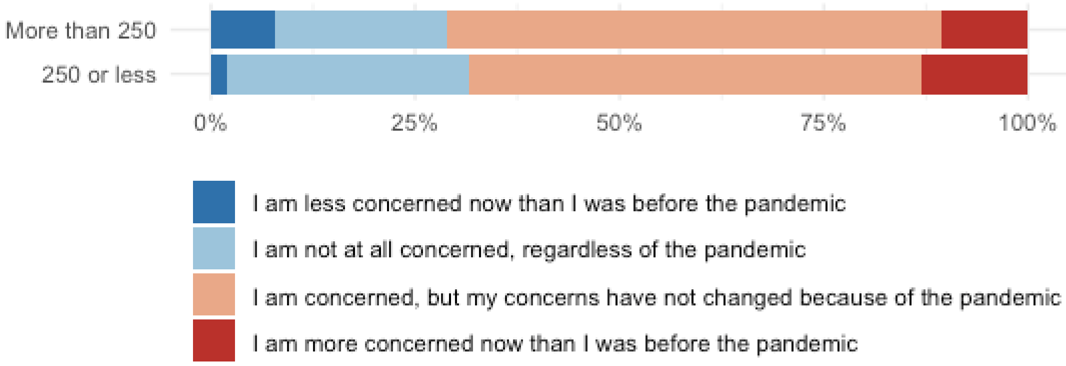


Figure 23: Changes in concerns about security and privacy with regards to the pandemic

[3] This question and the question on challenges with pandemic-related security policies was asked to the participants with at least one role that is not security or privacy related tasks, 94 participants in total

The majority of the respondents in both large organisations and SMEs highlighted working remotely at least at some point during the pandemic. A large share (37% in large companies and 47% in SMEs) already had experience with remote work before the pandemic, while for the rest of them working remotely was a new experience.

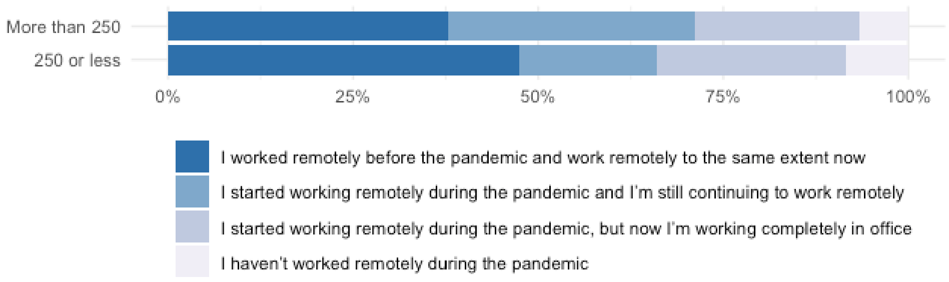


Figure 24: Experience with remote work before and during the pandemic

When asked about remote work policies in their organisation, the vast majority of the participants (85% out of 67 participants who answered the question) answered that they considered the policies to be either not at all challenging or mostly not challenging. The rest of the participants, however, mentioned either perceiving the policies to be mostly challenging, or were not aware of the existence of such policies; moreover, some of the participants, mostly in SMEs, said that their workplace did not have any such policies at all.

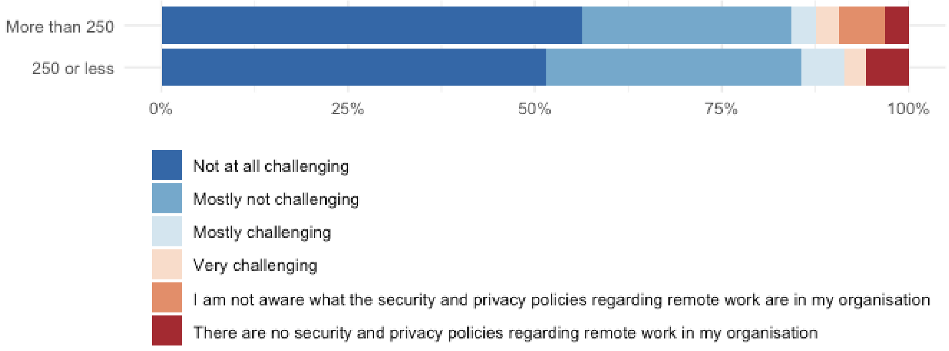


Figure 25: Perceived challenges with security policies regarding remote work

The participants who answered that their role in the organisation included either IT-security or IT-administration tasks (51 participants, 28 from SMEs and 23 from large organisations) were asked about the specific policies related to remote work that their organisation adopts (Figure 26). Among the participants who responded to this question, the respondents from large companies mostly mentioned having worked only on company-provided devices, while the most commonly mentioned policy by respondents from SMEs was working only through the organisation's VPN. Only a few participants mentioned measures not included in the proposed list.[4] [5]

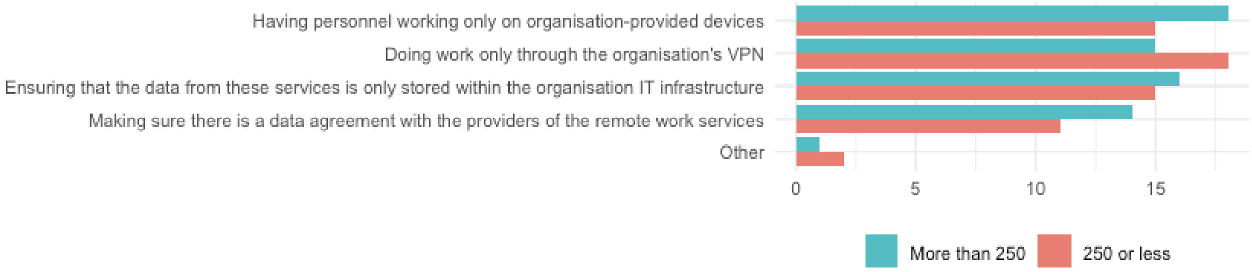


Figure 26: Number of participants mentioning policies adopted for remote work

[4] The questions also had an option "don't know", aimed, among others, at participants who were not present at the company before the GDPR entry and therefore unable to comment on changes.

