UTRECHT UNIVERSITY

MASTER THESIS

Mental models of Shadow IT

Author:
Floris Jansen

1st Supervisor:
dr. Katsiaryna Labunets
2nd Supervisor:
dr. Slinger Jansen
External Supervisor:
Niels Wagenaar

A THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN

Business Informatics
Department of Information and Computer Sciences

August 16, 2023

Abstract

[Background] In large organizations, various employee cohorts have differing perceptions of shadow IT and its impact on the threat landscape. This leads to distinct mental models influencing the use or avoidance of these unapproved systems. Despite recognizing significant risks, an awareness-action gap exists, leading to the continuing use of shadow IT. [Aim] This study aims to understand employee perceptions of shadow IT and its associated risks to find the mental models that influence the shadow IT decision-making process and to identify measures to manage these challenges. [Method] We adopt a mixed-methods approach, including a systemic literature review on mental models in cybersecurity, a survey with 450 responses to uncover types of shadow IT, and 32 interviews to extract mental models. [Result] We found types of shadow IT throughout the cohort groups, demonstrating an inclination towards familiar tools. We found ten distinct mental models that influence shadow IT behaviour, categorized as risk-averse or risk-tolerant. Both previous shadow IT consequences and external factors, such as discussions or training, affect these mental models. An individual may hold a combination of mental models. Moreover, we identified an awareness-action gap, with individuals aware of risks but not acting upon this knowledge. [Conclusion] Measures like open discussions for technology needs, awareness training, and implementing shadow IT protocols are suggested to better manage the challenges associated with shadow IT. Future research should focus on identifying all mental models present in organizations, how these models affect shadow IT behaviour, and how to shift towards a safer and more governed direction in shadow IT behaviour.

Contents

1 Introduction

1.1 Introduction

In the current state of the digital economy, businesses heavily rely on information technology (IT) and employees are increasingly adopting new digital solutions to accomplish tasks. Studies by Mingay (2014) and Haag and Eckhardt (2015) show that the use of applications, that the management and IT department of the organization do not know of is increasing. These applications are called shadow IT.

These applications can range from software like Spotify and Dropbox to hardware in the form of private phones or laptops. If these are allowed by the organization's policy, it is called Bring Your Own Device (BYOD) (Käss et al., 2021), and are often used by individual employees or departments to solve specific business problems, improve workflows, or simply because of personal preference (Haag and Eckhardt, 2015). This phenomenon can potentially be seen in all departments, end-users, and contractors in an organization. While shadow IT can provide benefits, such as increased productivity and innovation (Dhillon et al., 2016), it can also pose risks to an organization, including security breaches and compliance violations (Mingay, 2014). Forbes and IBM Insights released a study that surveyed 353 executives across the globe. Here 46% of the executives said that shadow IT makes it impossible to protect all of their data, systems, and applications all the time. Moreover, due to the fact that systems and processes within an organization are becoming more and more connected, a single flaw in the system due to an occurrence of shadow IT can lead to great consequences within a company. (Forbes Insights, 2019)

Shadow IT brings new vulnerabilities to the cybersecurity landscape of an organization. How can organizations protect what they cannot control? In order to find out security mitigation of shadow IT-related threats, we need to understand *how, when, why* different employees perceive shadow IT. Different roles, teams, and expertise within an organization might have different understandings of what shadow IT is and what consequences it may cause. This is why we focus on the understanding of shadow IT across different departments and ranks.

In order to formalize these different understandings, we use mental models. Mental models are the internal representations of external reality that individuals use to understand, predict, and make decisions about the world around them (Johnson-Laird, 1983). These models are shaped by an individual's experiences, education, and cultural background, and they influence how they perceive and interact with the world (Kahneman et al., 2011). Several mental

model studies have been conducted on cybersecurity concepts, and end users often have incorrect mental models of these concepts (Fulton et al., 2019; Krombholz et al., 2019). In the context of shadow IT, mental models play a crucial role in how different cohorts understand and approach the use of unapproved technology within their organization. By understanding these mental models, organizations can better manage and mitigate the risks associated with shadow IT, while still enabling different teams to use technology in ways that support their work.

1.2 Contributions

This study explores the mental models of employees regarding shadow IT in a corporate context. Specifically, we try to understand how employees in different groups in large professional services companies perceive the concept of shadow IT, the impact of shadow IT applications on the threat landscape, and the factors that influence their decision to adopt or avoid shadow IT instances.

By eliciting the mental models of different employees, we can find gaps in their understanding of shadow IT and potential misconceptions that may explain their behavior. This information then informs the development of tailored training interventions that bridge these gaps and address these misconceptions (Rohrmann, 1992), ultimately improving the cybersecurity of corporate environments.

In addition, an investigation into the mental models of users can reveal use cases that have been overlooked, highlighting areas to improve the resiliency of shadow IT and increase awareness in this regard. By identifying areas for improvement, we can enhance the effectiveness of these tools in meeting the needs of corporate users, while minimizing their impact on the organizational threat landscape.

1.3 Research aim

Overall, this thesis aims to explore the mental models across different employee groups (department and rank) that drive the use of shadow IT and identify ways in which organizations can leverage these mental models to better manage the risks and benefits of shadow IT. To accomplish this, we conduct a systemic literature review (SLR) on existing research on mental models of cybersecurity concepts, followed by a survey and mental-model extraction interviews. The results of the SLR and the survey provide an initial understanding of the occurrence of shadow IT and a guide on how to elicit the mental models. The overarching research question that we try to answer is: **What are the implications of the similarities and differences in shadow IT mental models across different cohorts in a large organization?**

1.4 Thesis layout

This thesis follows a step-by-step approach, employing a mixed-methods approach. After the introduction, chapter 2 presents related work on both shadow IT and mental models. Chapter 3 introduces the research methods, research questions, context, and potential threats to validity, while also explaining how different parts of this research connect with each other. Chapter 4 is dedicated to a literature review on building mental models of cybersecurity concepts. We then find an exploratory survey on the occurrences of shadow IT in chapter 5. In chapter 6, we present the interview findings and extract the mental models. We analyze the obtained results in chapter 7, where we identify patterns in the occurrence of the mental models across cohorts. In chapter 8, the discussion evaluates these patterns by combining insights from the findings with the implications of previous chapters, providing a comprehensive overview of the results, limitations, and contributions to both the academic field and practical applications. Finally, we answer the main research question in chapter 9 and conclude this research. In addition, we offer suggestions for future work in the field.

2 Related work

This section provides context and background for the two main concepts of this thesis: shadow IT and mental models, and discusses related work.

2.1 Shadow IT

First, we are going to get a better understanding of the concept of shadow IT and the risks and implications it brings. Recent work by Gadellaa (2022) notes an extensive tertiary literature review on the concept of shadow IT.

2.1.1 The concept of shadow IT

This review focused on the following aspects: (i) the definition of shadow IT, (ii) which parts of an organization's IT ecosystem are covered by this concept, (iii) related concepts, and (iv) research directions. For this research, we briefly synthesize the most important information about the definition of shadow IT and related concepts.

Early work on shadow IT focuses on extensions to big information systems, such as CRM or ERP systems (Kretzer and Maedche, 2014), and therefore defines it as: "unofficial IT extending an existing IS". Other research defines it as: "process supporting IT systems, IT service processes, and IT staff [...]" (Zimmermann and Rentrop, 2012). However, because of fast developments in enterprises, there was a need for an overarching definition due to the constant adaptation of shadow IT in new forms. Kopper and Westner (2016) developed a concept hierarchy for shadow IT, defining "feral practices" as the overarching concept. Next to the taxonomy (see Figure 2.1), this research was one of the first that analyzed the causes, consequences, and governance of shadow IT. This taxonomy led to an increased presence of the concept of business-managed IT, which is distinguished from shadow IT based on what scenario it is observed in.

Multiple new concepts that resemble a shadow IT form are defined due to trends, creating some overlap between those concepts. However, Käss et al. (2021) adds three new specific aspects to shadow IT and business-managed IT:

- *Lightweight IT*, introduced by Bygstad (2015), encompasses smaller-scale IT initiatives undertaken by business units and supports front-end work by enabling quick adaptation of new innovations. It is a positive view of what business-managed IT can contribute (Godefroid et al., 2021).

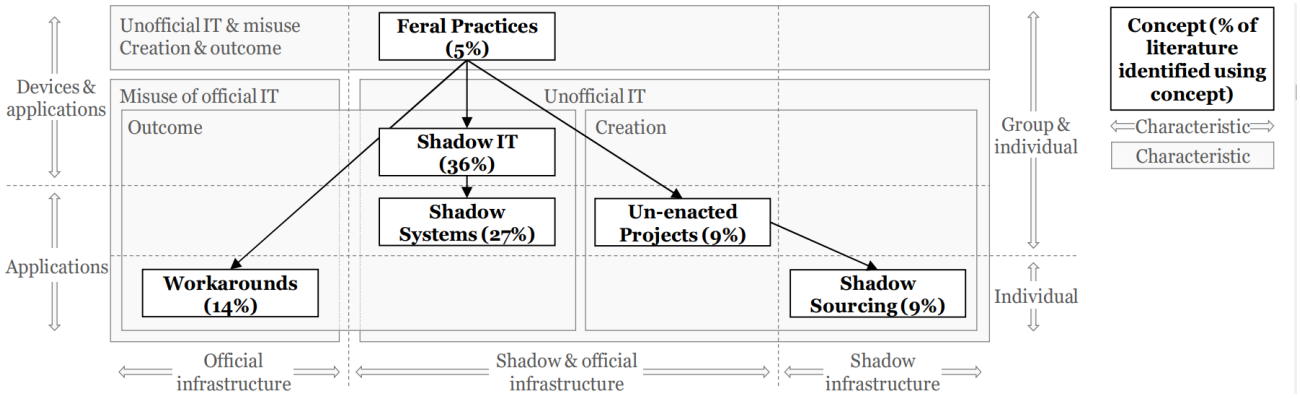

FIGURE 2.1: Taxonomy for shadow IT (Kopper and Westner, 2016)

- *IT consumerization* refers to the trend of using consumer-oriented devices, applications, and services for business purposes, as shown by Yan et al. (2016). Although it may result in shadow IT, it primarily refers to the trend and enabling/causing factor, rather than the specific devices or applications observed within an organization.
- *BYOD* (Bring Your Own Device) is a form of IT consumerization, as described by Käss et al. (2021), where employees use their private devices for work purposes instead of company-owned devices. It holds solely to hardware and is mostly used to describe the policy allowing the use of such devices. However, the policy may lead to shadow IT in the form of unapproved applications, despite acknowledging and allowing the use of these devices (French et al., 2014).

Despite the lack of a single agreed-upon concept in the literature, a consensus can be seen regarding the overall definition of shadow IT. While various specific directions are explored with success, the definition remains consistent. The difference between shadow IT and business-managed IT introduced by Kopper, Fürstenau, et al. (2018) is useful to indicate a situation where initial shadow IT is managed more specifically by a business unit. From the review by Kopper, Fürstenau, et al. (2018), it shows that the definition of Haag and Eckhardt (2017) best covers the concept of shadow IT, as was mentioned in all but one of the SLRs used for the tertiary review: **"Shadow IT is hardware, software, or services built, introduced, and/or used for the job without explicit approval or even knowledge of the organization."**.

Within this definition, Mallmann et al. (2018) categorized shadow IT occurrences in the topology illustrated in Table 2.1. We adopted this topology as it helps to identify various shadow IT occurrences.

2.1.2 Cyber threats related to shadow IT

Gadellaa (2022) conducted an exploratory study on cyber threats associated with shadow IT. The literature in the mapping study highlights that shadow IT creates cybersecurity risks for organizations. Empirical records also support this concern, with security issues being the most mentioned risk of shadow IT by IT managers. However, it is not always clear why or how this is the case.

Unapproved cloud services	Use of Internet-based Software and Software as a Service (SaaS) that are not approved or unknown by the IT department. These systems are also called Mobile Shadow IT once they can be accessed outside the workplace.
Self-made solutions	Use of solutions developed by employees on the company's computers to perform their work tasks. For example, an Excel spreadsheet or an application developed by employees
Self-installed applications	Use of software installed by employees to perform their work tasks on the company's computers. For example, downloading and installing software available free of charge on the internet.
Self-acquired devices	Use of devices owned by employees. These devices are purchased directly from retail rather than being ordered through the official catalog of the IT department. It includes the use of applications in the employee's personal devices at the workplace.

TABLE 2.1: Shadow IT topology by Mallmann et al., 2018

One of the most interesting findings of Gadellaa (2022) is that very few specifics are mentioned with regard to actual cyber threats. The first papers that actually do this are based on grey literature (Johnson, 2013; Walters, 2013). The first extensive approach is from Silic and Back (2014), their research determined that shadow IT caused significant problems like opening the network to malicious users and data integrity or exposure issues.

At the governance level, the primary challenges produced by shadow IT are the lack of professional quality assurance and accountability for maintenance. These issues may result in unpatched systems and old software versions. Unfortunately, the literature lacks clear and concrete security threats and instead only mentions noncompliance and governance issues. Because of this, developing a mitigation strategy for shadow IT security is challenging.

2.2 Mental Models

In Volkamer and Renaud (2013) we find a brief introduction to the concept of mental models and their relation to security. We synthesize some key findings from this research in this section. The concept known as the 'mental model' was introduced in the book by Craik (1967) called 'The Nature of Explanation'. He defined this concept as some functional internal construct that operates similarly to the process it represents. However, whilst not introducing the concept, the same idea had already been discussed before this. Johnson-Laird (2005) wrote about the history of the evolution of mental models, and showed that Boltzmann (1890) had first discussed the idea, specifically "forming an internal representation of the external world". The definition we use for this research is as follows: a mental model refers to a person's thought process about how the world works. It is a kind of internal symbol or representation of external reality, hypothesized to play a major role in cognition, reasoning, and decision-making. In essence, a mental model is a framework or cognitive structure based on one's life experiences, perceptions, and understandings of the world (Johnson-Laird, 1983).

2.2.1 Capturing Mental Models

Since mental models are internal representations of a person's knowledge, this raises the question of how to capture mental models, specifically, how to capture the details and nuances in them. D. A. Norman (2014) found that mental models can be incomplete and unstable, moreover they can be confused with one another. Jones et al. (2011) confirms this by illustrating that mental models are inconsistent and are subject to adaptation and growth over time. This illustrates the difficulty of capturing mental models since these are not static. Researchers typically do this by letting participants express their comprehension of a certain subject. Payne (1991) observed that while participants were verbalizing their thoughts, they were evolving and therefore found that verbalizing might not be the best way to capture mental models. This is supported by work from Richardson et al. (1994), whose work showed that capturing mental models could lead to the change of these mental models.

In order to find out what elicitation methods work best for capturing mental models, Rowe and Cooke (1995) compared several methods in which he compared the quality of the models. A main finding was that the think-aloud method did not yield good results, moreover, that diagramming yielded good depictions of mental models if the participant had a good mental model.

Similar research in comparison of different mental model elicitation techniques has been done by Langan-Fox et al. (2000). This leads to the conclusion that the optimal elicitation methods are very dependent on the merits of the research itself and the practicalities involved. Specifically, Volkamer and Renaud (2013) notes that: "Accessing a mental model is challenging because one runs the risk of interfering with what one is attempting to measure. Even so, it is important to elicit mental models and, in the process, try to alter them as little as possible. Drawing diagrams where applicable seems to be the most promising approach."

2.2.2 Mental Models of Security

We must combine security interactions, instructional activities, and risk communication with users' mental models to minimize threats. Individuals are only able to defend themselves when their mental models include an awareness of potential vulnerabilities that might be targeted. Therefore, it may be required to adapt or change users' mental models to maximize the likelihood of them taking appropriate actions to protect themselves. Understanding how individuals conceptualize system security is essential for security researchers and developers, as it helps in designing secure interactions and evaluating user interfaces.

To explore mental models, researchers employ various methods such as interviews, user studies, and card sorting. These approaches serve different purposes, including enhancing the design of security interactions, communicating risk effectively, tailoring educational efforts, and evaluating the impact of user interfaces on mental models. The development of accurate mental models is crucial for guiding individuals toward safe cybersecurity choices.

In the following section, we present an overview of major research on the subject of human-centered security, highlighting discoveries, limitations, and advances in improving security

interfaces. Specific security-related mental models as outlined in Volkamer and Renaud (2013) are also presented.

Camp (2006) found the following general mental models of security that were used to talk about security and privacy challenges:

- *Physical Security Model* (Due to the lock metaphors)
- *Medical Model* (due to the phrase 'infected by a virus')
- *Criminal Model* (due to the idea of being arrested if you hack into a system)
- *Warfare Model* (due to intrusion detection and firewall tools)
- *Market Model* (due to people losing money)

These mental models are explained with the positive and negative implications that they bring with regard to user behavior security decisions. She clarifies that each mental model only addresses certain aspects of security and privacy issues, therefore provides only protection against a few possible attacks. The found mental models in Camp (2006) are validated in Liu et al. (2007) through card sorting and interviews, and in Furman et al. (2011) through in-depth interviews. The mental models were validated between experts and non-experts. Their findings revealed that many identified security risks were linked to a few of the identified mental models.

A study conducted by Wash (2010) identified folk models of security threats to home computer users to find their choice of security software and capture participant understanding of security advice. He identified eight separate folk models and demonstrated how these motivated participants to deviate from following general recommendations. He found four folk models for *risks*, these folk models focus on the participant's understanding of viruses:

- *Viruses - generally bad* - but only high-level understanding
- *Viruses causes mischief* - understanding that viruses cause annoying problems with the computer or data
- *Viruses intentionally downloaded in buggy software* - the computer will crash or not work anymore.
- *Virus that supports crime* - by stealing personal or financial information.

Besides, he identified four folk models that described user understanding of *threats*. These folk models focus on participant understanding of hackers:

- *Hackers perceived as geeks* - who want to impress friends
- *Hackers are criminals* - who target rich and important people
- *Hackers support crime* - looking for large databases or other information
- *Hackers are burglars* - by stealing personal or financial information

The mental models that individuals adopted influenced their decision to make backups, install antivirus software, and their openness to security-related guidance. For instance, some participants felt that they were only able to contract a virus if they accessed unsafe parts of the Internet, and therefore had the incorrect mental model of being invulnerable when on the Internet. Other participants considered themselves too unimportant to be targeted by hackers

and believed they were not at risk. This study was re-run in Kauer, Günther, et al. (2013), where three additional mental models were identified. These extra mental models were variants of the existing eight mental models with a focus on governmental aspects of computer security, illustrating the understanding that the government could deploy viruses and hackers to gain information.

Besides the mental models on general security aspects. We find studies of more specific concepts such as a secure network connection (Friedman et al., 2002). This research presents the following mental models:

- *Transit* - secure the data during transfer, thus making the transit secure
- *Encryption* - using an encoding and decoding mechanism to secure the data itself
- *Remote side* - protecting the data upon arrival at recipient. Participants assumed that the connection is always secure.

The study of (Benenson et al., 2012) illustrates the difference in mental models of privacy and awareness between Android and iOS users. He found two mental models, the *Android* mental model, and the *iPhone* mental model. The research found that Android users were more privacy-aware and they cared more for technical features. On that same note, the participants that did not care so much for technology mostly had an iPhone.

To summarize, we observe that mental models are vital for understanding (cyber) security and shaping individuals' behaviors. They are internal constructs that resemble the processes they represent. Capturing dynamic and evolving mental models is challenging, but methods like verbalizing thoughts and drawing diagrams show, however, the methods need to be tailored to the research. Aligning security interactions, education, and risk communication with users' mental models is crucial for effective safeguarding. Accurate mental models can guide better-informed security decisions and address specific issues. Understanding users' mental models helps design secure interactions and encourage engagement. Overall, mental models contribute to human-centered security research, offering insights and improvements in security.

2.3 Differences in Mental Models

A study by Staggers and Norcio (1993) illustrated that there are big differences in the mental models of experts and non-experts. That was confirmed by multiple studies after (Liu et al., 2007; Asgharpour et al., 2007; Furnell et al., 2007). Moreover, Asgharpour et al. (2007) illustrated that there is a link between the mental models of security risks and expertise in security. These researches all reported discrepancies between the mental models of participants in different groups.

In another study conducted by Bravo-Lillo et al. (2010), an investigation into mental models examined how both experts and laypersons make decisions regarding following or disregarding security warnings. Experts were defined as individuals who took a minimum of one year of relevant coursework or had engaged in a relevant assignment for a minimum of one year.

The study found distinct differences between novice and expert users, confirming previous research findings. Experts actively sought vulnerabilities and considered multiple factors when encountering potential risks, whereas novices performed fewer security checks. Novices often associated warnings with viruses or disregarded them altogether. Moreover, when beginners performed an activity, they were inclined to evaluate its safety only afterward, while experts demonstrated greater caution by evaluating the safety of a task beforehand, considering prior moves, the nature of the data, and potential consequences. Novices had a higher level of confidence in big organizations' abilities to prevent harm to them, assuming that banking was secure due to its established reputation for reliable safety.

These insights all align with other studies (Wu et al., 2006; Friedman et al., 2002; Kauer, Kiesel, et al., 2012), which showed that novices based their decisions on the visual appearance of websites. In contrast, experts acknowledged that banking sites containing these cautionary messages were often untrustworthy. The study also uncovered wrong perceptions related to online data retention. Novices assumed that keeping a record posed a greater risk than opening it, considering file opening as a protected glimpse while downloading that same record locally was perceived as having an immediate threat to their system due to the record's presence.

Overall, numerous studies have shown that there are differences in the way experts and non-experts think about security. Experts take security more seriously, actively looking for vulnerabilities and considering various factors when faced with risks. On the other hand, non-experts tend to be more careless, ignoring warnings or thinking they are just about viruses. Non-experts also often assess the safety of their actions after the fact, while experts are more cautious and think ahead.

We observe different mental models across groups of experts vs non-experts with regard to security cybersecurity concepts. This implies that dependent on how groups are made, differences in mental models can be observed and lead to a better understanding of how to influence behavior in these groups to better protect all end users across these different groups. This sets the stage for the rest of this research.

3 Research Approach

3.1 Research Goals

The overall research goal is to understand how different groups in a large company conceptualize shadow IT and the risks it brings, using mental models. We gather all empirical data from a large professional services company which we further elaborate on in section 3.5.

To try and accomplish this, we analyze the organization through 2 cohorts: department and rank. The different departments are:

1. **Support staff: HR, accounting, and legal**
2. **Client facing staff**
3. **Internal IT security department**,
4. **Management: partners and (associate) directors**

For the rank, we try to uncover the difference in mental models across:

1. **Junior**
2. **Senior**
3. **Manager**
4. **Senior Manager**
5. **Management**

In order to elicit the mental models on shadow IT, we conduct an SLR to find out how to elicit mental models on cybersecurity-related concepts. Then by means of an exploratory survey, we gain actual insight into the current occurrence of shadow IT per cohort. We synthesize the information from the SLR and insights from the survey to create the mental-model-extraction interview protocol. These interviews further clarify the level of shadow IT knowledge per cohort. We analyze the results from the interviews and extract the mental models. Finally, we analyze the mental models and identify patterns in the occurrences.

3.2 Research Questions

The research goals above are accomplished by answering the main research question:
(MRQ) **What are the implications of the similarities and differences in shadow IT mental models across different cohorts in a large organization?**

The main research question is guided by four sub-questions. We answer the first sub-question

through a systemic literature review on mental models of cybersecurity concepts.

(RQ1) **How are mental models used to explore user understanding of cybersecurity-related concepts?**

The next question aims to gain an understanding of the current status of shadow IT. We answer this question by employing an exploratory survey that illustrates what applications of shadow IT can be observed across different cohorts.

(RQ2) **What types of Shadow IT can be observed across different cohorts?**

The following sub-question aims to gather empirical data on how shadow IT is perceived by different cohorts using extensive, qualitative, interpretive methods. With the information gained from the SLR and insights from the survey, we create an interview protocol. These interviews extract the mental models and provide context to user understanding of shadow IT. The information from the interviews answers the following sub-question:

(RQ3) **Across different cohorts, what is the perception of the concept of Shadow IT, and what are the perceived risks and implications of shadow IT?**

This section aims to find patterns in the mental models found across different cohorts. We identify mental-model occurrence patterns through departments and ranks, answering the last sub-question:

(RQ4) **What patterns are found across cohorts regarding shadow IT mental models?**

Understanding the difference in how different cohorts perceive shadow IT using mental models, provides the knowledge on how to create specific guidelines so that the implications of shadow IT are minimized. This motivates IT departments to divert from a 'one size fits all' approach to a tailored approach towards different groups of end-users. Moreover, this sets the motivation for future mental model research to uncover differences and similarities in mental models of different cybersecurity concepts across different cohorts of participants.

3.3 Research Methods

Table 3.1 illustrates the research questions, the methods used to answer each question, and the section where the results can be found. We explain the research methods in the next sections of this chapter.

Question	Method	Results
Main	All of the below	Chapter 9
RQ1	Systematic literature review	Chapter 4
RQ2	Survey	Chapter 5
RQ3	Interviews	Chapter 6
RQ4	Analysis of SQ3	Chapter 7

TABLE 3.1: Overview of methods

3.3.1 Systematic literature review

In order to answer the first sub-question: *How are mental models used to explore user understanding of cybersecurity-related concepts?*, an SLR into mental models describing cybersecurity-related concepts provides the basis for the actual creation of mental models later in this research. An SLR is a method of gathering, reviewing, and analyzing data from existing manuscripts on a specific research topic or phenomenon in order to provide a comprehensive overview, explanation, and evaluation of the topic (Kitchenham, 2004). The SLR is done according to the guidelines and steps set by Keele et al. (2007) and Petticrew and Roberts (2008) to gather the current state of the art on the creation of mental models on cybersecurity-related concepts. As outlined by the guidelines, our study follows three stages: *planning*, *execution*, and *documentation* of the review. The SLR is driven by the need to uncover how mental models are used in the cybersecurity landscape. We searched for similar studies in academic search engines. However, we did not find any SLR about mental models on cybersecurity-related concepts, with similar goals and objectives.

3.3.1.1 SLR Protocol

We answer the first research question by analyzing the manuscripts along two components: (see Table 3.2 for assessment variables).

1 - Scope In what domain do the found manuscripts describe mental models and what are the goals of the manuscripts? This section outlines all cybersecurity concepts that have been described with mental models. In addition, the applications within these domains can be outlined to get an overarching overview and perhaps identify gaps for further research. Moreover, we assess if the manuscript creates a mental model. We provide a yes/no answer for each manuscript.

2 - Method What are the most common ways to create mental models and how are these portrayed? Mental models have been used in a number of different disciplines and there are over 10 ways to elicit them (Hudson-Doyle et al., 2022). This component focuses on what elicitation methods and procedures are used and illustrates the relevance and qualities of each elicitation method. Furthermore, what did the division of participants and demographics look like? Finally, this component focuses on how the mental models are depicted in the found manuscripts. This component is only relevant for manuscripts that create mental models and therefore we expect to display these characteristics only for a subset of the found manuscripts.

Mental Models on cybersecurity concepts (RQ1)		
Scope		Domain
		Goals
		Creates Mental Model
Method	Technique	Technique X
		Technique Y
		Technique Z...
	Type of analysis	Qualitative
		Quantitative
	Participants	Amount
		Cohort
		Age
		Requirements
		Recruitment
	Representation	Method A
		Method B
		Method C...

TABLE 3.2: Assessment variables for answering RQ1

3.3.1.2 Search Strategy

The relevant manuscripts are found through an automatic search with a search string. From Brereton et al. (2007), we learned that the search terms should be grouped. In this case, the scope of the study is set into the area of mental models. Secondly, we discuss shadow IT or cybersecurity-related concepts such as threat, cyber, and security. This resulted in the following search terms per group:

1. ("mental model*" OR "mental image" OR "mental representation") AND
2. ("cyber*" OR risk OR threat OR security OR "Shadow IT")

3.3.1.3 Sources to be searched

For the automatic search, we used the following databases: **Scopus**[1]**, Web of Science**[2]**, ACM Digital Library**[3]**, IEEE Xplore**[4] **and Wiley Inter Science Journal Finder**[5]. These electronic databases are selected through the overview and criteria by Gusenbauer and Haddaway (2020). Four of these search systems are labeled "principal search system", meaning these electronic databases met all the quality requirements. We included the supplementary search engine IEEE Xplore to find specific information systems research. To ensure that only high-quality sources are considered, we only used electronic databases with peer-reviewed works. In addition, these databases have to support complex queries and searching in metadata (title, keywords, abstract). We did not consider databases that rely on crawlers, such as Google

[1]https://www.scopus.com
[2]https://webofscience.com
[3]https://dl.acm.org
[4]https://ieeexplore.ieee.org
[5]https://journalfinder.wiley.com

Scholar and Microsoft Academic since they can include grey literature and produce inconsistent results (Orduña-Malea et al., 2015). We use the previously named search engines as follows: we use Scopus as the primary database and to identify any potentially missed manuscripts we searched: Web of Science, ACM Digital Library, IEEE Xplore, and Wiley Inter Science Journal Finder.

3.3.1.4 Screening and filtering

Several screening and filtering steps ensure that the manuscripts used for the final analysis are relevant and of high quality. We use a three-step filtering process: (i) remove duplicates, (ii) apply inclusion and exclusion criteria and (iii) assess manuscript quality according to the scoring system introduced later in this section.

Especially the inclusion/exclusion criteria and scoring system criteria must be just right; if the criteria for including manuscripts are too broad, it is possible that low-quality manuscripts are included, which can weaken the overall quality of the results. On the other hand, if the criteria are too strict, the number of manuscripts that are included may be small and may not be representative of the broader population, making it difficult to generalize the findings to a larger group. It is important to strike a balance between these two considerations in order to ensure the validity and reliability of the research Meline (2006). Table 3.3 presents the inclusion and exclusion criteria.

Inclusion criteria:
• Manuscripts that create or describe mental models of cybersecurity concepts • Manuscripts that relate to computer science • Manuscripts that are published through a conference or journal • Manuscripts published in English
Exclusion criteria:
• Manuscripts that were published before 2010 • Manuscripts that were not fully available • Manuscripts that were grey literature • Short publications and posters (<3 pages)

TABLE 3.3: Inclusion and exclusion criteria

We include manuscripts that construct or describe mental models of cybersecurity concepts, are related to computer science, and those published in an English-language conference or journal. These criteria aid in ensuring that the articles chosen are focused on mental models of cybersecurity concepts and are published through quality-assuring channels. Exclusion criteria, on the other hand, seek to exclude manuscripts that are irrelevant, incomplete, or of poor quality. Therefore we exclude manuscripts that are published before 2010, are not fully available, and are grey literature or posters with fewer than three pages.

Since we use digital search, there is a lot of noise in the quality of the results. In order to assess the quality of the found manuscripts, we use an internal scoring system. This scoring system checked the following aspects of a found manuscript: Research.com rank (for both

the conference[6] and journal papers[7]), for conference papers the CORE[8] ranking portal. For journal papers: the SJR[9] ranking data, the number of citations, and the year of publication. We briefly explain each metric in the following section.

Research.com relies on multiple sources of data that undergo cross-correlation and thorough examination and validation to guarantee the accuracy and dependability of our rankings. The primary aim is to highlight premier venues for research and provide a platform for aspiring researchers to be motivated by renowned scientists. For the conferences: Research.com indexes major conferences in the area of computer science and electronics. The ranking of the best conferences is based primarily on the H5-index indicator provided by Google Scholar[10] together with other valuable indicators including the indexing of proceedings, sponsoring bodies, number of editions, and the profiles of its steering committees. For the journals, Research.com provides a list of top-rated journals in various fields, which are subject to annual selective review based on various metrics that assess the quality of published papers and the journal's impact score.

We use the *CORE ranking portal* in addition to the Research.com data to assess the rank of conferences. The classification system categorizes conference and journal venues as follows: (i) A* - premier venues in the field, (ii) A - highly esteemed venues, (iii) B - reputable venues, (iv) C - venues that meet the basic criteria, and (v) Unranked - insufficient data has been supplied to establish a ranking.

The *SJR journal rank* is a publicly accessible platform that showcases journals and country-specific scientific metrics derived from the data in the Scopus database. These metrics serve as a tool for evaluating and analyzing scientific domains. The classification of journals is as follows: (i) Q1 - top 25% of journals, (ii) Q2 - 25% to 50% of journals, (iii) Q3 - 50% to 75% of journals, (iv) Q4 - 75% to 100% and (v) - Unranked, there is not enough data to establish a ranking.

The *number of citations* is considered in the internal scoring system, however, since there is no clear evidence that citations reflect other key dimensions of research quality (Aksnes et al., 2019), it only has a minor impact on the scores. This also holds for the year of publication. More recent papers get a better score, however, this impact on the total score is also minor.

All these metrics accumulate to a score per manuscript. We set a threshold value that decides the final set of manuscripts. After all relevant, high-quality papers have been selected, we conduct forwards and backward snowballing to identify potentially missed publications. We perform snowballing with the help of the guidelines by Wohlin (2014) in order to ensure that the snowballing is done in a structural and systematic way.

[6] https://research.com/conference-rankings/computer-science
[7] https://research.com/journals-rankings/computer-science
[8] http://portal.core.edu.au/conf-ranks/
[9] https://www.scimagojr.com/journalrank.php?area=1700
[10] https://scholar.google.com/intl/en/scholar/metrics.html

3.3.1.5 Data extraction

Table 3.2 illustrates the assessment variables used to structure the information that was needed to answer RQ1. To follow the three-step process of Petticrew and Roberts (2008), (i) we organize the found manuscripts in these categories, (ii) then we need to analyze the findings within each of the categories and (iii)finally synthesize the findings across all found manuscripts.

3.3.1.6 Quality assurance

A second researcher performs a separate data extraction on a random 10% of found manuscripts to compare and discuss the results, ensuring high data quality.

Moreover, we validated the search string by adding the title, keywords, and abstracts of all manuscripts that were included in the SLR in one file, and letting a natural language processing program[11] find all keyword pairs. This list can then be compared to the original search string.

3.3.2 Survey

We use an exploratory survey to answer the second research question: *What types of Shadow IT can be observed across different cohorts?*. The responses from the survey allow us to gain insights into the current shadow-IT situation. These insights lay a foundation for later in this research, upon which the interview results can be contextualized.

3.3.2.1 Methodology

To depict the differences in the occurrences of shadow IT, we first identify the places and forms that it occurs in. We use the topology by Mallmann et al., 2018, also provided in section 2.1.1 to specify the types of shadow IT. This topology defines the following types of shadow IT: *Cloud services*, *Self-installed applications*, *Self-built applications*, and *private devices*.

Next, we uncover in what setting these types of shadow IT can occur. We created a structure with three scenarios where a shadow IT instance can possibly occur through querying multiple cybersecurity experts. Together these scenarios are mutually exclusive and collectively exhaustive: meaning that combined, they cover all the possibilities where shadow IT can occur however they do not overlap. The scenarios are as follows:

- *(Shadow IT occurring in)* Specific client projects
- *(Shadow IT occurring in)* General work tasks, so not for specific projects
- *(Shadow IT occurring in)* Personal use

The found shadow-IT types and scenarios serve as the backbone of the survey and guide the structure and content of the questions.

[11] https://app.sketchengine.eu/#keywords

3.3.2.2 Development, Deployment, and Data Collection

We implemented the survey development within the framework of a Utrecht University-supported Qualtrics[12] environment. We create the survey through an extensive iterative process across multiple phases. Initially, we propose an initial set of questions and answer options, and create the proceeding revisions based on pilot testing and verbal feedback from participants. This iterative approach helped to improve question layout, explanation, and formulation of both questions and answer options. We performed three rounds of piloting, with two participants in each round. Notably, the pilot testing involves a fresh set of participants for each iteration, ensuring diverse perspectives and minimizing bias. Eventually, we conduct a split test with a within-subjects design, comparing the two most promising versions of the survey and resulting in the selection of the final version.

We divide the core of the survey into four main sections, the first three sections each describe one of the three scenarios described in section 3.3.2.1. Each of these first three sections contains three questions: one for a type of shadow IT, namely *Cloud services*, *Self-installed applications*, and *Self-made solutions*, which fall outside the scope of their organization. The fourth and final section covers the *Self-acquired devices*. This separation was a result of the feedback in the iterative process when developing the survey.

In addition to the core questions, the survey contains several supplementary sections. These sections include an informed consent section, a demographics section, a detailed explanation section, and a final section providing participants with the opportunity to leave their email addresses to enter the raffle and opt-in for follow-up interviews.

We asked respondents what types of applications or services they used in certain scenarios through multiple choice questions with multiple answer options. The initial answer options for the different types of shadow IT were derived from the types found by Gadellaa (2022). We tested and modified these answer options through pilot surveys. However, for each question, there also was an *Other* answer option if the respondent used an application type that was not present within the answer options. If a respondent answered they used a certain type of application, we then asked the name of that application. We thus then have both quantitative data about how many respondents use what types of applications, and qualitative data in the form of what applications they used.

Data collection for the survey spanned the months of April and May 2023. The recruitment strategy employed both digital and physical means. Digital recruitment involved leveraging mailing lists to send invitations to potential participants. These invitations included a comprehensive overview of the research's purpose, a digital copy of the survey flyer, and a link for accessing the survey. Physical recruitment efforts meant distributing flyers within office spaces, accompanied by face-to-face communication to explain the research's objectives. The flyers incorporated a QR code that directed interested individuals to the survey. Participants did not receive financial compensation for their involvement in the survey, however, to enhance response rates, we raffled four prizes comprising two gift cards and two goodie bags.

[12] Utrecht University Qualtrics portal: https://survey.uu.nl

Winners were selected randomly following the survey's closure, and the distribution of prizes occurred during the first week of June.

The final anonymized version of the survey can be found in appendix D

3.3.2.3 Statistical Methods

Gathering enough responses allows for statistical analysis. The dataset provides interesting insights into the patterns of certain types of shadow IT within different cohorts within the organization. The cohorts that are analyzed are department and rank. Statistical methods decide with a significance level of 0.05 with Pearson's Chi-Square test if certain cohorts are statistically different (McHugh, 2013). Moreover, if the sample sizes would have been equal, this would also illustrate if certain groups are statistically similar with the Chi-square test for homogeneity. However, our different cohorts are of different sizes and therefore we can not run this test. The Chi-square holds the following assumptions: (i) *the data in the cells should be frequencies*, (ii) *the variables are mutually exclusive*, (iii) *each respondent can only contribute to one cell per analysis*, (iv) *the study groups must be independent*, (v) *there are 2 variables, that are both measured as categories* and finally, (vi) *the value of the cell must be 5 or more in at least 80% of the cells*. This last assumption is also a significant issue for this research, since within the department cohort, the group for IT staff is very small and might therefore yield incorrect results. We thus enhance the statistical analysis by also performing Fisher's exact test. This test also compares categorical variables, however, is capable of computing more accurate p-values with expected frequencies under 5 per cell (Conover, 1999). Moreover, Fisher's exact test holds the following assumptions: (i) *the variables must be mutually exclusive*, (ii) *The row and column totals must be constant*, (iii) *Both variables under consideration should be categorical*, (iv) each observation is independent of the other observations. (Fisher, 1992)

Beasley and Schumacker (1995) states that no Chi-square test should stop with the computation of a Chi-square statistic, therefore we perform a post-hoc test using residuals to find out what groups cause the statistically significant difference. This residual analysis finds the specific data points that have the biggest influence on the chi-square computation results (Sharpe, 2015). This then allows for analysis of why certain groups in different cohorts have such influence on this answer option. According to Sharpe (2015), the residual value represents the difference between the observed and expected frequencies. These are standardized so that they can be compared with different population sizes. This value can both be positive and negative, where positive means the observed occurrence is greater than the expected occurrence and vice-versa for negative residual values. Moreover, a residual value closer to 0 means there is a small difference in the observed and expected occurrences. According to Haberman (1973), if the absolute residual value is larger than 2 the data point contributes significantly to the chi-square result. The interpretation of the residual values is, therefore, a key element in finding significant information from the statistical tests. We present the procedure for performing the residual calculations:

- (i) *Calculate expected frequencies*: add an extra column and row where we calculate the total of each row and column, in addition, we also calculate the grand total. Then per cell, we calculate the (row total * column total) / grand total.
- (ii) *Calculate observed - expected*: subtract the expected frequency from the observed frequency. This value can both be negative and positive.
- (iii) *Calculate standardized residual*: divide the difference from the previous step by the square root of the expected frequency for each cell.

Moreover, if we rely on the results of Fisher's exact test, we can not perform the residual calculations. However, we can do pairwise comparisons. This implies that we perform multiple Fisher's exact tests, one for each pair of groups in that cohort. We need to be careful with doing more tests because doing so increases the chance that we find statistical significance by chance and hence we perform the Bonferroni correction upon the found Fisher p-values (Simes, 1986).

The Chi-squared test is an approximation that relies on the central limit theorem (Greenwood and Nikulin, 1996), and hence its accuracy increases with larger sample sizes. So when the assumptions of the Chi-squared test are not violated, we use the Chi-square p-value and perform the residual calculations. On that same note, we use Fisher's exact test p-value if the Chi-square assumptions are violated. Consequently, we perform the pairwise comparisons with Bonferroni correction if we find a significant Fisher's p-value.

3.3.2.4 Survey design limitations

With this survey design, we find a few limitations and threats to validity. Firstly by providing answer options, we limit the spectrum of types of applications and set boundaries for shadow IT to occur. Even though we provide an *other* option, there is still a bias towards the other answer options.

Secondly, the survey is lengthy and holds some nuances. We split the survey according to four different shadow IT types, and prompt questions in three different scenarios. Thus if respondents do not read the explanation and context carefully enough, the responses can be prone to errors. To try and prevent this, we introduce the following section after the demographics section. Here we try to contextualize the research, by illustrating that we want to observe applications outside of the organization's scope and provide clear and concise meaning to the scenarios.

Please read the following with care. This ensures the rest of the survey can be filled in **quicker** and more **accurately**.

We will ask you questions regarding the software you use that is **outside the [ORGANZATION] scope**.
This means we are interested in applications that are **not facilitated by [ORGANZATION]**.

The survey is split into sections concerning **THREE SCENARIOS**

1. Software needed for *specific client projects*
2. Software needed *work related tasks*, but in general so **not** for specific projects
3. Software needed *for personal use*

By understanding the distinction you can now swiftly go through the rest of the survey!

In addition, at the beginning of the page of each of the three main scenarios, we prompted the respondents a reminder for the applications that were not facilitated by the organization:

IT applications in engagements

This section concerns all applications you had to use for specific clients/engagements that are **not** standard [ORGANZATION] applications.

Note: Standard [ORGANZATION] applications are all applications (e.g. MS Office) that are installed on your laptop or available through the [ORGANZATION] appstore.

IT applications in non-client work-related tasks

This section concerns all applications you had to use for work-related tasks, that were **not** for specific engagements.

Note: Standard [ORGANZATION] applications are all applications (e.g. MS Office) that are installed on your laptop or available through the [ORGANZATION] appstore.

IT applications for personal use

This section concerns all applications you used for personal reasons (non-work related tasks) on your [ORGANZATION] device

3.3.3 Interviews

The interview methods result from the SLR since the main motivation for the SLR is to uncover how mental models of cybersecurity concepts are built. The results from the SLR, therefore, impact the methodology of the interviews significantly. Hence we present the methods used to conduct these interviews in the chapter where the interviews are discussed. We synthesize the main findings from the SLR and find the main implications as to how the mental models for this research are elicited.

3.4 Ethical considerations

We conduct this research with participants, both through the survey and through interviews. In order to comply with privacy regulations and the ability to re-use the data, the research setup underwent careful consideration and review. To ensure the correct handling of participants and their data we did a quick ethics scan at the Science-Geo Ethics Review Board (SG ERB) at Utrecht University for the research protocol and did not find any issues.

