

Cybersecurity & Privacy– Exploration

Interview Guide

Introduction (5 min)

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

Thank you for taking time out of your day to talk with us. We really appreciate it. To kick things off, I just want to provide you with some background on us and why we are doing this interview.

I work in a Research Center in ITU called Center for Information Security & Trust (CISAT). This is a collaborative research project between ITU and SDU. The reason we are doing this research is to better understand the cybersecurity and privacy protection practices adopted by the Danish organizations.

There is no right or wrong way to answer the questions. I am just interested in learning about your way of thinking, so I would like for you to just think aloud as you go along and express your opinion.

Your participation is anonymous. We will not reveal the names of any participants in our report.

Is it alright if I record the session? The recording will only be shared with the relevant people in ITU and SDU only for this project. The collected data will be deleted after the completion of the project.

Any questions before we begin? The interview will take 1 hour.

Opening questions (10 min)

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

- 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
- Do you think about security and privacy in your regular work?
 - Is yes: How often and for what?
 - If no: Why not?
- What is most important to you when it comes to security and privacy? (e.g. specific aspects, technology, business needs and constraints, etc.)
- How do you incorporate security and privacy in your daily work life?
- 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 (15-20 min)

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.

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

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

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

- When do you typically implement security and privacy in your development cycle?
- 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?
- Do you personally believe that your development cycles are including security considerations to the extent that they should?
- Do you get sufficient resources and training to enable this?
- Do you follow Agile methodology in your development cycle? If so, do you think that Agile processes inhibits the developers to do continuous integration of security in development cycles?
- Is management buy-in a contributing factor for this inhibition? According to you what role can management play in encouraging adoption of security and privacy inclusion in development cycles?

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

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

- How has data collection behavior in your organization changed after GDPR?
 - What all has changed? Could you provide some examples?
- When is the data-collection management planning done?
 - Is it done early in the stage with proactive planning or post fact 'fixing'?
- 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 (15-20 min)

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

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