[5] Due to a small number of respondents to these questions, we do not provide a breakdown into larger and smaller companies

3 Interviews

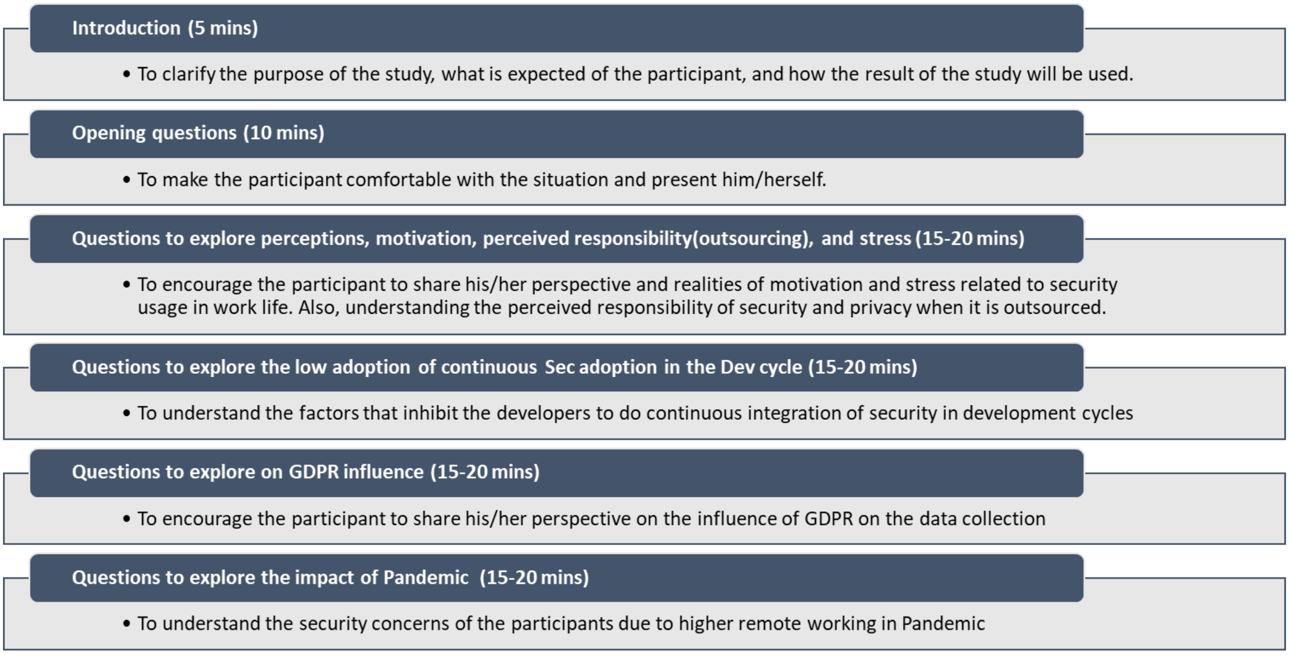
In this section we present the findings from the individual interviews starting by describing how the interviews were planned, the reach-out strategy, and conclude with the interview analysis.

3.1 Interview structure planning

The initial insights from the survey detailed in the previous section were used as a base to discover the areas to be investigated in-depth during the ethnographic interviews, i.e., a method used in qualitative research as a source of data collection. An ethnographic interview is a conversation between a researcher (interviewer) and interviewee, where knowledge is constructed in the interaction between them (Spradley, 1979). In such conversations, the researcher and the interviewee interchange view about a topic or topics of mutual interest, to understand a phenomenon.

The interviews took place during September-November 2020. To adapt to the COVID19 regulation and personal sensitivities of the involved people on the matter, most interviews were conducted over video calls using MS Teams.

The interviews were planned by creating an interview guide focusing on the specific key areas that were explored through semi-structured conversations with the participants. Figure 26 visualizes the interview guideline adopted with six phases targeting a duration of 1h.



Introduction (5 mins)

- To clarify the purpose of the study, what is expected of the participant, and how the result of the study will be used.

Opening questions (10 mins)

- To make the participant comfortable with the situation and present him/herself.

Questions to explore perceptions, motivation, perceived responsibility(outsourcing), and stress (15-20 mins)

- 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.

Questions to explore the low adoption of continuous Sec adoption in the Dev cycle (15-20 mins)

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

Questions to explore on GDPR influence (15-20 mins)

- To encourage the participant to share his/her perspective on the influence of GDPR on the data collection

Questions to explore the impact of Pandemic (15-20 mins)

- To understand the security concerns of the participants due to higher remote working in Pandemic

Figure 27: The interview guideline adopted.