A comprehensive data management plan (DMP), the results from the quick ethics scan, the survey informed consent form, the complete survey, interview informed consent form, and interview protocol can be accessed in the appendices as follows: Appendix A: Data Management Plan, Appendix B: summary from the ethics quick scan, Appendix C: Survey Informed Consent Form, Appendix D: Survey, Appendix E: Interview Informed Consent Form, Appendix G: Interview Protocol. Throughout this research, we identify participants by using numerical identifiers, e.g. "P 03". Moreover, we use male pronouns to discuss findings about particular participants. These identifiers illustrate the chronological order of the interviews. Furthermore, participants gave explicit consent to be quoted literally.

3.5 Context of this study

We illustrated the research groups as cohort groups in section 3.1. All participants in this study, both for the survey and the interviews, are from a single large professional services firm. Therefore, there are a few organizational aspects that set the baseline for the potential contextualization of findings. For the survey, in order to contextualize how well-represented the participant sample is to the general population within the organization, we provide a comparison when discussing the participant demographics.

With regard to shadow IT, the organization has specific policies in place. The main note of these policies is that employees should not use non-managed solutions to perform work-related tasks. However, this policy is needed because employees can download and install applications at will, both on their mobile device and their laptop provided by the organization.

To ensure that all employees are knowledgeable about this policy and other guidelines, the organization provides mandatory periodic awareness training. This cybersecurity training concerns sections with regard to shadow IT, however, there are also subjects that need awareness training. Therefore this training does not always contain shadow IT aspects.

The organization has a system in place to perform due diligence on external applications. In other words: the organization has a process to convert shadow IT applications to managed applications. This due diligence is performed by a central entity within the organization.

3.6 Threats to validity

To increase the quality and repeatability of empirical research in the field of computer science, Zhou et al. (2016) provides an overview of threats to validity in SLRs. They introduce four types of validity: (i) Construct validity, (ii) Internal validity, (iii) External validity, and (iv) Conclusion validity. Zhou et al. (2016) illustrates what threats can impact a certain type of validity, we discuss the threats that are relevant to this SLR and the survey in the following section. We present the validity threats of the interviews, except for the external validity, sequentially with the interview methods section in 6.1.

3.6.1 Construct validity

Construct validity is a fundamental feature of study design that concerns the degree to which a variable's or concept's operational definition fits its theoretical definition. Construct validity issues can arise when researchers fail to accurately measure or modify the intended 'construct', resulting in incorrect conclusions or misleading findings.

Construct validity threats can arise in the survey when the questions fail to accurately reflect the underlying construct we try to capture. This can also be mitigated through expert validation of the survey questions. In addition, the survey is prone to social desirability bias. Since the survey concerns cybersecurity behavior, which is sensitive information, participants may be reluctant to report negative or negligent patterns. This has to be accounted for during the analysis of the survey data.

3.6.2 Internal validity

Internal validity concerns the accuracy of the findings and ensures the findings are not due to methodological errors.

For the SLR, this concerns publication bias, meaning studies with positive results are more likely to be published than those with negative results. This could e.g. lead to an overestimate of a certain elicitation technique. In addition, selection bias can occur if the search strategy is not comprehensive enough to find all relevant manuscripts. We tried to mitigate this by validating that no keywords were missed for the found manuscripts. This was done by adding the title, keywords, and abstracts of all manuscripts that were included in the SLR in one file, and letting a natural language processing program[13] find all keyword pairs as illustrated in section 3.3.1.6. This list was compared to the original search string and no new terms were identified through this method. Moreover, we conducted a quality assurance check with a second researcher to ensure consistency in the data extraction as per section 4.1.4

With regard to the survey, response bias can lead to a significant internal validity threat. This is why the response ratio (responses/total employees) in a certain department is important

[13] https://app.sketchengine.eu/#keywords

to the validity of the data and will be accounted for during the analysis to discuss the credibility of the conclusions. To mitigate this we compare the survey population to the overall population in terms of: *department*, *role*, *age*, and *gender*.

For the survey, internal validity threats arise from social desirability bias. Since questions regarding cybersecurity behavior are sensitive, participants may want to present themselves in a positive light and avoid judgment by giving socially desirable answers.

The final threat to internal validity is reactivity bias: participants might change their behavior or responses because they know they are being observed. This can occur if participants feel pressured to provide certain responses or if they want to conform to perceived expectations. This can not be fully mitigated, however, by making it possible for participants to participate anonymously and be able to leave at any time without being penalized should reduce the pressure and need for conformity during the survey.

3.6.3 External validity

External validity refers to the extent to which the results of the study can be generalized to other domains and contexts.

The research sets out to find out what the differences are between the mental models of shadow IT across different departments and ranks. These departments are chosen on the assumption that the employees within these cohorts may hold different mental models. This is due to the different knowledge the employees within these cohorts might have about cybersecurity. The study conducts both a survey and interviews within a single large professional services company. In this type of organization, all employees are assumed to possess a standard level of academic performance and skills.

We illustrate and contextualize this in the demographics section for both the survey (section 5.2) and interviews (section 6.2). **In order to generalize the findings of this research to other domains, it is necessary to ensure that the individual standard in terms of academic performance and knowledge is similar to those cohorts in other domains and therefore possess comparable baseline knowledge to that observed in this study**. If this is not the case, the results may only be partially generalized.

3.6.4 Conclusion validity

Conclusion validity refers to the extent to which the conclusions drawn from the research are reasonable and based on data.

For the SLR, this could be that the electronic databases are incomprehensible, or the inclusion & exclusion criteria are wrong. This could then lead to wrong conclusions. To mitigate this, the SLR research protocol with the criteria is evaluated by experts (Zhou et al., 2016).

4 Mental Models in Cybersecurity

This chapter provides the steps taken and the results of the SLR. Finally answering the first research question: *How are mental models used to explore user understanding of cybersecurity-related concepts?*

4.1 SLR steps

In Figure 4.1 we see the results of the digital search steps taken as outlined in section 3.3.1.1.

Filtering 1	Remove duplicates
Filtering 2	Apply inclusion and exclusion criteria
Filtering 3	Apply quality assessment

FIGURE 4.1: Search process. The digital libraries were searched in January and February 2023.

4.1.1 Digital search

The SLR was conducted in January and February of 2023, with the search string mentioned in section 3.3.1.2. Scopus returned 319 manuscripts, Wiley Journal Finder 164, IEEE Xplore 110, ACM text collection 45, and Web of Science 33. We only searched in abstract, keywords, and title. In ACM this was not possible in one search, hence the search was split into separate searches for the title, keywords, and abstract and the results were combined into one list. The total number of found manuscripts was 672.

4.1.2 Screening and filtering

To deduce the final list of high-quality relevant manuscripts, we used the three-step filtering and screening process according to section 3.3.1.4.

Step 1 - Remove duplicates

Manuscripts are considered duplicates when they have the same title, author, and year of publication. We used EndNote reference manager[1] to automatically flag duplicates and checked all found duplicates manually. In addition, we performed another manual check to ensure the filtered list had unique manuscripts. We removed 2 duplicates from Scopus, 3 from Wiley Journal finder, 25 from Web of Science, 40 from ACM Digital Library, and 65 from IEEE Xplore. Removing a total of 135 duplicate manuscripts, leaving 537 unique manuscripts.

Step 2 - Inclusion and exclusion criteria

Table 3.3 shows the inclusion and exclusion criteria for this search. In order to pass the first inclusion criteria, each found manuscript was scanned by the researcher. This quick scan included reading the title, keywords, and abstract in order to decide if the manuscript was creating, describing, or analyzing mental models of cybersecurity-related concepts. If this was unclear, the scan was extended to the introduction, research methods, and conclusion of the manuscript. Criteria like the publication year, language, availability, and type of paper could be handled through filtering options in the digital search systems. Applying the criteria removed a total of 456 manuscripts.

Step 3 - Quality assessment

The quality assessment was based on the metrics in section 3.3.1.4. The score threshold was set at a level where all papers from unranked conferences and journals were dropped. More specifically, only journals where the SJR ranking was Q1 or Q2 made it to the final selection. Moreso, all but one conference paper with a rank of C or lower did not make it to the final selection. This paper had a lot of citations and hence made it to the final list of 40 manuscripts.

4.1.3 Snowballing

We performed forward and backward snowballing according to Wohlin (2014) on the found 40 manuscripts. All found relevant papers were subject to the same inclusion and exclusion criteria and quality assessment. Which lead to 11 additional manuscripts.

4.1.4 Quality assurance

We performed the quality assurance check as described in section 3.3.1.6. The second researcher found too many discrepancies in the extraction of the data. Therefore we discussed the findings and did a complete re-run of the data extraction. After this data extraction, we

[1] https://endnote.com/

performed another round of quality assurance on 10% of the papers and found only minor discrepancies.

4.2 Results

4.2.1 Overview of manuscripts

In Figure 4.2, a time graph is provided of the 51 total manuscripts that are used in this SLR. The overall interest in mental models on cybersecurity concepts is somewhat constant with 5 publications per year on average with a peak of publications in 2019.

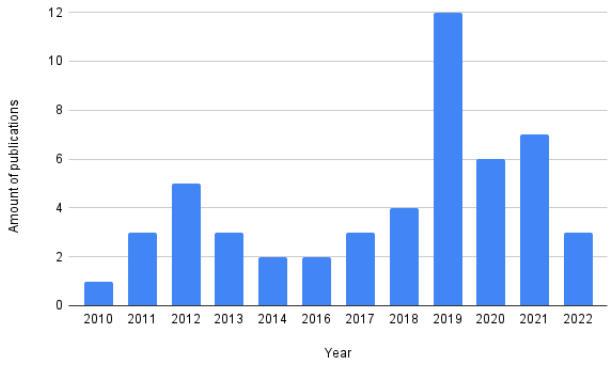

FIGURE 4.2: Year of publication for the selected manuscripts

4.2.2 Assessment criteria

Table 4.1 illustrates the scope of the found manuscripts according to the criteria in section 3.2. Since not all manuscripts create a mental model, the methodology criteria are not relevant for those manuscripts and therefore are left out. The methodology can be seen in Tables F.1 and F.2.

4.2.3 Findings

We see that of the 51 total manuscripts, 10 do not create mental models. These manuscripts are relevant to understand the whole research agenda and focus on mental models in cybersecurity-related concepts. First, we look at these non-mental-model-creating manuscripts. After this, we provide the findings for the manuscripts that elicit mental models.

4.2.3.1 Studies not eliciting Mental Models

Going through these manuscripts chronologically we find several research agendas within the security mental model area. An important finding by Wash and Rader (2011) that is used frequently in later research is that mental models do not have to be technically correct in order to lead to desirable security behaviors. In other words, sometimes even wrong mental models produce good security decisions. and explains how this can be helpful for making home computer users make better security decisions. Moreover, the research agenda by Volkamer

Sum	41			
ID	MM	Reference	Domain	Goals
1	✓	Wash, 2010	Computer warnings	Identify and describe the 'folk models' of security threats that home computer users use to make decisions about their security.
2	✓	Bravo-Lillo et al., 2010	Computer warnings	Improve users' understanding and response to computer security warnings.
3	✗	Wash and Rader, 2011	Mental model research	Propose a research agenda that will help us learn how to shape the mental models of regular non-technical computer users.
4	✗	Raja et al., 2011	Firewall warnings	Design personal firewall warnings that are easy to understand and encourage safe behavior by visualizing the functionality of a firewall based on a physical security mental model.
5	✓	Lin et al., 2012	Mobile app privacy	Understand users' expectations and perceptions of mobile app privacy and to develop a new model for privacy that combines crowdsourcing and traditional security approaches.
6	✓	Furman et al., 2011	Cyberthreat understanding	Investigate users' understanding of online security and identify correct perceptions, myths, and potential misperceptions
7	✓	Benenson et al., 2012	Mobile app security	Establish mental models of IT security when using mobile devices.
8	✓	Wästlund et al., 2012	Credentials research	Investigate how mental models of average users work with regards to anonymous credentials and to evoke their correct mental models with various experiments.
9	✗	Blythe and Camp, 2012	Mental model research	Explore how mental models of security can be implemented to predict user behavior and improve network security.
10	✓	Javed and Shehab, 2013	Social media privacy	Propose a scheme to help users better manage their privacy settings on social networking websites by detecting misconfiguration patterns and enhancing users' mental models of sharing.
11	✓	Kauer, Günther, et al., 2013	Computer security	Compare American and German folk models of home computer security and to identify areas for improvement in security software
12	✗	Volkamer and Renaud, 2013	Mental model research	Provide an overview of mental model research and its application to human-centred security, as well as to identify promising research directions and limitations in the field
13	✓	Renaud, Volkamer, et al., 2014	End to end encryption	Understand why end-to-end encryption is not widely adopted by email users and to identify ways to improve end-user mental models related to email security.
14	✗	Coopamootoo and Groß, 2014	Privacy mental models	Use mental models theory to better understand the links between privacy concerns and behavior.
15	✓	Renaud, Flowerday, et al., 2016	Privacy	Understand the lack of protest against dragnet surveillance in the UK by exploring the mental models of well-informed individuals in terms of privacy and confidentiality.
16	✓	Märki et al., 2016	Developer security	Use the structure formation technique as a first step to develop the mental models of software developers when dealing with security measures
17	✓	Thompson and McGill, 2017	Computer security	Apply quantitative techniques to understand mental models of security and their impact on information security decisions.
18	✓	Maier et al., n.d.	Dashboard design	Find out how experts vs novice see security aspects to craete dashboards
19	✗	M. A. Mohamed et al., 2017	Usability design for security	Establish the foundations for developing a mental model that bridges the gap between usability and security in user-centred designs. T
20	✓	Winter et al., 2018	TOR browsing	Investigate how users perceive, understand, and use onion services, and to identify challenges and opportunities for improving their usability and security 5
21	✓	Zou and Schaub, 2018	Risk awareness	Investigate consumers' mental models, risk perceptions, and protective actions related to credit bureaus and the Equifax data breach
22	✓	Albalawi et al., 2017	Cognitive mapping of security aspects	Explore the importance of considering human behavior in designing security models and to provide insights into how decision-making towards security and usability can be improved through the cognitive map approach.
23	✓	Oates et al., 2018	Privacy	Explore the overlaps and disconnects between expert and lay conceptions of privacy, and to inform privacy-related visual design by understanding which aspects of privacy frameworks lend themselves to visual representation
24	✓	Kang et al., 2015	General user privacy	Examine the relationship between people's knowledge and their privacy and security behavior in today's Internet environment, and to move towards a better understanding of the kinds of Internet knowledge users need to have.
25	✓	Krombholz et al., 2019	HTTPS	Examine the mental models of end users and administrators regarding HTTPS and message encryption, and to identify any misconceptions or differences in understanding.
26	✓	Abdi et al., 2019	Home speaker devices	Explore the security and privacy perceptions of Smart Home Personal Assistants.
27	✓	Ramokapane et al., 2017	Cloud data deletion	Investigate users' cloud deletion practices and coping strategies, and to identify the factors that influence these practices and strategies
28	✓	Zou, Mhaidli, et al., 2018	Credit bureaus	Investigate consumers' risk perceptions and protective actions after the Equifax data breach
29	✓	J. Wu and Zappala, 2018	Encryption	Understand how users perceive encryption and to identify mental models that can inform the design of more usable encryption systems.
30	✓	Fulton et al., 2019	Media influence	Identify areas where usable security research is needed to improve existing methods or invent new ways of handling security issues.
31	✓	Gerber et al., 2019	Privacy mental models	Gain insight into users' mental models of privacy consequences, obstacles for privacy protection, and strategies for privacy protection.
32	✓	Horvath et al., 2019	API's	Investigate how learners of APIs develop mental models and how these models can be used to improve the usability of APIs.
33	✓	Wash and Rader, 2015	Mental model Behaviour	Explore the relationship between users' mental models and their protective behaviors, and to identify the different mental models that users have about computer security.
34	✗	Votipka et al., 2020	Reverse engineering for malware	Provide insights into the complex process of reverse engineering and improve interaction design for reverse engineering tools
35	✗	Liljestrand et al., 2019	Computer security	Enhance the usability of security applications by considering human factors and developing the user's mental model.
36	✓	Baig, R. Mohamed, et al., 2020	Home DNA test privacy	Explore users' privacy perceptions and mental models of at-home DNA testing companies and their services.
37	✓	Abu-Salma and Livshits, 2020	Private browsing	Investigate why users often misunderstand the benefits and limitations of private browsing mode and to suggest recommendations for improving the design of disclosures.
38	✓	Mai et al., 2020	Cryptocurrency	Identify and analyze the mental models of cryptocurrency systems held by users, and to understand how these models affect users' security and privacy.
39	✓	Tolsdorf and Dehling, 2020	Privacy	Examine the mental models of German office workers' privacy perceptions in order to lay a basis for future tool developments.
40	✗	Spero and Biddle, 2020	Cybersecurity mental models	Help users develop better mental models of the security-relevant aspects of software functionality through interface design.
41	✗	Chen, 2020	Cybersecurity mental models	Develop effective risk communication strategies in cyberspace by understanding users' mental models of risk.
42	✓	Velykoivanenko et al., 2021	Fitbit data privacy	Investigate how fitness-tracker users perceive the utility of the features they provide and the associated privacy-inference risks.
43	✓	Baig, Kazan, et al., 2021	Media influence	Evaluate how much media affects the mental models of technical users in the domain of security.
44	✓	Schaewitz et al., 2021	End to end encryption	Gain insight into how non-specialists construct their understanding of E2EE and which metaphors are most effective in helping them comprehend its benefits and limitations.
45	✓	Brodsky et al., 2021	Internet mental models	Uncovering differences in mental models that students and kids have of the internet
46	✓	Hassanzadeh et al., 2021	Data breaches	Explore how users understand data breaches and their perceptions of the causes, responsibilities, consequences, prevention, and appropriate follow-up, in order to inform communication practices and interventions aimed at empowering users and improving cybersecurity
47	✓	Akgul et al., 2021	End to end encryption	Investigate the potential of using educational messages to improve users' understanding of end-to-end encryption.
48	✓	Marky et al., 2021	smart home devices	Understand the differences in privacy mental models of smart home visitors and residents, and to provide insights on how to address their concerns.
49	✓	Binkhorst et al., 2022	VPN	Investigate the similarities and differences between experts and non-experts in their perception of VPN technology in a professional services firm in the Netherlands.
50	✓	Dutkowska-Zuk et al., 2022	VPN	Investigate how and why people use VPNs, their mental models of VPNs, how they choose which VPN to use, and their awareness and attitudes about data collection practices of VPNs
51	✓	Bieringer et al., 2022	Machine learning	Investigate the mental models of industrial practitioners regarding adversarial aspects of machine learning (AML) and to identify potential security challenges that practitioners may not fully understand

TABLE 4.1: Scope aspects of SLR manuscripts

and Renaud (2013) illustrates a literature review of mental model research in the context of human-centered security. And found that end-users are not the enemies but rather the allies in creating secure systems. By eliciting the mental models of the end-users we can find the comprehension of the system and thus design systems more securely. A final research agenda by Coopamootoo and Groß (2014) illustrates the need for mental models in security research and specifies the implications for this specified on privacy. Providing a valuable structure to investigate links between privacy concerns and end-user behavior.

Few other early manuscripts support the overall use of mental models in application security. Both Raja et al. (2011) and Blythe and Camp (2012) do some form of empirical research to validate that the use of mental models is beneficial in terms of user behavior. Blythe and Camp (2012) did this by proposing the implementation of an existing mental model to simulate human security behavior in an agent model. Raja et al. (2011) illustrates how the use of a mental model, in this case, the "physical security" mental model, improves the security understanding of a firewall. This shows that using a certain mental model that the user is familiar with, and a concept that the user is unfamiliar with, yields good results. Blythe and Camp (2012) then continues this by using the found mental models by Wash (2010) to predict user behavior and create a way for others to implement mental models. These early papers suggest and find understanding the end-user through mental models to create secure systems is key.

In later research, we see several manuscripts on how mental models on security can be used for enhanced usability of systems. Liljestrand et al. (2019) investigates how to enhance the usability of security applications by considering human factors. This showed that system alterations made based on mental models improved user behavior in terms of security. Providing an application of mental models we find Spero and Biddle (2020), they present a set of patterns for user interface designers to help users better protect themselves from cyberattacks, The main goal of this research is to create a system that supports the mental models of cybersecurity that resembles the way people manage security in the physical world. Validating the idea of Raja et al. (2011) that using familiar concepts to build mental models of unfamiliar concepts yields good results. The final manuscript addressing usability is M. A. Mohamed et al. (2017). This research creates a meta-model for developing a mental model that bridges the gap between usability and security in user-centered designs. Again building towards the idea that end-user understanding benefits the usability and security aspects of a system.

Highly relevant for this research are the various mental models that other groups of end-users may have depending on their level of expertise in a certain field. Wash and Rader (2015) shows how distinct users have different understandings of certain concepts. And find that within a big pool of participants, not everyone holds the same beliefs and behaviors. This leads to the thought that educating users about security is not simply a more-is-better issue, and not all users should receive the same guidelines. Chen (2020) supports this by emphasizing the importance of differentiating between the diverse expert users of groups when using mental models for research. Especially in communication to influence user behavior. Supporting the thought that there is no "one size fits all" in creating guidelines for end-user behavior. In

the following section, we discuss more manuscripts that create mental models for different end-user groups.

4.2.3.2 Studies eliciting Mental Models

The main rationale for the SLR is to uncover how mental models are built for cybersecurity concepts. In this section, we look at the 41 manuscripts that do create mental models. First, we take a look at what concepts have been explored with mental models, followed by the rationale for why mental model research is needed. Finally, we dissect the found manuscripts according to the assessment criteria found in section 3.2. The results of the quality assessment can be found in Tables F.1 and F.2. This section aims to answer the first research question: *How are mental models used to explore user understanding of cybersecurity-related concepts?*

4.2.3.2.1 Scope

The domains of the found manuscripts cover a wide range of topics related to privacy, data, and user behavior in the context of cybersecurity. Some studies focus on specific aspects of computer or mobile security, such as VPN (Binkhorst et al., 2022), mobile app privacy (Lin et al., 2012; Benenson et al., 2012), and end-to-end encryption (Renaud, Volkamer, et al., 2014; Schaewitz et al., 2021; Akgul et al., 2021).

Others explore more broad topics such as privacy (Javed and Shehab, 2013; Renaud, Flowerday, et al., 2016; Oates et al., 2018; Kang et al., 2015; Gerber et al., 2019; Tolsdorf and Dehling, 2020; Velykoivanenko et al., 2021; Coopamootoo and Groß, 2014) and computer security (Kauer, Günther, et al., 2013; Thompson and McGill, 2017; Liljestrand et al., 2019). Other manuscripts investigate the design of security measures, such as dashboards (Maier et al., n.d.) and usability design for applications (M. A. Mohamed et al., 2017). There are also studies that examine specific technologies, such as TOR browsing (Winter et al., 2018), HTTPS (Krombholz et al., 2019), and home speaker devices (Abdi et al., 2019). A common theme, however, is investigating how users perceive and manage privacy and security risks in the context of technology.

The creation of mental models to understand security started with the research of Wash (2010). This research provides 8 mental models (in this research called "folk models") of computer security divided into two groups concerning: "viruses" and other malware and "hacker". This research was rerun by Kauer, Günther, et al. (2013), which resulted in the same two groups, however, with 3 more specific folk models within these groups. This research laid the foundation for further mental model research. This is supported by Bravo-Lillo et al. (2010), which illustrates that computer warnings can be very ineffective because they do not adhere to the mental model of the end-user. Moreover, Furman et al. (2011) also found that end-users are aware and concerned with online security, but lacked the expertise to actually protect their online data. These four works are specifically mentioned since they are frequently cited in more recent papers to illustrate the gap that mental model research is trying to fill and the

importance of doing mental model research in this area. Therefore these manuscripts form the foundations of recent mental-model research motivation on cybersecurity concepts.

4.2.3.2.2 Technique

In the manuscripts, we found six different elicitation methods. These are (i) interviews, (ii) drawing exercises, (iii) surveys, (iv) crowdsourcing, (v) think-aloud sessions, and (vi) an experiment. In about 44% (18/41) of the found manuscripts, more than one method was used to elicit the mental models. Most mental models were elicited through (semi-structured) interviews. Roughly 80% (33/41) of the mental models were elicited this way. Intuitively, it seems logical that this methodology is the most used since it allows for a deeper user understanding, uncovering the rationale for why a participant holds certain thoughts or perspectives. The second most used elicitation technique is the drawing method. Where the participant is asked to visualize their thoughts, sometimes with a think-aloud exercise. Especially the combination of those presented in studies like (Volkamer and Renaud, 2013; Maier et al., n.d.; Binkhorst et al., 2022), hold very extensive mental models and rationale for how and why a participant holds certain thoughts. On the contrary, just quantitatively gathering data through a survey (or crowdsourcing) is only found in five manuscripts (Lin et al., 2012; Javed and Shehab, 2013; Thompson and McGill, 2017; Albalawi et al., 2017; Wash and Rader, 2015). These papers generalize the found mental models over a larger population, therefore. A limitation of this is that because of this generalization, certain individual nuances can be missing.

In 15 of the manuscripts that created mental models, we found that the authors used scenarios in the elicitation of the mental models. Scenarios can be a powerful tool, helping find how people think and make decisions in these areas, by probing them with niche situations and finding how they react.

In studies focused on computer threats (Wash, 2010; Bravo-Lillo et al., 2010; Kauer, Günther, et al., 2013), we find scenarios such as discovering a virus on a computer, a hacker compromising a system, or falling victim to identity theft, to help us understand how ordinary people think and react to these threats. Similarly, when looking at mobile and smart devices (Lin et al., 2012; Abdi et al., 2019), we observe scenarios regarding app-rights access or managing smart home devices. These give a great deal of information to help uncover the user privacy understanding of the participants.

When investigating more technical topics like secure communication (Renaud, Volkamer, et al., 2014; Krombholz et al., 2019; J. Wu and Zappala, 2018; Akgul et al., 2021; Binkhorst et al., 2022), scenarios like sending an encrypted message, online banking, or using a corporate VPN are used to find the extent of user understanding, but also the points of confusion around some of these concepts. An interesting pattern that appears is the adaptation of scenarios to the participant's level of expertise. For example, research on domains like VPNs or machine learning (Binkhorst et al., 2022; Bieringer et al., 2022) use scenarios like using the corporate VPN from a coffee bar or illustrating potential threats in industrial machine learning. These

concrete applications of a certain concept allow the researcher to capture a wide spectrum of aspects with regard to the participant's mental models.

4.2.3.2.3 Participants

Qualitative studies had an average of 26 participants (*in a range of 2 - 109*) and quantitative had an average of 1124 participants (*in a range of 44 - 5360*). For qualitative research, the occurrence of very few participants is due to either a highly required high level of expertise or that research is still ongoing.

Manuscripts generally reported basic demographics like age and gender for their participants. We find some manuscripts that are focused on a specific topic or field. Even if these manuscripts do not research mental models across different groups, they often require a certain level of expertise or other requirements for participants to be able to contribute to their research. When observing the requirements in Tables F.1 and F.2. We find the requirements fall into four categories.

- First, we observe *regional and language requirements*. Several manuscripts require participants to live in specific regions, such as the U.S. or Canada, or even to hold citizenship or residency in the U.S. We also find that *language proficiency* was necessary for some manuscripts. Participants were often required to be fluent in the regional language. This could be in English, but there were studies requiring fluency in German or French. The combination of these requirements often meant targeting participants who could understand the study context and effectively illustrate their experiences and thoughts. Since mental models are about internal representations of a certain concept, being able to vocalize your thoughts well is an understandable requirement.
- Secondly, we observe the requirement for some *technical expertise*. This ranged from having IT skills, such as software development skills or cybersecurity expertise, to familiarity with specific technologies or platforms like the Tor Browser or Fitbit application. The level of technical expertise often depended on the research objectives, focusing on non-expert users, experts, or sometimes a mix of both.
- Thirdly, we find that *other demographic attributes* like age and educational background played a significant role in participant selection. The age threshold was typically set at 18, with one manuscript specifically targeting middle school students. Educational requirements varied, with some studies focusing on the field of study.
- Finally, we observe *task-based experience or ownership of specific technology*. This included owning a home computer or a Smart Home Personal Assistant or having experience with certain services or products such as DNA testing kits or specific cryptocurrencies.

We observed the found manuscripts used three main recruitment strategies: *digital platforms*, *academic institutions*, *and personal networks*. Digital platforms, such as Amazon's Mechanical Turk (AMT), Prolific, online forums, and social media were frequently used. AMT was especially used for large participant groups. Specialized platforms and mailing lists, like Bitcoin-related ones, were used for specific research along with websites like Craigslist and Kijiji.

The second recruitment strategy was through academic institutions. Studies often involved students from researcher's universities for example Carnegie Mellon University and King's College London. On campus, traditional methods like flyers and advertisements were used to recruit participants. Finally, we observe a high usage of personal networks of researchers and participants. A frequent occurrence of this is snowball sampling, which relies on referrals from existing participants or professional contacts. Some participants were directly recruited from businesses or via professional invitations, to cater to their niche expertise within a certain field.

Looking at the cohort of participants, we find that 8 manuscripts explicitly researched mental models in more than two groups (Bravo-Lillo et al., 2010; Renaud, Volkamer, et al., 2014; Kang et al., 2015; Krombholz et al., 2019; Brodsky et al., 2021; Marky et al., 2021; Baig, Kazan, et al., 2021; Binkhorst et al., 2022). The nature of the division between those groups was either a classification by the researchers on the expertise of the participants within a certain field or a classification based on self-reported knowledge of a particular concept. Six out of the eight manuscripts provide a binary split in the participant group. Two manuscripts divide the group into three levels of expertise. (Binkhorst et al., 2022)

The importance of doing research in different groups has been clearly outlined in the previous section. Even though the numerical data, 8 out of 41, does not reflect this. We do observe a recent wave of publications of mental model research in different groups since 5 out of 8 have been published in the last couple of years. Hence suggesting that the importance of finding differences in mental models across groups is gaining momentum.

4.2.3.2.4 Representation

The selected manuscripts contain two representations of mental models: textual and diagrams. We observe a visual representation of mental models in 14/41 manuscripts. While mental models are a visual representation of a certain concept, text-based descriptions offer the precision to describe complex concepts and nuances in a mental model. In addition, text-based descriptions allow for a description of abstract concepts such as privacy and security. One could argue that in some cases a combination of both diagrams and textual can provide the most effective way to represent mental models: the visual component of the diagram with the nuances of the text-based. Moreover, the choice of representation depends heavily on the nature of the concept itself.

We observe a pattern for representation when looking at the techniques used in a manuscript. Of the 14 manuscripts that use a drawing component to elicit the mental models, we find 10 of these manuscripts use visual representations to depict the mental models. Moreover, these manuscripts often regard a concrete technique. We find manuscripts about TOR, VPN, HTTPS, APIs, end-to-end encryption, and machine learning all use visual representations to depict the mental models. For more abstract topics like general computer security or privacy,

it is harder to use visuals since these are not concepts that one could easily draw or visualize and therefore need more in-depth text-based descriptions to formulate a participant's thoughts with regard to the object of study.

4.2.3.2.5 Trends

Several trends can be seen throughout the manuscripts. When mobile phones with app stores were first introduced, there were several mental model studies regarding the privacy of mobile apps. Lin et al. (2012) used crowdsourcing to capture users' expectations of what sensitive data is used by mobile applications and report on where these expectations do not align with reality. Furthermore, Benenson et al. (2012) showed that the number of security threats on mobile phones is increasing, and end users do not have the correct mental models to prevent these threats. Also, the introduction of surveillance by the government through the "dragnet surveillance" in the UK allowed for mental model research on the area of privacy. Renaud, Volkamer, et al. (2014) illustrates why end-to-end encryption in email communication is not widely used, even after the introduction of the surveillance. This is due to fundamental issues such as incomplete threat models, misaligned incentives, and a general absence of understanding of the email architecture. In order to circumvent this, there had to have been a focus on building comprehensive end-user mental models. In addition, Renaud, Flowerday, et al. (2016) did research on why there was a lack of protest against this dragnet surveillance and concluded this also was due to incorrect mental models on what privacy is and what the implications can be.

4.2.4 Conclusions

When analyzing the research agendas in this literature study, we find that they outline the necessity of understanding end-user mental models when building secure systems. We present numerous research agendas with regard to mental models in cybersecurity, including the discovery that mental models do not need to be technically correct in order to lead to desired security behaviors. Empirical research backs up the usage of mental models in application security, demonstrating that leveraging familiar concepts to develop mental models of unfamiliar topics delivers positive outcomes. Furthermore, the manuscripts emphasize the importance of distinguishing between distinct categories of end-users when using mental models for research. Overall, the research agendas analysis underlines the importance of end-user awareness in improving a system's usability and security.

To answer RQ1: *How are mental models used to explore user understanding of cybersecurity-related concepts?*, we briefly summarize the SLR results. We have seen a collection of manuscripts covering a wide range of topics related to threats, data, and user behavior in the context of cybersecurity. Amongst the domains are specific aspects of computer and mobile security, as well as broader topics like privacy and general computer security. The central theme of the manuscripts is the elicitation of mental models, to understand how users think about cybersecurity-related concepts. The number of recent publications illustrates the increasing interest in the research on user understanding of cybersecurity concepts.

In the manuscripts, we find six different elicitation methods to build mental models: interviews, surveys, crowdsourcing, think-aloud sessions, drawing exercises, and experiments. Most mental models were elicited through interviews, which allow for a deeper understanding of the rationale for why a participant holds certain thoughts or perspectives. The second most used elicitation technique is the drawing method, which involves participants visualizing their thoughts, sometimes with a think-aloud exercise. The combination of these methods results in very extensive mental models and rationale for how and why a participant holds certain thoughts. **Therefore we decided to adopt a combination of interviews, drawing, and a think-aloud exercise to extract the mental models in our study.**

The manuscripts use two representations of mental models: textual and diagrams. Textual descriptions offer precision in describing complex concepts and nuances in a mental model, while diagrams provide a visual representation of a certain concept. Only three of the found manuscripts contained diagrams of the mental models. Textual descriptions are particularly useful for abstract concepts such as privacy and security, but diagrams can be helpful in providing a quick overview of the mental model. **Therefore, we use both a textual description and a visual representation as the representation methods of the found mental models in this research.**

In conclusion, by exploring the internal representations that humans use to grasp and make decisions about security and privacy threats in the context of cybersecurity-related concepts, mental models are used to investigate user understanding of these concepts. To gather mental models from participants, we find a variety of elicitation methods. The mental models reveal how end-users think about cybersecurity and assist academics and IT experts in understanding the reasoning behind end-user viewpoints. The manuscripts describe the collected mental models from the participants through textual descriptions and diagrams, providing a deep grasp of the concepts and nuances of user understanding.

4.3 Takeaways for next chapter

In the following chapter, we empirically explore the occurrence of shadow IT instances across several cohorts, laying the foundation for the rest of this research. Key insights from our literature review guide this: mental models are a great way to comprehend end-users' cybersecurity perspectives, even if not technically accurate. These models are best elicited using a mix of interviews, drawing, and think-aloud exercises, providing deep insight into users' thought processes. The mental models are represented both textually and diagrammatically to allow for both nuances and visual understanding. We identify the importance of different user categories and their awareness levels, we focus on understanding user perception of shadow IT through their mental models. These insights align with the increasing research interest in user understanding of cybersecurity, all aiding in the process to enhance system security.

5 Occurrence of Shadow IT

We conduct an exploratory survey to get insights into the current status of shadow IT and analyze these occurrences of shadow IT per cohort. This data allows for a preliminary analysis of what occurrences of shadow IT are present within a large organization. The survey tries to answer the second research question: *What types of Shadow IT can be observed across different cohorts?*

5.1 Preparation for analysis

As outlined in section 3.3.2.2, the questions in the survey are multiple-choice, but also with multiple answer options. As previously outlined in the statistical analysis methods section 3.3.2.3, we perform a Chi-square test and Fisher's exact test. The second assumption of these tests is that the variables it tests on must be mutually exclusive. This is not the case since we allow multiple answers per question. The original structure of the data from the survey as seen in Table 5.1 can therefore not directly be used for the Chi-squared test to compare the overall usage of different shadow IT types across cohorts. However, we can compare each of the options separately by introducing the value that this shadow IT type does not occur in a cohort. This value is mutually exclusive with the number of times that shadow IT does occur in that cohort. Hence we add an extra column per option that displays the value of that cohort that has not responded with this answer option, as can be seen in Table 5.2 and perform the Chi-square test and Fisher's exact test individually for each of the: Shadow IT types, answer options, scenarios, and cohorts. Moreover, we provide the percentage of respondents that answered a certain answer option. Note that the percentages do not add up to 100% since a respondent can choose multiple options.

	Answer A	Answer B
Cohort group 1	21	40
Cohort group 2	4	19
Cohort group 3	11	29

TABLE 5.1: Survey data structure

	Answer A			Answer B		
	F	T	%	F	T	%
Cohort group 1	154	21	13%	134	40	23%
Cohort group 2	35	4	10%	20	19	49%
Cohort group 3	62	11	15%	44	29	40%

TABLE 5.2: Processed survey data structure

In addition to the statistical analysis, we analyze the data to find patterns and similarities in the occurrence of certain shadow IT types. Transformation and analysis using R Studio provided contingency tables and relevant statistical calculations.

5.2 Participant demographics

Overall, a total of 638 individuals started the survey, showing initial interest and willingness to participate. However, during the data cleaning process, we observed that 180 respondents did not complete the survey, leaving 458 completed responses. To ensure the reliability of the answers, we cleaned the data based on the time that respondents took to complete the survey. If the survey was completed hastily, the participants' responses may lack accuracy because they did not pay careful attention to the instructions. On the other hand, if the response time is excessively long, there is a risk that participants may lose sight of the survey's objectives, leading to inaccurate answers. Specifically, we removed respondents whose survey duration fell beyond the mean plus or minus two standard deviations (Ilyas and Chu, 2019). The final number of responses for data analysis is 450.

We provide a summary of the demographics in Table 5.3. Furthermore, we illustrate some of the demographics visually in order to outline some key aspects of the demographics.

Variable	Scale	Mean/ SD	Distribution
Gender			56% male, 43% female, 1% preferred not to answer
Age	Years	32.7 $\pm$ 9.4	2% between 18-22; 20% between 23-25; 36% between 26-30; 16% between 31-35; 6% between 36-40; 13% between 41-50 and 7% 51+
Work experience	Years	8.74 $\pm$ 9.0	45% worked 5 years or less; 24% worked 6-10 years; 15% worked 11-20 years; 11% worked 21-30 years and 5% worked 30+ years
Rank			39% junior; 24% senior; 15% manager; 12% senior manager and 9% management
Education			86% Scientific Education (WO); 10% Higher Professional Education (HBO); 1% PhD and 3% Other
Department			85% Client facing staff; 8% Support staff; 6% Management staff and 2% IT staff

TABLE 5.3: Demographic summary of the survey participants

When analyzing the demographics of the respondents, it is clear that there is a minor gender difference within the sample. Out of all the respondents, 56% identified as male, while 43% identified as female, and 1% of the respondents preferred not to disclose their gender. The distribution of the gender in the organization is 57% male and 43% female[1]. We therefore can state that in terms of gender distribution, the survey respondents accurately depict the corresponding population in the organization.

Respondents did not enter their age but selected an age group. If we take the average age for each age group, and 60 for the 60+ group. We find that the mean age $\approx$ 32.7 with a standard deviation of roughly 9.4. The complete age distribution can be found in Figure 5.1.

[1]These percentages were derived from the annual report from the organization

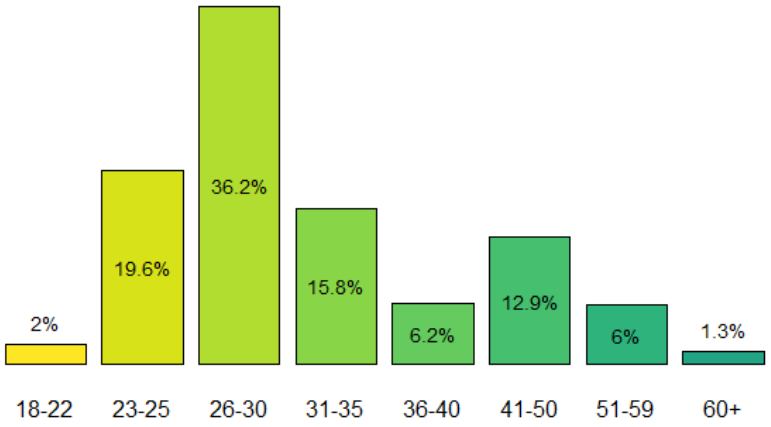

FIGURE 5.1: Age distribution

Within a large professional services company, there is a hierarchical rank structure, resembling a pyramid, where each higher level has fewer employees. The distribution of employees across different ranks is depicted in Figure 5.4. This pattern is also observed in the distribution of survey respondents, again indicating that the sample is representative of the general population in terms of rank distribution. As discussed in section 3.6.3, the company places a strong emphasis on academic achievement during recruitment, which is reflected in the distribution of education levels shown in Figure 5.3.

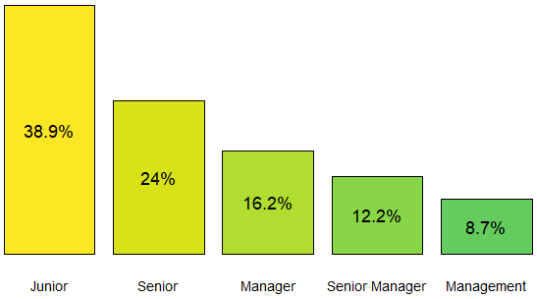

FIGURE 5.2: Rank distribution

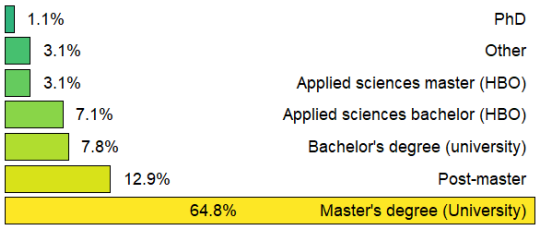

FIGURE 5.3: Highest completed education distribution

In addition, when looking at the distribution of respondents across various departments, it seems there is a significant difference. However, when considering the ratios, these differences resemble the estimated proportions of employees in each department within the organization. We depict both the survey's and organization's department distribution[2] in Table 5.4. These percentages offer a means to assess how the survey's distribution aligns with an estimated distribution of employees within the organization. We find that even though the differences seem significant, in comparison with the organizational distribution, the survey's department distribution clearly resembles the organization's department distribution.

So, in the survey conducted on our sample of the organization, we observe that the distribution of *gender*, *rank*, and *department* is well-represented compared to the original population.

[2]Note that percentages are based on estimates and are provided solely to compare the survey's distribution against an estimate of the organization's distribution

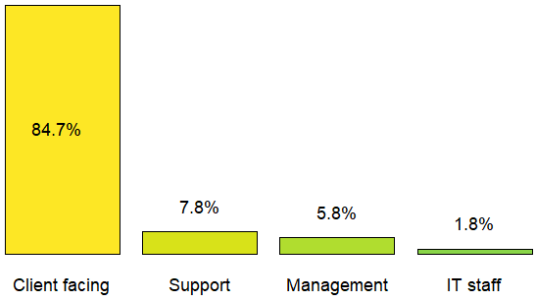

FIGURE 5.4: Department distribution

	Survey	Organization	Δ
Client facing	84.7%	78.7%	+6.0%
Support	7.8%	16.6%	-8.8%
Management	5.8%	4.2%	+1.6%
IT	1.8%	0.6%	+1.2%

TABLE 5.4: Department distribution comparison

5.3 Survey results

In this section, we present the survey results in detail. We present the results through all scenarios and shadow IT types. We explore the results in detail to eventually identify patterns, thus following a bottom-up approach. Recognizing that some readers might prefer a concise overview rather than a granular exposition, we have condensed our key findings in section 5.4. Readers seeking a summary are encouraged to proceed directly to that subsection.

We analyze the findings per scenario and try to find statistically significant data points. In addition, we observe the behavior across cohorts. We do this by first giving the question that was asked in the survey and providing information about the relative occurrence across cohorts[3]. Finally, we conclude the main insights from the survey and provide takeaways for the next chapter.

5.3.1 Cloud services

Cloud services provide innovative, good quality, and often free access to all sorts of solutions that do not have to be installed on a device. This can range from niche functionalities to online storage services. When respondents were asked what cloud services they have used that were not provided by the organization, we prompted the following answer options:

- Browser extensions
- Browser tools
- Cloud storage
- None, I used only standard applications
- Other

Table 5.5 illustrates the results of the statistical tests on the cloud services data. The table holds the data for the three defined scenarios as described in Section 3.3.2.1 (abbreviated in the table with *S1*, *S2*, and *S3*). Moreover, the table holds the data for both cohorts; department and rank (abbreviated in the table as *Dep* and *Rank*). Then per answer option, we provide the Chi-square value as $\mathcal{X}^2$, the Chi-square p-value as $\mathcal{X}^2$ p, and the Fisher p-value as Fisher p.

[3]these are given as percentages in the occurrence table. Please note that the percentages do **not** add up to 100%, these percentages illustrate the number of respondents within that group that responded with this answer option

We look for statistical significance with a p-value lower than 0.05 for both the Chi-square test and Fisher's exact test. Statistical significant values have been made bold to outline them.

Cloud		Browser Extension			Browser Tool			Cloud storage			Other			None		
		$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p
S1	*Dep*	1,12	0,77	0,91	2,38	0,5	0,58	2,68	0,44	0,48	7,09	0,07	0,063	7,00	0,07	0,06
	Rank	1,34	0,85	0,86	1,76	0,78	0,73	2,02	0,73	0,74	2,27	0,69	0,68	0.48	0,97	0,98
S2	*Dep*	2,71	0,44	0,69	1,6	0,66	0,89	1,69	0,64	0,86	4,09	0,25	0,33	3.64	0,31	0,39
	Rank	3,74	0,44	0,41	6,84	0,14	0,11	3,68	0,45	0,48	3,08	0,54	0,55	1,77	0,78	0,80
S3	*Dep*	8,20	**0,042**	**0,022**	3,84	0,28	0,27	1,47	0,69	0,73	1,54	0,67	0,67	1,64	0,65	0,67
	Rank	7,31	0,12	0,12	9,51	**0,049**	0,053	3,54	0,47	0,48	0,29	0,99	0,98	3,49	0,48	0,48

TABLE 5.5: Cloud services statistics

5.3.1.1 Cloud services in client projects

"For **specific engagements**, what **cloud services** have you used that were **not** provided by [ORGANZATION]?"

Using cloud services to do work on client projects is often not encouraged by the organization. Especially since the data in such projects is often client-related and therefore the impact of a data leak increases because of it. In contrast to this, we do see some usage of different cloud services across the organization.

The statistics indicate that for the first scenario, there are no statistically different groups in both cohorts. A remarkable finding is that in this scenario, which was for specific client projects, the support group had some occurrence of cloud services. However, the nature of this group is to facilitate internal processes and not perform any work on client projects. These answers illustrate they might have not understood the question, or did not read carefully enough.

In Tables 5.6 and 5.7 we illustrate the findings for cloud services in client projects through both cohorts. We find that the distribution of cloud tools across ranks is somewhat similar, with a maximum difference throughout the entire table in the relative occurrence of 9%. This indicates that employees across ranks behave similarly in terms of the use of cloud services in client projects.

S1	Extension			Tool			Storage			Other			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	32	3	**9%**	34	1	**3%**	26	9	**26%**	31	4	**11%**	14	21	**60%**
Client facing	355	26	**7%**	353	28	**7%**	302	79	**21%**	362	19	**5%**	104	277	**73%**
IT staff	8	0	**0%**	8	0	**0%**	8	0	**0%**	8	0	**0%**	0	8	**100%**
Management	25	1	**4%**	23	3	**12%**	20	6	**23%**	22	4	**15%**	10	16	**62%**

TABLE 5.6: Cloud services in client projects, grouped by department

The **cloud tools** that were used the most are online collaboration tools like Jira, Trello, and Mural, which are present throughout all ranks. In addition, we also find the use of Chat-GPT, Adobe creative cloud, and Figma, only in the client-facing group. These tools are more present in the junior and senior ranks throughout the organization. In terms of cybersecurity,

S1	Extension			Tool			Storage			Other			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	162	13	**7%**	165	10	**6%**	139	36	**21%**	164	11	**6%**	50	125	**71%**
Senior	103	5	**5%**	100	8	**7%**	81	27	**25%**	103	5	**5%**	33	75	**69%**
Manager	67	6	**8%**	68	5	**7%**	61	12	**16%**	68	5	**7%**	19	54	**74%**
Senior Manager	51	4	**7%**	49	6	**11%**	44	11	**20%**	53	2	**4%**	15	40	**73%**
Management	37	2	**5%**	36	3	**8%**	31	8	**21%**	35	4	**10%**	11	28	**72%**

TABLE 5.7: Cloud services in client projects, grouped by rank

ChatGPT can bring consequences since prompting is prone to data leakage. Other tools that are mentioned that bring similar risks are tools like Google Translate or Deepl. Therefore it is surprising to find that these tools are being used for specific client projects, where a data leak has the most impact on the organization since it handles client data. We observed a few different types of **browser extensions**: ad-blockers, password managers, and a font-finding tool. However, no major extensions were reported.

Furthermore, we note some usage of **cloud storage services**. These are present through all departments except for the IT staff, and throughout all ranks with over 20% of the respondents using different storage solutions for client projects. The most used services are Dropbox, Google Drive, and WeTransfer. It is surprising to find so many occurrences of cloud storage devices outside of the organization's scope in client projects since the organization has a clear policy on the usage of external cloud storage and the tools in place to facilitate this. Some of the tools in the **other** category were virtual data rooms and file-sharing applications for a niche group.

5.3.1.2 Cloud services in other work tasks

"For **work-related tasks**, what **cloud services** have you used that were **not** provided by [ORGANZATION]?"

Similarly to the cloud services in engagements, we do not find statistical differences in the cloud services utilization across the cohorts for other work-related tasks according to Table 5.5. Looking at Tables 5.8 and 5.9, we notice a trend that the general usage of cloud services in other work tasks is lower than in specific projects. This is illustrated through the percentage of *None* in both cohorts is equal or higher compared to the first scenario.

S2	Extension			Tool			Storage			Other			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	34	1	**3%**	34	1	**3%**	31	4	**11%**	35	0	**0%**	4	31	**89%**
Client facing	358	23	**6%**	365	16	**4%**	333	48	**13%**	372	9	**2%**	76	305	**80%**
IT staff	8	0	**0%**	8	0	**0%**	8	0	**0%**	8	0	**0%**	0	8	**100%**
Management	26	0	**0%**	26	0	**0%**	24	2	**8%**	24	2	**8%**	4	22	**85%**

TABLE 5.8: Cloud services in general work tasks, grouped by department

S2	Extension			Tool			Storage			Other			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	169	6	**3%**	172	3	**2%**	151	24	**14%**	170	5	**3%**	33	142	**81%**
Senior	101	7	**6%**	102	6	**6%**	92	16	**15%**	105	3	**3%**	24	84	**78%**
Manager	67	6	**8%**	68	5	**7%**	68	5	**7%**	72	1	**1%**	12	61	**84%**
Senior Manager	51	4	**7%**	52	3	**5%**	50	5	**9%**	55	0	**0%**	8	47	**85%**
Management	38	1	**3%**	39	0	**0%**	35	4	**10%**	37	2	**5%**	7	32	**82%**

TABLE 5.9: Cloud services in general work tasks, grouped by rank

When looking at the browser extensions, we find similar applications compared to the first scenario like ad-blockers and password managers, mainly present in the *Client-facing* group and the *Support* group. In addition, we find extensions like Grammarly, Clockify, and Slidefox. These extensions help employees in their general work tasks: creating documents and presentations, and tracking time. We see more occurrences in the lower ranks. This makes sense since those are the ranks doing most of these work-related activities, while the higher ranks occupy themselves with reviewing the work, client contact, and project management. Moreover, when looking at the browser tools, we find tools with similar purposes like Notion and Zapier, mainly present in the *Junior* rank. Also, we find the same kinds of collaboration tools which are only present in the *Client-facing* group, however, there are fewer occurrences than in the first scenario.

Even though the organization facilitates cloud storage in multiple ways, we still observe external cloud storage applications for work-related tasks. Instances of Dropbox, Google Drive, iCloud, and WeTransfer can be seen through all departments but the *IT staff* group, and throughout all ranks.

5.3.1.3 Cloud services for personal use

"For **personal use**, what **cloud services** have you used?"

Having information on what cloud services are used personally, provides the opportunity to assess how employees see the boundary of using certain applications in a private versus work setting. In this section, we do observe a statistically significant cohort for the **browser extensions**, namely in departments with a $\mathcal{X}^2$ p-value of 0.0419 and a Fisher's p-value of 0.0216. This illustrates there is a significant difference between one of the groups in terms of browser extension usage. When we look at the occurrences, we find that in 3 out of the 8 cells have a value lower than 5. This violates one of the assumptions of the Chi-square test in 3.3.2.3, therefore we look at the Fisher p-value and compute the pairwise comparisons with Bonferroni correction.

We perform these calculations to find out what group causes this statistical difference and we present the results in Table 5.10. We find that the adjusted p value is lower than 0.05. However, we find that the value between the *Management* and *client facing* group has an almost significant value. Even though this does not exceed the arbitrary value of 0.05, it still implies the difference in these groups has influenced the initial statistical calculation the most out of

all the groups. However, since there is no one group that significantly influences the results of this test, we conclude that these significant results are due to differences spread across multiple groups and responses.

Group 1	Group 2	Fisher -*p*	Adjusted *p*
Support	*Client facing*	0,09	**0,56**
Support	*IT staff*	0,47	**1,00**
Support	*Management*	0,50	**1,00**
Client facing	*IT staff*	1,00	**1,00**
Client facing	*Management*	0,01	**0,08**
IT staff	*Management*	0,24	**1,00**

TABLE 5.10: Posthoc pairwise comparisons with Bonferroni correction for browser extensions

On that same note, we find another statistically significant value in this scenario. We observe a $\mathcal{X}^2$ *p*-value of 0.049 for **browser tools** in the rank cohort, however, the corresponding Fisher *p*-value is 0.053. When looking at the occurrence numbers in Table 5.12 we see that 3 out of the 10 cells used for this calculation have a value lower than 5. In the assumptions of the Chi-square test in section 3.3.2.3, we note that the value in 80% of the cells must be higher than 5. This is not the case and hence the assumptions of the Chi-square test are violated. Therefore we use the Fisher *p*-value and find that this value is not statistically significant.

S3	Extension			Tool			Storage			Other			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	33	2	**6%**	31	4	**11%**	20	15	**43%**	35	0	**0%**	16	19	**54%**
Client facing	316	65	**17%**	364	17	**4%**	221	160	**42%**	368	13	**3%**	188	193	**51%**
IT staff	7	1	**13%**	8	0	**0%**	6	2	**25%**	8	0	**0%**	3	5	**63%**
Management	26	0	**0%**	25	1	**4%**	17	9	**35%**	25	1	**4%**	10	16	**62%**

TABLE 5.11: Cloud services for personal use, grouped by department

S3	Extension			Tool			Storage			Other			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	146	29	**17%**	161	14	**8%**	105	70	**40%**	170	5	**3%**	80	95	**54%**
Senior	86	22	**20%**	106	2	**2%**	66	42	**39%**	104	4	**4%**	54	54	**50%**
Manager	63	10	**14%**	68	5	**7%**	38	35	**48%**	71	2	**3%**	40	33	**45%**
Senior Manager	50	5	**9%**	54	1	**2%**	29	26	**47%**	53	2	**4%**	28	27	**49%**
Management	37	2	**5%**	39	0	**0%**	26	13	**33%**	38	1	**3%**	15	24	**62%**

TABLE 5.12: Cloud services for personal use, grouped by rank

By examining the **None** values in Tables 5.11 and 5.12, we see that the use of cloud services for personal use is very high compared to the first two scenarios. The biggest difference compared to the previous scenarios and notably most present group for personal use is the **cloud storage**. **Cloud storage** is well represented throughout both departments and ranks. We find very high occurrences of Google Drive, Dropbox, WeTransfer, and OneDrive. This high presence of cloud storage services might explain why the external cloud storage services are very high

in the first two work-related scenarios. If employees are used to a certain way of storing and sharing files in a certain solution, they might be prone to use these in a work setting, even though the organization has well-supported cloud storage services. In addition to the larger cloud service providers, we see a few specialized cloud storage applications in the *IT staff* like NAS solutions, with several extensions to manage and support this.

Moreover, we see similar types of **Browser extensions** as in work-related scenarios like ad-blockers and password managers, but we also find additional functionalities like crypto-wallets and VPN services. In terms of **browser tools**, we find a similar list of collaborative tools as in the work-related scenarios. A reason why these tools might be used personally is that these tools have functionalities like to-do lists and provide planning functionalities. The occurrence of these tools is not as significant as the **cloud storage**, however, the reasoning behind the usage of these tools personally and in a work environment can be similar. We do however not know why an employee used a tool. The translation can be from personal space to work, but also the other way around. However, if an external tool has been introduced at work and now is used personally, this does reinforce the habit of using that external tool which then translates to more usage in work environments.

5.3.2 Self-installed programs

Self-installed applications have a wide range of functionalities, from a wide range of developing organizations. It was therefore hard to come up with a list of types, however through iterations of pilot surveys and a comprehensive desktop-loadset analysis we created a list of types of applications. Downloading and installing applications can have greater cyber risk consequences compared to using cloud services since applications have easier access to the hardware and data on the system. When respondents were asked what self-installed applications they use that are not provided by the organization, we prompted the following answer options:

- Remote workspaces
- Conferencing tools
- Virtual machines
- Code editors
- Media players
- ERP/CRM systems
- PDF readers/editors (non-standard)
- Screencapture tools
- Streaming services
- Browsers (non-standard)
- Other
- None

Tables 5.13 and 5.14 hold the results of the statistical analyses of the self-installed occurrences. Similarly to the cloud services, we present the data for both cohorts; department and rank (abbreviated in the table as *Dep* and *Rank*). Then per answer option, we again provide the Chi-square value as $\mathcal{X}^2$, the Chi-square p-value as $\mathcal{X}^2$ p, and the Fisher p-value as Fisher p

Install		Workspace			Conferencing			VM			Code editor			Media player			Other		
		$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p
S1	*Dep*	7,84	**0,049**	**0,035**	14,32	**0,0025**	**0,0022**	2,81	0,42	0,69	7,10	0,07	0,06	2,81	0,42	0,69	0,87	0,83	1,00
	Rank	4,77	0,31	0,32	21,56	**0,00024**	**0,00021**	5,14	0,27	0,23	7,31	0,12	0,12	7,63	0,11	0,16	15,89	**0,0032**	**0,0017**
S2	*Dep*	1,33	0,72	1,00	5,62	0,13	0,16	1,66	0,65	1,00	1,85	0,60	0,86	0,93	0,82	1,00	1,27	0,74	0,46
	Rank	8,75	0,07	0,75	15,83	**0,0033**	**0,0034**	1,84	0,77	0,79	3,06	0,55	0,62	5,06	0,28	0,35	3,45	0,48	0,41
S3	*Dep*	2,27	0,52	0,37	0,12	0,99	0,98	0,36	0,95	1,00	1,33	0,72	1,00	1,95	0,58	0,39	1,10	0,78	1,00
	Rank	7,30	0,12	0,12	0,79	0,94	0,95	1,38	0,85	1,00	4,12	0,39	0,53	4,32	0,36	0,46	3,43	0,49	0,48

TABLE 5.13: Self-installed applications statistics (1/2)

Install		Screencapture			Streaming			Browser			ERP/CRM			PDF reader			None		
		$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p
S1	*Dep*	7,07	0,07	**0,037**	2,71	0,44	0,43	1,58	0,66	0,73	2,62	0,45	0,76	4,88	0,18	0,17	9,56	**0,023**	**0,022**
	Rank	2,06	0,72	0,76	5,24	0,26	0,27	4,25	0,37	0,37	2,73	0,61	0,47	5,13	0,27	0,27	8,77	0,07	0,07
S2	*Dep*	3,95	0,27	0,37	0,87	0,83	1,00	0,61	0,89	0,88	1,57	0,67	0,49	2,28	0,52	0,37	2,34	0,97	0,98
	Rank	5,67	0,23	0,26	13,54	**0,0089**	**0,017**	8,75	0,07	0,07	3,77	0,44	0,36	1,50	0,83	0,82	3,88	0,42	0,42
S3	*Dep*	0,95	0,81	0,54	1,45	0,69	0,79	1,32	0,73	0,72	5,04	0,17	0,28	1,02	0,80	0,77	2,33	0,51	0,52
	Rank	0,83	0,93	0,98	14,03	**0,0072**	**0,0084**	2,90	0,57	0,59	3,18	0,53	0,44	1,16	0,88	0,92	1,62	0,81	0,81

TABLE 5.14: Self-installed applications statistics (2/2)

5.3.2.1 Self-installed applications in client projects

"For **specific engagements**, what types of applications have you **downloaded and installed** on your laptop/phone that were **not** provided by [ORGANZATION]?"

Within client projects, tooling is a central point of attention. Most tools that are needed are therefore also provided by the organization. In this section, we focus on self-installed applications that have not been provided by the organization. First, we focus on the statistically significant data points, then we focus on the occurrence patterns and observations. Moreover, we illustrate qualitative examples that groups have provided in the survey.

In Tables 5.13 and 5.14 we find that there are four data points where we find a combined $\mathcal{X}^2$ p-value and Fisher p-value of 0.05 or lower: **remote workspace** for department, **conferencing tool** for both department and rank, and **other** for rank. However, for the department cohort of the **screencapture tool**, we find only the Fisher p-value lower than 0.05. Looking at the occurrence Table 5.22 we find that in 3 out of the 8 cells used for this analysis, the value is lower than 5. The assumptions of the Chi-square test are therefore violated and hence we take the Fisher p-value to determine there is a statistical significance here. Moreover, we compute the pairwise Fisher's exact tests with Bonferroni correction across all departments to find out which department is statistically different. On that same note, the same assumption is violated for the **remote worspace** by department, we therefore also perform the pairwise corrections with Bonferroni correction.

We perform the post hoc calculations to find out what departments cause the statistical significance for the **remote workspaces** (Table 5.15) and **conferencing tools** (Table 5.16). For the **remote workspaces** we observe there is no significant p-value. This implies that there is no *one* department that has a significant impact on Fisher's exact test, suggesting that the differences may be spread across multiple cells. The examples for **remote workspaces** that are provided across departments are Citrix and Amazon Workspace.

Group 1	Group 2	Fisher p	Adjusted p
Support	*Client facing*	0,03	**0,16**
Support	*IT staff*	0,34	**1,00**
Support	*Management*	1,00	**1,00**
Client facing	*IT staff*	1,00	**1,00**
Client facing	*Management*	0,10	**0,59**
IT staff	*Management*	0,42	**1,00**

TABLE 5.15: Posthoc remote workspace per department

	Observed		Expected		Residual	
	F	T	F	T	F	T
Support	30	5	22,94	12,06	**1,47**	**-2,03**
Client facing	247	134	249,77	131,23	**-0,18**	**0,24**
IT staff	7	1	5,24	2,76	**0,77**	**-1,06**
Management	11	15	17,04	8,96	**-1,46**	**2,02**

TABLE 5.16: Posthoc conferencing tool per department

For the **conferencing tool**, we do find both the *support* group and the *management* group have an absolute true residual > 2. Meaning the absence of **conferencing tools** in the *support* group and the excessive presence in the *management* group both have had a significant impact on the Chi-square test results. This implies that the *support* group uses statistically fewer conferencing tools as compared to the other groups and the *management* group statistically more conferencing tools. When looking at the nature of their work this makes sense. Where the *support* group does internal work only, and therefore does not have the need for any other conferencing tools outside the ones provided by the organization, the *management* group is responsible for landing new projects and therefore is involved in a lot of calls. The applications that are given as examples are WebEx, Zoom, and Skype. Looking at the *support* group, this finding implies that there is also a statistical difference with the *IT* staff which also does internal work and therefore would not need any conferencing tools outside the ones provided by the organization. A possible cause for this statistical difference could be the small sample size of *IT* staff.

Table 5.17 illustrates the posthoc test for the **conferencing tool** per rank. We observe two absolute residual values > 2. This implies that the lack of **conferencing tools** amongst the *junior* group, and the extra presence amongst the *senior manager* group has influenced the Chi-squared test significantly. This can also be understood by looking at how tasks are divided in a hierarchical organization. Junior employees tend to handle more hands-on work, while senior employees are more involved in managing projects and thus have to communicate with clients more frequently. We can observe this pattern emerging from the data as we analyze the percentage increase from 11% up to 33% in the use of conferencing tools in relation to higher-ranking positions in Table 5.21.

	Observed		Expected		Residual	
	F	T	F	T	F	T
Junior	135	40	114.58	60.42	**1.91**	**-2.63**
Senior	69	39	71.20	36.80	**-0.26**	**0.36**
Manager	44	29	48.11	24.89	**-0.60**	**0.83**
Senior Manager	27	28	36.25	18.75	**-1.53**	**2.13**
Management	20	19	25.86	13.14	**-1.15**	**1.63**

TABLE 5.17: Posthoc conferencing tool per rank

	Observed		Expected		Residual	
	F	T	F	T	F	T
Junior	170	5	164,11	10,89	**0,46**	**-1,78**
Senior	98	10	101,28	6,72	**-0,33**	**1,27**
Manager	63	10	68,46	4,54	**-0,66**	**2,56**
Senior Manager	55	0	51,58	3,42	**0,48**	**-1,85**
Management	36	3	36,57	2,43	**-0,09**	**0,37**

TABLE 5.18: Posthoc for other per rank

The next statistical significance regarding the use of self-installed applications in client projects can be observed within the **other** category for the specific cohort of individuals based on their rank. We note an absolute residual value > 2 for the group of managers. To explain this statistical significance, it is necessary to examine the specific options entered under the **other** category. We have identified a couple of application types that managers use, which were not originally listed as answer options. These applications can be categorized into two groups: (i) *data analysis tools* and (ii) *networking and remote access tools*. Examples of applications in the data analysis category include Azure Data Studio and R Studio, while examples in the networking and remote access category include FileZilla, PuTTY, WinSCP, and Wireshark. The presence of these applications differentiates the manager group statistically from other groups. However, determining a singular reason why these tools are exclusively used by managers proves challenging.

We perform the residual calculations for the *none* answer option in the department cohort in Table 5.19. We find that no one group has a statistically significant impact on the results of the Chi-square test.

	Observed		Expected		Residual	
	F	T	F	T	F	T
Support	14	21	9.96	25.04	**1.28**	**-0.81**
Client facing	104	277	108.37	272.63	**-0.42**	**0.26**
IT staff	0	8	2.28	5.72	**-1.51**	**0.95**
Management	10	16	7.40	18.60	**0.96**	**-0.60**

TABLE 5.19: Posthoc none per department

Group 1	Group 2	Fisher p	Adjusted p
Support	*Client facing*	0.01	**0.09**
Support	*IT staff*	1.00	**1.00**
Support	*Management*	0.03	**0.17**
Client facing	*IT staff*	0.61	**1.00**
Client facing	*Management*	0.78	**1.00**
IT staff	*Management*	0.55	**1.00**

TABLE 5.20: Posthoc pairwise comparisons for screencapture tools with Bonferroni correction

Finally, we calculate multiple Fisher p-values for the pairwise test across all departments for the **screencapture tool**. We present the calculated p-values before and after the Bonferroni correction Table 5.20. We do not observe any statistically significant values in the adjusted p-values and therefore conclude the found statistical significance is not due to one department but likely a combination of differences spread across multiple cells. We do find a clear distinction in groups by observing the occurrences in Table 5.22. There are no occurrences in the *support* and *IT* groups, and $\approx 15\%$ relative occurrence in the *client facing* and *management* groups. Implying that the **screencapture tools** are in some way needed for client projects.

Tables 5.21 and 5.22 provide the occurrences of self-installed applications for client projects per department and tables Tables 5.23 and 5.24 provide this information per rank. We find that both the *support* group and the *IT staff* have some occurrences of self-installed applications for client projects. However due to the nature of their work, those groups do not engage in projects, and hence the expected occurrence here would be 0.

In Table 5.15 we found no single group was responsible for the statistical significance for

remote workspace in departments. However, when observing the occurrences, we find an increased usage of these tools amongst the *client facing* group. There is one application throughout both department and rank that dominates the **remote workspaces** in terms of presence, this is Citrix. This provides an interesting finding, namely that for the organization these

S1	Workspace			Conferencing			VM			Editor			Media player			Other		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	34	1	**3%**	30	5	**14%**	35	0	**0%**	35	0	**0%**	35	0	**0%**	33	2	**6%**
Client facing	316	65	**17%**	247	134	**35%**	366	15	**4%**	336	45	**12%**	366	15	**4%**	356	25	**7%**
IT staff	7	1	**13%**	7	1	**13%**	8	0	**0%**	8	0	**0%**	8	0	**0%**	8	0	**0%**
Management	25	1	**4%**	11	15	**58%**	26	0	**0%**	25	1	**4%**	26	0	**0%**	25	1	**4%**

TABLE 5.21: Self-installed applications in specific projects, grouped by department (1/2)

S1	Screencapture			Streaming			Browser			ERP/CRM			PDF reader			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	35	0	**0%**	31	4	**11%**	29	6	**17%**	35	0	**0%**	30	5	**14%**	16	19	**54%**
Client facing	327	54	**14%**	350	31	**8%**	289	92	**24%**	367	14	**4%**	311	70	**18%**	248	133	**35%**
IT staff	8	0	**0%**	8	0	**0%**	7	1	**13%**	8	0	**0%**	6	2	**25%**	3	5	**63%**
Management	22	4	**15%**	22	4	**15%**	19	7	**27%**	26	0	**0%**	17	9	**35%**	20	6	**23%**

TABLE 5.22: Self-installed applications in client projects, grouped by department (2/2)

applications are considered shadow-IT, however, the nature of a remote workspace is to provide a centralized desktop. This reduces the likelihood of employees installing unauthorized applications since the IT is managed centrally. Moreover, tools like Citrix allow for detailed monitoring, making it easy to detect if employees are attempting to use unauthorized software, so these behaviors can be tackled at the source. When observing **remote workspaces** through the rank cohort, we find somewhat of a division between on one side the *junior* and *senior* groups, and the three more managerial ranks. This is understandable since people in these positions mainly perform most of these work tasks, in the **remote workspaces**. In contrast, those at higher levels primarily focus on overseeing the work, interacting with clients, and managing projects. We see the same division for the **other browsers**, illustrating that the need for external browsers arises due to work tasks in client projects.

The **virtual machines** are present solely in the *client facing* group. We see similar behavior for the **code editor** and **media player**. Occurrences of Both **virtual machines** and **code editors** are tools used to do work tasks, hence it makes sense that these tasks are performed by the *client facing* staff. We find a lot of different code editors within the *client facing* staff, the most popular are: Notepad++, VSCode, and Anaconda. Compared to other applications, the **media player** does not serve as a tool needed to do actual work, and therefore it remains unclear why this is not present in other groups. In terms of rank, we observe an even spread of occurrences of these tools, with few notable patterns or observations.

S1	Workspace			Conferencing			VM			Editor			Media player			Other		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	154	21	**12%**	135	40	**23%**	172	3	**2%**	154	21	**12%**	170	5	**3%**	170	5	**3%**
Senior	86	22	**20%**	69	39	**36%**	103	5	**5%**	93	15	**14%**	106	2	**2%**	98	10	**9%**
Manager	62	11	**15%**	44	29	**40%**	69	4	**5%**	66	7	**10%**	67	6	**8%**	63	10	**14%**
Senior Manager	45	10	**18%**	27	28	**51%**	52	3	**5%**	53	2	**4%**	53	2	**4%**	55	0	**0%**
Management	35	4	**10%**	20	19	**49%**	39	0	**0%**	38	1	**3%**	39	0	**0%**	36	3	**8%**

TABLE 5.23: Self-installed applications for client projects, grouped per rank (1/2)

S1	Screencapture			Streaming			Browser			ERP/CRM			PDF reader			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	153	22	**13%**	154	21	**12%**	135	40	**23%**	171	4	**2%**	148	27	**15%**	98	77	**44%**
Senior	93	15	**14%**	103	5	**5%**	77	31	**29%**	106	2	**2%**	83	25	**23%**	78	30	**28%**
Manager	61	12	**16%**	68	5	**7%**	61	12	**16%**	70	3	**4%**	61	12	**16%**	49	24	**33%**
Senior Manager	49	6	**11%**	51	4	**7%**	43	12	**22%**	52	3	**5%**	44	11	**20%**	35	20	**36%**
Management	36	3	**8%**	35	4	**10%**	28	11	**28%**	37	2	**5%**	28	11	**28%**	27	12	**31%**

TABLE 5.24: Self-installed applications for client projects, grouped per rank (2/2)

5.3.2.2 Self-installed applications for work-related tasks

"For **work-related tasks**, what types of applications have you **downloaded and installed** on your laptop/phone that were **not** provided by [ORGANZATION]?"

The organization tries to fulfill the need for IT for its employees, however, sometimes employees install external applications to support their work tasks. This section focuses on the occurrences of these applications, we first present the statistically significant data points and consecutively focus on the occurrence patterns, and provide qualitative examples provided with the survey.

We find a statistically significant data point for **conferencing tool** within the rank cohort and for **streaming service** in the rank cohort. For the conferencing tool, none of the assumptions of the Chi-square test are violated and we provide the residual calculations in Table 5.25. For the streaming services, we find that 4 out of the 10 cells have a value lower than 5, and therefore compute the pairwise comparisons with Bonferroni correction in Table 5.26.

	Observed		Expected		Residual	
	F	T	F	T	F	T
Junior	155	20	143,11	31,89	**0,99**	**-2,11**
Senior	89	19	88,32	19,68	**0,07**	**-0,15**
Manager	59	14	59,70	13,30	**-0,09**	**0,19**
Senior Manager	39	16	44,98	10,02	**-0,89**	**1,89**
Management	26	13	31,89	7,11	**-1,04**	**2,21**

TABLE 5.25: Posthoc conferencing tool per rank

Group 1	Group 2	Fisher p	Adjusted p
Junior	*Senior*	0,03	**0,27**
Junior	*Manager*	0,03	**0,28**
Junior	*Senior Manager*	0,03	**0,31**
Junior	*Management*	0,13	**1,00**
Senior	*Manager*	1,00	**1,00**
Senior	*Senior Manager*	0,67	**1,00**
Senior	*Management*	1,00	**1,00**
Manager	*Senior Manager*	1,00	**1,00**
Manager	*Management*	1,00	**1,00**
Senior Manager	*Management*	1,00	**1,00**

TABLE 5.26: Posthoc for streaming services per rank

The results of the Chi-square test for the **conferencing tool** have been influenced significantly by the absence of these tools in the *junior* rank and excessive presence in the *management* rank. We also observed this significance in client-specific projects, where it logically flows from the distribution of tasks within a project. However part of the explanation for more general work-related tasks proves more difficult. For the *management* group, the excessive presence still makes sense because even in non-project situations, one of their main responsibilities is talking to potential clients. This group provided Zoom and WebEx as the main applications used within **conferencing tools**. The significant absence of **conferencing tools** for the *junior* rank is harder to explain since someone within that group would logically use the same amount of **conferencing tools** outside projects as e.g. a *senior* or *manager*.

We find the posthoc test results for the **streaming services** in work-related tasks is influenced by the excessive presence of the *junior* rank. We find no statistical significance however do observe higher occurrences of these services amongst the *junior rank*. The most named examples of this group are Spotify and iTunes.

S2	Workspace			Conferencing			VM			Editor			Media player			Other		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	34	1	**3%**	31	4	**11%**	35	0	**0%**	34	1	**3%**	34	1	**3%**	33	2	**6%**
Client facing	367	14	**4%**	311	70	**18%**	372	9	**2%**	354	27	**7%**	371	10	**3%**	364	17	**4%**
IT staff	8	0	**0%**	8	0	**0%**	8	0	**0%**	8	0	**0%**	8	0	**0%**	7	1	**13%**
Management	26	0	**0%**	18	8	**31%**	26	0	**0%**	25	1	**4%**	26	0	**0%**	25	1	**4%**

TABLE 5.27: Self-installed application in general work tasks, by department (1/2)

S2	Screencapture			Streaming			Browser			ERP/CRM			PDF reader			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	35	0	**0%**	33	2	**6%**	28	7	**20%**	35	0	**0%**	31	4	**11%**	15	20	**57%**
Client facing	352	29	**8%**	356	25	**7%**	300	81	**21%**	375	6	**2%**	335	46	**12%**	178	203	**53%**
IT staff	8	0	**0%**	8	0	**0%**	6	2	**25%**	8	0	**0%**	6	2	**25%**	4	4	**50%**
Management	25	1	**4%**	25	1	**4%**	22	4	**15%**	25	1	**4%**	21	5	**19%**	12	14	**54%**

TABLE 5.28: Self-installed application in general work tasks, by department (2/2)

In Tables 5.27 and 5.28 we illustrate the occurrences of answer options grouped by department. A global pattern that arises when compared to the first scenario is that there are no answer options that in total have more occurrences than for client projects. On the contrary, when we compare the *none* value from client projects in Table 5.22 to this value, we find that the relative occurrence is somewhat similar, except for the *management* group. We find that this group uses a lot fewer self-installed applications for specific projects than for general work tasks. The largest difference can be found in the absence of **conferencing tools**. On that same note, we see the number of applications used for client projects, like **remote workspaces** and **conferencing tools** in general have decreased. We do observe a wide variety of **conferencing tools** like Zoom, Skype, WebEx, Bluejeans, and Teamspeak.

Similarly to the department cohort, we observe a decrease in occurrences of answer options in the rank cohort. We illustrate the occurrences in Tables 5.29 and 5.30. The occurrence however

of **remote workspaces** and **conferencing tool** across different groups is surprising. The nature of working in a **remote workspace** is to connect to a remote desktop that the client has set up in order to access their systems and data. Finding an explanation for this observation remains a challenge. Moreover, using external **conferencing tools** does not seem logical for non-client-specific projects. Examples of the tools that are given are WebEx, Zoom, Slack Teamviewer, and Teamspeak.

S2	Workspace			Conferencing			VM			Editor			Media player			Other		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	169	6	**3%**	155	20	**11%**	172	3	**2%**	164	11	**6%**	170	5	**3%**	170	5	**3%**
Senior	104	4	**4%**	89	19	**18%**	106	2	**2%**	100	8	**7%**	107	1	**1%**	103	5	**5%**
Manager	71	2	**3%**	59	14	**19%**	71	2	**3%**	66	7	**10%**	69	4	**5%**	67	6	**8%**
Senior Manager	52	3	**5%**	39	16	**29%**	53	2	**4%**	53	2	**4%**	54	1	**2%**	52	3	**5%**
Management	39	0	**0%**	26	13	**33%**	39	0	**0%**	38	1	**3%**	39	0	**0%**	37	2	**5%**

TABLE 5.29: Self-installed application in general work tasks, by rank (1/2)

S2	Screencapture			Streaming			Browser			ERP/CRM			PDF reader			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	166	9	**5%**	155	20	**11%**	132	43	**25%**	173	2	**1%**	156	19	**11%**	72	103	**59%**
Senior	97	11	**10%**	104	4	**4%**	80	28	**26%**	107	1	**1%**	92	16	**15%**	51	57	**53%**
Manager	66	7	**10%**	71	2	**3%**	64	9	**12%**	72	1	**1%**	62	11	**15%**	38	35	**48%**
Senior Manager	53	2	**4%**	54	1	**2%**	48	7	**13%**	54	1	**2%**	49	6	**11%**	29	26	**47%**
Management	38	1	**3%**	38	1	**3%**	32	7	**18%**	37	2	**5%**	34	5	**13%**	19	20	**51%**

TABLE 5.30: Self-installed application in general work tasks, by rank (2/2)

5.3.2.3 Self-installed applications for personal use

"For **personal use**, what types of applications have you **downloaded and installed** on your laptop/phone?"

Gaining insights into the self-installed programs individuals use personally allows for assessing employees' perceptions of the boundary between using specific applications in personal and work settings. Moreover, it provides information on what applications employees think they can download and install on a work device.

	Observed		Expected		Residual	
	F	T	F	T	F	T
Junior	107	68	124,06	50,94	**-1,53**	**2,39**
Senior	85	23	76,56	31,44	**0,96**	**-1,51**
Manager	54	19	51,75	21,25	**0,31**	**-0,49**
Senior Manager	44	11	38,99	16,01	**0,80**	**-1,25**
Management	29	10	27,65	11,35	**0,26**	**-0,40**

TABLE 5.31: Posthoc for streaming services by rank

We find a statistically significant value for **streaming services** in the rank cohort. We find that the Chi-square assumptions are not violated and therefore compute the residuals in Table 5.31. We find the *junior* group has had a significant influence on the results of the Chi-square test.

Looking at the occurrence in Table 5.35, we clearly see a relative excess of **streaming services** in this group. Examples of these services the *junior* group has provided are Spotify, Netflix, and Videoland.

We provide the occurrences of self-installed applications on departments in Tables 5.32 and 5.33. We find the overall occurrences of self-installed applications is lowest for personal use. We do find some **conferencing tools** within the *client facing* group. Sorted by occurrence, these are Zoom, Skype, WebEx, and Google Meet.

S3	Workspace			Conferencing			VM			Editor			Media player			Other		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	35	0	**0%**	29	6	**17%**	35	0	**0%**	34	1	**3%**	34	1	**3%**	34	1	**3%**
Client facing	377	4	**1%**	319	62	**16%**	379	2	**1%**	367	14	**4%**	368	13	**3%**	369	12	**3%**
IT staff	8	0	**0%**	7	1	**13%**	8	0	**0%**	8	0	**0%**	7	1	**13%**	8	0	**0%**
Management	25	1	**4%**	22	4	**15%**	26	0	**0%**	26	0	**0%**	25	1	**4%**	26	0	**0%**

TABLE 5.32: Self-installed applications for personal use, by department (1/2)

S3	Screencapture			Streaming			Browser			ERP/CRM			PDF reader			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	33	2	**6%**	26	9	**26%**	28	7	**20%**	34	1	**3%**	33	2	**6%**	16	19	**54%**
Client facing	369	12	**3%**	267	114	**30%**	296	85	**22%**	380	1	**0%**	351	30	**8%**	202	179	**47%**
IT staff	8	0	**0%**	7	1	**13%**	5	3	**38%**	8	0	**0%**	7	1	**13%**	3	5	**63%**
Management	25	1	**4%**	19	7	**27%**	21	5	**19%**	26	0	**0%**	25	1	**4%**	11	15	**58%**

TABLE 5.33: Self-installed applications for personal use, by department 2/2)

Moreover when looking at the occurrence tables of the rank cohort in Tables 5.34 and 5.35. We find the presence of the **conferencing tools** are spread evenly across the ranks. The same holds for the **streaming services**. While the *client facing* group had significantly more of these services, we see that they have also spread evenly across the ranks.

We also observe an evenly spread use of **other browsers**. The browsers named by respondents are Google Chrome, Mozilla Firefox, Safari, Brave, and QQ browser. Especially the latter one is interesting since the browser has been the topic of privacy leaks and other cybersecurity consequences (Knockel et al., 2016). When cross-referencing the example in the rank cohort, we find the example is given by someone in the *management* staff.

S3	Workspace			Conferencing			VM			Editor			Media player			Other		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	174	1	**1%**	147	28	**16%**	174	1	**1%**	166	9	**5%**	169	6	**3%**	171	4	**2%**
Senior	107	1	**1%**	88	20	**19%**	107	1	**1%**	105	3	**3%**	101	7	**6%**	103	5	**5%**
Manager	73	0	**0%**	63	10	**14%**	73	0	**0%**	72	1	**1%**	72	1	**1%**	70	3	**4%**
Senior Manager	54	1	**2%**	46	9	**16%**	55	0	**0%**	53	2	**4%**	54	1	**2%**	55	0	**0%**
Management	37	2	**5%**	33	6	**15%**	39	0	**0%**	39	0	**0%**	38	1	**3%**	38	1	**3%**

TABLE 5.34: Self-installed applications for personal use, by rank (1/2)

S3	Screencapture			Streaming			Browser			ERP/CRM			PDF reader			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	168	7	**4%**	107	68	**39%**	134	41	**23%**	175	0	**0%**	161	14	**8%**	93	82	**47%**
Senior	104	4	**4%**	85	23	**21%**	82	26	**24%**	107	1	**1%**	100	8	**7%**	57	51	**47%**
Manager	71	2	**3%**	54	19	**26%**	55	18	**25%**	72	1	**1%**	66	7	**10%**	39	34	**47%**
Senior Manager	54	1	**2%**	44	11	**20%**	47	8	**15%**	55	0	**0%**	52	3	**5%**	25	30	**55%**
Management	38	1	**3%**	29	10	**26%**	32	7	**18%**	39	0	**0%**	37	2	**5%**	18	21	**54%**

TABLE 5.35: Self-installed applications for personal use, by rank (2/2)

5.3.3 Self-made solutions

Self-made solutions entail the creation of a solution by an employee itself. These entities are referred to as 'shadow' not just because they replicate data from official systems, but also because they perform tasks that would ideally be handled by a more controlled and organized system (Gadellaa, 2022). When we asked respondents what self-made solutions they used, we prompted the following answer options:

- Self-made software
- Self-made website
- External spreadsheet
- System coupling
- Other
- None

With regard to self-made solutions, employees have the opportunity to create their own tools and applications within the services provided by the organization. This means developing applications within work-related cloud environments or building solutions using platforms for which the organization holds licenses. These instances do not qualify as shadow IT since the organization is fully aware of and we therefore explicitly seek examples of self-made solutions that were not facilitated by the organization itself. We prompt this after every question to ensure the respondents understand this nuance.

Own		Own software			Own website			External spreadsheet			System coupling			Other			None		
		$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p
S1	*Dep*	4,45	0,22	0,19	1,10	0,78	1,00	0,27	0,97	0,92	0,92	0,82	1,00	2,01	0,57	0,53	0,80	0,85	0,95
	Rank	4,01	0,40	0,48	0,90	0,93	0,93	0,46	0,98	0,98	4,29	0,37	0,44	2,39	0,66	0,64	2,30	0,68	0,71
S2	*Dep*	3,70	0,30	0,28	0,92	0,82	1,00	7,29	0,06	0,06	1,10	0,78	1,00	2,04	0,56	0,84	4,55	0,21	0,21
	Rank	2,15	0,71	0,75	2,95	0,57	0,48	3,54	0,47	0,49	2,93	0,57	0,59	5,24	0,26	0,36	1,03	0,91	0,91
S3	*Dep*	0,73	0,87	1,00	2,27	0,52	0,37	0,88	0,83	0,75	0,18	0,98	1,00	0,92	0,82	1,00	3,20	0,36	0,36
	Rank	3,87	0,42	0,47	5,66	0,23	0,11	6,19	0,19	0,21	7,20	0,13	0,21	2,05	0,73	0,80	5,13	0,27	0,30

TABLE 5.36: Own solutions statistics

Table 5.36 provides the statistical calculations for the self-made shadow IT types. We illustrate the data for both cohorts and find there are no statistically significant results. We, therefore, look at the patterns and occurrences of these instances across cohorts and provide context with the qualitative examples that respondents provided to illustrate what self-made solutions are present.