The interview guide helped to initiate the discussion with the participants over broad areas, and then navigating the evolution of the discussion as per the interaction. These interviews helped capturing the viewpoint of the participants in the key areas and deriving important insights. For every key area, a set of question were drafted to be asked. For more information on the questions, we refer the interested reader to https://ascd.dk/results/interview_guidelines.pdf.

3.2 Participant and Reach-out Strategy

Considering the project objectives, timelines, and research best-practices, it was decided to conduct 10–12 interviews with specific participants encompassing two dimensions to decide the participants' composition: stakeholder type and company type.

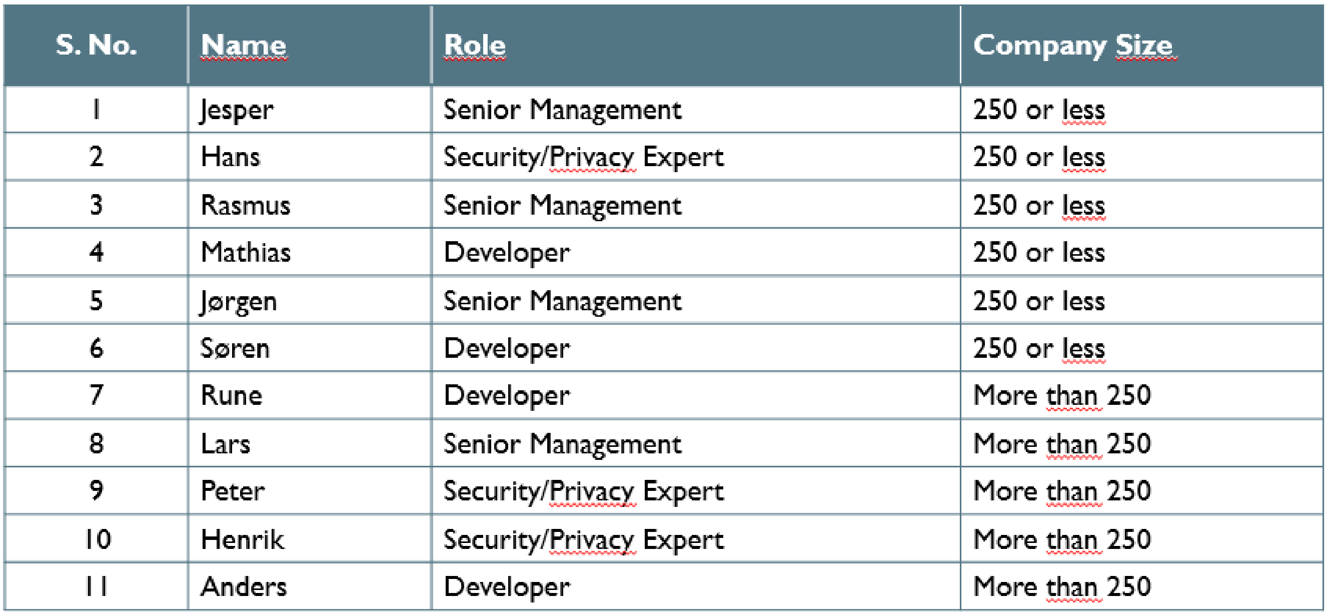
For the stakeholder dimension, it was vital to cover different points-of-view on the same issues for triangulating the perspectives, avoiding anecdotal conclusions, and drawing nuanced insights. Three stakeholder groups were covered: senior managers, security expert & policy makers, and developers.

For the company dimension, the organizations were segmented into two broad categories to cover a wide range of organizations in all the regions of Denmark. Also, this categorization helped collate the company dimension with the company segmentation in the survey. The two company dimensions which were covered were: SMEs (250 or less employees) and large organizations (more than 250 employees).

After the finalization of the stakeholder groups and the company size, the potential participants for the interviews were identified by leveraging different channels such as networks of the group members, LinkedIn, Google. These stakeholders were reached out and engaged through emails and LinkedIn messages. If the stakeholders did not have time for the interview, we asked for referrals in their organization to fit in with the relevant stakeholder group.

The profile of the participants can be viewed in Table 5. There were six participants from small organizations and five from large organizations. These organizations cover the industry sector in Denmark ranging from developing software product, financial startups, retail, manufacturing, consumer goods, construction, and service providers. These interviews had been transcribed and refined to make them more coherent. To keep the opinions of participants safe, their names and organizational details have been anonymized.[6]

[6] To widen the scope of these interviews, women participants were reached. However, due to general underrepresentation of women in the software development field and time constrains, unfortunately, we did not manage to arrange participation with the women participants that we reached out to. Including more diverse perspectives on cybersecurity would be an important direction of future work.



S. No.	Name	Role	Company Size
1	Jesper	Senior Management	250 or less
2	Hans	Security/Privacy Expert	250 or less
3	Rasmus	Senior Management	250 or less
4	Mathias	Developer	250 or less
5	Jørgen	Senior Management	250 or less
6	Søren	Developer	250 or less
7	Rune	Developer	More than 250
8	Lars	Senior Management	More than 250
9	Peter	Security/Privacy Expert	More than 250
10	Henrik	Security/Privacy Expert	More than 250
11	Anders	Developer	More than 250

Table 5: Profiles of the participants.