5.3.3.1 Self-made solutions in client projects

"For **specific engagements**, what **own solutions** have you created that were **not** facilitated by [ORGANZATION]?"

We find the occurrences of self-built solutions in Tables 5.37 and 5.38. An observation that we notice immediately when observing the *none* values. The overall usage of self-made solutions in client projects is lower than both cloud services and self-installed applications. Due to the nature of the work in client projects, we would actually expect solely responses from the *client facing* group and the *management staff* throughout all answer options. However, we also find responses from the *IT staff* and the *Support* staff.

Responses with **own website** and **system coupling** are only from the *client facing* group. We see a few responses for the **own website**, however, we only find WordPress as a suitable example given. For the **system coupling**, we find other examples like Automatic Data quality checks and IFTTT. The latter is a tool to automate home devices. With one occurrence outside of the *client facing* staff, examples that were provided for the **own software** are web scrapers, Django applications, optimization tools, and one respondent reported creating a "*Custom hacking tool*".

S1	Own software			Own website			External spreadsheet			System coupling			Other			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	35	0	**0%**	35	0	**0%**	29	6	**17%**	35	0	**0%**	33	2	**6%**	7	28	**80%**
Client facing	360	21	**6%**	375	6	**2%**	327	54	**14%**	376	5	**1%**	370	11	**3%**	80	301	**79%**
IT staff	7	1	**13%**	8	0	**0%**	7	1	**13%**	8	0	**0%**	8	0	**0%**	1	7	**88%**
Management	26	0	**0%**	26	0	**0%**	22	4	**15%**	26	0	**0%**	26	0	**0%**	7	28	**80%**

TABLE 5.37: Self-made solutions in client projects, by department

S1	Own software			Own website			External spreadsheet			System coupling			Other			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	164	11	**6%**	173	2	**1%**	150	25	**14%**	174	1	**1%**	171	4	**2%**	38	137	**78%**
Senior	102	6	**6%**	106	2	**2%**	92	16	**15%**	105	3	**3%**	104	4	**4%**	25	83	**77%**
Manager	69	4	**5%**	72	1	**1%**	61	12	**16%**	72	1	**1%**	72	1	**1%**	14	59	**81%**
Senior Manager	54	1	**2%**	54	1	**2%**	48	7	**13%**	55	0	**0%**	52	3	**5%**	10	45	**82%**
Management	39	0	**0%**	39	0	**0%**	34	5	**13%**	39	0	**0%**	38	1	**3%**	5	34	**87%**

TABLE 5.38: Self-made solutions for client projects, by rank

We observe the most occurrences within the **external spreadsheets** answer option. The occurrences are spread evenly between both departments and ranks. In the context of client projects, we observe external spreadsheets are mostly used for niche calculations and employee understanding of certain topics or models. In addition, we find certain tracking spreadsheets for either financial data or project management. In the *management* group, we find use cases for forecasting models and managing commercial opportunities. We observe a few occurrences of the *other* options, mostly in the *client facing* group but also some in *support*. The occurrences are spread evenly across ranks. Examples of applications that were provided are Alteryx, a data analytics creation tool, and Asana, a to-do list tool. For these tools, the question arises if they really are self-built solutions or just tailored settings in an existing tool to accomplish some set of tasks.

5.3.3.2 Own solutions for work-related tasks

"For **work-related tasks**, what **own solutions** have you created that were **not** facilitated by [ORGANZATION] ?"

When asked about work-related tasks, respondents provided insights into their own solutions that are not facilitated by the organization. In doing so, respondents shared various approaches they developed to address challenges. We find the occurrences of self-built solutions in Tables 5.39 and 5.40. We observe similar patterns in the occurrences compared to self-built applications in client projects.

We find some **own software** examples in the form of AI scripts hosted on Heroku, which were found in the *junior* department. These scripts enable automated tasks and streamline processes. We see this in tools like IFTTT and Power Automate, which help in automating various actions and creating workflows. Surprisingly, we find a web scraper tool created by the *support* team.

S2	Own software			Own website			External spreadsheet			System coupling			Other			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	34	1	**3%**	35	0	**0%**	28	7	**20%**	35	0	**0%**	35	0	**0%**	8	27	**77%**
Client facing	371	10	**3%**	376	5	**1%**	354	27	**7%**	375	6	**2%**	370	11	**3%**	43	338	**89%**
IT staff	7	1	**13%**	8	0	**0%**	7	1	**13%**	8	0	**0%**	8	0	**0%**	1	7	**88%**
Management	26	0	**0%**	26	0	**0%**	24	2	**8%**	26	0	**0%**	26	0	**0%**	2	24	**92%**

TABLE 5.39: Self-made solutions in general work tasks, by department

S2	Own software			Own website			External spreadsheet			System coupling			Other			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	170	5	**3%**	174	1	**1%**	163	12	**7%**	173	2	**1%**	171	4	**2%**	21	154	**88%**
Senior	106	2	**2%**	107	1	**1%**	99	9	**8%**	107	1	**1%**	105	3	**3%**	13	95	**88%**
Manager	70	3	**4%**	71	2	**3%**	68	5	**7%**	72	1	**1%**	69	4	**5%**	9	64	**88%**
Senior Manager	53	2	**4%**	54	1	**2%**	47	8	**15%**	53	2	**4%**	55	0	**0%**	8	47	**85%**
Management	39	0	**0%**	39	0	**0%**	36	3	**8%**	39	0	**0%**	39	0	**0%**	3	36	**92%**

TABLE 5.40: Self-made solutions for work tasks, by rank

For the *client facing* group we observe some similar **external spreadsheets**. Namely for personal understanding, pivot tables, and specific calculations of certain concepts. **External spreadsheets** were used also by the *IT staff* to aid in the asset management and life-cycle management of devices. The *support* group uses these to create macros and overviews of candidate procedures, and *management* group provided financial forecasting models examples of using **external spreadsheets** in this context. The self-built solutions illustrate the resourceful nature of the employees, demonstrating that employees will create their own solutions for simple tasks, even if that means using resources not provided by the organization.

5.3.3.3 Own solutions for personal use

"For **personal use**, what **own solutions** have you created?"

We asked respondents about their own solutions in a personal setting to benchmark the self-made solutions to solutions created in a work setting. We provide the occurrences in Tables 5.41 and 5.42.

On a general note we find that, contrary to the cloud services and self-installed applications, the use of self-built tools is lower in a personal context than in a work-related context. We observe this through the average *none* percentage This implies that the adoption of self-made solutions is not driven by personal preferences or habits derived from personal experiences. Instead, it arises from the need to address work-related tasks for which the organization lacks a straightforward solution.

S3	Own software			Own website			External spreadsheet			System coupling			Other			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	35	0	**0%**	35	0	**0%**	32	3	**9%**	35	0	**0%**	35	0	**0%**	3	32	**91%**
Client facing	377	4	**1%**	377	4	**1%**	349	32	**8%**	380	1	**0%**	376	5	**1%**	39	342	**90%**
IT staff	8	0	**0%**	8	0	**0%**	7	1	**13%**	8	0	**0%**	8	0	**0%**	2	6	**75%**
Management	26	0	**0%**	25	1	**4%**	25	1	**4%**	26	0	**0%**	26	0	**0%**	3	32	**91%**

TABLE 5.41: Self-made solutions for personal use, by department

S3	Own software			Own website			External spreadsheet			System coupling			Other			None		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	172	3	**2%**	174	1	**1%**	164	11	**6%**	175	0	**0%**	173	2	**1%**	14	161	**92%**
Senior	108	0	**0%**	108	0	**0%**	100	8	**7%**	108	0	**0%**	106	2	**2%**	11	97	**90%**
Manager	73	0	**0%**	72	1	**1%**	68	5	**7%**	73	0	**0%**	73	0	**0%**	6	67	**92%**
Senior Manager	54	1	**2%**	53	2	**4%**	46	9	**16%**	54	1	**2%**	54	1	**2%**	10	45	**82%**
Management	39	0	**0%**	38	1	**3%**	35	4	**10%**	39	0	**0%**	39	0	**0%**	4	35	**90%**

TABLE 5.42: Self-made solutions for personal use, by rank

Within the *client facing* group we see several personal tracking tasks using **external spreadsheets**. This group provided the following examples: hour administration, expense tracking, holiday tracking, and task tracking. Moreover, this group provided two inventive solutions: a robot that sends a notification when a home was for rent in a certain location, and a robot that would ping the user if a certain lease car would be re-entered into the lease pool.

We have seen that employees often create their own solutions, possibly because the tools given by their company do not fully meet their needs. It seems like employees are looking for tools that are more tailored to their specific tasks and goals than the standard tools provided. These self-made solutions show how creative and problem-solving employees can be. However, we must account for the potential risks when dealing with these self-made tools. Understanding why employees use these self-made solutions can help organizations, and allow them to provide better tools.

5.3.4 Occurrence of private devices

Large organizations often discourage the use of personal devices for work-related activities by facilitating employees with laptops and mobile phones. These devices allow the organization to monitor the data that is handled and regulate the usage of applications and networks. They allow IT departments to ensure proper engagement in security protocols, thus reducing the risk of data breaches and keeping the organization's data on the organization's systems. These devices also ensure uniformity in software, which facilitates troubleshooting and maintenance. Organizations aim to find a middle ground between convenience, productivity, and security in the digital workspace by providing devices that are managed by the organization. Therefore, insights into the usage of private devices will become useful in finally understanding the reasons behind this.

We uncover this by prompting respondents with the question above, and providing the following answer options:

"For what work related tasks have you ever used your private phone, tablet, laptop or other private devices?"

We uncover this by prompting respondents with the question above, and providing the following answer options:

- Forwarded email to a personal account to access it there
- Scheduling appointments
- Contacting clients
- No, I have never used my private phone/laptop for any work related tasks
- Other

	Personal mail			Scheduling appointments			contacting clients			Other			None		
	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p	$\mathcal{X}^2$	$\mathcal{X}^2$ p	Fisher p
Dep	3,78	0,29	0,34	0,66	0,89	0,89	5,09	0,17	0,20	5,09	0,17	0,20	0,98	0,81	0,87
Rank	5,85	0,21	0,21	1,55	0,82	0,89	4,52	0,34	0,26	1,06	0,90	0,88	8,12	0,09	0,09

TABLE 5.43: Private devices statistics

We perform statistical calculations in both cohorts to find out if there is significantly more usage of private devices in certain groups and provide the results in Table 5.43. We find there are no statistically significant results and therefore we look for patterns in the occurrences and give qualitative examples of tasks done on private devices by the respondents.

	Personal mail			Scheduling			Contacting clients			Other			No		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Support	33	2	**6%**	33	2	**6%**	33	2	**6%**	34	1	**3%**	7	28	**80%**
Client facing	355	26	**7%**	358	23	**6%**	361	20	**5%**	346	35	**9%**	91	290	**76%**
IT staff	8	0	**0%**	8	0	**0%**	8	0	**0%**	7	1	**13%**	1	7	**88%**
Management	24	2	**8%**	24	2	**8%**	22	4	**15%**	25	1	**4%**	7	19	**73%**

TABLE 5.44: Private devices, by department

The occurrences by department are illustrated in Table 5.44 and by rank in Table 5.45. In general, we do not observe a lot of usage of private devices, and looking at the *none* values in both tables, the usage is well spread across both cohorts.

The use cases of using private devices and solutions in a work-related context can be categorized into a few main categories. The first and most occurring tasks revolve around mailing and communication, including emailing colleagues, and calling clients and candidates. We find these tasks throughout all ranks, and throughout all departments. The second most occurring tasks focus on calendars and reminders, where work and private calendars are sometimes merged, and private reminders can be set for work. This mostly occurs in the *junior* rank.

Private devices	Personal mail			Scheduling			Contacting clients			Other			No		
	F	T	%	F	T	%	F	T	%	F	T	%	F	T	%
Junior	149	26	**15%**	162	13	**7%**	166	9	**5%**	161	14	**8%**	53	122	**70%**
Senior	99	9	**8%**	102	6	**6%**	99	9	**8%**	100	8	**7%**	18	90	**83%**
Manager	69	4	**5%**	69	4	**5%**	72	1	**1%**	65	8	**11%**	14	59	**81%**
Senior manager	48	7	**13%**	52	3	**5%**	51	4	**7%**	51	4	**7%**	12	43	**78%**
Management	35	4	**10%**	38	1	**3%**	36	3	**8%**	35	4	**10%**	9	30	**77%**

TABLE 5.45: Private devices, by rank

A remarkable finding is that some employees found they had to use personal laptops because work laptops were incompatible or not powerful enough, particularly for coding purposes. These occurrences were in the *client facing* group, in the *junior* or *senior* rank. One employee even mentioned that the use of a personal laptop was due to the crashing of a work laptop. Another set of tasks involves document handling, such as downloading or uploading non-confidential documents, reviewing them, printing at home, or accessing them through personal accounts. In all of these instances, employees explicitly named the 'non-confidential' in their examples. This suggests a good awareness of the use of private devices.

Employees also use personal devices for arranging appointments, and meetings, and scheduling team calls. In certain cases, personal devices are necessary for time tracking and design work. Some employees prefer using a single device for reading work emails, forwarding meeting invites to personal accounts, and managing their workflow efficiently.

We found that while large organizations generally discourage the use of personal devices for work-related activities, there is still a notable presence across departments and ranks. We observe that the most common tasks conducted on personal devices are related to mailing and communication, such as emailing colleagues and contacting clients and candidates. Calendar and reminder management are also found amongst *junior* ranks. There are a few occurrences where the use of personal laptops is due to incompatibility or lack of resources. Therefore we stress the need for organizations to strike a balance between convenience, productivity, and security in the digital workspace with regard to personal devices. As employees continue to use personal devices for work tasks despite the organization's efforts to provide their own devices.

5.4 Summary of Survey Findings & Discussion

We have seen the occurrences of the four different shadow IT types, across cohorts in different scenarios. We present the main findings in this section.

We uncover how employees use all kinds of cloud services, even though external tools are not allowed to do any business-related tasks by the organization. We observe that employees use these services a lot, for both work tasks as well as for personal use. It is interesting that these services are used across all job levels and in all kinds of situations, and this gives the incentive to uncover *why* employees use different kinds of cloud services. *It is evident that employees use what they are familiar with and prefer, even if it is not the organization's policy*. Going forward, we want to analyze the thoughts behind this data and uncover how employees think about the use of different types of cloud services.

Our findings indicate that self-installed applications have a significant role in the workflow across departments and ranks. We discovered a statistically significant use of remote workspaces, conferencing tools, and the "other" categories of tools by different departments and ranks, which also spikes the interest to uncover the reasoning behind these external tools. Across scenarios, we encounter differences in the occurrences of self-installed applications. We find an apparent decrease in the use of self-installed applications in general work tasks compared to client-specific projects and an increase in the personal use of self-installed applications. The difference in usage of work-related and personal applications gives an initial idea of how employees see the use, and hence place the potential risks of different applications on a work device, and hence mitigate risks and prevent occurrences like the QQ Browser in the *management* group.

Employees find the need to create their own solutions sometimes, indicating a gap between their unique needs and the tools provided by their organizations. They demonstrate resourcefulness and creativity in using their own software, websites, external spreadsheets, and system couplings, among other solutions. These solutions span from niche calculations to tracking spreadsheets, forecasting models, and task automation. We find that self-built solutions are lower in personal contexts, suggesting that they are driven by work-related needs rather than personal preferences. We find this across all roles. The patterns imply that all employees, regardless of their roles, encounter tasks for which existing systems do not offer standard solutions.

Despite large organizations discouraging the use of personal devices for work-related activities, there is a trend among employees, notably in *client-facing* group and across both *junior* and *senior* ranks, to use personal laptops for tasks ranging from coding to document handling. The reasons for this include work laptops being incompatible or insufficiently powerful, and even prone to crashing. Employees use personal devices for a wide range of activities like scheduling appointments and team calls, time tracking, design work, and email management. However, there is a certain awareness when using these devices, since respondents emphasized the non-confidential nature of documents accessed or handled on their personal devices.

5.5 Survey limitations

When analyzing the survey results, we find a combination of explainable and inexplicable observations. We discuss these aspects in this section and try and contextualize the bigger picture of the survey.

We observe that the distribution of departments in the survey resembles the distribution of departments in the larger organization (see table When observing the department distribution in Table 5.4). However, this means the respondents are mainly from the *client facing* group. This resulted in a lot of responses and possibilities of finding nuances within the ranks of this group. Since the total number of respondents in the other groups is a lot smaller, these nuances can be overlooked in the survey results because of a lack of responses from these groups.

Moreover, the size of the populations differs a lot. Especially with the assumptions of the Chi-square test that 80% of the cells must contain a value higher than 5 is endangered by these group sizes. We only find this issue with the department cohort, since the distribution of the rank groups is spread more evenly.

A remarkable finding is that both cohorts have a management group. The department cohort holds 26 responses in the *management staff*, and the rank cohort holds 39 responses in the *management* group. We account for this difference due to the fact that certain *management* staff oversees a certain team. Thus even though they are in the managerial role for the department they responded with the team that they manage.

In section 3.3.2.4, we illustrated a limitation of the survey is providing answer options. Especially in the self-installed applications we notice a very low occurrence of certain applications and a very high occurrence in the *other* group. For example, we observe a lot of data analytics tools and networking tools. We tested the survey in three rounds of pilots, with two participants each. Even though these participants were from different ranks and departments, we did not account for some of the differentiation within departments. Especially within the *client facing* group there is a lot of variety in application usage. Therefore we conclude that we used a too-narrow spread of individuals within the departments to do the pilot surveys.

We observe a few answers where an explanation is hard to find. The nature of the work of the *support* group is to facilitate internal processes. They do internal projects and keep the organization running from the inside, without actually doing any work that generates revenue. Therefore finding responses within this group for specific engagements is a surprising finding. We find instances of this group in cloud services, self-installed applications, and in self-built solutions. This either means some of the respondents within the *support* are used for client-specific projects, or this means that the respondents within this group did not fully grasp the nuances made within the scenarios. We tried to avoid the latter by introducing the nuances within the survey through the explanatory section and the nuances at the start of each section as described in section 3.3.2.4.

In hindsight, we could have created the flow of the survey such that if the respondent entered the *support* department in the demographics section, this scenario of *client-specific work* could have been skipped, since it is the nature of their work to not do any work for client projects. However now that we have these findings, it might implicate overall less accurate results. Resulting from a too-complex nuanced survey structure that the questions fall in.

One of the answer options within the self-installed applications provides food for thought on how to address certain aspects in the rest of this research. This is the **remote workspace** application. This sparks an interesting finding for the nature of the shadow-IT occurrences for the *client facing* group. Within this group, there was very high usage of these types of tools. These tools are not directly facilitated by the organization and therefore are classified as a shadow IT occurrence, however, the reason to use **remote workspaces** is so that employees within the *client facing group* have their own work environment for the specific project they are doing. This means these employees do not have to use file-sharing tools to get the data or install tooling to work with this data. Since this is all accounted for by the client organization. Therefore we introduce the **perspective** of shadow IT applications in client projects. Some of the employees that are temporarily working at another client can even get a laptop from that client that has been set up for them to do work tasks in. Thus, we need to understand the context of the work tasks. Moreover, we must perceive shadow IT from multiple perspectives to account for the risks for a certain organization: for which organization do we label an application as a shadow IT instance?

5.6 Takeaways for next chapter

We observed the occurrences of different types of shadow IT throughout scenarios across departments and ranks. We find a larger presence of shadow IT occurrences in the *client facing group*. By now understanding where and in what forms shadow IT occurs, we find the need to uncover why these applications are used throughout different scenarios. Moreover, by understanding why these applications are used, we can uncover the employee perception of the use of shadow IT applications, and what they think are the implications of the use of these applications. Additionally, for the *client facing* group we find the need to account for the **perspective** through which shadow IT instances are labeled. Understanding how employees work in their client project environments and what environments are provided by clients understands the nuances of what is labeled as shadow IT for which organization.

6 Understanding of the concept of Shadow IT

To answer RQ3, we aim to find the perception of shadow IT and the risks and implications of shadow IT across cohorts. We do this by conducting semi-structured interviews with participants in these cohorts. Since the research methods of the interview result from the findings in the SLR, we first provide the research methods, then immediately after we present the findings of the interviews and consecutively, we build the mental models different employees have of shadow IT. Moreover, these interviews then aim to answer: *Across different cohorts, what is the perception of the concept of Shadow IT, and what are the perceived risks and implications of shadow IT?*

6.1 Research methods

In this section, we present the methodology for the interviews. These methods are selected based on the SLR results.

6.1.1 Interview participants

The subjects of this interview study are employees within a large professional services company. We divide the interviews into two rounds. In the first round, we select the interview participants from the departments and ranks that have been named in section 3.1. In order to get a representative dataset, we use two sampling methods. *Cluster sampling*; we cluster the participants according to the departments in section 3.1. In addition, we will use *stratified sampling* within the department clusters on rank, meaning that within each cluster, we want to sample all the ranks. From the four departments, we will try to interview all ranks within that department and analyze the results. We combine the survey results with the first round of interviews and identify which combination of cohorts provides the most relevant information for this research. We then decide on what participants to recruit for the second round of interviews.

When determining the appropriate number of interviewees for code saturation, Guest et al. (2006) conducted a well-referenced analysis in qualitative research. According to these findings, the majority of codes are uncovered within six interviews, with very few new codes emerging beyond twelve interviews. However, a more recent comparison in IS research by Marshall et al. (2013) suggests that the lower limit of this estimate might be insufficient. It is

crucial to justify sample sizes in qualitative IS research to ensure scientific rigor, yet this aspect is frequently overlooked. (Marshall et al., 2013). Therefore, we try to conduct six interviews per department across different ranks for the first round, then based on the results we decide what participants to recruit for the final interviews.

6.1.2 Protocol development and execution

The interview protocol creation is guided by Turner (2010). To elicit the mental models, we combine semi-structured interviews with drawing and a think-aloud method. This allows the participants to visualize their mental model (Morgan et al., 2002). Doing this, we find several advantages: (i) each of these methods provides different types of information about the participant's mental model, and they will complement each other to gain a comprehensive mental model (Byrd et al., 1992), (ii) using multiple methods will increase the accuracy of the mental model since the participant's response can be verified across different methods (Jones et al., 2011), (iii) alternating between different methods will reduce participant fatigue and keep the participants engaged throughout the interview process (Greyson et al., 2017).

After creating the interview protocol, we did pilot interviews to validate that the questions aligned with the research objectives. In this regard, we followed the guidelines proposed by Castillo-Montoya (2016): explicitly linking interview questions to research goals, introducing topics before asking main questions, and preparing specific probes to guide participants in providing detailed insights on potential risks and implications they think shadow IT can bring. Specifically, we asked participants the following:

- Their understanding of shadow IT
- The reasons they use shadow IT
- Their perception of implications of the use of shadow IT
- Their awareness of relevant policies with regard to shadow IT
- How shadow IT is discussed amongst colleagues
- How well they feel they are informed about shadow IT

Moreover, for the participants within the *client facing* staff we have an extra section. We perform a drawing and think-aloud exercise after probing the participants with a certain scenario that is only relevant to this group. In addition to questions directly related to shadow IT occurrences and the risks and implications, we gathered similar information with regard to the participant's demographics as in the survey: professional work experience, department, and rank.

To minimize potential language barriers for participants, we conducted the interviews in the natural language of the participant. Most of the interviews have been conducted in Dutch, and two interviews have been conducted in English. We conducted the interviews in person if possible, and if not we chose Microsoft Teams as the interview platform due to its widespread adoption within the sector and its ability to facilitate convenient recording of the interviews while ensuring data privacy, as Utrecht University has a data processing agreement with this vendor.

During the interviews, we found out that the drawing component caused confusion. This was discussed amongst the research group and we decided to keep the scenario prompt for the *client facing* staff, but we would leave out the drawing component. The interviews were transcribed, taking into account filler sounds and repeated words. However, in one of the interviews, a connection issue occurred, resulting in the interview being interrupted and unable to be completed in a single session. As a result, the interview was conducted in two parts. Before starting the second part, all the questions and answers from the first part were revisited to ensure the continuity of the participant's answers. This allowed the participant to resume the interview from where we had previously left off.

6.1.3 Data analysis

We perform open and axial coding using Atlas.ti [1] to uncover different shadow IT occurrences, the reasons for the usage of these applications, and the perception of the concept and the implications that it brings. Structure and answer options from the survey serve as pre-set code categories, which served as domains. Quotes within the text were attributed to lower-level concepts, which were subsequently assigned to the relevant categories or added as additional emergent codes or categories.

Following the transcription of interviews, we used a multiple-coding approach to ensure rigor as described by Barbour (2001). For this, we used an iterative approach where the leading researcher developed an initial code book by coding one interview. Then the second researcher independently coded the same interview, and the discrepancies were compared, contextualized, and agreed upon. In total six interviews were coded separately by both researchers, where each iteration lead to fewer discrepancies. With the last transcription not yielding any discrepancies at all. Finally, the first researcher coded two more transcripts and removed the codes, leaving the quotations marked, and sent it to the second researcher. The second researcher then coded the same two transcripts to compute the *Inter Coder Agreement*, Krippendorff's alpha binary metric to assess the agreement between the two researchers Krippendorff (2011). This metric gives insights into the similarities in coding between two researchers. For the first two documents, we observed a score of 0.802. Then to ensure this high value was constant we performed the same process with removed codes on two more transcripts and found a value of 0.959. This means there is high inter-coder agreement and we can limit the bias introduced by potentially inconsistent application of codes.

Following the initial agreement, the first researcher took charge of coding the remaining transcripts. Subsequently, the second researcher carefully reviewed all the coded transcripts to ensure the consistent application of codes. During this process, a few minor discrepancies were identified. However, these issues were discussed and resolved without any major conflicts or disagreements. Moreover, the codebook was discussed together with a third researcher, both during development as well as after coding to ensure an incorrect frame of reference did not influence results significantly (Garcia and Quek, 1997).

[1] https://atlasti.com (23.2.1)

6.1.4 Mental Model Extraction

The purpose of these interviews is to extract the mental models of shadow IT from the participants. Since there is not a single question that makes participants illustrate their mental model, different participants may reveal their understanding of shadow IT at various points during the interviews. As we analyze the transcripts, we mark any quotes that offer insight into these mental models.

This process results in a collection of shadow IT mental models shared by participants throughout the discussions. From there, we group similar instances together, identifying the prevailing attitude within each mental model. In addition, we try to find the implications of certain mental models, grounding these with the examples provided.

6.1.5 Threats to Validity

We treat the same categories of validity threats as described in section 3.6. Construct validity threats can arise through interviewer bias. This is where the interviewer's expectations influence the responses of the participants by asking leading questions. We partially mitigate this by validating the interview questions through experts.

Internal validity threats arise from social desirability bias. Since questions regarding cybersecurity behavior are sensitive, participants may want to present themselves in a positive light and avoid judgment by giving socially desirable answers. Moreover, we find reactivity bias: participants might change their behavior or responses because they know they are being observed. This can occur if participants feel pressured to provide certain responses or if they want to conform to perceived expectations. Both social desirability bias and reactivity bias can not be fully mitigated, however, by making it possible for participants to participate anonymously and be able to leave at any time without being penalized should reduce the pressure and need for conformity.

Sampling bias can be introduced if the sample of participants is not representative of the studied group. This is mitigated through *cluster sampling* and *stratified random sampling*. We cluster based on department and within the clusters we take random samples but account for every rank.

We support the findings with literal quotes from participants. Therefore we 'ground' the statements directly from the data to minimize conclusion validity.

6.2 Interview steps

The thirty-two interviews all took between 20 and 35 minutes. As described in section 6.1.1, we tried to interview six participants per department, spread across ranks for the first round. In Table 6.1 we present the matrix of participants interviewed for the first round. Due to time and resources, we were unable to speak to more than two participants in the management staff. On that same note, we were not able to recruit any participants from the IT department.

	Junior	*Senior*	*Manager*	*Senior manager*	*Management*	**Total**
Client facing	2	2	1	1	-	6
Support	1	2	3	1	-	7
Management	-	-	-	-	2	2
IT	0	0	0	0	-	0
Total	3	4	4	2	2	**15**

TABLE 6.1: Participant cohort matrix for the first 15 interviews

As noted in section 5.6, we observed the most occurrences of shadow IT within the *client facing* group. After the initial interviews, we discussed the preliminary results informally amongst a group of researchers and concluded that for the final interviews, we focus on this *client facing* group. We decide this due to the fact that this is the participant group that allows for a deeper understanding of the *perspective* of the shadow-IT component that we need to further investigate. However, we keep trying to recruit participants from the *management* and *IT* groups for the second round of interviews to try and conduct six interviews per department.

During the interviews, we found that the drawing component together with the think-aloud component during the scenario caused confusion amongst the participants. We therefore continued the scenario, however, rather than drawing we focused solely on the think-aloud component.

	Junior	*Senior*	*Manager*	*Senior manager*	*Management*	**Total**
Client facing	6	4	5	6	-	21
Support	1	2	3	1	-	7
Management	-	-	-	-	4	4
IT	0	0	0	0	-	0
Total	7	6	8	7	4	**32**

TABLE 6.2: Participant cohort matrix for the final 32 interviews

We present the final participant cohort Table 6.2. Code saturation was reached after the twenty-second interview. Meaning we conducted ten more interviews, without finding any new codes. We therefore can already observe completeness in the findings due to this high saturation.

Unfortunately, we were not able to recruit any participants from the *IT* group during the second round of interviews. However, we did manage to interview two more participants in the *management* group. The detailed participant demographics can be found in Table 6.3. In this table we provide the *ID*, *Rank*, *Department*, *Highest degree*, *age group*, and *experience* (in years) of the participants. We provide the age groups similarly to the age groups of survey respondents.

6.3 Interview results

Similarly to the results of the survey, we report in-depth interview results and ground the results with quotes from participants. Recognizing the potential preference for a more concise

summary, the synthesized findings can be found in section 6.4. Readers wishing for a more succinct overview are advised to refer directly to that section.

We grouped the codes into five main groups and ordered them based on the order of the questions that provided the codes within these groups to resemble the interview structure. In total, we found 105 codes:

- **Context (15 codes)** - the context holds codes with regard to the type of work done by the participant. In addition, these codes also hold information about the device usage of a participant and codes that influence the *perspective* aspects of shadow IT
- **Shadow IT (67 codes)** - these codes contain information to any shadow-IT related question. This concerns the: *definition*, *occurrence*, *reasons*, *implications*, and *scenarios*.
- **Policy & Awareness (12 codes)** - this group illustrated codes about the awareness of relevant policies and the discussions about shadow-IT utilization. Moreover, this group holds codes with regard to how well-informed participants feel about the use of technology.
- **Contradictions (1 code)** - We labeled certain contradicting statements within the same interviews. These remarkable findings illustrate gaps in user understanding of several shadow IT aspects.
- **Mental Models (10 codes)** - These codes hold the shadow IT mental models found throughout the interviews.

ID	Rank	Department	Highest degree	Age group	Experience
P1	Junior	Client facing	Master's (University)	23-25	0-3
P2	Senior	Client facing	Postmaster	26-30	3-6
P3	Junior	Client facing	Master's degree (University)	23-25	0-3
P4	Junior	Support	Master's degree (University)	23-25	0-3
P5	Manager	Support	Applied sciences master (HBO)	51-59	30+
P6	Manager	Support	MBO	51-59	26-30
P7	Management	Management	Master's degree (University)	51-59	26-30
P8	Manager	Support	Master'sf degree (University)	36-40	16-20
P9	Senior Manager	Client facing	Post-master	41-50	16-20
P10	Manager	Client facing	Master's degree (University)	26-30	3-6
P11	Senior Manager	Support	Applied sciences master (HBO)	41-50	21-25
P12	Senior	Client facing	Master's degree (University)	26-30	3-6
P13	Senior	Support	Master's degree (University)	23-25	0-3
P14	Management	Management	Post-master	51-59	30+
P15	Senior	Support	PhD	41-50	16-20
P16	Manager	Client facing	Master's degree (University)	31-35	7-10
P17	Junior	Client facing	Master's degree (University)	26-30	3-6
P18	Junior	Client facing	Master's degree (University)	23-25	0-3
P19	Senior	Client facing	Master's degree (University)	26-30	0-3
P20	Senior	Client facing	Master's degree (University)	31-35	3-6
P21	Senior Manager	Client facing	Master's degree (University)	51-59	30+
P22	Manager	Client facing	Master's degree (University)	31-35	7-10
P23	Manager	Client facing	Applied sciences master (HBO)	41-50	21-25
P24	Manager	Client facing	Master's degree (University)	41-50	16-20
P25	Senior Manager	Client facing	Master's degree (University)	36-40	11-15
P26	Junior	Client facing	Master's degree (University)	26-30	0-3
P27	Junior	Client facing	Master's degree (University)	26-30	0-3
P28	Senior Manager	Client facing	Post-master	41-50	11-15
P29	Senior Manager	Client facing	Bachelor's degree (university)	60+	30+
P30	Management	Management	Post-master	51-59	16-20
P31	Management	Management	Post-master	41-50	26-30
P32	Senior Manager	Client facing	Applied sciences bachelor (HBO)	51-59	26-30

TABLE 6.3: Interview participant demographics

In the following section, we display the codes per group. Within the groups, we illustrate them by occurrence, which ATLAS.ti refers to as *groundedness*. However, we analyze the findings qualitatively, and therefore the numbers are not representative of scale. *Groundedness* can indeed offer a level of 'top-of-mindness' for a certain code, but we do not analyze the instances quantitatively. In addition to *groundedness*, we also note the *coverage*, which is the number of unique participants who stated a particular code. For instance, 'Code X (10/5)' was referred to ten times by five separate participants.

To support our findings, we illustrate direct quotes from the participants whenever applicable. These were translated by the researchers who speak both Dutch and English fluently. However, not all direct quotes could be used due to a lack of permission from the interviewees. The transcription was partially automated, resulting in several punctuation mistakes in the transcripts. We rectified these in the translations to enhance readability. We anonymized any application, name, team, or organization. We replace them with labels like [application type], [team name], [name], or [organization], also including their functionality when relevant. This was done as an extra anonymization step, given that a certain name is not needed to understand the context of the statement and to keep the transcripts as anonymous as possible. The complete codebook with all descriptions of codes can be found in appendix H.

6.3.1 Context

Please state your rank, team, education, and years of professional work experience. What is the nature of your work? Do you do work in engagements? If so, how many engagements have you done? What kind of work do you do?

In this section, we find the codes used for the context: work type and codes for the use of physical devices. Finally, we find codes that relate to statements about the shadow IT *perspective* of employees. We illustrate this in figure 6.1.

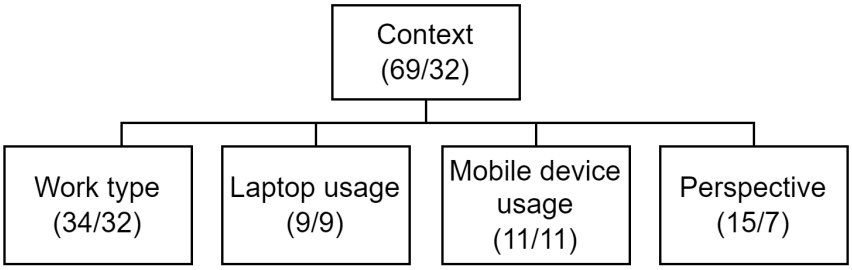

FIGURE 6.1: Context components with groundedness and cover metrics

6.3.1.1 Work type

We observed the following work types across the participants: **Client-based**, **Internal**, and **Project-based**, and we present the occurrences in Figure 6.2. Participants that do client-based work perform the same tasks for different clients. Whereas the participants

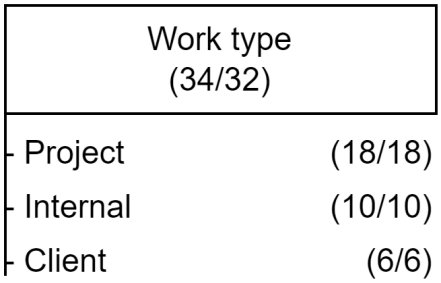

FIGURE 6.2: Occurrence of Work types

that work project-based work on a project basis. Each participant in the *support* group did internal work. This work type implies that the participant's job responsibilities do not directly generate revenue but are instead focused on sustaining the organization. For both client and project-based work, we find literal quotes in the text. However, the internal label was provided if the participants did not mention any project or client-related work. Therefore, we do not provide quotes to support this code.

We observe that there are 34 codes for 32 participants. This is due to some participants in the *management* group. We found that participants in this group did work in all three work types. Meaning that there is a variety of responsibilities within this group, and some participants had their responsibilities split between multiple work types. While some of the participants in this group are responsible for the delivery of projects, some are responsible for the handling of dedicated clients and others are responsible for managing the organization internally.

"[...] I also did a few projects abroad before that. Now I only do about 20% on projects, this was 50-50 before, but now I do that 20% and 80% [internal activity]." [P7]

"[...] because I do not do as much actual work anymore, I am mostly responsible for managing the final project [...]" [P30]

We observed a split in the work type of participants within the *client-facing* group. We found that some participants were dedicated to certain clients, and managed (parts of) a client portfolio. Whereas other participants within this group work project-based.

"I have a set amount of dedicated clients. About five or six. You might think that is not a lot. Yet every month they have certain questions, for those questions see seek an expert, someone who knows their company." [P29]

"[...] some projects are finished within a month. Right now I am working on a large [project type] for already 10 months now. It varies a lot. " [P14]

This split in the *client-facing* group has a significant impact on shadow-IT utilization. As previously stated, participants that work client-based perform the same tasks for different clients. This implies that work-related tasks and therefore the technical solutions do not change. Whereas the participants that work project-based, potentially need to solve a different problem for each new project, where new technical solutions might be needed. This significantly increases the potential for shadow IT for the participants working project-based.

While analyzing the survey data, we came across a pattern regarding the usage of specific applications among different ranks. This observation led us to consider the possibility that lower-ranked individuals are more actively engaged in performing the actual work, while those in higher ranks are comparatively less involved in hands-on tasks. Two participants from the *manager* group provided helpful insights during the interviews with regard to this topic:

"My work changed through the years. You see an increased number of types of applications with people who are more hands-on. The further you progress in your career, the less you encounter those applications so now I mainly just use [application] [...]" [P22]

"Compared to more junior staff, as a manager you have less of an IT footprint" [P24]

6.3.1.2 Laptop usage

With regard to the use of hardware that creates a potential source for shadow IT. We observe if participants have separate hardware to do personal tasks. We present the occurrences in Figure 6.3. We find that certain participants use **Combined laptop**, meaning that they must perform all their tasks on their work laptop, whereas others explicitly mention **Separate laptops**. Even though there are only a few occurrences of the combined laptop. We find all of these instances reported by a participant in the 41-50 age group or older.

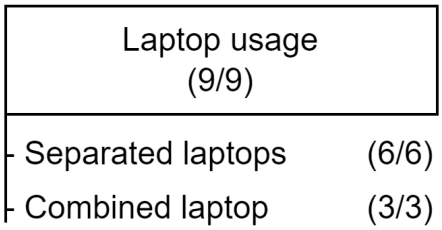

FIGURE 6.3: Occurrence of Laptop usage

"Well, not on a private laptop, because I do not have one, I do have a private email address. But not a laptop." [P6]

We also find a clear distinction between devices. Where participants clearly illustrate their awareness with regard to cybersecurity risks, and the potential implications their actions have if they would perform these on their work laptops.

"[...] On my personal laptop, I'll install it right away and we'll see where we end up. But never on my work laptop [...]" - [P19]

6.3.1.3 Mobile device usage

The occurrence of shadow IT in mobile devices is likely to increase, just as it does with laptops when employees use the organization-provided device for both personal and work purposes. We observe two codes in this category: **Combined mobile device** and **Separate mobile devices**, presented in Figure 6.4. Just like with laptops, we observe that older participants are more likely to have a single mobile device.

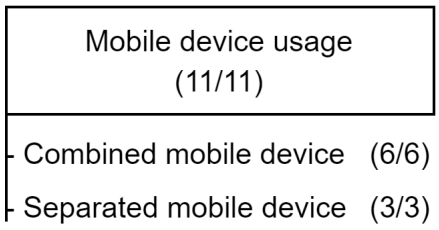

FIGURE 6.4: Occurrence of Mobile device usage

"I just have one cell phone [...] Your generation, you all have a cell phone before you start working and so you have two. People my age did not have a cell phone when they started working, so I got my first one from my work." [P21]

The introduction of work-related communication on a mobile device is well-received by some participants, while others greatly value the clear separation between work and personal matters: *"So I use two separate phones for two main reasons: one to just keep work and personal stuff separate. And with that comes that I only have to install work-related apps on my work device" [P1]*

On the other hand, there are those who prefer the combination of both, allowing them to quickly address any minor issues that come up: *"[...] so I have one phone for work and personal use, that kind of blurs the line between the two [...] However as [role] I like to be available at all times. If something small comes up I'd rather deal with it straight away and get it fixed." [P13]*

6.3.1.4 Perspective

The *perspective* of shadow IT refers to the shift in shadow-IT perspective when an individual engages in a client project and, as a result, operates on a client-provided laptop or online workspace. This shift of perspective puts all applications installed on the client's machine outside the professional services company's scope, altering the employee's shadow IT perspective. This concept is therefore linked to the *client facing* group. We find the means to shift perspective through: **Client laptop devices**, **Remote workspaces**, and **Client licenses**. We present these in Figure 6.5.

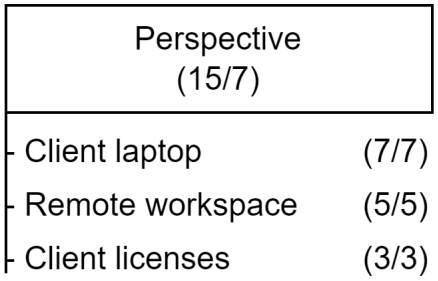

FIGURE 6.5: Occurrence of *Perspective*

We illustrate one example by a participant that describes the phenomenon of *perspective* and describes all three aspects:

"So that would mean we would need an environment at the client. This can be a client laptop, or client environment through [remote workspace]. Both with the tools installed, so that the client pays for licenses, and puts the responsibility for updating at the client. Moreso to put the risk of these applications in their shoes" [P22]

We observe that participants that do longer projects for a single client often get a physical device in the form of a **Client laptop**. They need to do a mini-on-boarding process to install all relevant software, but in doing so they mitigate any shadow IT threats for their own organization:

"So then we need to be on-boarded, this means you get a laptop from the client, and then you need to go through the system on their side" [P19]

"Sometimes we work on laptops provided by the client. And then the rulebook changes because it is theirs, so then you have a lot of contact with the client's IT team" [P17]

Remote workspaces are deployed for the same principle: designing a dedicated place for individuals to work in, have access to data and have access to certain applications. The separation of systems is less than with a separate physical device but still gives a closed environment for

employees doing work tasks: *"So then often it is [remote workspace]. So that within this environment you work for the client, and also sometimes in the [remote workspace] of the client" [P12]*

We observe the **Client licenses** as the least separated option to distinguish the *perspective*. Clients share the licenses of different applications to work in a controlled-application environment: *"The client uses a certain application, we will copy that and just work from their accounts in those systems" [P10]*

6.3.2 Shadow IT

This group of codes provides information on the core aspects of this research. We focus on the definition, occurrence, reasons, implications, and thought processes of shadow IT. We analyze each in a sequential manner in the following sections, and if present, identify any patterns with regard that the cohort of the participants. We present the components of shadow IT, with groundedness and coverage in Figure 6.6.

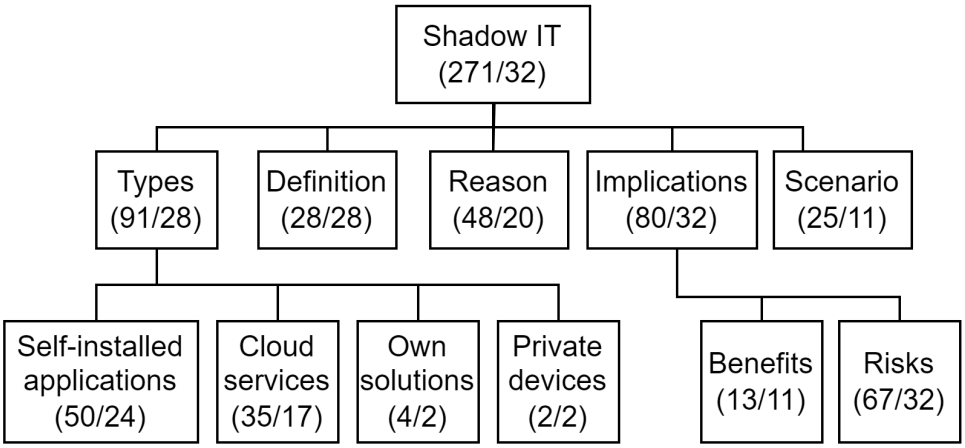

FIGURE 6.6: Shadow IT components with groundedness and cover metrics

6.3.2.1 Definition of shadow IT

What is Shadow IT for you?

We asked participants what shadow IT meant for them. This research sets to set out if employees understand the concept of shadow IT. A participant can understand and act upon the concept, without knowing the exact definition. However, to get an indication of how well-known this definition is, we classified the responses as binary: **Familiar** and **Unfamiliar** with regards to the concept of shadow IT. We illustrate these in Figure 6.7. Later in this research, we will address how well-known the concept of shadow IT is across participants. This section focuses on the definition. Notably, all participants that are familiar with shadow IT are in the

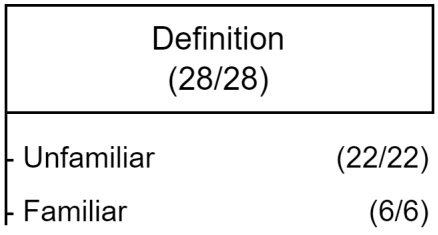

FIGURE 6.7: Occurrence of shadow IT definition

client facing group, present throughout all ranks. Moreover, the participants that were familiar with shadow IT almost all gave a near-perfect definition.

"For me shadow IT is anything that is IT: applications, services, platforms that you use that are not approved by your organization. Even if they are okay for one organization does not mean they are okay for your organization. And as long as that is not the case, it will remain shadow IT" [P22]

6.3.2.2 Occurrence of shadow IT

Have you ever used any shadow IT instances?

We asked participants, similar to the survey, if they ever used any shadow IT instances. We categorize the found instances according to the same split used in the survey, based on the topology of Mallmann et al. (2018).

6.3.2.2.1 Unapproved cloud-services

When coding the cloud services, we started with similar codes with regard to the survey. Namely *browser tools*, *browser extensions*, and *cloud storage services*. After the instances were labeled, we identified more specific categories of cloud services if these patterns emerged and we found the following categories of unapproved cloud services: **Browser extensions**, **Cloud storage services**, **Generative LLM tools**, **Online collaboration tools** and **Translate tools**. We illustrate the occurrences in Figure 6.8.

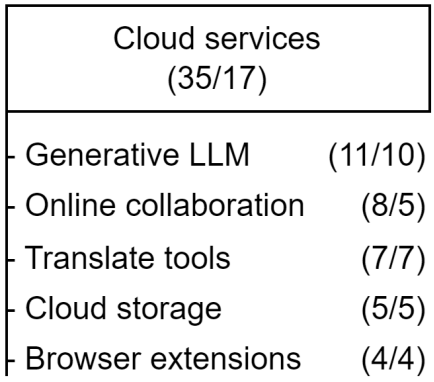

FIGURE 6.8: Occurrence of unapproved cloud services

The most used tool within these cloud services is the **Generative LLM tools**. These web-based applications allow for a quick study of certain specific concepts: *"[...] I hear it is used quite often, just to quickly find out some information. Sometimes even entire problems are entered to see if the general line of thinking is in the right direction." [P20]*

Moreover, such advanced applications can account for context understanding when trying to solve complex problems: *"[...] I now switched to [LLM tool] [...] instead of reading someone else's problem and solution, you can now get a solution made for your specific problem." [P23]*

The second most named cloud service tool is a **Translation tool**. In a work environment where the participant's first language is not necessarily the spoken language at work, translation tools are often used to double-check for errors or increase the formality of written communication: *"I sometimes use [translation tool] [...] this tool allows me to write more professionally [...] [P13]"*

The following tool we observe are **Online collaboration tools**. These tools are not just used to communicate, but also to share any relevant documents. We find these tools throughout

ranks and departments: *"[...] So we use these applications for exchanging documents, and also for collaborating [...]" [P12]*

We observe a number of **Browser extensions**. These are mostly used for niche functionalities: *"[...] I could not listen to music anymore, so I installed an ad-blocker extension so I could listen to music on [streaming platform]." [P2].* Similarly to the translation tools, we find extensions that aid in improving written language on work-related matters: *"I use an extension called [spelling checker], which does automatic spelling check so I do not have to double check my emails." [P27]*

The final observed occurrence of unapproved cloud services is the **Cloud storage tools**. We observe the occurrences not for long-term storage of files. But rather a medium to transfer large files: *"I think [cloud storage service] is used a lot. Since we can only e-mail files up to 25MB. So if you have larger files think gets complicated. That is why sometimes you need to use something different." [P24].* However, some participants use another cloud storage service for all their files: *"Well, because I use [cloud storage service] for everything basically" [P2]*

6.3.2.2.2 Self-installed applications

We did not set any codes before coding the self-installed applications. This was one of the limitations of this type of shadow IT during the survey, where we found a lot of different types of applications in the *other* section. We find fifteen different types of self-installed applications in the interviews and sort them by occurrence in Figure 6.9.

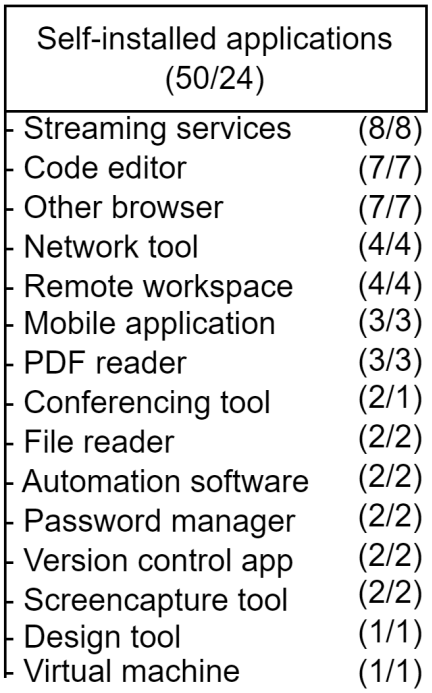

FIGURE 6.9: Occurrence of self-installed applications

We observe several **Code editors** throughout the *support* and *client facing* groups and mostly in the lower ranks. We find that this type of self-installed application can be crucial for some participants:

"[Code editor] is not a standard [organization] application. However, it is very important for us to be able to do our data modification [...] [P5]"

"That is where we write our scripts in, and we also edit those in [code editor]. [...] we use that application a lot." [P23]

Non-standard browsers occur throughout the *support* group and *client facing* group, mainly in the higher ranks: *"We use [standard browser] and also [non-standard browser] since not all applications run smoothly on [standard browser]. So we need the other one as well. [P5]"*

"I use multiple browsers. Officially you can get [browser] through the internal app store, but if you download it through there it does not work [...] I need those browsers to test if applications work cross-browser as well" [P16]

Streaming services are applications that are mostly used by participants personally. However, we specifically asked the participants to name the applications used for or during work purposes. We find the streaming services mostly in the *junior* rank throughout departments. Moreover, we observe that certain participants are very keen on using these services for their work tasks: *"Then I downloaded [streaming service]. At some point in time, this did not work anymore, but you could use a proxy to still be able to use it" [P2]*

We find occurrences of **Remote workspaces** only in the *client facing* group. As discussed in section 6.3.1.4, these applications are used to access client environments. Therefore we observe that these applications are not top-of-mind when thinking about shadow IT instances: *"Only just now I realized we also use [remote workspace] [...] [P10]"*

Network tools are used to connect to FTP servers or monitor some network activity. These occurrences are found in the *manager* ranks, in the *client facing* and *support* groups and are used for niche use cases:

"We use [networking tool] a lot, this an FTP-application. We use this FTP because of security restrictions within [organization] it is hard to transfer files [P5]"

"I downloaded [network tool] for some research I was doing, that is a network-diagnostics tool, a hacker tool of some sorts [...]" [P23]

We observe **Non-standard PDF readers** with more functionality than the standard tool which is used a lot by participants: *"It is a sort of program that allows you to open PDFs. But in addition, you can also edit them and verify certificates. So we use this a lot [...] [P18]"*. We find these tools only in the *client facing* group, throughout all ranks.

We observe **Mobile applications** in the *client facing* and *support* groups, throughout ranks. We found that some participants explicitly named and understood the significance of the implications of mobile applications: *"[...] I think that in discussing risks, our mobile phones might be a bigger risk since people are more inclined to download certain apps on their mobile phone that are unsafe." [P8]*

Non-standard **Conferencing tool** are observed only a few times. Solely in the *client facing* group in the *senior* rank. However, we observe them for multiple purposes. Namely, to communicate with clients in their preferred tool: *"Sometimes we use [external conferencing tool] rather than [standard conferencing tool] when it is the client's preferred tool." [P12]*

However, we also see this for internal communication within teams: *"Yes, within our own team within [organization], we use [non-standard conferencing tool] daily to communicate." [P12]* This observation is rather intriguing, as there are clearly defined standards for internal communication within teams. When the participant was prompted with a follow-up question as to why this alternative platform was used, the response was that it had been used for such a long time and it was just part of their standard workflow: *"[...] I don't know, I think sometime a while ago it was introduced and it has stayed up until now [...] over time it has grown to what it is now for us." [P12]*

Automation software can be used for all sorts of tasks. We observe the use of this tool in the *client facing* and *support* groups for the automation of manual tasks: *"[...] we also use [automation tool] [...] That is a program that allows you to make some sort of bot. Therefore tasks that had to be done manually before can now be done by the bot [...] [P5]"*

We encounter **File readers** only in the *support* group. We observe them for specific nice applications: *"[...] I also use another tool: [file reader], which allows me to read log files. When longer scripts are running, they generate lots of log files. This allows me to read the most recent log files in a convenient way. [P15]"*

Using external **Password managers** intuitively feels sensitive since the wrong handling of passwords can have significant consequences. Similar to the file readers, we find the password managers only in the *support* group. We observe that the use of these tools is adopted throughout certain teams: *"I think that this [password manager] also is an application that we started using at some point, even though this application is not facilitated by [organization] [P23]"*

Staying on that same note we encounter the **Version control** tools also only present in the *support* group: *"We also use a system for version control [...] Let me start the application, ah yes the name is [version control tool]. [P15]"*

We find external **Screencapture tools** in the *management* and *client facing* group, throughout ranks: *"But we also use tools like [screencapture tool] [...] [P14]"*

The final self-installed applications participants gave were a **Design tool**: *"With that, I only can think of a sort of design tool, I used it because I had to build something real quick" [P25]* and a **Virtual machine**: *"[...] So that was specific to do server-sided. Next to that we also used virtual machines to run this in [...]" [P16]*. These types of applications were mentioned only by a single participant.

6.3.2.2.3 Self-made solutions

We find few occurrences of self-made solutions throughout the interviews. This aligns with the survey findings. We present these in Figure 6.10. We observe **External spreadsheets**, in the *junior* and *client facing* group: *"I created an Excel sheet once to keep track of my progress of different tasks." [P1]*

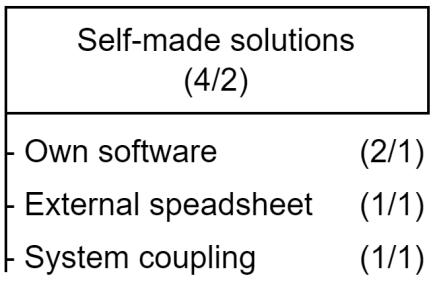

FIGURE 6.10: Occurrence of self-made solutions

In addition, we found **Own software** in the *manager* rank and *client facing* department: *"I built a tool to transfer my mobile phone contacts from one phone to another, back then it was not so easy to transfer them, so I just wrote a script to do that" [P22].*

Finally, we observe ad-hoc **System coupling**, also in the *manager* and *client facing group*: *"I know people who connected the lease car-pool to a notification tool. They then created the notification tool themselves, so every time a new car was available to the pool they got a notification instantly [...]" [P22]*

6.3.2.2.4 Private devices

From the occurrences of different shadow IT types, we only observe two instances both in the *manager* rank and the *client facing* department, as presented in Figure 6.11. We encounter **Personal laptops**: *"Sometimes you need to do a task on your personal laptop because you simply can not do it on your work laptop. You just need the tool. So then you'll send it back and forth and get it done. [P20]"*

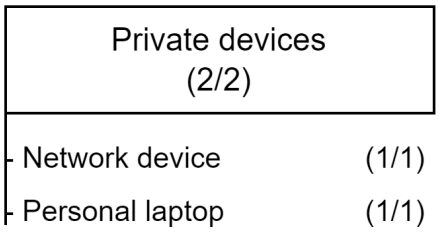

FIGURE 6.11: Occurrence of private devices

In addition, we find **Network devices**. The introduction of this type of private hardware was used in a niche project that needed specific tools: *"Well when we gave a [type of workshop] workshop for a client, we needed to use a router, rubber ducky, etc. [...]" [P22]*

6.3.2.3 Reasons for shadow IT

Why have you used these shadow IT instances?

The main rationale for the interviews is to uncover the reasons for the use of shadow IT instances. We prompted each participant for the reasons for the use of the shadow IT instance right after they expressed that they used one. Between the found reasons we find some nuances and overlap. For instance, *Insufficient standard* is a more specific version of *Need for specific functionality* since a participant seeks a certain functionality, that apparently is covered insufficiently in the provided solution. If this is the case, we label the most specific code to that instance. We present the following reasons for the use of shadow IT in Figure 6.12.

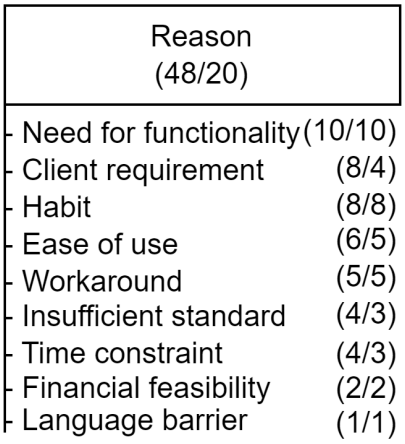

FIGURE 6.12: Occurrence of reasons for using shadow IT

We discuss these reasons for the use of shadow IT in the current section and try to identify patterns across cohorts.

We observe a **Need for specific functionality** the most. This reason implies that an employee uses an external tool because the tools provided by the organization do not cover all the tasks that employees need to perform. We find this reason across ranks and departments.

"Well, it is often for work-related matters, that there is no such thing within the current tools [...]" [P3].

"Well, all most always because we do not have the options within [organization] infrastructure. So we just want the functionality, just the tool [...]" [P24] We prompted some of the participants with

a follow-up question as to why they did not go through the official channels to get to a solution. We discovered that certain participants were unsure about the appropriate individuals to contact in order to find a solution. Furthermore, we noticed that when attempting to do so, there is a possibility that the official channels lack a tool that aligns with their specific request. As a result, receiving a definitive "no" leaves them unable to proceed with the engagement. This possible outcome of not being able to continue impacts the participant's decision to not go through the proper channels:

"I don't even know who IT is and with that comes the risk that you might receive a "no" to your request. Meaning you cannot do the engagement, while you do need the functionality. So by approaching IT you enter a negotiation you need to win [...]" [P22]

Moreover, another participant noted that the process is both complicated and takes a lot of time. Again influencing the decision to not go through the proper channels:

"If you really want to do it the right way, you approach the IT department to ask what is allowed and what is not. However, I see this as a complicated process, which takes a lot of time" [P10]

We observe **Client requirements** as an important reason for the use of shadow IT applications. This is a code that was applied if the participant had to use a certain shadow IT application because of a client project.

We observe the instances for *client requirements* only in the *client facing* group, within the *senior* and *manager* ranks: *"For a project, I had to install [program] to get access to the [organization tool]" [P16]*

Moreover, we find out that whenever participants install something, the system asks for the reason for installing it. This ensures employees make conscious decisions as to why they install certain applications:

"Yes, I have always used them for client projects. I have never installed anything that I did not need for a client project [...] Whenever we have to install something from an unknown source the system wants you to enter a reason why you are installing this application. For me, the reason is always to support a client project" [P22]

We observe that the adoption of external tools is driven because of their **Ease of use**. This reason is found across ranks and departments. We notice that participants do not speak about this reason extensively. When this reason was mentioned, participants made it seem evident that it was: *"no big deal"[P3].*

"[...] and the other thing it, these tools allow me to do it quick and easy." [P3]

"Well quite simply because these tools can be used very easily [...]" [P11]

The next reason we encountered for the use of shadow IT is **Habit**. We observe this phenomenon in individual adaptations:

"[...] And now I have worked with it for years, so then it also becomes a habit and I'm happy with it. That is also why I do not want to try anything new" [P 5]

"I mean my [application type]. I never heard if that is allowed or not, I just use what I am familiar with" [P22]

We also find the adoption of tools across entire teams due to habit. This is especially significant since this implies the unregulated use of technology is structurally integrated within a regulated workflow. This creates governance gaps and potential threats. We note that the teams that structurally incorporate shadow IT in their workflow belong to the *support* and *client facing* groups. We find the instances across all ranks due to the team-wide adoption of this tool:

"We have used these tools for years, we are used to it now and if we were to switch tools it will be a hassle and a lot of trouble to switch [...]" [P15]

"[...] I don't know, I think sometime a while ago it was introduced and it has stayed up until now [...] over time it has grown to what it is now for us." [P12]

We encounter **Time constraint** as a reason for using shadow IT only in the *client facing* group.

We previously found that a reason for not going through the proper channels when needing to adopt shadow IT, was that a "no" by the IT department could lead you unable to proceed with the project. Then through further prompting the participants with why receiving a "no" is of such tremendous impact. Such impact that they risk not following the proper protocols in order to ensure safe data handling. We note an important finding that significantly applies to the *client facing* group. We note that there is a certain work pressure to get the work finished. This provides context as to the pressure and stress that employees may be facing:

"I think the main issue with that is that the show must go on [...] [P20]".

"Some licenses are not provided by [organization] and the work pressure is high so you make it as easy as possible for yourself" [P27]

Moreover, we find time pressure on the participants to meet deadlines:

"I can not explain to a client that certain tasks have not been completed. This means that sometimes employees enter a grey area, perhaps even cross it by doing this they shouldn't. I think everyone is aware of this [...]" [P20]

The following reason we find is **Insufficient standard** tooling, meaning that the current solution provided by the organization does not fulfill all needs of the employees, and hence they seek some other tooling externally. Those needs might differ per participant: some might need specific functionality but have mentioned this is due to the lack of that functionality in the provided system, while others might have a personal distaste for a provided application. We applied this code when a participant specifically mentioned some flaw in the provided solution. These instances are mostly found in the *client facing* group across ranks. In the following example, we observe the use of a non-standard system because the usability of the provided system is subpar. This led to the team-wide adoption of a tool, that since then has grown into a habit for the team:

"[...] we use the system for [tasks] because we do not like the system provided by [organization]. I believe they already adopted this before I started working here, so it has been going on for a while" [P12]

We also observe individual adaptation of external tools due to insufficiently provided tooling:

"We use [standard browser] and also [non-standard browser] since not all applications run smoothly on [standard browser]. So we need the other one as well." [P5]

We find instances of **Financial feasibility** only within the *support* group. Both instances explicitly note that the financial implications of tools are considered when selecting tools. Moreover, one participant notes that there is no budget they can use for tools and thus need to select tooling based on costs.

"Well quite simply because these tools are free [...] since we do not have a credit card we sort of depend on free tooling"[P11]

"I must say that if [organization] needs to pay for all the little things, that will be quite an investment. So it is very nice that there are alternatives" [P13]

In one specific instance, we observe **Language barrier** as the reason for using shadow IT. This label was applied because the participant explicitly stated to need an external translation tool in order to conduct work tasks. This was due to the participant not being able to speak the common language of the organization, and was therefore reliant on this tool:

"Sometimes even using [translation tool] I'm extra careful. Should I put this to be translated or not? But then I cannot function without the translate, so I have no option but to use it." [P9]

In the initial list of codes for the reasons for shadow IT we mention **Workarounds**. While coding we found that a workaround is not an actual reason for using shadow IT: meaning that participants do not use shadow IT just to find unauthorized paths to external solutions. We observe that the workaround is rather employed to get access to the shadow IT applications. The complexity of a workaround provides information as to how much participants are willing to circumvent security measures and value the use of external tools.

"[...] So we just want the functionality, just the tool. If a website is blocked, but you need to access it, or you do want to send that email you grab your phone, where it is not blocked, or you use another device or browser. If they really need it people will find a way" [P24]

"Sometimes you need to do a task on your personal laptop because you simply can not do it on your work laptop. You just need the tool. So then you'll send it back and forth and get it done." [P20]

We find the workaround as a means to get some tasks finished in both examples above. All but one occurrence of a workaround then also comes from the *client facing* group, specifically the *senior* and *manager* ranks. We observe a single instance in the *support* group. Similarly to the habit reason in this group, we find that this workaround is adopted throughout the entire team:

"We use [networking tool] a lot, this an FTP-application. We use this FTP because of security restrictions within [organization] it is hard to transfer files" [P5]

We discuss the implications of team-wide adoption of shadow IT instances and workarounds in section 6.3.3 since this phenomenon significantly impacts the awareness of individuals.

6.3.2.4 Implications of shadow IT

What do you think are the risks and implications of shadow IT?

Part of constructing the mental model of shadow IT is based upon the understanding of the implications that participants think shadow IT brings. After we asked the participants if and why they had ever used shadow IT, we then asked them to think about any risks or problems that could arise from using shadow IT. By contextualizing the perceived consequences of shadow IT, we can observe the relation between what a participant knows and how they act upon this knowledge. We found two main categories of answers: **Benefits** and **Risks**. We illustrate these in the following section, sorted on occurrence.

6.3.2.4.1 Benefits

We provide an overview of the found perceived benefits in Figure 6.13. The perceived benefit we encounter the most is **Efficiency**. Participants note that certain tools allow them to work more efficiently. Therefore it is no surprise we find most of these instances in the *client facing* group. We previously observed the potential time pressure that these participants might experience. A partial solution for this is doing certain work-related tasks more efficiently, hence saving time:

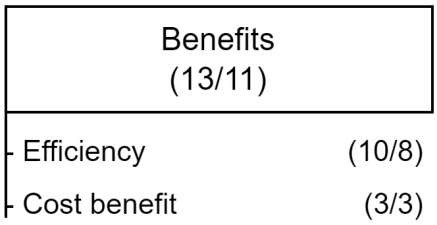

FIGURE 6.13: Occurrence of perceived benefits of shadow IT

"Well.. [tool] is convenient since I have to do a lot of [working task] and therefore have to do a lot of writing. So my increase in efficiency is evident here" [P27]

"[Tool] can be used for a variety of things. For example yesterday I had to do [working task], I then used that tool and it just saves me so much time" [P27]

We find **Cost benefit** as a positive result of the use of external tools. Notably, we observe this from the same participants in the *support* that named the financial feasibility as a reason to use shadow IT instances, and one more instance in the *client facing* group:

"[...] as well as the costs for the organization. I mean, if everyone went to IT for every small thing, that would not work [...]" [P16]

6.3.2.4.2 Risks

The majority of the responses with regard to implications were negative consequences of the use of external tools. Through observing the risks, we find how participants observe potential outcomes of their actions with regard to using shadow IT and provide insights into the participants' mental models. We present the found risks and we sort these on occurrence in Figure 6.14.

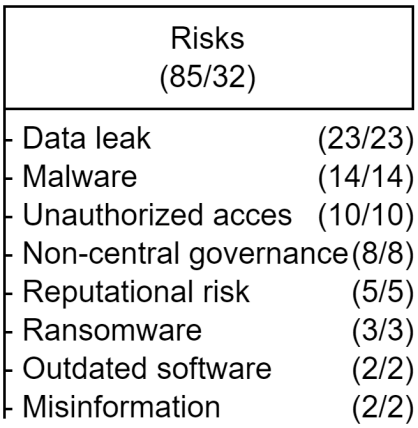

FIGURE 6.14: Occurrence of perceived risks of shadow IT

We most encountered perceived risk is a **Data leak**. Even though we do not quantitatively analyze the results, we can see through the occurrence overall that this risk is very top of mind. Moreover, this risk is perceived both across all ranks and departments. Some participants actively describe the term "data leak":

"I think the main risk obviously concerns data leaks" [P13]

"For me, my biggest concern is and always will be data breaches. So this is when we consciously send our data somewhere we cannot oversee the risks anymore" [P30]

Other participants described the concept rather than explicitly naming them:

"In general it is quite hard to find out who is behind the tool and what exactly they do to your data [...]" [P25]

Collectively we observe a very high awareness of data consciousness. We find this risk often as the first risk that participants mention, and we find it at the center compared to other risks. For instance, we find **Malware** instances as a predecessor of data leaks. The only specific type of malware that was mentioned is a virus. However, some participants described infected or malicious programs. We collectively labeled these instances as malware. We often find malware as a risk that could lead to a data leak:

"I suppose it could lead to viruses [...] This can then lead to the access of certain data on your laptop" [P23]

Similarly to the data leaks, we find instances of malware through departments and ranks. We also find a similar distinction between participants who named the term and participants who described the concept:

"When you download software that could just be malware, this can infiltrate your computer. This opens up the [organization] network and then anything can happen with regard to data" [P3]

Furthermore, we also observe some participants naming a virus, whereas others note it as an insecure or infected program:

"[...] I heard that at some point someone downloaded something which lead to all kinds of data being stolen. All due to the download of an insecure application." [P20]

We encounter **Unauthorized access** in a similar way as malware: namely as a predecessor of a data leak. We find that some participants explicitly state a threat actor like a "hacker", while others refrain from this and focus on the unauthorized access by some entity. We do not observe any occurrence patterns in the cohorts of the participants that mention this risk.

"I think the most important danger is giving access to others. Access that allows them to access data that they shouldn't" [P10]

"Hackers can get access to our system and then they can access sensitive data from clients. They can then exploit this data." [P15]

Non-central governance concerns the principle at the core of the potential threats related to shadow IT, even preceding the malware and unauthorized access. Namely, shadow IT instances fall outside of the scope of the organization, and therefore the organization can not perform standardized cybersecurity checks on these instances. The observed instances all fall within the *client facing* group and this group seems to be aware of this principle:

"What if you were to download something that is monitored by your employer, you could always get an alert or notification that says hey something is wrong here. So if you go outside of the employer, you bypass all checks and expose yourself to vulnerabilities" [P1]

"The disadvantage is always that if it is not checked by [organization], even if there might be very evident risks, they will not be aware of this" [P19]

The following observed risk is rather a consequence than a predecessor, namely, **Reputation risk**. We observe occurrence through all departments and ranks, but it has been explicitly mentioned as the biggest risk in the *management* group:

"The biggest risk of all is the reputation damage for [organization] due to data breaches. Since all the work we do is confidential, and sometimes even holds price-sensitive information" [P14]

Naturally, individuals in *management* ranks within an organization tend to prioritize the organization's reputation. However, to contextualize this observation, we notice that even among the more junior ranks, there is a significant level of awareness regarding reputation. This implies there is significant reputational awareness throughout the organization.

"So if we do something that makes [organization] untrustworthy, this can impact the name and therefore everyone in the organization" [P4]

We observe a few instances of **Ransomware** as a perceived risk of shadow IT. Similar to reputation damage, this is an instance that follows as a result of unauthorized access, or malware infection. We encounter these instances across ranks and departments, where some participants name the term and others describe the phenomenon:

"[...] you might expect anything from ransomware to other forms of cyber attacks" [P1]

"Hackers can enter our system and then blackmail us. They then have the power to block our systems so we can not access any files, then they make us pay a high fee to get rid of the blockade" [P15]

A shadow IT risk that strongly relates to non-central governance is **Outdated software**. This instance is named in both *client facing* and *support* departments in the *manager* rank.

"These applications should be known and kept up-to-date. Since if they are not up-to-date they can lead to vulnerabilities. So then it becomes a potential attack factor for criminals" [P16]

The last perceived risk of shadow IT instances is **Misinformation**. Notably, this is a risk that was named in combination with the generative Large Language Models (LLM) instances from section 6.3.2.2.1. These tools provide a new dimension in contextualized search, however, the validity of the answers is a risk that participants perceived:

"[...] if you just copy the answers as they come out and if you do not use your common sense anymore, naively thinking that the answer is always true, that is a big risk." [P11]

6.3.2.5 Thought process for introducing shadow IT

What is the process of using non-standard solutions?

We prompted participants from the *client facing* staff with a hypothetical situation and asked what the processes were for tackling this situation. We prompted them with the following statement:

Explain the process, step by step, how you would tackle the following situation: the client has asked you to work towards goal X, to do this you need an application that you do not have at the moment, how do you address this?

This step-by-step process provides information and context on how these participants view the position of external tools in their IT landscape, and how these issues are tackled in their organization. We observe two types of responses, internal and external. Where internal are steps taken by the individual. Whereas external refers to actions where individuals reach out to other entities to gain information as to what to do. We encounter the following process steps, sorted on occurrence in Figure 6.15.

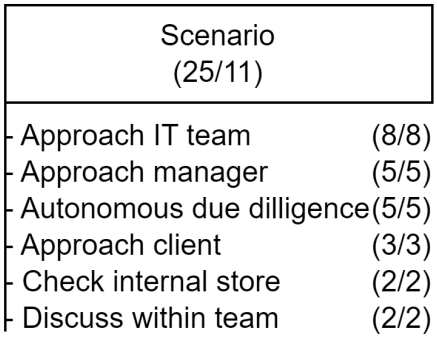

FIGURE 6.15: Occurrence of process steps in client scenario

In the ideal world, all employees should **Approach IT** before engaging in using external tools. Participants note that going to IT might take a lot of time, this can be complicated, and you could get a "no" response as illustrated in section 6.3.2.3. However, we observe that seeking advice from IT is the most occurring step taken and observe the instances for approaching IT mostly in the *junior* rank:

"Well, applications are managed by a central authority in global [organization]. So if we want something new we need to put the application through the governance processes for being accepted at [organization]." [P26]

We find **Approach higher up** as an additional process step in this situation. That is named frequently after inquiring the IT team. This step involves conferring this situation with another individual that has a higher rank or carries a certain responsibility. Similarly to approaching IT, we find that most instances of approaching higher up are in the *junior* rank. Moreover, we observe a high cybersecurity awareness amongst the participants when prompted with such a specific scenario:

"Often IT knows what is allowed and what is not. And if they do not have an answer I'll go back to the manager. So I would never just install something, because I know we're screwed" [P17]

"You will speak with [higher up], explain the problem and give your findings. There are certain tools out there, however, we cannot offer them right away. So how will we tackle this? I think you can not make those decisions on your own. Especially not if the solution is a central point in solving a client problem." [P27]

Autonomous due diligence refers to participants internally validating if a certain tool can be deemed trustworthy or appropriate. This implies getting information about this tool online and through previous experiences and then combining this information into a personal assessment if the tool can be used or not. We encounter the instances in the *manager* group. Moreover, we observe that if participants have to make a trade-off between doing the assessment themselves to save time, or approaching IT and letting IT follow standard protocols for this, participants are inclined to do the assessment themselves:

"I think I would just start searching myself. Usually, you do not have the time to perform all checks yourself, but I will not go to another entity for this within [organization]" [P10]

"Well if we need something externally. So on the one hand we look at the producer of the software and the maturity of that organization. At least for how well one can assess this from the outside. If it is a shady organization it becomes a no-go quite quickly. But if it is a large reputable organization then we can have a bit more trust." [P16]

The last of the stakeholders that we perceive as an entity to approach for participants is through a **Client approach**. We observe this step as a final resort when both the internal IT team do not have a solution and any more experienced colleagues also can not provide an answer. To go back to the client to try and let them take the responsibility for finding an external program. This step concerns shifting the *perspective* of the shadow IT instance. If the client organization takes responsibility for checking and monitoring an application, the liability and shadow IT risks are mitigated by the participant's organization. We find a great example of this by a participant in the *manager* rank, who illustrates this step would not have occurred when he was a *junior*:

"I would try and let the client take responsibility for the risk. Because they are the ones asking for this tool. However I would not have thought of that when I was younger, but I know now" [P22]

"If we really do not have it and it is not something we can deliver with a detour then we need to go back to the client and discuss with them" [P12]

The second internal option we find is to **Check internal app store**. This is a step to see if there is a certain tool available that has already been approved by the IT department. We observe these instances in the *junior* and *manager* ranks:

"I look at [organization platform] a lot. Do we already use a similar tool for a similar problem? And next to that we also check the [internal app store]" [P17]

Finally, participants mentioned a **Discussion within own team** as a means of figuring out the next steps. This entails conferring with close colleagues to discuss if there have been similar problems that have needed similar solutions before, or to discuss whom to approach for further steps:

"So some others may have similar projects, with similar goals for the use of the application. I would always ask around first" [P10]

6.3.3 Policy & Awareness

We observe and analyze how well-informed participants are about relevant organizational policies with regard to shadow IT. Were refer to this policy as the acceptable use of technology policy. The components of this section are presented in Figure 6.16.

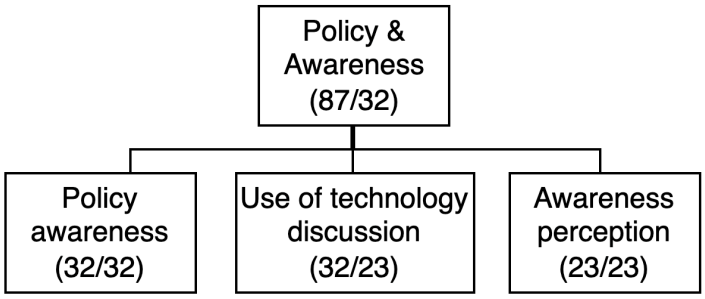

FIGURE 6.16: Policy & Awareness components with groundedness and cover metrics

6.3.3.1 Policy awareness

Are you aware of the [organization policy name]?

When observing how well participants know the policy related to shadow IT, we find that none of the participants consciously remember this specific policy. Therefore we label the responses of understanding of the concept with either **Familiar** or **Unfamiliar.** We find a fairly even distribution between the two, presented in Figure 6.17.

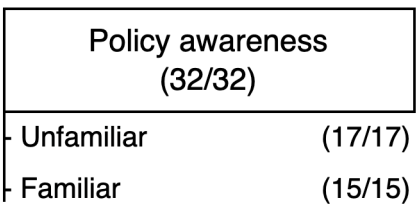

FIGURE 6.17: Occurrence of policy definition familiarity

Of the fifteen **Familiar** instances, we find one occurrence within the *support* group, and the others are within the *management* and *client facing* groups across ranks:

"You may only use applications that are approved by [organization]. I mean they have the [internal app store] for a reason right, in addition to a whole protected environment with work applications and services [...]" [P2]

In the group which is **Unfamiliar** with the policy, there is a clear division. Some participants openly admit to not knowing about the policy, while others go on to mention different cybersecurity courses they have taken in an effort to prove their understanding. This second group seems to have a need to express their awareness of cybersecurity guidelines and protocols:

"Well recently I did some mandatory courses so now I am a bit more aware again. To give a concrete example of why this is the case, recently we found a USB drive at the office. Back in the day we would just plug it in and see what is on but now we don't do that anymore. I think more and more people are aware of these things, mostly due to all the trainings and courses that we do." [P14]

Moreover, other participants provide an explanation to a completely different policy, or some other proof with regard to their cybersecurity-related understanding. We can explain this due to the sensitivity of the concept, and the potential consequences 'not being aware enough' can have in a work environment since employees are expected to be well educated about these cybersecurity topics:

"Ehm, I think I should be familiar with this. I think it says something like just use your common sense when handling technology right?" [P13]

We observe an example of a participant who had a moment of realization that the provided information in the interviews could be self-incriminating, in the sense that participants provide information with regards to not being aware of cybersecurity standards:

"Ah now I understand why this interview is anonymous. I think you will really get punished for this kind of stuff" [P25]

6.3.3.2 Use of technology discussion

Have you discussed the use of technology among co-workers?

We ask participants to give insights into how they discuss the use of external tools to get a good picture of how cybersecurity awareness is spread within the organization. We identified the following answers, presented in Figure 6.18.

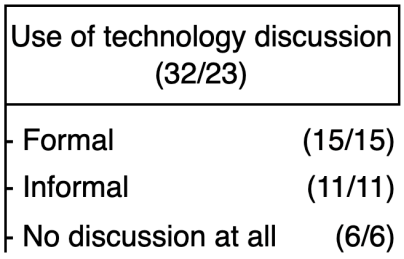

FIGURE 6.18: Occurrence of *use of technology* discussions

We observe the majority of the **Formal discussion** instances in the *client facing* group. However, they are present in the other groups as well, across all ranks. The majority of the formal discussions take place in periodic team meetings:

"Last week we had a team meeting with the [management] about this topic. It was about what you should and should not do in this regard bla bla... I think we are all aware of these things but it is good to remind everyone once in a while" [P3]

We find more variety in the provided examples when observing the **Informal discussion**. We find instances in the *client facing* and *management* groups. Participants provided examples like *"This is a typical coffee corner conversation" [P12]* and *"It is not an actual agenda item" [P25]*.

More on that same note, we find that **No discussion**. This is an interesting observation since the explanation for not discussing is enriched with expected behavior patterns. Participants illustrate there is an implicit trust in the work that they perform:

"No we definitely do not discuss this. Look, in our department they just expect you to know this stuff. You need to have a certain knowledge of these things. I mean you follow a certain education and you get all these e-learnings." [P18]

6.3.3.3 Personal perception of awareness

Do you feel you have been well informed about the use of technology?

As a final question, we asked participants if they feel well-informed about the use of technology. Since this question concerns a participant's perception, this is a rather more personal question. The answer to this question allows for a comparison to the actual observed shadow IT instances and therefore if the participants have a true or false sense of awareness: meaning, do participants act upon the knowledge that they think to be well-informed about? We categorize the observed instances into three groups, sorted on occurrence in Figure 6.19.

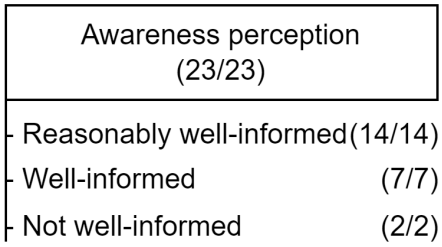

FIGURE 6.19: Occurrence of personal perception of awareness

The classification for instances in the well-informed and not-so-well-informed are evident. However, sometimes participants illustrated that they felt informed to some degree. We classified these instances as reasonably well-informed.

We observe the majority of the instances in the **Reasonably well informed** group. We find a high occurrence of participants referring to their training:

"Well, we do have the mandatory courses which teach us all sorts of things that can go wrong. So we need to be very aware, I think there is a great awareness of how to handle things in this regard" [P5]

Moreover, participants demonstrate having adequate knowledge of how they should act, but do not always act accordingly:

"I have a good idea of what I should and should not do. However, I do not always fully act like it [...]" [P16]

We then observe participants who feel **Well-informed**. We find these instances mostly in the *management* and *senior manager* ranks due to their experience:

"Yes I am very well aware, but that is also because I grew up in this place [...]" [P30]

We notice some participants that are well-informed due to their specific backgrounds and expertise. We encounter these instances across the *senior* rank across departments:

"I think I am well-informed, but also because I am really into this topic. So I am spending a lot of time thinking about it, what is okay and what is not [...]" [P19]

Perhaps due to the self-incriminating nature of the question, we observe few **Not so well informed** responses. We observed instances in the *junior* rank and surprisingly in the *senior manager* rank. In both the *client facing* and *support* department.

In some cases, we prompted a follow-up question if the participants thought the awareness team could do more in terms of educating employees. Several participants noted that there is more than enough being done on the awareness side and when asked if the awareness team should do more we encountered the following response:

"Definitely not [...] Like you can bombard people with information, but in my opinion, the information you provide to the people should not be more than five bullet points with the most required information that would let them use anything literally." [P26]

Moreover, we observe that the courses are not always tailored to the type of employee. Participants note that the courses need to be passed. Passing a course is done by making a test, however, when some of the courses are irrelevant to some individuals for whom the test is mandatory, this causes a negative association with these courses:

"We are mandated to do lots of courses that do not apply to us. As a consequence, you absorb less of the information because you know it is irrelevant. So you just do it quickly and guess on the exam, hoping to pass" [P11]

6.3.4 Contradictions

During the interviews, participants were prompted with questions concerning their use of shadow IT tools, their understanding of associated risks, implications, and their knowledge of the relevant policy and awareness measures. As detailed in section 6.4, a gap between individual knowledge and corresponding action was detected. Interestingly, we also found a number of contradictory statements or patterns within participants' responses. We categorize these instances in this section and provide a contextual understanding of their nature.

Due to the incriminating nature of these contradictions, we do not name the participant that provided the concrete example. To keep track of which statements were made by what participant we address them as *[Px]*, *[Py]* ... *[Pz]*

These findings illustrate gaps in user understanding of comprehensive understanding of all shadow IT aspects. We observe concrete examples of the above phenomenon, where participants illustrate perfect comprehension of the risks and dangers of shadow IT. However, someway rationalize their own use of shadow IT instances. In the following example, we find

a participant that is very well aware of all the risks that shadow IT can bring, however, earlier in the interview provided several shadow IT tools. We observe an *awareness-action gap*:

"During a mandatory course, I learned that you really need to be careful using tools outside the [organization] scope. Because doing so can leak data, and can have multiple negative consequences" [Px]

"I think [tool] is not within the [organization] scope. Oh yeah and also the [tool], I think this one also falls out of the [organization] scope" [Px]

We found that certain participants used shadow IT due to the wide adoption of an external tool within a team as provided in section 6.3.2.3. Moreover, we observed there is a team-wide workaround to circumvent security protocols. Since such tools are explained to employees when on-boarding, they do not question the cybersecurity risk related to these tools. The awareness discussion provided an opportunity to confront the participants about this gap in their awareness. We found that even when explicitly asked about the team-adopted shadow IT instances participants defended the use due to the team-wide adoption, therefore contradicting their awareness of the concept rather than becoming aware of the risks that the use of these shadow IT instances brings:

"I think you always need to be critical with what software you use. There is always a risk if you use non-standard software [...]" [Py]

"Well there was someone who was acquainted with [external tool], and everyone saw the advantages of working with it [...] So we were persuaded rather swiftly and now we've already worked with it for years so you don't want to change anymore" [Py]

We encountered two situations where participants, upon facing the paradox within their statements, experienced a moment of realization. They figured that their depicted behavior was in conflict with the organization's protocols and could lead to consequences:

"Yes you should always be careful with these things. I don't know, to be honest, perhaps, we might be already crossing a line here. I don't know. Now thinking about it this way, I do not think it is allowed. Because it is not a [organization] tool" [Pz]

"We just need to put this into practice. So perhaps I should ask my superiors about our usage of tools outside the [organization] toolbox" [Pa]

The second type of contradiction concerns the necessity of shadow IT instances. On multiple occasions, we noted participants stating that they refrained from using any external tools, as the organization had supplied all the necessary tooling. However, later provided contradicting statements:

"All tools we use are from a fixed number of applications, a fixed pattern. I think we have everything that we might need" [Pb]

"I can very well imagine that lots of employees use [external tool], or install a nice [external tool] from a nice website [...]" [Pb]

6.3.5 Mental Models

The rationale for the interviews is to build mental models of the participants. It is not possible to pinpoint a single question that elicits an explicit expression of their perception of shadow IT. However, during the interviews, we observed that participants occasionally subtly illustrate their conceptualization of shadow IT at various points in the conversation.