3.3 Interview Analysis

The analysis of the individual interviews has been conducted using the thematic analysis methodology [10] to distill a set of key themes across all the ethnographic interviews. Following Braun and Clarke, *a theme should capture something important about the data in relation to the research question and represent some level of patterned response or meaning within the data set.*

The analysis of these ethnographic interviews resulted in nine broad theme-elements which were leveraged as key themes. The purpose of these key themes is to capture the security and privacy related traits of the stakeholders and hence the key themes were mapped manually with the related traits of the stakeholders from each of the eleven individual interviews. The key themes emerging from the individual interviews are as follows:

1) Importance of security/privacy

2) Incorporating security/privacy in daily work-life

3) Challenges for security/privacy

4) Security/privacy measures adopted – in development cycles

5) Agile impact

6) GDPR influence

7) Pandemic impact

8) Training availability

9) Senior Management appreciation of Cybersecurity

In the following we detail the analysis of each emerging key themes.

3.3.1 Importance of Security/Privacy

How important is security/privacy for the participant?

During the interview sessions, participants showed different levels of inclination towards the importance of security/privacy. All of them clearly mentioned that security/privacy is important for them, however they showed a varying degree of sensibility towards security/privacy. The importance of security/privacy for an individual depends on her/his knowledge of deploying it in various parts of the organization, what priority it holds for the individual, and how critical it is for her/his organization.

Rune, Mathias, Peter, Henrik, and Anders showed a high sensitivity regarding security and privacy. For Rune, security is one of his top priorities at work, and he spends time learning about it. While developing, he keeps in mind that software should secured and checked for not being compromised, especially when he has to balance security with user experience. Similarly, Peter thinks that security is a critical aspect of a good business model and should be treated as an integral part of the latter. He feels that the security measures taken by any organization should not obstruct its workflow, instead they can be leveraged by the business to grow stronger, by having a clear picture of the Cybersecurity risks they are subject to. The participant mentioned that security cannot reside only at the infrastructural and operational levels of the organization, but it needs to be well embedded at all levels of the organization. This can be enabled by providing continuous support to the developers by making sure that they have the right skill sets and are using the right platforms and tools to develop secure code.

While still attributing importance to security, other participants did not stress its importance too much. Rasmus expressed that he is not thinking about security and privacy on an everyday basis. However, when he is handling personal data, he makes sure that he is aware of the compliance around GDPR. For Jesper, security is seen only from their product point-of-view. He believes that his organization has secured their product. Similarly, Jørgen's focus on Cybersecurity is related to the specific branch he is working on, and not on global aspects of it.

3.3.2 Incorporating security/privacy in daily work life

How are participants embedding security/privacy in their day-to-day work?

In the interviews, it was clearly seen that the participants included security/privacy behaviors in their work habits with different levels of involvement. Jesper, Rasmus, Søren, and Jørgen reflected a partial level of security/privacy incorporation during work. Jesper relies on the knowledge of the developers in his organization and trusts that they are taking enough measures to deploy it in their daily work. Similarly, Søren, mentioned that his company has outsourced a significant part of their IT systems and he thinks that security compliance is the responsibility of the external partner. Rune mentioned that the management in his organization does not prioritize developer time spent on implementing security practices, assuming it is the developers' responsibility to make sure they incorporate security measures while developing the product. However, Rune reports that it is difficult to realize that assumption, since developers do not have enough knowledge in the first place.

Peter, Mathias, Henrik, and Anders showed instead a high level of security/privacy incorporation at work. Peter makes sure that the information classification framework in his organization is up-to-date and clear to everyone. He regularly follows the classification himself, so that others are inspired to emulate the same behavior. Similarly, Mathias mentioned that, as a part of his work profile, he uses internal procedures to check the security of their networks periodically.

3.3.3 Challenges for security and privacy

Is security/privacy challenging to implement? why?

The incorporation of security/privacy has been a major challenge for many organizations as they need to make an effort to seamlessly blend it with their business needs. Mathias highlighted that it is difficult to regularly balance high-security needs with business needs, during the development cycle. He feels that the workflow of the employees gets affected, as his company has put restrictions around data access. He also mentioned that the deletion of data from the system in order to be GDPR-complaint is a tedious task. He emphasized that the security/privacy measures have added extra costs on their organization.

Similarly, Peter emphasized that companies need to provide more tools to developers and encourage them to discover hidden vulnerabilities in the applications, so that they can develop secure products continuously. This will help companies to counteract the agenda of malevolent adversaries, who are also continuously searching for new vulnerabilities in their products.

Notwithstanding their level of incorporation of security/privacy measures, many participants in the interviews emphasized that security/privacy implementation is not a challenge for their organizations. For example, Jesper mentioned that security implementation is not a challenge as he has an inherent trust in the technology they are developing and feels that it is quite robust. He does not expect security threats in their internal organization, as external partners are expected to be responsible for the outsourced data. A similar pattern was observed in the behavior of Søren and Jørgen.

3.3.4 Security/privacy measures in the development cycle

Is security/privacy continuously getting incorporated in the development cycle? What are the measures and procedures followed?

During the interviews, the organizations of the participants showed different levels of security and privacy incorporation in the development cycle.

Peter mentioned that his organization is proactively working on what kind of security measures should be given to the developers, so to make the continuous incorporation of security in the development cycle seamless for them. his organization has a high level of continuous security and privacy incorporation in the development cycle.