We observe ten mental models among the participants and find that participants hold different combinations of mental models. These mental models illustrate internal drivers that influence participants' attitudes with regard to shadow IT. We notice a split in the identified mental models, specifically regarding their impact on individuals' *behavior* towards shadow IT. On one hand, certain mental models promote risk aversion, leading individuals to adopt more cautious behaviors when dealing with shadow IT. On the other hand, there are mental models that foster risk-taking, increasing individuals' risk appetite with regard to shadow IT. We present these two types of mental models in Figure 6.20.

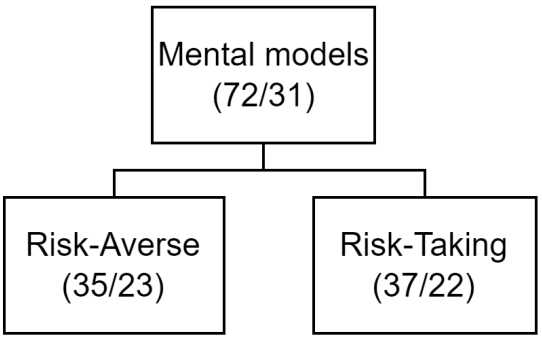

FIGURE 6.20: Types of Mental Models with groundedness and cover metrics

6.3.5.1 Risk-Averse Mental Models

We observe four mental models that seem to promote more secure behavior of individuals. These mental models provide internal motivation to stay conscious of potential threats and discuss shadow IT instances. We provide the risk-aversing mental models, sorted on occurrence, presented in Figure 6.21.

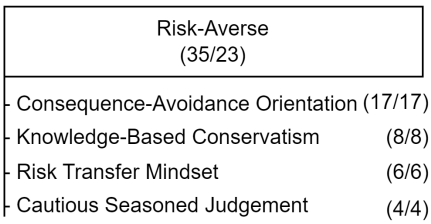

FIGURE 6.21: Risk-aversing mental models

1. Consequence-Avoidance Orientation

The consequence-avoidance orientation refers to a mindset where individuals prioritize steering clear of negative outcomes or consequences when making decisions and taking action.

Throughout the interviews, we observed a high awareness of all sorts of consequences. In certain cases, we find that the perceived impact of these consequences is the reason that participants do not engage in the use of shadow IT instances. This "to be safe I will just use

nothing external" attitude is exactly what denotes this mental model. We find that participants have a strong aversion to unfavorable implications and are therefore cautious to negate potential negative impacts.

"Think about all the consequences. I think those hold the biggest risks. Which is also the reason I don't have anything external." [P19]

"At [organization] confidentiality is highly valuable. Extremely valuable, with everything we do. That just can not end up on the street. This is also the reason that I do not have any of those things." [P29]

2. Knowledge-Based Conservatism

Knowledge-based conservatism is a mindset characterized by a tendency to rely on established knowledge and wisdom when making decisions. We observed a subset of the participants to be significantly more aware of the concept of shadow IT, but also the risks, implications and overall had a great understanding of technology. This understanding was due to expertise within the field of technology and provided these participants with the knowledge to understand the navigation around the challenges faced with shadow IT. Moreover, we denote this mental model when participants' expertise in technology influenced more secure shadow IT behavior:

"I am very aware of all sorts of risks. It is because of my role as [role]. So, therefore, I am aware of certain things, certain things that the average Joe here won't think off" [P7]

"Well, I'm not very aware of what the policy says about that. But I think in general we are a lot more careful and aware than many others, simply because we are in the field of study" [P22]

3. Risk Transfer Mindset

The risk transfer mindset is a mental model characterized by the idea to shift risks onto others or external entities. In this case, we observed participants within the *client facing* group try and manage any shadow IT consequence by shifting the *perspective* of shadow IT to clients. This strategic approach creates a more convenient way of working for a client and mitigates any potential shadow IT threats. Therefore having this mindset really benefits the overall potential consequences of shadow IT:

"In all of the projects I know, and for the people in my team that actually implement the work. The client opens up access to their systems and then we can access it and then it's game on. This way we never need to have the tooling on our own laptop" [P24]

"I would try and let the client take responsibility for the risk. Because they are the ones asking for this tool. However I would not have thought of that when I was younger, but I know now" [P22]

4. Cautious Seasoned Judgement

Cautious seasoned judgment refers to a mental model denoted by careful decision-making based on experience. It is similar to *Knowledge-based conservatism*, however rather than niche

knowledge of a certain field or object of study, the behavioral choices are motivated by 'seasoned' experience. This experienced father figure is not something individuals implement to influence their shadow IT behavior directly. However, employees may have a colleague that fills the shoes of a 'cautious seasoned judge' for them to consult with whenever necessary. Thus influencing others to implement the value of accumulated wisdom and experience in making well-considered decisions.

Moreover, we find an example of learning through the experience of consequences due to shadow IT decisions. Therefore the combination of mental models that an individual hold may be subject to change over time.

"So if they have any questions, and they need a specialist in the field [...] Since I have a bunch of experience I know a thing or two" [P29]

"I have seen it all, but actually you should go through a data breach once just to see how bad it really is. After that, you'll think twice about your actions. You learn this through trial and error over the years" [P30]

6.3.5.2 Risk-Taking Mental Models

We observe six mental models that seem to support more insecure behavior of individuals. These mental models provide an internal motivation to engage in shadow IT instances. Therefore neglecting potential threats and discussions with regard to shadow IT. We provide the risk-taking mental models, sorted on occurrence in Figure 6.22.

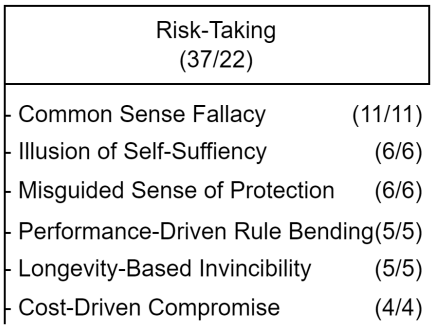

FIGURE 6.22: Risk-taking mental models

5. Common Sense Fallacy

This mental model denotes the attitude that participants have with regard to the handling of shadow IT, but also other cybersecurity-related topics. Namely, that they should not have to be discussed as much. It comes from a baseline expectation of a certain level of 'common sense'. It suggests that each individual should already have a basic understanding of cybersecurity concepts.

Individuals with this mental model have a natural sense of allowed and not allowed in a situation. However, not everyone might have this basic cybersecurity know-how. So, using this mental model and assuming that they do leads to fewer discussions within teams, which can be a problem for handling shadow IT. While this idea of 'common sense' is useful for quick decisions, they can also push necessary discussions and hard thinking to the side, which negatively impacts overall shadow IT behavior.

"[...] Look, in our department they just expect you to know this stuff. You need to have a certain knowledge of these things. I mean you follow a certain education and you get all these e-learnings." [P18]

"I think in our values it states we should all just behave normally, to summarize it. I think it is no more than common sense" [P7]

6. Illusion of Self-Sufficiency

The illusion of self-sufficiency illusion refers to the mental model where an individual has the belief of not needing any shadow IT applications because they think everything is provided, whilst giving examples of shadow IT instances and thus illustrating the 'illusion' This implies that an individual has the idea that they are no danger in terms of shadow IT, due to the belief that all applications are facilitated by the organization. This illustrates that this mental model lowers the internal guard for any potential cybersecurity threats that might occur. We find a pattern where all of the participants that had this mental model, none of them were familiar with shadow IT. Therefore, this gap in an individual's understanding might result in the notion that all the tools that they use are facilitated, while this is not the case. This 'I have everything so I'm safe' attitude is exactly what denotes this mental model:

"No, for me this is not a thing to consider because we have everything taken care of" [P6]

"[...] I think in terms of work-related things we have everything that we need" [P19]

7. Misguided Sense of Protection

A misguided sense of protection refers to the mindset where individuals hold on to a false or misguided idea that they are protected. We observe participants with these insecure norms throughout the interviews. We find that participants name experiences with other security measures, for example, phishing and viruses, and therefore have the belief that they are therefore also protected against shadow IT. and viruses,

So, we find that individuals have the belief that they are safe from harm due to the idea that they are protected by the organization. In terms of cybersecurity, this notion of invincibility can severely impact the behavior of participants in terms of shadow IT usage, since these individuals believe that no matter what they use or install if the instance is not allowed in some way they will be alerted, providing them with a *false sense of security*:

"[...] I think they watch what you downloaded, and if it is not okay then maybe it will go through a system that detects this, or maybe there is a team that reads everything, and you then get a message to delete it from your machine" [P15]

"And also you get a warning I think at [organization] if you have something on your system which is not good [...]" [P5]

8. Performance-Driven Rule Bending

Performance-driven rule bending refers to a mindset focused on achieving desired results, even if it involves deviating from established rules or guidelines. We observe a concrete example of this, time pressure, in section 6.3.2.3. We find that participants are sometimes willing to neglect, or even actively circumvent standard cybersecurity protocols in order to finish

work tasks on time. This mental model therefore negatively impacts the overall shadow IT behavior of individuals:

"I can not explain to a client that certain tasks have not been completed. This means that sometimes employees enter a grey area, perhaps even cross it by doing what they shouldn't. I think everyone is aware of this [...]" [P20]

I think the main issue with that is that the show must go on [...] [P20]

9. Longevity-Based Invincibility

Longevity-based invincibility refers to the mental model where individuals think that the long-term presence of a concept grants them a sense of immunity from negative consequences. This is a form of survivorship bias, where participants overlook the potential negative consequences of shadow IT due to the positive experience they have had with the tool for a longer period of time. With this mental model participants gain the notion of 'invincibility'.

We observe the team-wide adoption of certain tools. The time span of the adoption of these tools provided these individuals with an illusion of safety. Due to the long adoption, certain newer employees have been onboarded with a specific tool and therefore it makes sense that they are not aware of the risks of such a tool. This 'we've used it for so long, never had any troubles' attitude is therefore exactly what denoted this mental model, and brings down all internal guards for the proper handling of shadow IT instances:

"We have used these tools for years, we are used to it now and if we were to switch tools it will be a hassle and a lot of trouble to switch [...]" [P15]

"[...] I don't know, I think sometime a while ago it was introduced and it has stayed up until now [...] over time it has grown to what it is now for us." [P12]

10. Cost-Driven Compromise

Cost-driven compromise refers to the mindset in which individuals make trade-offs based on financial considerations. We observe an explicit prioritization for cost savings when making shadow IT decisions across participants. The 'we use it because it is free' attitude is exactly what makes this mental model negatively impact the shadow IT behavior of individuals:

"I wonder about, for example [tool], since we used it because it provides a free package. One might wonder how good that is [...]" [P5]

"[...] as well as the costs for the organization. I mean, if everyone went to IT for every small thing, that would not work" [P16]

6.4 Summary of Interview Findings

We synthesize the findings per code group and provide the most important statements and implications.

Context

In short, we observed three primary work types: client-based, internal, and project-based, with each group demonstrating unique tasks, responsibilities, and potential for shadow IT. The *client-facing* group, working either client-based or project-based, had different needs and risk levels concerning shadow IT, due to the consistency or variability of their tasks. Notably, we find that project-based work has a greater potential for shadow IT since each project might bring the need for new technical solutions. An observable pattern also suggested that lower-ranked employees were more engaged in direct work tasks, while higher-ranked individuals were less involved in hands-on duties. This suggests that lower-ranking employees are more likely to resort to shadow IT than their higher-ranking counterparts.

In relation to hardware usage, interviewees were found using either a single laptop for all tasks or separate laptops for personal and work tasks, with the single-laptop users predominantly among the 41-50 age group or older. This distinction revealed awareness of cybersecurity risks and the potential implications of their actions if personal tasks were performed on work laptops. Mobile device usage mirrored these findings; older participants tended to use a single mobile device, while others preferred separation or a combination of personal and work purposes on their devices.

Finally, the *perspective* of shadow IT, present only among the *client-facing* group, holds three different preventive measures: using physical devices, remote workspaces, and program licenses provided by clients. These measures, ranging from fully separated hardware to shared application licenses, were perceived to mitigate potential shadow IT risks, offering secure environments for employees and a controlled-application setting for the clients.

Shadow IT

In summary, we found significant awareness about the implications of shadow IT, even though inconsistencies and gaps were observed. Participants generally felt informed but did not always act accordingly. The findings highlight the need for targeted education, effective policy communication, and continued efforts to create a shared understanding and behavior change to improve shadow IT governance. We encounter a complex relationship between the perceived benefits, risks, and mitigation strategies used by individuals in the workplace when exploring shadow IT occurrences and implications. We find instances of shadow IT, particularly among *client-facing* and *support* groups. We observe a drive to enhance efficiency and a need for cost savings. These motivated the use of these non-standard solutions, in some cases under significant time pressure.

However, the awareness of potential risks associated with shadow IT seemed equally present, finding a delicate balance between benefits and drawbacks. Among these, we observe the risk of a data leak as a prime concern across all ranks and departments, resembling a high level of data consciousness in the organization. We encounter other perceived risks such as malware, unauthorized access, non-central governance, reputation risk, ransomware, misinformation, and outdated software, further highlighting possible threats due to shadow IT.

Despite these risks, the decision-making process for shadow IT adoption illustrated a picture of internal and external strategies combined. Most commonly, participants sought the advice of the IT team first, indicating adherence to the IT governance structure within the organization. We also found that 'higher-ups' were frequently consulted, particularly by *junior* participants, thus reflecting on the element of hierarchical decision-making within such organizations. We found autonomous due diligence more common among *managers*, indicating that individuals at this rank often relied on their own judgment. We see a pattern emerging that suggests a correlation between rank and autonomy. Specifically, individuals in higher ranks tend to have greater autonomy, while those in more junior positions tend to rely more on consulting other entities, again supporting hierarchical-based decision-making. Finally, we encounter the approach of the client, internal application checks, and discussions within an individual's own team as additional strategies, suggesting a mix of responsibility sharing, internal and external shadow IT protection, and collective decision-making.

In summary, **the occurrence and implications of shadow IT within organizations present a dichotomy**: a push towards non-standard solutions for efficiency and cost reasons, balanced against a broad awareness of the significant risks, specifically data leaks. We find a wide range of strategies that bring together individual autonomy and collective decision-making, all due to the importance of shadow IT governance. However, the findings suggest a need for consistent risk awareness across the organization and improved education to further manage and mitigate the complexities of shadow IT.

Policy & Awareness

We observed policy awareness and discussions about the relevant shadow IT policy. This provides insight into participants' understanding of organizational protocols regarding shadow IT. The distribution of policy familiarity was almost equal, indicating communication gaps about the policy. Even though participants demonstrated a basic understanding of cybersecurity, they struggled to link it to the specific policy. This then raises the question if individuals should know the policy, or should just know how to act according to the contents of this policy. To focus on the latter, we found that due to the presence of knowledge about the contents of the policy, participants were very aware of cybersecurity consequences. Specifically, data leaks were very top-of-mind for participants.

Conversations about technology use, formal or informal, were present across different ranks

and groups. Formal discussions usually took place during team meetings, primarily in *client-facing* roles, while informal talks emerged spontaneously during casual interactions. Surprisingly, some participants reported no discussions, implying that the responsible use of technology was based on implicit trust and assumed knowledge for all colleagues within their department.

Most participants considered themselves as reasonably or well-informed with regard to the use of technology, often naming mandatory training and in some cases personal interest or expertise. However, we observe an awareness-action gap, with participants admitting they did not always act according to their understanding of this awareness due to a number of reasons. A minority admitted to being not-so-well-informed, highlighting concerns across both *junior* and *senior manager* ranks. Even though we have observed lots of both formal and informal discussions, courses, and e-learning, we find that these measures do not cover all individuals in the organization. Therefore suggestions for improvement include more tailored courses for certain employee groups.

Contradiction

We find a difference in participants' understanding and actions related to shadow IT. Despite acknowledging risks, they justified personal shadow IT usage through the team-wide adoption of instances, in two instances leading to realizations of harm. Further, participants claimed they did not need any external tools, however, seemed to acknowledge the motivation to use these tools. These contradictions aid the creation of mental models by providing gaps in an individual's conceptualization of shadow IT in these instances.

Mental Models

We extracted ten distinct shadow IT mental models from the participants, highlighting the different ways they perceive shadow IT. We found a clear dichotomy in these mental models: four demonstrate risk-aversion, promoting caution in dealing with shadow IT, while six embody risk-tolerance, increasing risk-taking willingness.

We find that participants can hold a combination of mental models that may change over time. Moreover, an individual might hold different mental models in different situations due to time pressure or the complexity of the task at hand.

Risk-averse mental models, such as *consequence-avoidance orientation*, *knowledge-based conservatism*, *risk transfer mindset*, and *cautious seasoned judgment*, imply enhanced cybersecurity behaviors. Participants under these models are generally aware of the potential impacts of shadow IT and want to mitigate these through tactical decision-making, specialized knowledge, and wisdom gained from experience.

On the other hand, risk-tolerant mental models, namely *common sense fallacy*, *illusion of self-sufficiency*, *misguided sense of protection*, *performance-driven rule-bending*, *longevity-based invincibility*, and *cost-driven compromise* tend to negatively impact cybersecurity behavior. These

mental models imply a variety of motives, ranging from relying on 'common sense,' to contain the basic sense of security, to a willingness to violate standards for efficiency and cost savings.

We note that the presence of various mental models among participants are subject to change over time, and can be shaped by the outcomes of previous actions. Participants have a set of mental models based on their experiences and training. This illustrates a cycle of continuous learning where, considering their personal and professional backgrounds, in a given situation, individuals make decisions about shadow IT. These decisions are influenced by the combination of mental models they hold and their prioritization. The outcomes of these decisions, in turn, may lead to consequences that individuals use to adjust the importance they assign to these mental models. Furthermore, individuals' combination of mental models may change through external factors like discussions, training, or other awareness-raising activities.

6.5 Interview discussion

As described in section 6.1.2, the drawing component led to confusion amongst the participants. We kept the same scenario prompt yet also prompted participants to think out loud and illustrate their thought processes throughout the scenario. This more 'brainstorm-typed setting yielded better results and improved the flow of the interviews. This however means that we have several participants' incomplete thought processes from the drawing exercise.

As provided in section 6.2, we find that the high code saturation means that all relevant aspects were provided by participants, however, we might have not captured all the relevant links between the codes. Moreover, the number of times some code is mentioned gives an idea of how top-of-mind an aspect it is but results should not be interpreted quantitatively.

We observe a high degree of awareness due to all sorts of training in section 6.3.3. This explains the participants' hesitation to self-incriminate. They are periodically reminded of certain cybersecurity threats and find themselves in an environment where the consequences as a result of these unsafe cybersecurity actions can be significant.

We observe an interesting trend among the participants. Many of them frequently expressed a sense of consensus bias. This is a cognitive bias that leads to individuals overestimate their own abilities and skills. This creates the belief that behavior and therefore actions are relatively widespread among the general population. We found that participants often compared their cautiousness regarding shadow IT with that of their colleagues. They emphasized their careful approach and expressed the belief that they know that others were not so careful in their approach to shadow IT. However, it is worth noting that almost all participants made this statement, suggesting a common pattern. This consistency in their responses indicates that participants may have been hesitant to self-incriminate or openly admit any potential shortcomings regarding shadow IT practices.

6.6 Interview limitations

The most apparent limitation of the interviews is that we were unable to recruit any participants from the *IT* department. Even though this team is part of the *support* group, we could aggregate the two in terms of work type and role in the organization. We scoped this research to contain separate data from the team that sets shadow IT mitigation policy and controls the IT governance. This is an unfortunate data gap and challenges comparisons from other teams with the governing entity in such an organization.

We observed a low occurrence of going to IT in the scenario question for the *client facing* group. Through informal inquiry after the interviews, we found that this is a basic step for individuals to take. In hindsight, we note that the nature of the prompt asked by the interviewer influenced the participants' responses. It seems that participants assumed the mentioned tool or solution had to be found externally, which led them to dismiss the possibility of approaching their internal IT team for a potential solution.

Some questions may be more difficult for participants who are unfamiliar with the different shadow IT types. Moreover in order to contextualize what shadow IT is and conceptualize the numerous types, we experience the need to provide concrete applications as examples in order to have the participants understand shadow IT. This introduces possible bias in participant replies. Notably, we frequently discovered the given probes as applications mentioned by participants.

6.7 Takeaways for next chapter

We identify a complex relationship between perceived benefits, risks, and reasons for using shadow IT. The dichotomy between risk-averse and risk-tolerant mental models presents interesting nuances that require further exploration. We will focus on the occurrence of these mental models across different departments and ranks, aiming to find whether there is a trend for specific mental models to occur in certain departments or at certain ranks. Furthermore, we observe an awareness-action gap and several contradictions in the participants' understanding and actions concerning shadow IT. This is a result of an individual potentially holding multiple mental models that influence their behavior differently depending on the situation.

7 Patterns of shadow IT Mental Models

In this chapter, we try to identify occurrence patterns of certain mental models across departments and ranks. We present each identified mental model and provide the occurrence tables. First, we encounter the risk-aversing mental models, followed by the risk-taking mental models. Moreover, we try to explain the presence of the mental model in the identified groups. In doing so we aim to answer: *What patterns are found across cohorts regarding shadow IT mental models?*

7.1 Occurrence of Mental Models

Initially, we present the occurrence tables for the risk-aversing mental models, followed by those for the risk-taking mental models.

7.1.1 Risk-Aversing Mental Models

1. Consequence-Avoidance Orientation

We report the occurrence of this risk-aversing mental model in Table 7.1. We detect this mental model across all ranks and departments. We come across this mental model more frequently in higher ranks, suggesting that the more experience an individual gets, the more aware they are due to the understanding of the potential consequences. We can see an example of this through a participant in the *management* group. His belief is that experiencing the negative impact firsthand is the only way to truly understand how important it is to actively mitigate these threats.

	Client facing	*Support*	*Management*
Junior	**2**	**1**	
Senior	**1**	**1**	
Manager	**1**	**3**	
Senior Manager	**5**	**1**	
Management			**2**

TABLE 7.1: *Consequence-Avoidance Orientation* mental model across cohorts

2. Knowledge-Based Conservatism

We come across a risk-averse and conservative approach coming from individuals' expertise and knowledge in a technical field in the *client-facing* group, illustrated in Table 7.2. This can be understood intuitively when considering in what departments we expect to find the necessity of specialized knowledge within an organization, namely the *client-facing* group. Interestingly, we observe this trend across various hierarchical levels, supporting the notion that expertise is derived not only from work experience but also from educational background and personal interest. Numerous instances have surfaced where participants' behavior is influenced by their respective areas of expertise.

	Client facing	*Support*	*Management*
Junior	**2**		
Senior	**2**		
Manager	**2**		
Senior Manager	**1**		
Management			**1**

TABLE 7.2: *Knowledge-Based Conservatism* mental model across cohorts

3. Risk Transfer Mindset

The Risk Transfer Mindset refers to an approach that focuses on the transfer of risks to external entities. This mental model comes from a heightened awareness of risks, shifting the *perspective* regarding shadow IT. This implies using a client-provided environment, physical or digital, to perform work tasks for that client. Meaning that the application licenses, data, and communication with the client all go through provided systems and hence shuts down a major risk for the occurrence of shadow IT instances.

We illustrate the occurrences in Table 7.3. As previously stated, we find this risk-aversing mental model within the *client-facing* group, particularly among *managers* and *senior managers*. This suggests that the shift of *perspective* towards clients to mitigate risk falls primarily on individuals who hold greater project responsibilities.

	Client facing	*Support*	*Management*
Junior			
Senior			
Manager	**4**		
Senior Manager	**2**		
Management			

TABLE 7.3: *Risk Transfer Mindset* mental model across cohorts

4. Cautious Seasoned Judgement

Cautious Seasoned Judgment refers to a mental model that guides behavior and decision-making based on experiences. This mindset is predominantly found among individuals in higher-ranking positions. We illustrate this in Table 7.4. Intuitively we find this mental model in the more senior ranks: *manager*, *senior manager*, and *management*. 'Seasoned' judgment is

a direct result of a great deal of experience. For individuals who do not strongly have this mental model, it is not possible to suddenly acquire a vast amount of experience.

	Client facing	*Support*	*Management*
Junior			
Senior			
Manager	**1**		
Senior Manager	**2**		
Management			**1**

TABLE 7.4: *Cautious Seasoned Judgement* mental model across cohorts

However, we can encourage individuals to take a more risk-aversing approach to question what a 'cautious seasoned judgment' would mean in a certain situation. Moreover, the individuals that have this mental model can transfer these insights to others, we have seen examples of this through both formal and informal discussions in section 6.3.3.2. This mental model expresses the significance of effective senior leadership in influencing shadow IT behavior in a positive way.

7.1.2 Risk-Taking Mental Models

5. Common Sense Fallacy

We encounter the occurrences of the common-sense-inducing mental model in Table 7.5. We find this mental model across all departments, although we do encounter it to a greater extent among individuals in the *junior* rank. This risk-tolerant mental model is perceived by participants to enhance individuals' secure behavior by encouraging them to act in a normal, common-sense manner, therefore avoiding any actions that induce negative consequences. This might be true to a certain extent. However, despite the expectation of shared common knowledge among individuals, by not addressing concrete aspects and keeping the safeguarding through secure behavior due to an unspoken implicit knowledge this mental model will negatively influence the behavior of individuals.

However, despite the expectation of shared common knowledge among individuals, by not addressing concrete aspects and promoting secure behavior. There could be a gap between what individuals are expected to know and what they actually know. This gap may result in wrong mental models that may negatively influence the behavior of individuals.

	Client facing	*Support*	*Management*
Junior	**5**		
Senior	**2**	**1**	
Manager	**1**		
Senior Manager			
Management			**2**

TABLE 7.5: *Common Sense Fallacy* mental model across cohorts

6. Illusion of Self-Sufficiency

We refer to the Illusion of Self-Sufficiency as the mental model of individuals that lower their guard when it comes to shadow IT because they believe they do not require anything beyond what the organization provides. We observe the occurrences of this mental model in Table 7.6. We find this attitude in the *client facing* and *support* groups across ranks. Notably, we find this across more senior ranks. We encounter this 'illusion' through participants who claim they have no need for external resources, yet during the same interview, provide evidence of their utilization of shadow IT instances.

	Client facing	*Support*	*Management*
Junior			
Senior	**1**	**1**	
Manager	**2**	**1**	
Senior Manager		**1**	
Management			

TABLE 7.6: *Illusion of Self-Sufficiency* mental model across cohorts

7. Misguided Sense of Protection

We come across the misguided sense of protection across various departments and ranks in Table 7.7. This attitude can motivate individuals to use external applications with a false sense of security. Individuals find themselves feeling safe when it comes to using shadow IT instances, under the belief that if any issues were to arise, the organization will detect and mitigate the associated threats. Seeing this pattern organization-wide is concerning. It demonstrates a potentially dangerous underestimation of the risks that shadow IT poses to an organization's security infrastructure.

	Client facing	*Support*	*Management*
Junior			
Senior	**2**	**1**	
Manager	**1**	**1**	
Senior Manager			
Management			**1**

TABLE 7.7: *Misguided Sense of Protection* mental model across cohorts

8. Performance-Driven Rule Bending

We frequently come across the occurrence of performance-driven rule-bending within the *client-facing* and *management* groups, as indicated in Table 7.8. Intuitively, this flows from the nature of their work tasks and the context in which they operate. These groups consist of individuals who are driven by the need to perform, meet deadlines, and satisfy clients. Particularly in the *junior* ranks, there may be a greater need for this attitude as individuals strive to prove themselves in the workplace.

	Client facing	*Support*	*Management*
Junior	**1**		
Senior	**1**		
Manager	**2**		
Senior Manager			
Management			**1**

TABLE 7.8: *Performance-Driven Rule Bending* mental model across cohorts

9. Longevity-Based Invincibility

We observed instances of this 'we have used it for so long so it must be okay' attitude across all departments. We thus find that within the organization, there are external solutions adopted for various reasons that due to their long-term adoption are not flagged as a potential shadow IT threat. We find the occurrences of this mental model in Table 7.9.

The knowledge about the presence of long-term adopted shadow IT instances is valuable. Now an organization can flag these instances and find long-term solutions for these instances.

	Client facing	*Support*	*Management*
Junior			
Senior	**1**	**1**	
Manager	**1**	**1**	
Senior Manager			
Management			**1**

TABLE 7.9: *Longevity-Based Invincibility* mental model across cohorts

10. Cost-Driven Compromise

Cost-Driven Compromise refers to a behavior where individuals prioritize financial considerations, illustrated in Table 7.10. Analyzing the occurrence, we find a significant presence in the *support* group.

The nature of the *support* group is to ensure the smooth internal operation of an organization. Given the nature of their work, it is often assumed that their work tasks are consistent, implying a non-changing range of systems. There might be implemented systems to facilitate their tasks effectively. However, we recognize that this assumption might overlook potential gaps in their responsibilities that current systems may not fully cover. A possible explanation can be that their tasks are not fully catered for by these systems, resulting in support staff employing financially viable tools to fill this gap.

	Client facing	*Support*	*Management*
Junior			
Senior		**1**	
Manager	**1**	**1**	
Senior Manager		**1**	
Management			

TABLE 7.10: *Cost-Driven Compromise* mental model across cohorts

Additionally, given their non-revenue-generating role, participants had the belief that the *support* group may not be prioritized for upgrades or updates. They had the idea that they fall under the shadow of our client-facing staff, who are the primary revenue generators. This might create a discrepancy in the resources allocated. It is therefore crucial for organizations to manage the use of external tools throughout the organization, ensuring all work tasks are covered by checked systems.

7.2 Occurrence Trends in Cohorts

We have identified the occurrence patterns per extracted mental model. We now synthesize these mental models across cohorts and find the overall resemblance of the presence of certain mental models across cohorts.

The cohorts used: department and rank, were chosen initially to divide individuals in an organization among 2 axes. The 'horizontal' axis is set to the department, this allows us to dissect the organization through the different competencies and responsibilities. On the other hand, we use rank as a 'vertical' axis to analyze the differences within the departments.

We visualize these two cohorts in two sets of radar graphs. Each of the axes represents one of the found mental models. We marked the risk-aversing mental models green and the risk-taking mental models red. The data points on each radial axis are the relative occurrence of that mental model in a cohort group. We normalized the data to the number of participants in a certain group. We did this by aggregating the occurrence tables in section 7.1 per cohort, meaning we have one aggregated table for the department and one aggregated table for rank. This table then holds the number of participants in each cohort group that had a certain mental model. Since the cohort groups are not of similar size we calculated the percentage of participants per cohort group. Then for each mental model and cohort group, we divided the number of occurrences of that mental model in the cohort groups by the percentage of that group. So that the graphs now illustrate the average presence of a mental model per cohort group.

Since the goal is to uncover patterns, we do not look at the absolute occurrences of mental models across cohorts, therefore, we leave out any numerical data. The rings in the figures are a means of comparing the relative occurrences of mental models across different cohort groups.

Departments

We provide a visualization of the presence of mental models in departments in Figure 7.1.

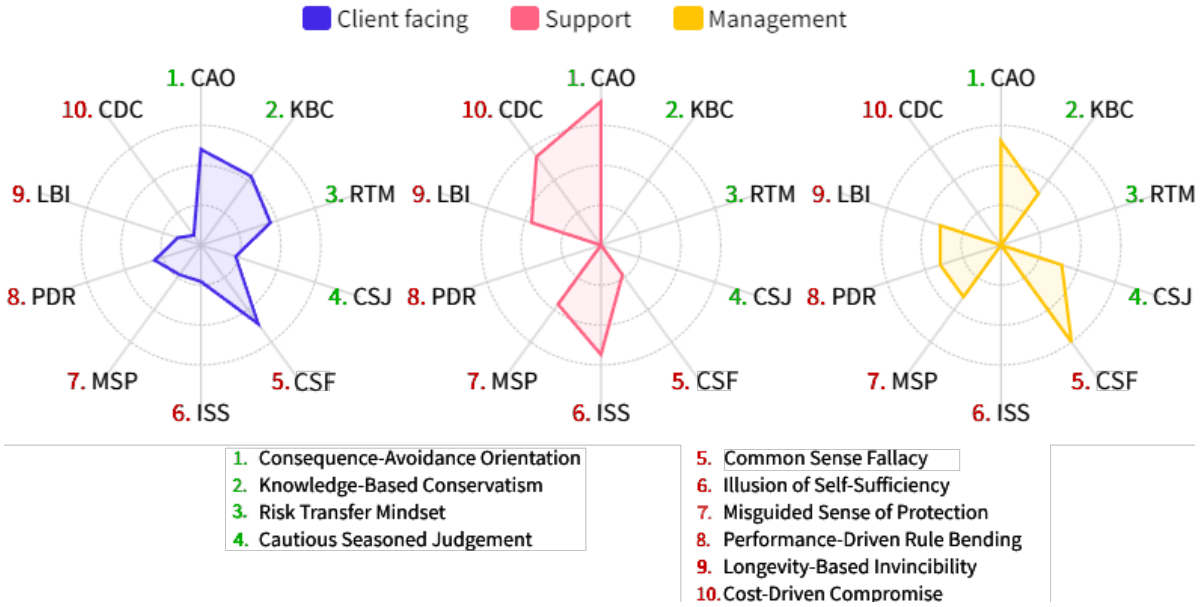

FIGURE 7.1: Relative occurrence of Mental Models in departments

We observe partial similarities throughout the mental models, however, we find that each of the departments has a unique pattern of mental model influences. We encounter four mental models that are present in all departments: *Consequence-Avoidance Orientation*, *common Sense Fallacy*, *Misguided Sense of Protection*, and *Longevity-Based Invincibility*. The majority of these are risk-tolerant models, suggesting that there is no general risk-aversing mental model that can be employed organization-wide.

A pattern that emerges is a resemblance between the *client facing* and *management* groups. We find this pattern in the presence of the risk-averse mental models: *Knowledge-Based Conservatism* and *Cautious Seasoned Judgement*, and in the risk-tolerant mental models in the *Performance-Driven Rule Bending*. This naturally flows from the fact that some of the individuals of the *management* group engage in similar work tasks and have similar responsibilities as individuals in the *client facing* group. Overall we find a light distinction between these two groups and the *support* group. This is mostly due to the further absence of risk-averse mental models besides *Consequence-Avoicance Orientation* in the *support* group.

Rank

We provide a similar visualization of the presence of mental models through ranks and present the normalized findings in Figure 7.2.

Through the rank cohort, we observe a few light trends. Firstly we find that there are two mental models that occur throughout all ranks. We find the risk-aversing *Consequence-Avoidance Orientation* and *Knowledge-Based Convervatism*. Implying that the awareness spread of the potential consequences of shadow IT and expertise to positively influence shadow IT behavior is prevalent throughout all ranks.

We identify two mental models with a significant presence in the higher ranks: *manager*, *senior manager*, and *management*. These are namely the *Risk Transfer Mindset* and *Cautious Seasoned Judgment*. These two risk-aversing mental models fit well with the responsibilities and challenges faced by individuals within these groups. This finding suggests that higher-level roles have a more risk-conscious approach to shadow IT decision-making. This further highlights the importance of the involvement of these groups in work scenarios.

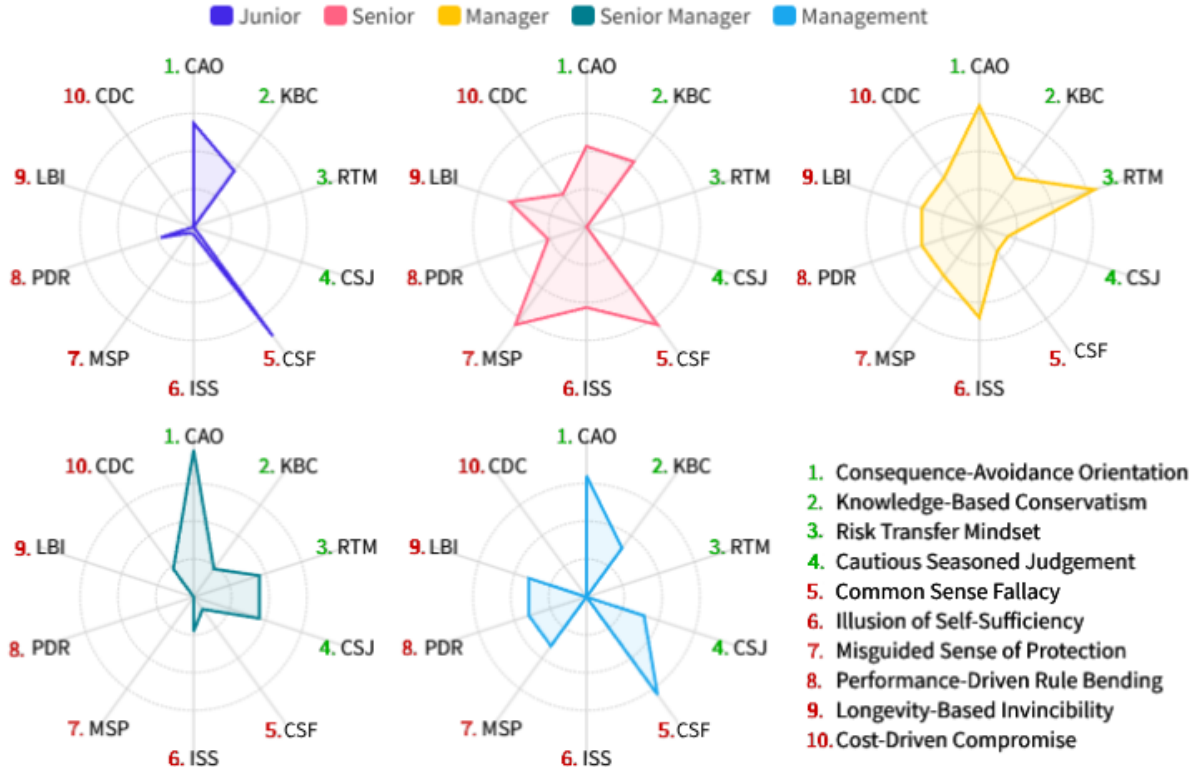

FIGURE 7.2: Relative occurrence of Mental Models throughout ranks

7.3 Conceptual Model

In this section, we present a pattern in the overarching research: a comprehensive overview of all relevant facets to construct a proper understanding of the research. We outline several findings and sequentially synthesize them into an overarching narrative.

1. From section 6.3.1.1, we find that individuals have certain characteristics like rank, department, experience, and work type. Each of these characteristics may impact an individual's knowledge of shadow IT.
2. We have seen that there are certain situations that provided a need for shadow IT solutions. This could be due to time pressure to meet a deadline (section 6.3.2.3), or to save costs (section 6.3.2.4.1). This illustrates that a specific situation might influence the presence of certain mental models in an individual.
3. We observed that individuals may hold different combinations of mental models in section 6.3.5, and these mental models are subject to change over time.
4. The presence of an individual's mental models can be influenced by external factors. Examples that have been provided in this research are online awareness training and

discussions about shadow IT in section 6.3.3.

5. We came across risk-aversing mental models, that influence more secure behavior towards the use of shadow IT in section 6.3.5.1 and risk-taking mental models, that influence less secure behavior towards the use of shadow IT in section 6.3.5.2.
6. We found that the consequences of these actions may rigorously influence the presence of mental models in an individual in the example provided for *Cautious Seasoned Judgement* in section 6.3.5.1.

Now synthesizing the above: individuals have a certain baseline knowledge about shadow IT due to personal and work-related characteristics (1). When this individual is in a certain situation, the situational context (2) determines the presence of an individual's combination of mental models in this situation. An individual may hold a combination of different mental models (3). The presence of these mental models can be influenced by external factors such as awareness training or discussions about shadow IT (4).

So, an individual in a given situation may hold a combination of different mental models, this may be any combination of mental models. The sum of all present risk-aversing mental models denotes the positive influence on shadow IT behavior and the sum of all present risk-taking mental models determines the negative influence on shadow IT behavior (5). Collectively, this leads to certain shadow IT behavior. This behavior might have consequences that then may impact the presence of an individual's mental models (6).

Mental Model-Driven Shadow IT Dynamics	
Theory overview	
We develop a theoretical model in which we describe how different individuals hold the combinations of ten distinct mental models that influence shadow IT behavior. This combination of mental models is based on several aspects and may lead to consequences that update their mental models, creating an iterative shadow IT-feedback loop.	
Theory Component	**Instantiation**
Means of representation	Words, diagram
Primary constructs	Personal characteristics, situational context, external factors, mental models, shadow IT behavior, consequences
Statements of relationship	The personal characteristics, situational context, and external factors have a composite causal relationship on the mental models. This entails that collectively these constructs influence the presence of mental models in an individual. The mental models influence an individual's shadow IT behavior. Shadow IT behavior might have consequences for an individual. Shadow IT consequences can influence the mental models in an individual.
Scope	The statements of relationships include no modal qualifiers. The scope of the theory is limited to organizations with similar characteristics as the organization used for data gathering as described in section 3.5.
Causal explanations	The statements of relationship include (composite) causal explanations.

TABLE 7.11: Mental Model-Driven Shadow IT Dynamics theory table according to Gregor (2006)

From Gregor (2006), find that a *theory of explanation* fits best with the overarching theory from this research. This type of theory is useful for understanding complex systems and identifying causal relationships. We name the theory: *Mental Model-Driven Shadow IT Dynamics*. In order to display such a theory, we provide the needed concepts in Table 7.11. A visual overview of the overarching narrative for this research can be found in Figure 7.3.

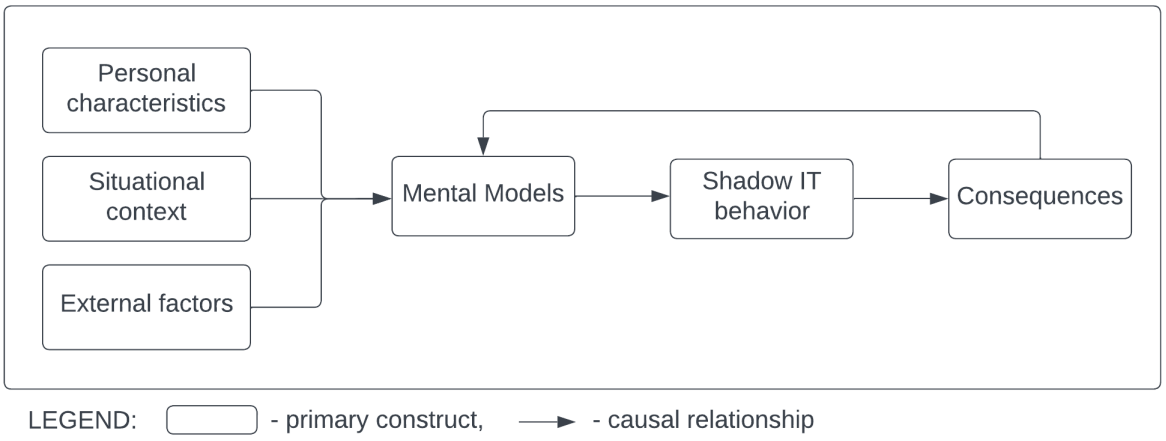

FIGURE 7.3: Mental Model-Driven Shadow IT Dynamics conceptual overview

This theory has some resemblances with existing theories, namely with *the Protection Motivation Theory* (PMT). It suggests that people are motivated to protect themselves from potential threats or risks by taking appropriate actions (P. Norman et al., 2015). We find similarities in two concepts:

- *Threat Appraisal*: In our theory, the concept of mental models influencing shadow IT behavior can be related to the threat appraisal component of PMT. Just as individuals assess the severity and vulnerability of a threat in PMT, they also assess the consequences and risks associated with shadow IT behavior based on their mental models.
- *Coping Appraisal*: The coping appraisal component of PMT aligns with our theory's concept of individuals updating their mental models based on consequences. The iterative loop involves a continuous process of evaluating outcomes, which is similar to the coping appraisal in PMT where individuals evaluate the effectiveness of their coping responses.