Mathias mentioned that his organization incorporates security and privacy depending on the needs of each product. He thinks that the developers have knowledge and understanding around the security implementation in the development cycle.

Contrarily, Rune emphasized that the developers in his organization have limited knowledge on security implementation in the development cycle, even though the management assumes that developers have enough knowledge on building safe and secure systems. Further investigations support this divergence of views between the developers and the management positions.

3.3.5 Agile impact

Does Agile processes inhibit the developers to do continuous integration of security in development cycles?

Most of participants do not believe that agile methodology hinders the continuous integration of security but mentioned that the lack of prioritization inhibits its continued integration. For instance, Peter, Mathias, Anders expressed that the lack of awareness in teams, along with unclearly stated security objectives, have a negative effect on the integration of security. Rune mentioned that it is the lack of priority from the developers and management that can be a barrier to the integration. He believes that management should enforce security integration initially when they are giving specifications to the development team and make sure that the developers are capable of implementing the security measures in the development cycle.

3.3.6 GDPR influence

What is the influence of GDPR on data record collection and management?

GDPR has changed the data collection and management processes in the organizations. It also mandates organizations to have a well-defined approach for providing control over data to their owners. In interviews participants from different organizations reflected on the influence of GDPR on their organizations at different levels. Some participants have high awareness on GDPR compliance and have knowledge on data record collection and management planning. Mathias mentioned that after the introduction of GDPR, his organization is proactively working towards data management. They are trying to make their processes seamless and more stringent as per the GDPR. However, they are facing operational challenges because their clients do not have a legal departments or expertise and are struggling with understanding legal implications of data protection agreements. A similar viewpoint was shared by Henrik that mentioned that GDPR has indeed changed processes in his organization. For him, GDPR is quite challenging and time consuming, but his organization is proactively doing data record collection and management planning in order to be GDPR compliant.

Some other participants have only partial awareness and an ad-hoc approach on GDPR compliance. Lars mentioned knowing that GDPR has changed the modality of data collection in his organization, but also reported that he was aware only of the establishment of the new legal declaration provided to their customers/users. Similarly, Rune was not specifically aware of data-record collection & management planning at his organization, nor the proper procedure to receive clarifications on GDPR-related matters. He felt that organizations just work on those aspects of privacy, which give them a minimum level of GDPR-compliance, rather than taking a proactive approach in this matter.

Some participants emphasize the cost of implementing GDPR, possibly trying to outsource this task externally. For example, Jesper reported that initially he believed that his organization did not store any customer data. However, after some product updates, they needed to revise those products again only for GDPR compliance. Those iterations frustrated him, since they took time and money, for no perceived added value. A similar point of view was reported by Jørgen, using a third party to process the data, even though the data is flowing through his systems.

3.3.7 Pandemic Impact

How do people feel about security risks due to pandemic? Have companies taken extra measures to mitigate such risks?

Covid-19 has changed the working environment in all organizations. Peter mentioned that the risk due to remote work has heightened the need to put security measures in place to avoid Cybersecurity attacks and his organization is taking it seriously. On the other hand, he stated that the pandemic facilitated conversations about security, making it possible to implement measures that would take much longer time otherwise.

Surprisingly, most of the participants from different organizations in the interviews believe that the pandemic did not raise too much the security risks, and some also see certain security advantages in working from home, e.g., ensuring that no one gets unauthorized physical access to sensitive documents and devices. Rune highlighted that Danish organizations work on inherent trust and they trust that the employees will take care of the company's data and their own network security while working from home. Similarly, Lars mentioned that his organization has not taken any extra measures to sustain long term remote working conditions since their enterprise data is secured in the Cloud.

3.3.8 Training availability

What is the status of security awareness training and secure code development training in the organisations?

When it comes to training, the participants were asked about the availability of general Cybersecurity awareness training and security training for developers. Most of the participants mentioned that there is no provisioning of either general Cybersecurity awareness training or specific security training for developers. Only a few participants reported that their companies organize regular security training sessions for the employees, and they are working on providing specific security training to the developers. Others mentioned that, while the management would be willing to pay for training their staff on security, they would not ask the developers to take that training, but expect the developers to be proactive and come forward asking for it themselves.

Jesper emphasized that the developers in his organization are fully aware of the security practices and do not need much training. He believes that, if a company has followed a good development strategy in the beginning and has a good infrastructure, they do not need further security measures or the continuous update those measures. Similarly, Rune mentioned that the security training or courses are not a usual part of the work. He reported that management does not check the developer's knowledge on security while hiring them in the company and assumes that developers know about it and they will implement it appropriately. He also mentioned that he has attended a few courses on his own and none were mandated by the management—there has not been much encouragement from management for regular security and privacy courses for developers.

Contrarily, Peter mentioned that his organization provides training on Cybersecurity (awareness). However, he mentioned that some training programs should be crafted for the developers, so that they can acquire the level of proficiency needed to secure their development cycle. A similar perspective was highlighted by Anders, whose organization provides training and awareness but no specific training to developers. Their companies expect the developers to acquire this knowledge on their own.

3.3.9 Senior management awareness of Cybersecurity

What role can management play in encouraging adoption of Cybersecurity in an organisation?

Senior management awareness of Cybersecurity is a crucial component in enforcing the Cybersecurity measures in an organization. In the interviews with different participants across different stakeholder groups, it came out as an important trait.

A few participants in the interviews stated that senior management has a strong focus on embedding Cybersecurity practices at both the levels of organization and product development. Peter mentioned that the senior management in his organization has a strong focus on security, however he reported that enterprises should be aware of the fact that there is a delicate balance between security and business needs. Similarly, Henrik mentioned that senior management in his organization prioritize security by reviewing whether people in the organization comply with the necessary policies and reminding them to do so.

Many participants in the interviews highlighted only a partial awareness of senior management on Cybersecurity. Jørgen's focus on security is entirely on the product that he will sell and its functional needs. A similar case was observed with Rasmus, who trusts employees to apply security measures in their work and he expects them to come forward in case they face issues.

4 Integrated Insights

In this section we summarize and discuss the main findings considering the survey and the interviews detailed in the previous sections. For presentation sake, we follow the themes that emerged from the interview analysis presented in the previous sections merging some of them when relevant.

4.1 Importance of security/privacy and its incorporation in daily work-life

As expected, due to targeted participants for the survey and the interviews, all the people believed security is important. Some believed in it for intrinsic reasons while others paid more attention to the cost, reputation or legal risk of not being secure. The survey shows that 40% of the participants were familiar with all the policies in the company, with the rest being either familiar with most but not all the policies, in the best case, or being unfamiliar with either most or all of them. When we come to interviews, we could see participants mentioning to not know exactly what policies exist or only describing them in very vague terms. On the other hand, some companies do take a more systematic approach, requiring every new employee to read the policies relevant to them. However, even the interviewees from these companies spoke of the existence of challenges of ensuring that the employees familiarise themselves with these policies in a thorough way.

From the interviews, we can see that people might feel that security is not prioritised, and that changes in workflows need to be done to incorporate, e.g., the GDPR requirements. Some of our interviewees believe these changes are hard to implement, especially for smaller companies. At the same time, the respondents from larger companies' report having more difficulties with policies, possibly because of the growing complexity of such policies with the size of the company.

4.2 Challenges for security/privacy

Participants in interviews talk about a lack of integration of security into their work processes, specifically mentioning that even if one considers its importance, it is treated as an afterthought and not prioritised. Participants from companies that take more measures to implement security also mention the importance of integrating security into daily tasks, not just the tasks of the security team, but also of developers and other people who need to be involved. Nonetheless, the survey shows that security is often treated as an afterthought, even in large companies (the reason possibly being the complexity of processes and roles).

As seen from the interviews, balancing security and privacy with business costs remains a challenge for many organisations. Conflicts with workflows, lack of resources, and interference from management are cited as the most popular reasons for security deviations within the survey. While adjusting procedures for more flexibility is not necessarily a negative thing, these reasons can be a problem for proper security protection, and the interviews further stress these points, naming proper integration in the workflow and support from management as crucial factors in success of security measures.

4.3 Security/privacy measures adopted in development cycles Agile Impact

In agreement with the latest empirical results [11], Agile development methodologies are not perceived as inhibitors of security in the development cycle. From the interviews, it emerged that, although many companies adopt Agile/DevOps practices, the journey is still at the beginning since there is a focus on the techniques rather than adopting the Agile/DevOps culture that brings the attention also to communication, shared values, and teamwork. As an example, some report that the management does not mandate the incorporation of security in user-stories/backlogs/business requirements, thus not prioritizing security and inhibiting the interest in addressing security issues, which are not perceived as mission critical. Others claim a lack of specific expertise for the integration of security in the development cycle, often leading to ad-hoc and not systematic approaches to its integration. Large companies seem better positioned than SMEs but, surprisingly, they report that security is often integrated only at the end and not in the entire life-cycle of their products, starting from the design phase and ending with the deployment in production.

Moreover, the survey pointed out that the frequency of software release is rather low, signalling that most of the companies has not reach a high level of Agile/DevOps adoption, that is characterized by multiple deliveries per day and/or delivery on demand.

4.4 GDPR influence

Both survey answers and interviews confirm that GDPR introduced a major undertaking for companies that had to change their data collection processes. Some companies, nonetheless, were not affected by the change, either because they did not perceive to be in possession of personal data (e.g., being a business-to-business company), or outsourced the handling of their assets, including personal data to third parties. Some of the interviewees commented that ensuring compliance with GDPR was a large task that required significant resources and expertise, also expressing concerns that smaller companies without such resources would not be able to properly ensure compliance. Another challenge with implementing GDPR compliance was shown to be lack of clear frameworks/guidelines, which could again become an issue in smaller companies operating without the support of a dedicated legal department.

4.5 Pandemic impact

Neither the survey nor the interviews revealed any major concerns about security and privacy during the pandemic. As such, most of the survey participants reported that their concerns did not change because of the pandemic; many of the interviewees furthermore noted that there were no major changes in their organization's security policies. One reason for this could be the widespread of remote work already before the pandemic[7]. On the other hand, as cybersecurity experts are warning

[7] https://fho.dk/blog/2020/09/29/danmark-i-top-med-hjemmearbejde/

about increased risks of cyber-attacks in connection with increased remote work in potentially insecure environments such as one's home network[8]

At the same time, while being a small minority, some participants in the survey felt less concern about security and privacy because of the pandemic. Some interviewees provide further insights into possible reasons, e.g., feeling that their sensitive documents or devices might be safer at home than in their office where unauthorised personnel such as cleaning staff might have access to them. The need to move online was also mentioned as a driver towards implementing procedures, including security measures, that would otherwise take a much longer time if they were not prioritised.