Moreover, we find similarities with the Theory of Planned Behavior (TPB): This theory is widely used to understand and predict human behavior, especially in the context of decision-making related to goal-directed actions (Ajzen, 1991). We find similarities in the following aspects:

- *Attitudes*: The mental models in our theory are similar to attitudes in TPB. Just as attitudes represent an individual's overall evaluation of a behavior's outcomes, mental models hold an individual's perceptions, beliefs, and thoughts about shadow IT and its consequences.
- *Subjective Norms*: The social aspect of our theory, where individuals' mental models are influenced by external factors, is related to the subjective norms component of TPB.

Individuals' perceptions of views and expectations from others play a role in shaping their shadow IT behavior, similar to how subjective norms influence behavior in TPB.

- *Perceived Behavioral Control*: The aspect of our theory where consequences update mental models can be compared to perceived behavioral control in TPB. Just as individuals assess the feasibility of performing a behavior in TPB, our theory highlights the influence of outcomes on individuals' mental models, which in turn impacts their subsequent behavior.

Lastly, we find a resemblance with *Fogg's Behavioral Model* (FBM). FBM explains behavior change through the interaction of three elements: motivation, ability, and triggers (Fogg, 2009). The model suggests that for a behavior to occur, all three elements must converge at the same moment. The model is often represented as: *Behavior* = *Motivation* + *Ability* + *Triggers*.

Trigger in this case is that there is a need to adopt a shadow IT instance. Then the ability refers to if an individual is able to adopt a shadow IT instance. Due to the policy of the organization as described in section 3.5, they are allowed to download and install external applications. Motivation refers to the shadow IT adoption reasons we have seen in section 6.3.2.3.

8 Discussion and interpretation

This chapter aggregates the results from all previous chapters. We summarize key findings and discuss their implications for science and practice, and we reflect on the research's limitations.

8.1 Key findings

We present the key findings of the different chapters by answering the sub-questions as posed in section 3.2.

SQ1: *How are mental models used to explore user understanding of cybersecurity-related concepts?*

We found manuscripts containing a variety of cybersecurity topics, ranging from specific aspects of computer and mobile security to broader issues such as privacy. We focused on research that tries to conceptualize users 'understanding of cybersecurity through mental models. We observed that the methods used to elicit these mental models in the manuscripts are diverse, but the most prevalent are interviews and drawing exercises, often together with think-aloud exercises. These methods offer an insightful understanding of why participants conceptualize the object of study in a specific way. Although we ultimately did not use all the intended methods in retrospect, the idea of employing a combination of these methods was a result of the literature study. The extracted mental models are typically presented textually and visually. Text-based descriptions provide precise, detailed nuances of concepts while diagrams offer a summarizing overview. By revealing how users perceive and respond to cybersecurity threats, mental models illustrate user perception of all sorts of concepts and therefore assist researchers and IT professionals in improving system usability and security.

SQ2: *What types of Shadow IT can be observed across different cohorts?*

We came across four types of shadow IT: *cloud services*, *self-installed applications*, *self-built solutions*, and *personal devices* across different cohorts. We observed that users choose familiar, preferred tools and services, therefore not adhering to organization policy, to meet work or personal requirements. The presence of *self-installed applications* and *self-built solutions* both suggest an attempt to close the gap between provided solutions and individuals' needs. Furthermore, we find a concerning trend of personal device use for work activities, indicating potential issues with organization-provided hardware. Due to the observed awareness concerning the confidentiality of accessed information, the occurrences highlight a significant need for a deeper understanding of individuals' behaviors, preferences, and motivations, for the adoption of shadow IT.

SQ3: *Across different cohorts, what is the perception of the concept of Shadow IT, and what are the perceived risks and implications of shadow IT?*

Across cohorts, we find a nuanced perception of the concept of shadow IT. While it is illustrated as a solution to enhance efficiency, meet demands, and save costs, it also brings significant risks. These risks include data leaks, malware, unauthorized access, non-central governance, reputational damage, ransomware, misinformation, and outdated software. Notably, we identify a pattern between rank and autonomy in decision-making related to shadow IT adoption, with more senior employees demonstrating more autonomous decision-making. Participants generally felt informed about shadow IT, but in some cases their behavior contradicted this awareness, showing an *awareness-action gap*. We found that the decision-making process for shadow IT adoption concerns a mix of internal and external options, with a need to consult with IT teams and higher-ranked individuals, reflecting the hierarchical structure within the organization.

We observed a fairly distributed awareness of policies around shadow IT, highlighting communication gaps. Moreover, we find that conversations with colleagues about technology use, both formal and informal, were found across different ranks and groups, though some reported no such discussions. Finally, we find that shadow IT presents a dichotomy: a push towards non-standard solutions for efficiency and cost reasons, balanced against a broad awareness of significant risks. We find the mental models of this dichotomy categorized into *risk-averse* and *risk-taking* mental models. Collectively we identify ten different mental models. Moreover, we find that individuals hold a combination of those mental models based on their age, experience, educational background, and awareness in a given situation.

SQ4: *What patterns are found across cohorts regarding shadow IT mental models?*

When exploring the distribution of mental models across departments, we discovered that the risk-averse models were common among the *client-facing* and *management* departments. We observe this as a reflection of the nature of the work that employees perform in these departments.

We encounter the *Consequence-Avoidance Orientation* and *Knowledge-Based Conservatism* models across all ranks, indicating a fundamental understanding and caution regarding shadow IT's potential risks due to the significant presence of awareness through organization-wide training programs. Interestingly, we observe models like *Risk Transfer Mindset* and *Cautious Seasoned Judgment* across higher ranks, influencing secure behavior with regard to shadow IT. This emphasizes the importance of senior leadership in an organization.

8.2 Scientifical Implications

We contribute to the body of science through an SLR on the creation of mental models within the cybersecurity domain. In doing so we provide an overview of the topics that have been addressed with mental models within this field of research. In addition, we provide a methodological overview of how mental models are elicited and represented. We illustrate the cohorts that have been researched and how participants have been recruited. This provides an overview and guidelines for other researchers if they want to conduct mental model research in cybersecurity. Moreover, the aggregated survey data, interview transcripts, and the associated codebook will be available to support further research on this topic.

By extracting mental models, we provide a more nuanced understanding of how employees perceive shadow IT and how these perceptions influence shadow IT decisions. We identify ten distinct mental models that influence the behavior of individuals. The identification of the combination of mental models revealed gaps in understanding and illustrated itself through contradicting statements in interviews. By illustrating these aspects, this research paves the way for a deeper understanding of what different combinations of mental models lead to certain shadow IT behavior.

Even though we did not uncover a clear pattern between cohorts and their mental models, we do observe different mental models in different groups of individuals. This research, therefore, does highlight the importance of doing mental model research across different groups of end-users. To account for all the different mental models present across larger populations.

8.3 Organizational Recommendations

The identification of different mental models and their influence on shadow IT usage within the organization carries significant implications for policy, practice, and organizational culture. We, therefore, recommend trying to **support the adoption of the risk-aversing mental models and demotivate the use of risk-taking mental models** among employees.

Moreover, we name a few general recommendations and a few for specific mental models:

- **Identify most prevalent mental models in an organization** - We have seen a varying number of mental models in an organization. However, due to the specifics of the setting of this research, other organizations' employees might employ different mental models influencing their shadow IT behavior. Therefore we encourage organizations to uncover what mental models are present within their employee group to be able to cater to the variety of present mental models. In doing so, organizations can both cater to technical solutions that mitigate threats introduced by these mental models. Moreover, an organization can make employees aware of certain mental models they have through their training program and therefore try to reduce the negative influences on their shadow IT behavior.
- **Continue the open lines of communication regarding shadow IT** - During the interviews, we found several means of discussing the use of technology. By fostering an

environment where employees feel safe and comfortable discussing their technology needs, organizations can identify and address potential shadow IT instances. This approach not only can mitigate risks associated with shadow IT use but also builds trust between the IT department and other employees, creating a more cooperative and secure digital work environment.

- **Maintain high awareness through training** - We have seen significant awareness of the possible negative consequences of shadow IT due to periodic mandatory training. Even though we did not analyze the occurrence of mental models quantitatively, we found that this constant reminder of possible threats and consequences was the most mentioned and therefore a positive impact on the shadow IT behavior of employees. Therefore we recommend a strong focus on spreading the perceived consequences of shadow IT through training. However, we observed that an abundance of training may result in reduced employee concentration. Consequently, it is necessary to provide a well-balanced approach regarding the quantity of training each employee is required to undertake, striving for an optimal balance.
- **Create shadow IT protocols** - During the interviews, we uncovered *Performace-Driven Rule Bending*. This research illustrates the presence of this phenomenon in the organization. Understanding this, organizations can develop protocols that support individuals in navigating rule-bending situations, thus influencing a rule-bending approach that is as safe as possible. This allows the organization to get a better grasp on the introduction of shadow IT instances and potentially find areas to provide structural long-term solutions.
- **Track down long-term instances** - Through the interviews we identified *Longevity-Based Invincibility*: the team-wide-long-term adoption of shadow IT tools. Now that its presence is evident, therefore knowing that there are teams within the organization that use long-term-adopted shadow IT tools, the organization can track these down and provide long-term managed solutions for each of the identified instances. Moreover, the organization can try and uncover why these were introduced, and why these tools have been adopted for such a long time period without anyone noticing.
- **Targeted training** - We also found the need for more targeted education and effective policy communication. We found examples of the *support* group who had to do training that was not relevant to them and therefore the overall perception of training is seen as less important. Therefore we recommend that the contents of the training are catered to employees.

8.4 Limitations of the study

We already provided the limitations for the survey in section 5.5 and for the interview in section 6.6. In this section we summarize those and provide limitations for the research as a whole.

We discover that the number of respondents in the survey is representative of that of the larger organization, resulting in a majority of responses from the *client-facing* group. This resulted in

fewer respondents for the other groups. Few responses and uneven group sizes can jeopardize the assumptions of the Chi-square test, where 80% of cells must contain a value greater than 5. Thus we adopted Fisher's exact test as an additional analysis to use when the assumptions of the Chi-square test were violated.

Both the department and rank cohorts have a *management* group, with the department and rank cohorts holding 26 and 39 responses respectively. We find this discrepancy due to the fact that some participants in the management staff responded on behalf of the teams they manage. This discrepancy was only present during the survey and may have impacted the results between the *client facing* and *management* group.

In addition, we find that the survey's answer options limit our understanding of certain aspects, especially regarding self-installed applications. We tried to mitigate this through three rounds of pilot testing with various individuals, but we overlooked certain demographic spreads. We validate the shortcoming of having to provide answer options in the survey through the answers we received during the interviews. We find a number of self-installed applications that participants mentioned that were not in the survey options.

Moreover, we identified answers with challenging explanations, especially from the *support* group, whose primary role is to perform internal tasks. Despite this, we found instances of their presence in specific client projects. This suggests they might have misunderstood the survey or were not focused enough when filling out the survey.

We also find limitations during the interviews, firstly the data gap due to the lack of participants from the *IT* team. Moreover, we have a single interview protocol used across a very diverse participant pool. This led to certain questions being hard for one participant, whereas it was too easy for another participant and therefore could have led to various understandings of the concept of shadow IT. To keep the flow of the interview going, we provided examples of specific applications, that potentially introduce bias in participant responses.

Furthermore, our interviews revealed a low tendency for the client-facing group to consult with IT in problem scenarios. Upon informal investigation, we learned that such consultation is a basic step for many, suggesting that the nature of our interview prompt influenced the participants' responses. Therefore, this step of approaching the IT team was often overlooked.

The most apparent limitation of the interviews is that we were unable to recruit any participants from the *IT* department. Even though this team is part of the *support* group, we could aggregate the two in terms of work type and role in the organization. We scoped this research to contain separate data from the team that sets shadow IT mitigation policy and controls the IT governance. This is an unfortunate data gap and challenges comparisons from other teams with the governing entity in such an organization.

8.5 Discussion

We have identified ten different mental models of shadow IT. This is the list of the mental models that were present in the participant group. However, this list is *not* complete as there may be other mental models present within the organization. We tried to mitigate this by diversifying the participants through clustering, however, there might be a variance in the presence of mental models within these clusters. Therefore, our sample size is not large enough to state that we have encompassed all mental models. On that same note, there might be different levels of aggregating certain mental models in occurrences within the organization that we might have missed due to the sampling. Finally, we have not grounded exactly what the behavioral change is of each identified mental model.

The section 7.2 uses radar charts to illustrate the prevalence trends across various cohorts. When analyzing the presence of mental models, one might question why some mental models are absent in certain cohorts. For instance, we did not observe the *Risk Transfer Mindset* within the *Management* group, which is surprising since this mental model is typically expected in this group as risk transfer allows them to evade responsibility. These gaps in mental model patterns between our findings and anticipated results could stem from a too-small sample size per cohort.

We observed some discrepancies between interview responses and survey results. Specifically, that meant individuals named more shadow IT instances during the survey than during the interviews. This could be due to a reduced inclination to self-incriminate during a face-to-face conversation compared to an impersonal survey. Furthermore, while both interviews and surveys were oriented around shadow IT, we intentionally employed more subtle language in the survey, referring to it as *the gap between the technology you use, and what is provided by organization*. This softer approach may have influenced the difference in responses.

Due to the specific nature of individuals within this research, the found mental models may only be suitable for this organization. Or organizations very similar, and these might not be very generalizable. However, this research does provide a roadmap of the steps to take in order to uncover similar results and might create a frame of reference for other sectors.

We have tried to formalize how shadow IT is perceived among employees in a large professional services company. However, in general, it is hard to formalize, store, and handle mental models. Future research might try to uncover better management of mental models. This will allow for more structured mental model research.

9 Conclusion

In this chapter, we answer the main research question:

MRQ: *What are the implications of the similarities and differences in shadow IT mental models across different cohorts in a large organization?*

To answer the main research question, this thesis investigated the perception of the concept of shadow IT, the occurrence of shadow IT, the mental models associated with it, and how it varies across different cohorts in a large organization. We find that shadow IT is an integral part of the organization's IT environment. It occurs in many different forms, including *cloud services*, *self-installed applications*, *self-built solutions*, and *personal devices*, with users opting for familiar tools and services to meet work or personal requirements.

Most threats associated with shadow IT revolve around risks such as *data leaks*, *malware*, *unauthorized access*, *non-central governance*, *reputational damage*, *ransomware*, *misinformation*, and *outdated software*. These risks are, however, perceived differently across the cohorts, reflecting varying degrees of risk awareness and actions toward mitigating these risks. Despite this awareness, we found inconsistencies and gaps in acting on this awareness, resulting in an *awareness-action gap*.

The understanding and perception of shadow IT across cohorts is conceptualized through ten different mental models. This varies from *risk-averse* to *risk-taking* mental models, and individuals typically hold a combination of these based on a number of personal factors, work-related factors, and in a given situation. We found that it is a combination of these mental models that influence individuals' shadow IT behavior.

We observe a few similarities across the cohorts, namely the universally present *Consequence-Avoidance Orientation*. Meaning that throughout the entire organization, employees are well aware of the consequences that shadow IT can bring. We encounter the *Misguided Sense of Protection* and *Longevity-based Invincibility* across all departments, and find *Knowledge-Based Invincibility* across all ranks. Moreover, we find differences in the combinations of mental models that participants have.

This research provides comprehensive and practical insights into the employee perception of shadow IT. It led to the identification of shadow IT's dichotomous nature: *a push towards non-standard solutions for efficiency and cost reasons, balanced against a broad awareness of significant risks*.

To manage the challenges related to shadow IT, we recommended measures such as fostering an environment where employees can openly discuss their technology needs, maintaining high awareness through training, creating shadow IT protocols for certain scenarios, and implementing mental model targeted training. This investigation of shadow IT, while providing practical insights and recommendations, also identifies the need for future work in understanding the behavioral impact of the combination of mental models of shadow IT. By exploring these implications, organizations can better manage shadow IT, minimizing potential risks while maximizing its benefits.

Our research uncovered a distinct number of shadow IT mental models existing within an organization, the implies that there is a wide variety of distinct mental models in an organization. These mental models are not present only in particular cohort groups, however, certain patterns linking certain combinations of mental models to certain cohort groups did emerge. This suggests that organizations could identify a list of different types of mental models present within their organization. After doing so, organizations could incorporate these mental models into the design of their training program to modify the presence that individuals have with regard to certain mental models.

9.1 Future work

This research leaves a gap for the mental models of the *IT staff* since we were unable to recruit any participants from that department. Future research could try to fill this gap.

In addition, future research might validate the found mental models with other participants in a similar organization and then explore how these mental models are combined and lead to a decision-making process in a game-like setting.

Continuing our line of research, future work could involve exploring the extent of variations of combinations of shadow IT mental models and the impact of several combinations on shadow IT behaviors. Moreover, this could uncover and propose interventions supporting more secure behavior by stimulating risk-averse mental models and validating them.

We have observed that individuals can hold a combination of different mental models. However, we did not uncover to what extent certain mental models are present. Rather than just a combination of different mental models, future research could set out to find out to what degree certain mental models are present in a certain situation. One might expect that a mental model is not present or absent, however, it can be present to some degree. Moreover, this research may find if there is a prioritization of certain mental models due to certain situational aspects.

We observed that shadow IT instances are not limited to individual users but also involve departments or smaller groups within an organization. We have taken certain cohorts to horizontally and vertically divide the employee group for analysis. However, we have not seen obvious patterns of shadow IT instances across our chosen cohorts. Future research might uncover what different cohorts provide the most optimal division of individual groups so that

clear patterns of the presence of combinations of shadow IT mental models in certain groups become apparent.

9.2 Data repository

The de-identified interview transcripts and aggregated survey results collected in this research project can be requested by email from the supervisor, Kate Labunets. At the thesis publication date, her email is k.labunets@uu.nl.

Acknowledgements

First of all, I would like to give a token of appreciation to my supervisors at UU and my external supervisor. Your guidance and feedback have been so valuable, not only in for the content and process of this thesis, but also for me personally. I can confidently say I have grown significantly, both academically and personally, thanks to your mentorship and support. The process of this thesis has left its mark by solidifying the first step of my career.

I want to express my heartfelt gratitude to all the participants that helped me during this thesis. I was surprised by the level of interest you showed in my research and the eagerness to contribute and learn more about my work.

Bibliography

Abdi, Noura, Kopo M Ramokapane, and Jose M Such (Aug. 2019). "More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants." In: *Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS)*.

Abu-Salma, Ruba and Benjamin Livshits (2020). "Evaluating the end-user experience of private browsing mode". In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–12.

Ajzen, Icek (1991). "The theory of planned behavior". In: *Organizational behavior and human decision processes* 50.2, pp. 179–211.

Akgul, Omer, Wei Bai, Shruti Das, and Michelle L Mazurek (2021). "Evaluating In-Workflow Messages for Improving Mental Models of End-to-End Encryption." In: *USENIX Security Symposium*, pp. 447–464.

Aksnes, Dag W, Liv Langfeldt, and Paul Wouters (2019). "Citations, citation indicators, and research quality: An overview of basic concepts and theories". In: *Sage Open* 9.1.

Albalawi, Tahani, Kambiz Ghazinour, and Austin Melton (2017). "Security mental model: Cognitive map approach". In: *Proceedings of the 4th International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, pp. 74–79.

Asgharpour, Farzaneh, Debin Liu, and L Jean Camp (Feb. 2007). "Mental models of security risks". In: *Proceedings of the 11th Financial Cryptography and Data Security*, pp. 367–377.

Baig, Khadija, Elisa Kazan, Kalpana Hundlani, Sana Maqsood, and Sonia Chiasson (Aug. 2021). "Replication: Effects of Media on the Mental Models of Technical Users." In: *Proceedings of the 17th Symposium on Usable Privacy and Security (SOUPS)*, pp. 119–138.

Baig, Khadija, Reham Mohamed, Anna-Lena Theus, and Sonia Chiasson (2020). "" I'm hoping they're an ethical company that won't do anything that I'll regret" Users Perceptions of At-home DNA Testing Companies". In: *Proceedings of the 2020 CHI conference on human factors in computing systems*, pp. 1–13.

Barbour, Rosaline S (2001). "Checklists for improving rigour in qualitative research: a case of the tail wagging the dog?" In: *British Medical Journal* 322.7294, pp. 1115–1117.

Beasley, T Mark and Randall E Schumacker (1995). "Multiple regression approach to analyzing contingency tables: Post hoc and planned comparison procedures". In: *The Journal of Experimental Education* 64.1, pp. 79–93.

Benenson, Zinaida, Olaf Kroll-Peters, and Matthias Krupp (2012). "Attitudes to IT security when using a smartphone". In: *Proceedings of the 2012 Federated Conference on Computer Science and Information Systems (FedCSIS)*. IEEE, pp. 1179–1183.

Bieringer, Lukas, Kathrin Grosse, Michael Backes, Battista Biggio, and Katharina Krombholz (Aug. 2022). "Industrial practitioners' mental models of adversarial machine learning". In: *Proceedings of the 18th Symposium on Usable Privacy and Security (SOUPS)*, pp. 97–116.

Binkhorst, Veroniek, Tobias Fiebig, Katharina Krombholz, Wolter Pieters, and Katsiaryna Labunets (Aug. 2022). "Security at the End of the Tunnel: The Anatomy of VPN Mental Models Among Experts and Non-Experts in a Corporate Context". In: *Proceedings of the 31th USENIX Security Symposium (USENIX Security)*, pp. 3433–3450.

Blythe, Jim and L Jean Camp (July 2012). "Implementing mental models". In: *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS)*, pp. 86–90.

Boltzmann, Ludwig (1890). "Die Hypothese van't Hoffs über den osmotischen Druck vom Standpunkte der kinetischen Gastheorie". In: *Zeitschrift für physikalische Chemie* 6.1, pp. 474–480.

Bravo-Lillo, Cristian, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri (2010). "Bridging the gap in computer security warnings: A mental model approach". In: *IEEE Security & Privacy* 9.2, pp. 18–26.

Brereton, Pearl, Barbara A Kitchenham, David Budgen, Mark Turner, and Mohamed Khalil (2007). "Lessons from applying the systematic literature review process within the software engineering domain". In: *Journal of systems and software* 80.4, pp. 571–583.

Brodsky, Jessica E, Arshia K Lodhi, Kasey L Powers, Fran C Blumberg, and Patricia J Brooks (2021). ""It's just everywhere now": Middle-school and college students' mental models of the Internet". In: *Human Behavior and Emerging Technologies* 3.4, pp. 495–511.

Bygstad, Bendik (2015). "The coming of lightweight IT". In.

Byrd, Terry Anthony, Kathy L Cossick, and Robert W Zmud (1992). "A synthesis of research on requirements analysis and knowledge acquisition techniques". In: *MIS quarterly*, pp. 117–138.

Camp, L Jean (Oct. 2006). "Mental models of privacy and security". In: *IEEE Technology and society magazine* 28.3, pp. 37–46.

Castillo-Montoya, Milagros (2016). "Preparing for interview research: The interview protocol refinement framework". In: *The qualitative report* 21.5, pp. 811–831.

Chen, Jing (2020). "Risk communication in cyberspace: A brief review of the information-processing and mental models approaches". In: *Current opinion in psychology* 36, pp. 135–140.

Conover, William Jay (1999). *Practical nonparametric statistics*. Vol. 350. john wiley & sons.

Coopamootoo, Kovila PL and Thomas Groß (2014). "Mental models for usable privacy: A position paper". In: *Proceedings of Human Aspects of Information Security, Privacy, and Trust: Second International Conference (HAS 2014)*. Springer, pp. 410–421.

Craik, Kenneth James Williams (1967). *The nature of explanation*. Vol. 445. CUP Archive.

Dhillon, Gurpreet, Tiago Oliveira, Santa Susarapu, and Mario Caldeira (2016). "Deciding between information security and usability: Developing value based objectives". In: *Computers in Human Behavior* 61, pp. 656–666.

Dutkowska-Zuk, Agnieszka, Austin Hounsel, Amy Morrill, Andre Xiong, Marshini Chetty, and Nick Feamster (Aug. 2022). "How and Why People Use Virtual Private Networks". In: *Proceedings of the 31th USENIX Security Symposium (USENIX Security)*, pp. 3451–3465.

Fisher, Ronald Aylmer (1992). *Statistical methods for research workers*. Springer.

Fogg, Brian J (2009). "A behavior model for persuasive design". In: *Proceedings of the 4th international Conference on Persuasive Technology*, pp. 1–7.

Forbes Insights (May 2019). "Perception Gaps in Cyber Resilience: Where are Your Blind Spots?" In: *Forbes*. URL: https://www.ibm.com/downloads/cas/KDL0MBN0 (visited on 02/18/2023).

French, Aaron M, Chengqi Guo, and Jung P Shim (2014). "Current status, issues, and future of bring your own device (BYOD)". In: *Communications of the Association for Information Systems* 35.1, p. 10.

Friedman, Batya, David Hurley, Daniel C Howe, Edward Felten, and Helen Nissenbaum (Apr. 2002). "Users' conceptions of web security: a comparative study". In: *Proceedings of the 2002 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pp. 746–747.

Fulton, Kelsey R, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L Mazurek (Aug. 2019). "The effect of entertainment media on mental models of computer security". In: *Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS)*, pp. 79–95.

Furman, Susanne, Mary Frances Theofanos, Yee-Yin Choong, and Brian Stanton (Mar.–Apr. 2011). "Basing cybersecurity training on user perceptions". In: *IEEE Security & Privacy* 9.2, pp. 40–49.

Furnell, Steve M, Peter Bryant, and Andrew D Phippen (2007). "Assessing the security perceptions of personal Internet users". In: *Journal of Computer Security* 26.5, pp. 410–417.

Gadellaa, Joost (2022). "Cyber Threats of Shadow IT in Dutch Higher Education and Research". MA thesis. Utrecht University.

Garcia, Lucia and Francis Quek (May 1997). "Qualitative research in information systems: time to be subjective?" In: *Proceedings of the 8th International Federation for Information Processing (IFIP)*, pp. 444–465.

Gerber, Nina, Verena Zimmermann, and Melanie Volkamer (2019). "Why johnny fails to protect his privacy". In: *Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, pp. 109–118.

Godefroid, Marie-E, Ralf Plattfaut, and Björn Niehaves (2021). "IT outside of the IT Department: Reviewing Lightweight IT in Times of Shadow IT and IT Consumerization". In: *Innovation Through Information Systems: Volume III: A Collection of Latest Research on Management Issues*. Springer, pp. 554–571.

Greenwood, Priscilla E and Michael S Nikulin (1996). *A guide to chi-squared testing*. Vol. 280. John Wiley & Sons.

Gregor, Shirley (2006). "The nature of theory in information systems". In: *MIS quarterly*, pp. 611–642.

Greyson, Devon, Heather O'Brien, and Jean Shoveller (2017). "Information world mapping: A participatory arts-based elicitation method for information behavior interviews". In: *Library & Information Science Research* 39.2, pp. 149–157.

Guest, Greg, Arwen Bunce, and Laura Johnson (2006). "How many interviews are enough? An experiment with data saturation and variability". In: *Field methods* 18.1, pp. 59–82.

Gusenbauer, Michael and Neal R Haddaway (2020). "Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources". In: *Research synthesis methods* 11.2, pp. 181–217.

Haag, Steffi and Andreas Eckhardt (2015). "Justifying shadow IT usage". In.

– (2017). "Shadow it". In: *Business & Information Systems Engineering* 59.6, pp. 469–473.

Haberman, Shelby J (1973). "The analysis of residuals in cross-classified tables". In: *Biometrics*, pp. 205–220.

Hassanzadeh, Zahra, Robert Biddle, and Sky Marsen (2021). "User perception of data breaches". In: *IEEE Transactions on Professional Communication* 64.4, pp. 374–389.

Horvath, Amber, Mariann Nagy, Finn Voichick, Mary Beth Kery, and Brad A Myers (2019). "Methods for investigating mental models for learners of APIs". In: *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–6.

Hudson-Doyle, Emma E, Sara E Harrison, Stephen R Hill, Matt Williams, Douglas Paton, and Ann Bostrom (2022). "Eliciting mental models of science and risk for disaster communication: A scoping review of methodologies". In: *International Journal of Disaster Risk Reduction*, p. 103084.

Ilyas, Ihab F and Xu Chu (2019). *Data cleaning*. Morgan & Claypool.

Javed, Yousra and Mohamed Shehab (2013). "Access control policy misconfiguration detection in online social networks". In: *Proceedings of the 2013 International Conference on Social Computing (SOCIALCOM 2013)*. IEEE, pp. 544–549.

Johnson, Steve (2013). "Bringing IT out of the shadows". In: *Network Security* 2013.12, pp. 5–6.

Johnson-Laird (1983). *Mental models: Towards a cognitive science of language, inference, and consciousness*. 6. Harvard University Press.

– (2005). "Mental models and thought". In: *The Cambridge handbook of thinking and reasoning*, pp. 185–208.

Jones, Natalie A, Helen Ross, Timothy Lynam, Pascal Perez, and Anne Leitch (2011). "Mental models: an interdisciplinary synthesis of theory and methods". In: *Ecology and society* 16.1.

Kahneman, Daniel, Dan Lovallo, and Olivier Sibony (2011). "Before you make that big decision". In: *Harvard business review* 89.6, pp. 50–60.

Kang, Ruogu, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler (July 2015). "my data just goes everywhere:" user mental models of the internet and implications for privacy and security". In: *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS)*, pp. 39–52.

Käss, Sebastian, Marie Godefroid, Vincent Borghoff, Susanne Strahringer, Markus Westner, and Ralf Plattfaut (2021). "Towards a taxonomy of concepts describing IT outside the IT department". In: *Proceedings of the 32nd Australasian Conference on Information Systems (ACIS2021)*.

Kauer, Michaela, Sebastian Günther, Daniel Storck, and Melanie Volkamer (2013). "A comparison of American and German folk models of home computer security". In: *Proceedings of Human Aspects of Information Security, Privacy, and Trust: First International Conference (HAS 2013)*. Springer, pp. 100–109.

Kauer, Michaela, Florian Kiesel, Felix Ueberschaer, Melanie Volkamer, and Ralph Bruder (2012). "The influence of trustworthiness of website layout on security perception of websites". In.

Keele, Staffs et al. (2007). *Guidelines for performing systematic literature reviews in software engineering*.

Kitchenham, Barbara (2004). "Procedures for performing systematic reviews". In: *Keele, UK, Keele University* 33.2004, pp. 1–26.

Knockel, Jeffrey, Adam Senft, and Ronald J Deibert (Aug. 2016). "Privacy and Security Issues in BAT Web Browsers." In: *Proceedings of the 6th USENIX Workshop on Free and Open Communications on the Internet (FOCI)*.

Kopper, Andreas, Daniel Fürstenau, Stephan Zimmermann, Stefan Klotz, Christopher Rentrop, Hannes Rothe, Susanne Strahringer, and Markus Reihlen (2018). "Shadow IT and Business-Managed IT: A Conceptual Framework and Empirical Illustration". In: *International Journal of IT/Business Alignment and Governance* 9.2 (July-December), pp. 53–71.

Kopper, Andreas and Markus Westner (2016). "Towards a taxonomy for shadow IT". In.

Kretzer, Martin and Alexander Maedche (2014). *Generativity of business intelligence platforms: a research agenda guided by lessons from shadow IT*. Univ. Mannheim.

Krippendorff, Klaus (2011). "Computing Krippendorff's alpha-reliability". In.

Krombholz, Katharina, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel Von Zezschwitz (May 2019). ""' If HTTPS Were Secure, I Wouldn't Need 2FA"-End User and Administrator Mental Models of HTTPS". In: *Proceedings of the 40th IEEE Symposium on Security & Privacy (S&P)*, pp. 246–263.

Langan-Fox, Janice, Sharon Code, and Kim Langfield-Smith (June 2000). "Team mental models: Techniques, methods, and analytic approaches". In: *Human Factors* 42.2, pp. 242–271.

Liljestrand, Isaiah, Marcelo Gonzales, and Dongwan Shin (2019). "Developing a mental model for use in the context of computer security". In: *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, pp. 2336–2339.

Lin, Jialiu, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang (Sept. 2012). "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing". In: *Proceedings of the ACM Conference on Ubiquitous Computing*, pp. 501–510.

Liu, Debin, Farzaneh Asgharpour, and L Jean Camp (Feb. 2007). "Risk communication in security using mental models". In: Lecture Notes in Computer Science 4886, pp. 1–12.

Mai, Alexandra, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz (2020). "User Mental Models of Cryptocurrency Systems—-A Grounded Theory Approach". In.

Maier, Janosch, Arne Padmos, Mortaza S Bargh, and Wolfgang Wörndl (n.d.). "Influence of Mental Models on the Design of Cyber Security Dashboards." In: pp. 128–139.

Mallmann, Gabriela Labres, Aline de Vargas Pinto, and Antônio Carlos Gastaud Maçada (2018). "Shedding Light on Shadow IT: Definition, Related Concepts, and Consequences". In: *Proceedings of the 18th Conference of the Portuguese Association for Information Systems*, pp. 63–79.

Märki, Heike, Miriam Maas, Michaela Kauer-Franz, and Marius Oberle (2016). "Increasing software security by using mental models". In: *Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity*. Springer, pp. 347–359.

Marky, Karola, Sarah Prange, Max Mühlhäuser, and Florian Alt (2021). "Roles matter! Understanding differences in the privacy mental models of smart home visitors and residents". In: *Proceedings of the 20th International Conference on Mobile and Ubiquitous Multimedia*, pp. 108–122.

Marshall, Bryan, Peter Cardon, Amit Poddar, and Renee Fontenot (2013). "Does sample size matter in qualitative research?: A review of qualitative interviews in IS research". In: *Journal of computer information systems* 54.1, pp. 11–22.

McHugh, Mary L (2013). "The chi-square test of independence". In: *Biochemia medica* 23.2, pp. 143–149.

Meline, Timothy (2006). "Selecting studies for systemic review: Inclusion and exclusion criteria". In: *Contemporary issues in communication science and disorders* 33.Spring, pp. 21–27.

Mingay, S (2014). "Embracing and creating value from shadow IT". In: *Gartner Group Research: Published* 9.

Mohamed, Mona A, Joyram Chakraborty, and Josh Dehlinger (2017). "Trading off usability and security in user interface design through mental models". In: *Behaviour & Information Technology* 36.5, pp. 493–516.

Morgan, M Granger, Baruch Fischhoff, Ann Bostrom, and Cynthia J Atman (2002). *Risk communication: A mental models approach*. Cambridge University Press.

Norman, Donald A (2014). "Some observations on mental models". In: *Mental models*, pp. 15–22.

Norman, Paul, Henk Boer, Erwin R Seydel, and Barbara Mullan (2015). "Protection motivation theory". In: *Predicting and changing health behaviour: Research and practice with social cognition models* 3, pp. 70–106.

Oates, Maggie, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Cranor (Oct. 2018). "Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration". In: *Proceedings on Privacy Enhancing Technologies* 2018, pp. 5–32.

Orduña-Malea, Enrique, Juan M Ayllón, Alberto Martin-Martin, and Emilio Delgado López-Cózar (2015). "Methods for estimating the size of Google Scholar". In: *Scientometrics* 104, pp. 931–949.

Payne, Stephen J (1991). "A descriptive study of mental models". In: *Behaviour & Information Technology* 10.1, pp. 3–21.

Petticrew, Mark and Helen Roberts (2008). *Systematic reviews in the social sciences: A practical guide*. John Wiley & Sons.

Raja, Fahimeh, Kirstie Hawkey, Steven Hsu, Kai-Le Wang, and Konstantin Beznosov (May 2011). "Promoting a physical security mental model for personal firewall warnings". In: *Proceedings of the 2011 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pp. 1585–1590.

Ramokapane, Kopo Marvin, Awais Rashid, and Jose Such (2017). "" I feel stupid I can't delete..."":: a study of users' cloud deletion practices and coping strategies". In.

Renaud, Karen, Stephen Flowerday, Rosanne English, and Melanie Volkamer (2016). "Why don't UK citizens protest against privacy-invading dragnet surveillance?" In: *Information & Computer Security* 24.4, pp. 400–415.

Renaud, Karen, Melanie Volkamer, and Arne Renkema-Padmos (2014). "Why doesn't Jane protect her privacy?" In: *Proceedings of the 14th International Symposium for Privacy Enhancing Technologies: (PETS 2014)*. Springer, pp. 244–262.

Richardson, George P, David F Andersen, Terrence A Maxwell, and Thomas R Stewart (1994). "Foundations of mental model research". In: *Proceedings of the 12th International Conference of the System Dynamics Society*, pp. 181–192.

Rohrmann, Bernd (1992). "The evaluation of risk communication effectiveness". In: *Acta psychologica* 81.2, pp. 169–192.

Rowe, Anna L and Nancy J Cooke (1995). "Measuring mental models: Choosing the right tools for the job". In: *Human resource development quarterly* 6.3, pp. 243–255.

Schaewitz, Leonie, David Lakotta, M Angela Sasse, and Nikol Rummel (2021). "Peeking Into the Black Box: Towards Understanding User Understanding of E2EE". In: *Proceedings of the 2021 European Symposium on Usable Security*, pp. 129–140.

Sharpe, Donald (2015). "Chi-square test is statistically significant: Now what?" In: *Practical Assessment, Research, and Evaluation* 20.1, p. 8.

Silic, Mario and Andrea Back (2014). "Shadow IT–A view from behind the curtain". In: *Computers & Security* 45, pp. 274–283.

Simes, R John (1986). "An improved Bonferroni procedure for multiple tests of significance". In: *Biometrika* 73.3, pp. 751–754.

Spero, Eric and Robert Biddle (2020). "Home and Away: UI Design Patterns for Supporting End-User Security". In: *Proceedings of the European Conference on Pattern Languages of Programs 2020*, pp. 1–9.

Staggers, Nancy and Anthony F. Norcio (Dec. 1993). "Mental models: concepts for human-computer interaction research". In: *International Journal of Man-machine studies* 38.4, pp. 587–605.

Thompson, Nik and Tanya McGill (2017). "Mining the Mind–Applying Quantitative Techniques to Understand Mental Models of Security". In.

Tolsdorf, Jan and Florian Dehling (Feb. 2020). "In our employer we trust: mental models of office workers' privacy perceptions". In: *Proceedings of the 24th Financial Cryptography and Data Security*, pp. 122–136.

Turner, Daniel W (2010). "Qualitative Interview Design: A Practical Guide for Novice Investigators". In: *The Qualitative Report* 15.3, pp. 754–760.

Velykoivanenko, Lev, Kavous Salehzadeh Niksirat, Noé Zufferey, Mathias Humbert, Kévin Huguenin, and Mauro Cherubini (2021). "Are those steps worth your privacy? Fitness-tracker users' perceptions of privacy and utility". In: *Proceedings of the 5th ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5.4, pp. 1–41.

Volkamer, Melanie and Karen Renaud (2013). "Mental models–general introduction and review of their application to human-centred security". In: *Number Theory and Cryptography: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday*, pp. 255–280.

Votipka, Daniel, Seth M Rabin, Kristopher Micinski, Jeffrey S Foster, and Michelle M Mazurek (2020). "An observational investigation of reverse engineers' processes". In: *Proceedings of the 29th USENIX Conference on Security Symposium*, pp. 1875–1892.

Walters, Richard (2013). "Bringing IT out of the shadows". In: *Network Security* 2013.4, pp. 5–11.

Wash, Rick (2010). "Folk models of home computer security". In: *Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS 2010)*, pp. 1–16.

Wash, Rick and Emilee Rader (2011). "Influencing mental models of security: a research agenda". In: *Proceedings of the 2011 New Security Paradigms Workshop*, pp. 57–66.

– (July 2015). "Too much knowledge? security beliefs and protective behaviors among united states internet users". In: *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS)*, pp. 309–325.

Wästlund, Erik, Julio Angulo, and Simone Fischer-Hübner (2012). "Evoking comprehensive mental models of anonymous credentials". In: *Proceedings of Open Problems in Network Security: IFIP International Workshop (IFIP 2011)*. Springer, pp. 1–14.

Winter, Philipp, Anne Edmundson, Laura M Roberts, Agnieszka Dutkowska-Żuk, Marshini Chetty, and Nick Feamster (Aug. 2018). "How do tor users interact with onion services?" In: *Proceedings of the 27th USENIX Security Symposium (USENIX Security)*, pp. 411–428.

Wohlin, Claes (2014). "Guidelines for snowballing in systematic literature studies and a replication in software engineering". In: *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, pp. 1–10.

Wu, Justin and Daniel Zappala (June 2018). "When is a Tree Really a Truck? Exploring Mental Models of Encryption". In: *Proceedings of the 14th Symposium on Usable Privacy and Security (SOUPS)*, pp. 395–409.

Wu, L Min, Robert C Miller, and Garfinkel (Apr. 2006). "Do security toolbars actually prevent phishing attacks?" In: *Proceedings of the 2006 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pp. 601–610.

Yan, Jie Kevin, Nebojsa Milic, Hope Koch, Patrick Curry, et al. (2016). "IT consumerization and new IT practices: Discriminating, firefighting and innovating". In.

Zhou, Xin, Yuqin Jin, He Zhang, Shanshan Li, and Xin Huang (Dec. 2016). "A map of threats to validity of systematic literature reviews in software engineering". In: *Proceedings of the 23rd Asia-Pacific Software Engineering Conference (APSEC)*. IEEE, pp. 153–160.

Zimmermann, Stephan and Christopher Rentrop (June 2012). "Schatten-IT". In: *HMD Praxis der Wirtschaftsinformatik* 49.6, pp. 60–68.

Zou, Yixin, Abraham H Mhaidli, Austin McCall, and Florian Schaub (June 2018). “" I’ve Got Nothing to Lose": Consumers’ Risk Perceptions and Protective Actions after the Equifax Data Breach.” In: *Proceedings of the 14th Symposium on Usable Privacy and Security (SOUPS)*, pp. 197–216.

Zou, Yixin and Florian Schaub (Apr. 2018). “Concern But No Action: Consumers’ Reactions to the Equifax Data Breach”. In: *Proceedings of the 2018 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pp. 1–6.

A Data Management Plan

Created using DMPonline (Digital Curation Centre (DCC), 2022) for the project 'Mental Models of Shadow IT'

Data collection

1.1 Will you re-use existing data ? f yes: explain which existing data you will re-use and under which terms of use.

- No, I will be collecting/generating new data

1.2 Describe your data. Fill the table below with a brief description of the data, including the type, format and volume.

Data Description	*Data Type*	*Format*	*Total Volume*
Interview recordings	Audio	.mp3	<20GB
Interview transcripts	Text	.docx	<100MB
Organized and analyzed transcripts	ATLAS.ti project	.altproj	<200MB
Informed consent forms	Text	.pdf	<10MB
Aggregated survey data	Tabular	.csv	<10MB
Survey analysis	R script	.R	<5MB

TABLE A.1

Data documentation

2.1 Describe the documentation and metadata that you will use to to make your data reproducible and interoperable. Describe which files you will provide, along with a brief description of the information they will contain, to make your data reproducible and interoperable. Describe the information that you will provide to make the data items in questions 2.1 reusable and interoperable. If using a specific metadata standard, please mention this below

- For the project as a whole, a README.md file will be written with references to published documentation of methods; the completed master's thesis.
- For both the audio files as well as the transcripts, the metadata will consist of only the file metadata (size, time of creation, duration, quality) while the file name (see 2.2) should provide the context necessary for re-use.
- Pseudonym identifiers will be stored with the recordings to make sure these are not accidentally shared together with the transcripts.
- Although not an open standard, the ATLAS.ti project is interoperable with other software from QSR, MaxQDA and Framework.
- Survey data will be collected anonymously and stored in a .csv format.