4.6 Trainings availability

When raising the topic of security training with the interview participants, some mentioned the lack of such trainings in their company. Interviews with management, on the other hand, reveal that in some cases the management is ready to pay for the trainings, but only if the employees come and ask for this themselves. This could be a problem if the employees are either not aware that they can ask, or if they are not knowledgeable enough to know which trainings to ask for, or even that they need any trainings at all. The survey indeed shows that a large percentage of employees in both small-medium and large companies are either unaware of the trainings, do not attend them or do not consider them useful. This suggests that the management needs to take a proactive role, ensuring that the employees are aware of the trainings and have the opportunities to participate in them. On their turn, trainings should actually reflect the needs of the employees, satisfying both their perceived and actual usefulness.

4.7 Senior Management appreciation of Cybersecurity

[8] https://www.computerworld.dk/art/251141/it-sikkerhedstruslerne-stiger-massivt-naar-du-arbejder-hjemme-brugerne-saenker-paraderne-fordi-fokus-er-et-andet-sted

The role of the management and the relations between the management and the developer teams was often stressed in the interviews. As such, one of the common themes was management putting trust on developers' knowledge when it comes to security and privacy incorporation into the development cycle. Such trust can have a very positive effect on the work environment, including the security culture of the organization, if the developers are indeed knowledgeable and motivated to implement proper security measures. However, it can potentially misfire when the developers lack in either knowledge or motivation in dedicating time and effort on security or feel that security- and privacy-related tasks are not prioritized highly enough by the management, and as such are treated as a distraction from spending resources on functional requirements, or conflict with these requirements altogether. If combined with lack of trainings or developer's lack of awareness about such trainings, as discussed above, management putting too much responsibility on the developers to take care of security can lead to a situation where no one feels responsible, hence, security gets neglected.

A further reason for a lack of appreciation of Cybersecurity and data protection could also be the lack of awareness about sensitive assets in the company, e.g., resulting from lack of knowledge of what can constitute personal data that is subject to the GDPR. Ensuring that the management properly understands the risks (hence, can communicate them to developers and priorities security and data protection correspondingly) is therefore of great importance.

5 Recommendations

Based on the analysis of the survey and the interviews, we encountered a wide variety of policies (or lack thereof) for handling Cybersecurity. Few organizations rely on standards like ISO but many also do not rely on established policies. At the time of writing this report, there are no Cybersecurity standards legally enforced except GDPR for data privacy. We expect that this will change in the next five years due to the activities of the European Union Agency for Cybersecurity (ENISA) and its EU certification framework program[9]. Due to the huge amount of work and costs involved in the adoption of the GDPR, the current adoption of Cybersecurity policies and standards, we expect that the application of the future ENISA standards can cause a disruption of the current status quo. For this reason, we recommend starting a series of activities to promote the adoption of Cybersecurity policies that will smooth the transition when the new certification process will come into effect. In particular, we recommend the creation of a task force constituted by a variety of stakeholders, e.g., Cybersecurity experts, social scientists, and policy makers. The task force should enhance existing efforts [12][13] and investigate how to better promote the establishment of policies compatible with the future ENISA directives and their effective implementation in the Danish society—by interfacing with ENISA, the Danish political institutions, the worker unions, and the companies.

As for the adoption of the policies and standards, we have witnessed that often only a few larger companies can sustain the cost of adopting and be successfully evaluated as standard certified. For SMEs, the adoption of expensive and knowledge-intensive standards is prohibitive. Thus, we recommend the study and definition of standards designed to be gradually adopted over time by SMEs, setting a reasonable roadmap for them to afford rising their standards of Cybersecurity. Another common topic that emerged from both the survey and the interviews is the possibility to improve the Cybersecurity training. There is a plethora of existing training opportunities but apparently, they do not reach the target of elevating the concreate expertise in Cybersecurity, especially at the management level. Trainings are often perceived not useful; they are not mandatory and often not actively incentivized with positive action from the top management. A further study is

[9] https://ec.europa.eu/digital-single-market/en/eu-Cybersecurity-certification-framework

needed to understand better why the trainings are perceived as not useful and find out the right incentives to nudge more workers to take them. As the results of the project have shown, it is crucial for the management to take initiative in establishing the security culture in the company, including leading by example. Thus, a special focus should be paid to managers of SMEs to incentivize their participation in such courses, which could possibly include designing seminars for the board and executive level only or training on Information Security Management Systems to ensure that IT-security related risks are identified, quantified, and managed as a top-down organizational task[10].

From our studies we also notice the emergence of discrepancies between the view of the managers and non-managers. We have experienced that managers often have a great trust on their employees, and they assume that they have all the expertise to provide a secure product. Such level of trust, also typical of the Danish society in general, can benefit security: for example, it enables people to report problems without fearing the consequences of their mistakes. However, Cybersecurity benefits from skepticism and the assumption that something is not secure if not proven otherwise. In our interviews indeed, we have seen that often the trust in the security of the products or the organization express by the managers is not shared by their employees that report lack of knowledge or time to prioritize security. Such assumptions can lead to misalignments regarding perceived responsibility in the organizations, with people assuming that Cybersecurity is something that someone else is supposed to take care of and, consequently, not taking the necessary precautions expected from them. We recommend further studies to properly quantify this discrepancy on security perception. We also recommend actions to increase the awareness of managers and encourage them to conduct periodic investigation involving all the stakeholders to evaluate the security of their products. Since many participants report to not know the policies to report problems, we also encourage managers to ensure that each of their employees is aware of how problems can be reported, possibly introducing "security champions" in teams that serve as go-to persons for security problems (as suggested by one of the interview participants and proposed in academic literature).

We would like to conclude with a recommendation on the study of the outsourcing policies. We have witnessed a significant number of SMEs that heavily outsource their security, for cost reasons. Clearly a partial outsourcing of security can be beneficial if acquiring internal expertise is too costly. On the

[10] An interesting ongoing project that goes in this direction is https://www.industriensfond.dk/Styrkelse-af-Strategiske-Cyberkompetencer

other side, it should be clear that outsourcing of security does not solve all the problems connected with security (e.g., responsibility of handling data and breaches), and that ensuring trustworthiness and accountability of providers is prioritized. As a general policy, we suggest to encourage managers to: a) reduce outsourcing as much as possible, considering that this has been shown to negatively affect operational performance [14]; b) evaluate partners and sub suppliers, defining what are and monitoring their responsibilities and duties, which cannot be delegated with outsourcing; c) considering the acquisition of insurance policies for Cybersecurity.

6 People

The IT University of Copenhagen and the University of Southern Denmark are the host institution of the ASCD project. The primary responsible scientists for the ASCD project are:

Name	Affiliation	Role	Area of Expertise
Oksana Kulyk	IT University of Copenhagen, Assistant Professor	Co-Principal Investigator	Human Factors in Security and Privacy
Jacopo Mauro	University of Southern Denmark, Associate Professor	Co-Principal Investigator	Software Engineering and DevSecOps

The other team members are:

Name	Affiliation	Role	Area of Expertise
Asmita Dalela	IT University of Copenhagen, Research Assistant	Researcher	Techno-Anthropologist, Behavioral Security, Trust
Saverio Giallorenzo	Università di Bologna, Assistant Professor Formerly, University of Southern Denmark, Postdoctoral Researcher	Co-principal Investigator	Microservice Security
Bjørn Høj Jakobsen	University of Southern Denmark, Compliance Consultant	Security Consultant	Security Standards
Elda Paja	IT University of Copenhagen, Assistant Professor	Researcher	Software Engineering

For contacting the team, please visit https://ascd.dk/contact/

References

[1]"State of Software Security v11", *Veracode*, 2020. [Online]. Available: https://www.veracode.com/state-of-software-security-report

[2]"DevOps Solutions", *Google Cloud*, 2019. [Online]. Available: https://cloud.google.com/devops/state-of-devops/

[3]Y. Sawaya, M. Sharif, N. Christin, A. Kubota, A. Nakarai and A. Yamada, "Self-Confidence Trumps Knowledge", *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2017.

[4]"IT-sikkerhed og datahåndtering i danske SMV'er | erhvervsstyrelsen.dk", *Erhvervsstyrelsen.dk*, 2018. [Online]. Available: https://erhvervsstyrelsen.dk/it-sikkerhed-og-datahandtering-i-danske-smver

[5]"Foranalyse af danskernes informationssikkerhed", *erhvervsstyrelsen.dk*, 2017. [Online]. Available: https://erhvervsstyrelsen.dk/foranalyse-af-danskernes-informationssikkerhed

[6]"Digital Tryghed – de væsentligste digitale udfordringer for forbrugerne i Danmark", *taenk.dk*, 2016. [Online]. Available: https://taenk.dk/sites/default/files/fbr_taenk_rapport_digitaltryghed_web.pdf

[7]"Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark | erhvervsstyrelsen.dk", *erhvervsstyrelsen.dk*, 2019. [Online]. Available: https://erhvervsstyrelsen.dk/arbejdsmarkedet-informationssikkerhedskompetencer-i-danmark

[8]P. Runeson and M. Höst, "Guidelines for conducting and reporting case study research in software engineering", *Empirical Software Engineering*, vol. 14, no. 2, pp. 131-164, 2009.

[9]T. LaToza, G. Venolia and R. DeLine, "Maintaining Mental Models: A Study of Developer Work Habits", *Microsoft.com*, 2006. [Online]. Available: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/p492-latoza.pdf

[10]V. Braun and V. Clarke, "Using thematic analysis in psychology", *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77-101, 2006.

[11]"State of DevOps", *Services.google.com*, 2019. [Online]. Available: https://services.google.com/fh/files/misc/state-of-devops-2019.pdf

[12]"Mærkningsordning til virksomheder for it-sikkerhed og ansvarlig dataanvendelse | Industriens Fond", *industriensfond.dk*, 2014. [Online]. Available: https://www.industriensfond.dk/maerkningsordning-for-IT-sikkerhed

[13]"Danish Hub for Cybersecurity", *Industriensfond.dk*, 2014. [Online]. Available: https://www.industriensfond.dk/Danish-Hub-for-Security

[14]N. Forsgren, "The 2019 Accelerate State of DevOps: Elite performance, productivity, and scaling | Google Cloud Blog", *Google Cloud Blog*, 2019. [Online]. Available: https://cloud.google.com/blog/products/devops-sre/the-2019-accelerate-state-of-devops-elite-performance-productivity-and-scaling