2.2 Describe the folder structure you will provide to make your data reproducible and interoperable. Describe the folder structure, naming conventions and/or version control you will use for this project.

The folder structure will contain a folder for the recordings, (anonymized) transcripts and the project as follows:

> Project-Folder
> > Survey-data
> > > Aggregated-survey-data.csv
> > > Survey-analysis.docx
> > ATLAS.ti-project.altproj23
> > Data-collection
> > > Pseudonym-identifiers.txt
> > > Informed-consent-orms.csv
> > > YYYYMMDD-Participant01.wav
> > > YYYYMMDD-Participant02.wav
> > Data-analysis
> > > YYYYMMDD-Participant-anonym01.docx
> > > YYYYMMDD-Participant-anonym02.docx

No version control methods will be used, except for the built-in version control that OneDrive provides in case of accidental removal of files.

Data storage

3.1 Select the storage solution where you will store and back-up your data. Select the locations where your data will be stored. You may select more than one. Please describe the storage solution and the backup strategy of your storage solution if it does not appear in the list below.

Everything will be stored in OneDrive. We use its built-in backup solution. Before downloading, the filled-in consent forms are stored in the UU Qualtrics instance. After the project's completion, data will be archived in Yoda.

Data privacy and security

4.1 Will you be collecting or using personal data? Personal data is any data which, alone or in combination with other information, can identify a living person. Such data must abide by the GDPR and requires additional safeguards and documentation to be processed lawfully.

- Yes, I will collect and/or use personal data

4.2 What is the legal basis by which you are collecting and/or processing this data? If you are uncertain as to which legal basis applies to your type of research; please do not hesitate to contact us at info.rdm@uu.nl or by using the "Request feedback" button and leaving a comment alongside this question.

- Informed consent

4.3 Select the privacy and security measures you will employ to protect the privacy of your data subjects. Check all that apply.

Secure storage, Pseudonymization, Minimizations, Access control, Encryption, Aggregation/Abstraction

The raw survey data is used for analysis. After the analysis, the raw data will be deleted and aggregated data tables will be used for publication and these aggregated tables will be retained on the OneDrive. Access to the recordings is restricted to the interviewer, who transcribes the recording and lets the interviewee review the transcript before it is further processed. Access to the transcripts is restricted to the researchers involved in the analysis. After analysis, the transcripts and results will be **thoroughly pseudo-anonymised**. The pseudo-anonymised transcripts will be double-checked by the project PI and one person who is not involved in the research project but works with the researchers at UU. The anonymisation of the transcripts will be done in line with the recommendations provided in Slide 31:

- Karcher, Sebastian (2019): Managing and Sharing Qualitative Data. figshare. Dataset. https://doi.org/10.6084/m9.figshare.7637288.v1

The pseudonym identifiers will be deleted after the end of the project (i.e., results publication), ensuring that the data are no longer considered personal. See for details https://www.dataprotection.ie/en/guidance/anonymisation-pseudonymisation. Data on OneDrive is encrypted in transfer and storage by default. All researchers use devices with disk-level encryption

4.4 Who is the controller of the personal data ? The controller of the personal data is the entity which determines what is done with the data. In most cases the controller is Utrecht University.

Utrecht University is the controller of the collected personal data. Nevertheless, the master student collecting and analysing the data will ensure that the data is handled and processed in accordance with the GDPR, in consultation with his supervisor.

4.5 How will ownership and intellectual property rights of the data be managed? Describe who controls access to the data and who determines what is done to the data.

The PI supervising this project will determine who has access to the data within the research group. All intellectual property rights belong to Utrecht University. During the project, only the master student and his supervisors have access to the data.

Data selection, preservation & sharing

5.1 Describe the data you will be preserving and the storage solution where it will be preserved? Describe which data will be preserved under long-term storage. You may refer back to the data described in question 1.2 to specify which data will be preserved. Explain where you will preserve your data, and how procedures are applied to ensure the survival of the data for the long term.

All collected data except audio recordings and pseudonym identifiers will be preserved. The audio recordings will be transcribed and pseudo-anonymised in text format and deleted afterwards. The pseudonym identifiers will be deleted after the end of the project (i.e., results publication). The aggregated survey and pseudo-anonymised interview data will be kept for

at least ten years. After completing the project, the data will be stored in Yoda. Yoda is an infrastructure developed at Utrecht University and provides an integrated collaboration, secure and (long-term) storage environment. The raw survey data will not be openly published due to restrictions from the organization side where this study is taking place. Only aggregated survey data will be stored.

5.2 Describe the data you will be sharing and the repository where it will be shared? Describe which data you will be sharing. Select where you will make your data findable and available to others. If selecting "Other" please specify below which repository and provide a URL. Please also write below if you will apply any conditions to the re-use of your data. (i.e. Creative commons license or Data Transfer Agreement).

- Other

The aggregated survey data, anonymized transcripts, and analysis in ATLAS.ti will be made publicly available through Yoda repository if the interviewee has separately opted-in for this. The results will be re-usable under a CC-BY 2.0 creative commons license.

5.3 Are specialized, uncommon or expensive software, tools or facilities required to use the data? Please list any specialized, uncommon or expensive software, tools or facilities that are absolutely required to obtain, use or handle your data, if any.

The anonymized transcripts can be accessed by free, open-source or non-proprietary software. This is also the case for the aggregated survey data. The ATLAS.ti project file can be opened with software from QSR, MaxQDA and Framework, all of which are proprietary packages. Some offer a trial or free version.

Data management costs and resources

6.1 What are the foreseeable research data management costs and how do you expect to cover them ? Please specify the known and expected costs involved in managing, storing and sharing your data. Also explain how you plan to cover these costs.

The data storage needs will not exceed the amount of storage allocated to each individual by Utrecht University, so no additional costs are expected. The long-term storage will be done in Yoda for 4€ per TB/month.

6.2 Who will be responsible for data management? Please specify who is responsible for updating the DMP and ensuring it is being followed accordingly.

- The project's PI Dr. Kate Labunets will be responsible for maintaining the DMP up to date, granting permissions, and ensuring the data is deposited in the repository.

6.3 State if you contacted an RDM consultant from Utrecht University to help you fill out your DMP. Please list their name and date of contact. This is mandatory for NWO grants.

- Natalie van Dis, data manager at the Department of Information and Computing Sciences, Utrecht University, was contacted for information about processing company data and informed consent on 12-04-2023.

B Ethics and Privacy Quick Scan response summary

Section 1. Research projects involving human participants

P1. Does your project involve human participants? This includes for example use of observation, (online) surveys, interviews, tests, focus groups, and workshops where human participants provide information or data to inform the research. If you are only using existing data sets or publicly available data (e.g. from Twitter, Reddit) without directly recruiting participants, please answer no.

- Yes

P2. Does your project involve participants younger than 18 years of age?

- No

P3. Does your project involve participants with learning or communication difficulties of a severity that may impact their ability to provide informed consent?

- No

P4. Is your project likely to involve participants engaging in illegal activities?

- No

P5. Does your project involve patients?

- No

P6. Does your project involve participants belonging to a vulnerable group, other than those listed above?

- No

P8. Does your project involve participants with whom you have, or are likely to have, a working or professional relationship: for instance, staff or students of the university, professional colleagues, or clients?

- Yes

P9. Is it made clear to potential participants that not participating will in no way impact them (e.g. it will not directly impact their grade in a class)?

- Yes

PC1. Do you have set procedures that you will use for obtaining informed consent from all participants, including (where appropriate) parental consent for children or consent from legally authorized representatives? (See suggestions for information sheets and consent forms on the website.)

- Yes

PC2. Will you tell participants that their participation is voluntary?

- Yes

PC3. Will you obtain explicit consent for participation?

- Yes

PC4. Will you obtain explicit consent for any sensor readings, eye tracking, photos, audio, and/or video recordings?

- Not applicable

PC5. Will you tell participants that they may withdraw from the research at any time and for any reason?

- Yes

PC6. Will you give potential participants time to consider participation?

- Yes

PC7. Will you provide participants with an opportunity to ask questions about the research before consenting to take part (e.g. by providing your contact details)?

- Yes

PC8. Does your project involve concealment or deliberate misleading of participants?

- No

Section 2. Data protection, handling, and storage

D1. Are you gathering or using personal data (defined as any information relating to an identified or identifiable living person)?

- Yes

DR1. Will you process personal data that would jeopardize the physical health or safety of individuals in the event of a personal data breach?

- No

DR2. Will you combine, compare, or match personal data obtained from multiple sources, in a way that exceeds the reasonable expectations of the people whose data it is?

- No

DR3. Will you use any personal data of children or vulnerable individuals for marketing, profiling, automated decision-making, or to offer online services to them?

- No

DR4. Will you profile individuals on a large scale?

- No

DR5. Will you systematically monitor individuals in a publicly accessible area on a large scale (or use the data of such monitoring)?

- No

DR6. Will you use special category personal data, criminal offense personal data, or other sensitive personal data on a large scale?

- No

DR7. Will you determine an individual's access to a product, service, opportunity, or benefit based on an automated decision or special category personal data?

- No

DR8. Will you systematically and extensively monitor or profile individuals, with significant effects on them?

- No

DR9. Will you use innovative technology to process sensitive personal data?

- No

DM1. Will you collect only personal data that is strictly necessary for the research?

- Yes

DM4. Will you anonymize the data wherever possible?

- Yes

DM5. Will you pseudonymize the data if you are not able to anonymize it, replacing personal details with an identifier, and keeping the key separate from the data set?

- Not applicable

DC1. Will any organization external to Utrecht University be involved in processing personal data (e.g. for transcription, data analysis, data storage)?

- No

DI1. Will any personal data be transferred to another country (including to research collaborators in a joint project)?

- No

DF1. Is personal data used to recruit participants?

- No

DP1. Will participants be provided with privacy information? (Recommended is to use as part of the information sheet: For details of our legal basis for using personal data and the rights you have over your data please see the University's privacy information at www.uu.nl/en/organisation/privacy.)

- Yes

DP2. Will participants be aware of what their data is being used for?

- Yes

DP3. Can participants request that their personal data be deleted?

- Yes

DP4. Can participants request that their personal data be rectified (in case it is incorrect)?

- Yes

DP5. Can participants request access to their personal data?

- Yes

DP6. Can participants request that personal data processing is restricted?

- Yes

DP7. Will participants be subjected to automated decision-making based on their personal data with an impact on them beyond the research study to which they consented?

- No

DP8. Will participants be aware of how long their data is being kept for, who it is being shared with, and any safeguards that apply in case of international sharing?

- Yes

DP9. If data is provided by a third party, are people whose data is in the data set provided with (1) the privacy information and (2) what categories of data you will use?

- Not applicable

DE1. Will you use any personal data that you have not gathered directly from participants (such as data from an existing data set, data gathered for you by a third party, data scraped from the internet)?

- No

DS1. Will any data be stored (temporarily or permanently) anywhere other than on password-protected University authorized computers or servers?

- No

DS4. Excluding (1) any international data transfers mentioned above and (2) any sharing of data with collaborators and contractors, will any personal data be stored, collected, or accessed from outside the EU?

- No

Section 3. Research that may cause harm

H1. Does your project give rise to a realistic risk to the national security of any country?

- No

H2. Does your project give rise to a realistic risk of aiding human rights abuses in any country?

- No

H3. Does your project (and its data) give rise to a realistic risk of damaging the University's reputation? (E.g., bad press coverage, public protest.)

- No

H4. Does your project (and in particular its data) give rise to an increased risk of attack (cyber- or otherwise) against the University? (E.g., from pressure groups.)

- No

H5. Is the data likely to contain material that is indecent, offensive, defamatory, threatening, discriminatory, or extremist?

- No

H6. Does your project give rise to a realistic risk of harm to the researchers?

- No

H7. Is there a realistic risk of any participant experiencing physical or psychological harm or discomfort?

- No

H8. Is there a realistic risk of any participant experiencing a detriment to their interests as a result of participation?

- No

H9. Is there a realistic risk of other types of negative externalities?

- No

Section 4. Conflicts of interest

C1. Is there any potential conflict of interest (e.g. between research funder and researchers or participants and researchers) that may potentially affect the research outcome or the dissemination of research findings?

- No

C2. Is there a direct hierarchical relationship between researchers and participants?

- No

Section 5. Your information.

Z0. Which is your main department?

- Information and Computing Science

Z1. Your full name:

- Floris Jansen

Z2. Your email address:

- f.j.jansen@students.uu.nl

Z3. In what context will you conduct this research?

- As a student for my master thesis, supervised by: Kate Labunets

Z5. Master programme for which you are doing the thesis

- Business Informatics

Z6. Email of the course coordinator or supervisor (so that we can inform them that you filled this out and provide them with a summary):

- k.labunets@uu.nl

Z7. Email of the moderator (as provided by the coordinator of your thesis project):

- g.wagenaar@uu.nl

Z8. Title of the research project/study for which you filled out this Quick Scan:

- Mental models on Shadow IT

Z9. Summary of what you intend to investigate and how you will investigate this (200 words max):

- We try to uncover the mental models of shadow IT of four different groups of employees within a large professional services company. These groups are (i) Support staff, (ii) Consulting staff, (iii) Management staff, and (iv) internal IT team.
  By uncovering the differences in mental models of these four groups, we can tailor guidelines per group, in order to minimize the shadow IT related risks.

We do this by conducting an SLR on the creation of mental models of different cybersecurity-related concepts. This SRL will guide as a foundation for the actual creation of mental models later in this research. Then by an exploratory survey, we try to uncover all the occurences of shadow IT within these four groups.
The analysis of the survey will point us to the most interesting direction to uncover more of. We will do semi-structured interviews with participants from the four groups, to either verify that there is no shadow IT (if none are found during the survey), or to take a deep dive in understanding the motivation for the found shadow IT use.

Z10. In case you encountered warnings in the survey, does supervisor already have ethical approval for a research line that fully covers your project?

- No

Scoring

- Privacy: 0
- Ethics: 0

C Informed Consent - Survey

This survey will only take about 5-10 minutes!

You will need to indicate that you have understood this information before you can continue. You must also be aged over 18 to participate.

This study aims to investigate the gap between the IT applications that [ORGANZATION] provides and the IT applications that employees need. By applications, we mean: any external tool that can be downloaded on your [ORGANZATION] system or used in the browser.

We promise to protect your privacy under the Privacy Policy and treat the information you give us as confidential. We will use the information you provide only for research purposes. Participation is entirely anonymous. However, if you wish to participate in the giveaway, we need a means of contacting you and, therefore, will collect your email address at the end. The email address is only used to contact the winner of the lottery. You can withdraw from participating in the survey at any moment before submitting it. We will respect your decisions about participating in the survey or discontinuing participation without question. The survey is conducted in April and May 2023, organized and conducted by a team of researchers from Utrecht University: Floris Jansen, Dr. Kate Labunets and Dr. Slinger Jansen.

Privacy policy

1. **The information that we collect** - When you participate in our research, we ask you to provide your personal experiences and demographic information, such as your age, work background, experience and use of IT applications. You may discontinue participation in a survey at any time.
2. **Confidentiality of survey responses** - We collect only anonymous data and do not ask for your personal information. We combine your survey responses with the responses of all others who participate and report those combined responses in a scientific paper. Your survey responses are collected, stored, or processed by Utrecht University. We are bound to keep confidential any information we collect and must protect it with high-security standards and practices, as requested by the European Data Protection Directive (Directive 95/46/EC). Anonymous data from this survey may be shared with the research community at large to advance science and practice.
3. **Use of cookies, log files, and other technologies on our website** - Cookies are small text files stored on your computer by a website that assigns a numerical user ID and stores certain information about your online browsing. We use cookies on the Qualtrics survey

site to help us provide you with a better experience, quality control, and validation functions. No personal information is stored on any cookie that we use. We use the Qualtrics platform for the online questionnaire administration. For further information, you can refer to the Qualtrics Privacy Policy: https://www.qualtrics.com/privacy-statement/.

4. **Ethical review** - This study has been reviewed by, and received ethics clearance through, the Science-Geo Ethics Review Board.
5. **How to contact us** - Questions regarding this policy, complaints about our practices, and access requests should be directed to Dr. Kate Labunets via e-mail (k.labunets@uu.nl) We will investigate all complaints and attempt to resolve those that we find are justified. If necessary, we will amend our policies and procedures to ensure that other individuals do not experience the same problem. If you remain unhappy or wish to make a formal complaint, please contact the relevant chair of the Science-Geo Ethics Review Board at the Utrecht University who will seek to resolve the matter in a reasonably expeditious manner: Chair, Science-Geo Ethics Review Board; Email: etc-beta-geo@uu.nl.

Statement of Consent

- I have read and understood the information about this survey.
- In consenting, I understand that my legal rights are not affected.
- I also understand that data collected as part of this research are fully anonymous and can be shared with the research community at large to advance science.
- I freely and voluntarily give my CONSENT to participate in the survey focusing on the IT alignment within [ORGANZATION] systems.

In summary, by clicking the button below, you acknowledge:

Your participation in the survey is voluntary. You are 18+ years old. You are aware that you may choose to terminate your participation at any time for any reason.

D Survey

Demographics

What is your gender?

- ❍ Male
- ❍ Female
- ❍ Prefer not to say

What is your role?

- ❍ Junior
- ❍ Senior
- ❍ Manager
- ❍ Senior Manager
- ❍ Management

What is your highest level of education?

- ❍ Applied sciences bachelor (HBO)
- ❍ Applied sciences master (HBO)
- ❍ Bachelor's degree (University)
- ❍ Master's degree (Universtity)
- ❍ Post-master
- ❍ PhD
- ❑ Other ····

What is you age?

- ❍ 18 - 22
- ❍ 23 - 25
- ❍ 26 - 30
- ❍ 31 - 35
- ❍ 36 - 40
- ❍ 41 - 50
- ❍ 51 - 60
- ❍ 60+

How many years of professional working experience do you have?

···

Please select your department?

- ❍ Support staff
- ❍ Client facing staff
- ❍ IT staff
- ❍ Management staff

Explanation

Please read the following with care. This ensures the rest of the survey can be filled in **quicker** and more **accurately**.

We will ask you questions regarding the software you use that is **outside the [ORGANZATION] scope**.

This means we are interested in applications that are **not facilitated by [ORGANZATION]**.

The survey is split into sections concerning **THREE SCENARIOS**

1. Software needed for *specific client projects*
2. Software needed *work related tasks*, but in general so **not** for specific projects
3. Software needed *for personal use*

By understanding the distinction you can now swiftly go through the rest of the survey!

Part 1 - Client projects

This section concerns all applications you had to use for specific clients/engagements that are **not** standard [ORGANZATION] applications.

Note: Standard [ORGANZATION] applications are all applications (e.g. MS Office) that are installed on your laptop or available through the [ORGANZATION] appstore.

For **specific engagements**, what **cloud services** have you used that were **not** provided by [ORGANZATION] ?
Please select all applicable options:

- ❑ Browser tools (e.g. Notion, Hubspot, Zapier, Jira)
- ❑ Cloud storage (Dropbox, Google Drive, and other peer-to-peer collaboration tools)
- ❑ Browser extensions
- ❑ Other ····
- ❍ None, I used only standard applications provided by [ORGANZATION]

What specific cloud services have you used in regard to the previous question?
You can enter multiple answers separated by a semicolon (;).

····

For **specific engagements**, what types of applications have you **downloaded and installed** on your laptop/phone that were **not** provided by [ORGANZATION] ?

- ❑ Remote workspaces (Citrix, Zspace, Amazon workspace)
- ❑ ERP/CRM systems (NetSuite, SAP)
- ❑ Video conferencing tools (Skype, Zoom, Slack)
- ❑ Virtual Machine (VMware)
- ❑ Code/text editors (VS Code, Notepad ++)
- ❑ External PDF readers
- ❑ Design/editing tools
- ❑ Screenshot/screenrecordging applications
- ❑ Streaming services (Spotify)
- ❑ Video and media players (VLC media player)
- ❑ Other browsers than MS edge
- ❑
- ❑ Other ····
- ❍ None, I used only standard applications provided by [ORGANZATION]?

What specific cloud services have you used in regard to the previous question?
You can enter multiple answers separated by a semicolon (;).

····

For **specific engagements**, what **own solutions** have you created that were **not** facilitated by [ORGANZATION] ?

- ❑ Created an excel spreadsheet outside [ORGANZATION] scope
- ❑ Self-developed software
- ❑ Self-built website
- ❑ Ad-hoc-coupling of systems
- ❑ Other ····
- ❍ None

What specific cloud services have you used in regard to the previous question?
You can enter multiple answers separated by a semicolon (;).

····

Part 2 - IT applications in non-client work-related tasks

This section concerns all applications you had to use for work-related tasks, that were **not** for specific engagements.

Note: Standard [ORGANZATION] applications are all applications (e.g. MS Office) that are installed on your laptop or available through the [ORGANZATION] appstore.

For **work-related tasks**, what **cloud services** have you used that were **not** provided by [ORGANZATION] ?
Please select all applicable options:

- ❑ Browser tools (e.g. Notion, Hubspot, Zapier, Jira)

- ❑ Cloud storage (Dropbox, Google Drive, and other peer-to-peer collaboration tools)
- ❑ Browser extensions
- ❑ Other ····
- ❍ None, I used only standard applications provided by [ORGANZATION]

What specific cloud services have you used in regard to the previous question?
You can enter multiple answers separated by a semicolon (;).

····

For **work-related tasks**, what types of applications have you **downloaded and installed** on your laptop/phone that were **not** provided by [ORGANZATION] ? ?

- ❑ Remote workspaces (Citrix, Zspace, Amazon workspace)
- ❑ ERP/CRM systems (NetSuite, SAP)
- ❑ Video conferencing tools (Skype, Zoom, Slack)
- ❑ Virtual Machine (VMware)
- ❑ Code/text editors (VS Code, Notepad ++)
- ❑ External PDF readers
- ❑ Design/editing tools
- ❑ Screenshot/screenrecordging applications
- ❑ Streaming services (Spotify)
- ❑ Video and media players (VLC media player)
- ❑ Other browsers than MS edge
- ❑
- ❑ Other ····
- ❍ None, I used only standard applications provided by [ORGANZATION]?

What specific cloud services have you used in regard to the previous question?
You can enter multiple answers separated by a semicolon (;).

····

For **work-related tasks**, what **own solutions** have you created that were **not** facilitated by [ORGANZATION] ?

- ❑ Created an excel spreadsheet outside [ORGANZATION] scope
- ❑ Self-developed software
- ❑ Self-built website
- ❑ Ad-hoc-coupling of systems
- ❑ Other ····
- ❍ None

What specific cloud services have you used in regard to the previous question?
You can enter multiple answers separated by a semicolon (;).

····

Part 3 - IT applications for personal use

This section concerns all applications you used for personal reasons (non-work related tasks) on your [ORGANZATION] device

For **personal use**, what **cloud services** have you used?
Please select all applicable options:

- ❑ Browser tools (e.g. Notion, Hubspot, Zapier, Jira)
- ❑ Cloud storage (Dropbox, Google Drive, and other peer-to-peer collaboration tools)
- ❑ Browser extensions
- ❑ Other ····
- ❍ None

What specific cloud services have you used in regard to the previous question?
You can enter multiple answers separated by a semicolon (;).

····

For **personal use**, what types of applications have you **downloaded and installed** on your laptop/phone?

- ❑ Remote workspaces (Citrix, Zspace, Amazon workspace)
- ❑ ERP/CRM systems (NetSuite, SAP)
- ❑ Video conferencing tools (Skype, Zoom, Slack)
- ❑ Virtual Machine (VMware)
- ❑ Code/text editors (VS Code, Notepad ++)
- ❑ External PDF readers
- ❑ Design/editing tools
- ❑ Screenshot/screenrecordging applications
- ❑ Streaming services (Spotify)
- ❑ Video and media players (VLC media player)
- ❑ Other browsers than MS edge
- ❑
- ❑ Other ····
- ❍ None

What specific cloud services have you used in regard to the previous question?
You can enter multiple answers separated by a semicolon (;).

····

For **personal use**, what **own solutions** have you created?

- ❑ Created an excel spreadsheet outside [ORGANZATION] scope
- ❑ Self-developed software
- ❑ Self-built website
- ❑ Ad-hoc-coupling of systems
- ❑ Other ····
- ❍ None

What specific cloud services have you used in regard to the previous question?
You can enter multiple answers separated by a semicolon (;).

····

Part 4 - Devices outside [ORGANIZATION] scope

This **final** section concerns the use of private devices for work-related tasks.

For what work related tasks have you ever used your private phone, tablet, laptop or other private devices?

- ❑ Forwarded email to a personal account to access it there
- ❑ Scheduling appointments
- ❑ Contacting clients
- ❑ Other ····
- ❍ No, I have never used my private phone/laptop for any work related tasks

What tasks did you perform?

···

Part 5 - Survey closing

Are you willing to participate in a follow up interview about IT applications within [ORGANZATION] ?

- ❑ Yes
- ❑ No

Enter your email address so we can contact you about the interview

···

ENTER THE GIVEAWAY

By entering your email address below, you enter the giveaway and **you agree that your email can be used to contact** you in case you win one of the prizes (2x giftcard, 2x [ORGANZATION] goodiebag)

If you do NOT wish to enter, just press the next button at the bottom of the page

E Informed Consent - Interviews

Informed consent

Information about the research
The interview you are asked to participate in is part of scientific research aiming to gain insights into the understanding and cybersecurity problems of shadow IT. Shadow IT is defined as "hardware, software, or services built, introduced, and/or used for the job without explicit approval or even knowledge of the organization" (Haag & Eckhardt, 2017).

How will the study be carried out?
The interview will take at maximum one hour, during which the researcher will ask questions in a semi-structured format. The interview will be recorded. After the recordings are transcribed, you will get the opportunity to remove any information from the text that should not be included in further analysis. Following the researchers' analysis of these transcripts, you will be asked to evaluate and add to a summary of the results that are based on the interviews. You will not be reimbursed for your participation in this study.

What will we do with your data?
During this interview, data about your experiences with shadow IT will be collected. Although the objectives and design of this study do not require specific personally identifiable information, the data collected should be considered as such. The interview will be recorded before it is transcribed. Interview recordings will be retained for up to six months until transcribed. The non-pseudonymised transcripts will only be processed by UU researchers who are collaborating in the study, or who are responsible for assessing its implementation. After analysis, the transcripts will be further pseudonymised as described in the next section. There are no specific increased privacy risks related to the nature of the collected personal data or the processing that the data will undergo. The data is stored and processed exclusively in the EU and all third party applications used have an appropriate data processing agreement with Utrecht University.

Processed data will be retained for at least 10 years for the purposes of research integrity. Before this archival, all personal information that can reasonably be traced back to you or your organization will have been removed or changed before the files are shared with other researchers or the results are made public. The researcher will keep a link that identifies you and your organization with the information, but this link will be kept secure and only available to the researcher. Any information that can identify you will remain confidential. The information in this study will only be used in ways that do not reveal who you are. You

and your organization will not be named or identified in publications about this study or in documents shared with other researchers.

What are your rights?
Participation is voluntary. We are only allowed to collect your data for our study if you consent to this. If you decide not to participate, you do not have to take any further action. You do not need to sign anything. Nor are you required to explain why you do not want to participate. If you decide to participate, you can always change your mind and stop participating at any time, including during the study. You will even be able to withdraw your consent after you have participated. However, if you choose to do so, we will not be required to undo the processing of your data that has taken place up until that time. The research data we have obtained from you up until the time when you withdraw your consent will be erased.

Approval of this study
The Ethics and Privacy Quick Scan of the Utrecht University Research Institute of Information and Computing Sciences classified this research as low-risk and did not reveal any ethical problems for this research.If you have a complaint about the way this study is carried out, please send an email to the secretary of this Committee: etc-beta-geo@uu.nl. If you have any complaints or questions about the processing of personal data, please send an email to the Data Protection Officer of Utrecht University: privacy@uu.nl). The Data Protection Officer will also be able to assist you in exercising the rights you have under the GDPR. Please also be advised that you have the right to submit a complaint with the Dutch Data Protection Authority (https://www.autoriteitpersoonsgegevens.nl/en).

More information about this study?
In case you have additional questions, please contact Floris Jansen (researcher and data controller for the study) at f.j.jansen@students.uu.nll or Kate Labunets (project supervisor for the study) at k.labunets@uu.nl.

Haag, S., & Eckhardt, A. (2017). Shadow IT. Business & Information Systems Engineering, 59(6), 469–473.

I have read and understood the study information dated {date://CurrentDate/PT}, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.

- Yes
- No

I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.

- Yes
- No

I understand that information I provide will be used for the report and publications in academic venues (like conferences or journals).

- Yes
- No

I understand that personal information collected about me that can identify me, such as my name or email address, will not be shared beyond the study team.

- Yes
- No

I additionally agree that my information can be quoted in research outputs

- Yes
- No

I give additional permission for the pseudonymised interview transcript that I provide to be archived in UU's Yoda as open-access data so it can be used for future research and learning.

- Yes
- No

Enter your name .....

Enter your email address.....

F Quality assessment

	Technique						Participants					Rep	
Sum	33	16	6	5	3	1						41	14
Ref	Interview	Drawing	Survey	Crowdsource	Think aloud	Experiment	Amount	Cohort	Age	Requirements	Recruitment	Text-based	Diagram
1	•						33	a diverse group of home computer users	19-70	Home computer users	Snowball from 3 different major us cities	•	
2	•						30	10 advanced users and 20 novice users.		18-63	advanced: Carnegie Mellon University known security experts, novice: users through messages on Craigslist and flyers	•	•
5				•			5360			Located in US + approval rate 75%	AMT	•	
6	•						40		21-79	Have an active email account		•	
7	•						24		18-50			•	
8						•	29	Different cultural backgrounds	18-57		On campus, through personal contacts and social media	•	
10				•			96			Have a 95% HIT approval rating	AMT	•	
11	•						26		18-60		Personal contact and snowball sampling	•	
13	•	•	•		•		I: 18, S:25	CS students vs non CS students	18-34		Personal and social networks. Through classroom for CS students	•	
15	•		•				46	a group of well-informed individuals		Well informed about security		•	
16	•						5	One group of software developers	22-55	Being software developer		•	•
17			•				609	a large and diverse sample of people who use IT for personal use.	18+	Use IT in their personal life	Third-party recruitment firm	•	
18	•	•			•		7		M:42 , SD:6.3)	Required to have expertise in cyber security and to be involved in cyber security	Personal contact and snowball sampling	•	
20	•		•				I:17, S: 517	maximize diversity	18-55	Required to have used Tor Browser and onion services	Online forums, social media related to TOR and privacy.	•	•
21	•	•					4			Speak English and have experience with credit bureaus	Convenience sampling in the U.S. Midwest in October 2017	•	•
22				•			44		18-55	Approval rate of 50%	AMT	•	•
23		•					366					•	
24	•	•					28	three groups	18-64	Technical: CS degree, lay no degree, community 30+ years	Flyers, personal contacts and online participant pool, and advertisement on craigslist	•	•
25	•	•					30	End users vs administrators	24-60	End users: be a non-expert user. For administrators: professional experience in IT security, work with HTTPS and TLS code	Social media, personal contacts, and local hackerspaces	•	•
26	•						17	Convenience sampling	18-60	Own a Smart Home Personal Assistant for at least one month	Prolific	•	
27	•						26	Convenience sampling	19-60		Convenience sampling, using social media and email lists	•	

TABLE F.1: SLR - quality assessment results (1/2)

Ref	Technique						Participants					Rep	
	Interview	Drawing	Survey	Crowdsource	Think aloud	Experiment	Amount	Cohort	Age	Requirements	Recruitment	Text-based	Diagram
28	•						24		21-68	U.S. citizens or permanent residents for 5+ years	Online platforms, emails to a university research pool	•	
29	•	•					19		20-69		Prolific	•	•
30	•	•					19		18-69		Craigslist in the DC region	•	
31	•						24		17-53	Fluent in German	Mailing list among undergraduate psychology student	•	
32	•	•					2					•	•
33				•			1993	One large representable group of US citizens	18-65+	18+ years old and have access to the internet	AMT	•	
36	•						27			1: 18+, 2: residing within Canada, 3: comfortable communicating in English, 4: had used at least one at-home DNA testing kit.	Kijiji or Facebook groups.	•	
37	•						25		18-75	1: An education in or work in CS, 2: expert in at least one programming language, 3: people asked them for computer advice	Interested participants were asked to complete an online screening questionnaire	•	
38	•	•					29	Convenience sampling		Self-reported level of cryptocurrency knowledge		•	•
39	•						22	Different professional and socio-demographic backgrounds				•	
42	•	•	•				I:19, S:227		18-33	1: Own a Fitbit compatible smartphone 2: sufficient mastery of French 3: not be current fitness trackers users	LABEX portal to recruit students	•	
43	•						23		18-65	Completed post-secondary education, completed or enrolled in either an undergraduate or a graduate degree.		•	
44	•						12		24-37	18 years or older and users of instant messengers.	German Facebook groups	•	
45	•	•					K:78, S: 109	middle schoolers vs college students	K:13.3, S:18.8	Middle school students ages 11-15. Students: born in 1996 or later		•	•
46	•	•					35		18-60		Recruitment posters, a Facebook page for user study recruitment	•	•
47				•			1st: 461, 2nd: 61	experimental group and a control group	18-50+	Participants were U.S. residents who did not have programming skills and use messaging apps	AMT	•	
48	•	•					30	Visitor group and resident group	18-64		Mailing lists, flyers, poster advertisements, and social networks.	•	
49	•	•			•		18	experts vs non-experts	25-60	Meet the criteria for being either an expert or a non-expert in computer security.	Participants were recruited within a professional services company	•	•
50	•		•				I:23, S:729	University students and general VPN users	18-54	Participants were recruited based on their experience with VPNs and their willingness to participate in the study	University students from university The general VPN user group was recruited through online forums and social media platforms	•	
51	•	•					20			Participants had to have adequate knowledge on ML	Professional networks and used snowballing	•	•

TABLE F.2: SLR - quality assessment results (2/2)

G Interview protocol

Pre recording

Thank the interviewee for their willingness to participate, reiterate the research goals, and set expectations for the duration of the interview (around 30 mins) and the topics that will be covered.

1. Introduction

Please state your rank, team, education and years of professional work experience
What is the nature of your work? Do you do work in engagements?
If so, how many engagements have you done?
What kind of work do you do?
What kind of software do you need for your work tasks?
Have you ever needed special software for your clients?
some more indented text some more indented text

2. Understanding Shadow IT

What is Shadow IT for you? (Could you please define what Shadow IT is?)
If definition is known: let the participant explain and introduce our definition
If definition is unknown: introduce our definition - "hardware, software, or services built, introduced, and/or used for the job without explicit approval or even knowledge of the organization"
Introduce four types of shadow IT
Cloud services
Downloaded and install programs
Self-built solutions
Private devices

Occurrence of Shadow IT - Have you ever used?

Cloud services - *for engagements? work tasks? personal use?*
Downloaded and install programs - *for engagements? work tasks? personal use?*
Self-built solutions - *for engagements? work tasks? personal use?*
Private devices - *for engagements? work tasks? personal use?*

If a participant ever used a certain application -> Why those occurrences?

Missing feature?
Client request?
Personal preference
Time constraints?

4. Risks and implications of shadow IT?

What do you think the risks are of the different types of shadow IT?

Risks for the user/participant?

Risks for your organization?

Risks for the client?

What do you think are other implications of the different types of shadow IT?

5. Drawing exercise (only for client-specific software)

Draw the process of the need to use client-specific applications.

So the client has asked you to work towards goal X, to do this you need an application that you do not have at the moment, how do you address this?

6. Policy and awareness

Are you aware of the [organizational policy]?

If yes: could you quickly explain the policy?

If no: ask what their perception of the use of technology is within your organization.

Afterwards, explain the policy

Have you discussed the use of technology amongst your team members?

Do you feel you have been well informed about the use of technology?

(either through web learnings, your colleagues, training)

- do you think policy and awareness should do more?

7. Interview closing

Would you like to add anything else?

Thank the interviewee for their time and explain further procedures of transcript review, member checking of codes, and sharing of results.

H Codebook

Final codebook used during the analysis of the interview transcript. Codes and sub-codes are sorted alphabetically.

Code	Description
Context	Contains information for work type, device usage for laptops and mobile and perspective aspects of shadow IT
Work type	Concerns the type of work a participant does, describes the nature of how a participant gets their work tasks
Client	A participant does work for a portfolio of (several) clients, for whom he performs the same work tasks
Internal	A participant does not engage in any projects or clients
Project	A participant does work on a project basis
Laptop usage	Concerns if a participant uses his work laptop also for private
One laptop	A participant only has one laptop, meaning all personal tasks must be done on the organization laptop
Separated laptops	A participant has more than one laptop, meaning not all personal tasks have to be done on the organization laptop
Mobile device usage	Concerns if a participant has a combined business and personal phone or separated phones
One device	A participant has only one mobile device, meaning all personal tasks must be done on organization device
Separated devices	A participant has more than one mobile phone, meaning not all personal tasks have to be done on organization device
Perspective	Concerns the perspective of the use of different kinds of applications in regard to shadow IT
Client laptop	A participant has a client laptop, shifting the shadow IT responsibility for all applications that are done on that laptop to the client
Client license	A participant gets licenses from a client to shift the perspective within one application to the client
Remote workspace	A participant has a remote workspace for a client, shifting the perspective for all applications needed that are now in the online workspace to the client
Shadow IT	Concerns all shadow IT related information

Unapproved cloud services	Cloud services that are not facilitated by the organization
Browser extensions	Concern any browser extensions not facilitated by organization
Cloud storage tools	Concern any online storage tool not facilitated by organization
Generative LLM tools	Concerns any generative large language model tool not facilitated by organization
Online collaboration tools	Concerns any form of online collaboration tool not facilitated by organization
Translate tools	Concerns any translation tool not facilitated by organization
Own solutions	Any self-made, externally facilitated tools
External spreadsheets	Concerns any excel spreadsheet outside the scope of the organization
Own software	Concerns any self-made software
System coupling	Concerns any ad-hoc coupling of systems
Self-installed applications	Concerns any self-installed application not facilitated by organization
Automation software	Concerns any automation software installed that is not facilitated by organization
Code Editor	Concerns any code editor that is not facilitated by organization
Conferencing tool	Concerns any conferencing tool that is not facilitated by organization
Design tool	Concerns any design tool that is not facilitated by organization
File reading tool	Concerns any file reading tool that is not facilitated by organization
Mobile application	Concerns any mobile application that is not facilitated by organization
Network tool	Concerns any network tool that is not facilitated by organization
Non-standard browser	Concerns any browser that is not facilitated by organization
Password manager	Concerns any password manager that is not facilitated by organization
Non-standard PDF reader	Concerns any PDF reader that is not facilitated by organization
Remote workspace	Concerns any remote workspace that is not facilitated by organization
Screencapture tool	Concerns any screencapture tool that is not facilitated by organization
Streaming services	Concerns any streaming services that are not facilitated by organization
Version control	Concerns any version control systems that are not facilitated by organization
Virtual machine	Concerns any virtual machine that is not facilitated by organization

Self-acquired hardware	Concerns any hardware that is not facilitated by organization
Network device	Concerns the use of a network device that is not facilitated by organization
Personal laptop	Concerns the use of using a personal laptop for work-related tasks
Shadow IT definition	Displays a participants knowledge on the definition of shadow IT
Familiar	A participant is familiar with the definition of shadow IT
Unfamiliar	A participant is not familiar with the definition of shadow IT
Shadow IT reason	Provides the reason why a participant has chosen to adopt a shadow IT instance
Client requirement	Participant has adopted shadow IT due to the fact that it was in some way needed or requested by the client
Ease of use	Participant has adopted shadow IT since the shadow IT application is very easy to use
Financial feasibility	Participant has adopted shadow IT because of financial or cost reasons
Habit	Participant has adopted shadow IT because of the familiarity with a tool
Insufficient standard	Participant has adopted shadow IT because the tool provided by the organization does not work well enough
Language barrier	Participant has adopted shadow IT to overcome a language barrier
Need for functionality	Participant has adopted shadow IT because he was in need of a certain functionality that was not provided by the organization
Personal preference	Participant has adopted shadow IT because of a personal preference for a tool
Time constraint	Participant has adopted shadow IT due to managing a time constraint
Workaround	Participant has adopted shadow IT by actively working around security measures in place in the organization
Shadow IT benefits	Perceived benefits from the adoption of shadow IT
Efficiency	Working more time-efficient, or quicker when doing work-related tasks
Cost	These tools are free to use, therefore can be used by participants if they do not have a budget from the organization
Shadow IT risks	Perceived risks from the adoption of shadow IT
Data leak	There is a data leak whenever: confidential, sensitive, or personal data gets leaked outside the scope of the organization
Malware	The introduction of viruses, worms or other forms of malicious attacks

Non-central governance	Shadow IT goes around the organization's IT system and therefore are not subject to any controls
Outdated software	Since applications are not controlled by the IT team you risk that software becomes outdated
Ransomware	The phenomenon of an attack that locks files and asks payment in order to give them back
Reputational risk	The organizational public damage after there is an cyber incident at the organization
Unauthorized access	Some external party gets access to the organization's data
Wrong information	Due to the rise of generative AI programs, there is the introduction of the risk of misinformation
Shadow IT scenario	Concerns the scenario that was probed to the client-facing staff with regards to the process of possible shadow IT adoption
Approach client	A participant goes to the client to discuss the next steps
Approach IT team	A participant goes to IT team to discuss next steps
Approach manager	A participant goes to the manager to discuss next steps
Autonomous due diligence	A participant performs a internal checklist in order to see if the application can be adopted
Check internal app store	A participant checks the internal app store to see if there are applications that are suitable to use in this context
Discuss with other within the team	A participants discusses the situation in their own team to informally get insights into this kind of situation
Policy & Awareness	**This section concerns the policy and awareness section**
Awareness discussion	This concerns if, and how participants discuss the use of technology amongst their teams
Formal	A participant notes that the use of technology is discussed formally in team meetings or dedicated set presentations by others
Informal	A participant notes that the use of technology is discussed informally, during lunch, at the coffee corner, or with close colleagues
No discussion at all	A participant notes that the use of technology is not discussed at all
Policy definition	Concerns if a participant is familiar with certain policies in the organization
Familiar	A participant is familiar with the policies within organization
Unfamiliar	A participant is unfamiliar with the policies within organization
Personal awareness perception	Concerns if a participant feels well-informed about the use of technology
Not so well informed	Participant does not feel well informed about the use of technology
Reasonably well informed	Participant feels reasonably well informed about the use of technology
Well informed	Participant feels well informed about the use of technology

Contradictions	This section concerns contradicting statements that participants gave
Contradictions	This is the label that contradicting statements got during labeling
Mental Models	This section concerns the found mental models across participants
Risk-Averse mental model	This concerns all mental models that cause more aversing towards risk
Cautious Seasoned Judgement	This mental model is denoted by a cautiousness due to lots of experience
Consequence-Avoidance Orientation	This mental model is denoted by avoiding all consequences through not adopting a single shadow IT instance, due to the fear of the consequences
Knowledge-Based Conservatism	This mental model is denoted by a cautiousness due to lots of expertise within a certain field
Risk Transfer Mindset	This mental model is denoted by consciously transferring the perspective of shadow IT towards other entities
Risk tolerant mental models	This concerns all mental models that cause more tolerance towards risk
Cost-driven compromise	This mental model is denoted by adopting shadow IT instances because of the reduced financial cost
Illusion of self-sufficiency	This mental model is denoted by not detecting any shadow IT instances anymore, due to the earlier belief that there would never be a need for such applications
Implicit sound judgment	This mental model is denoted by using common sense to deal with shadow IT, however, this leads to no discussions and potential discrepancies between what is known and what you should know
Longevity-based invincibility	This mental model is denoted by a sense of security due to the long-term adoption of a certain shadow IT instance and therefore not seeing the danger for that instance anymore
Misguided sense of protection	This mental model is denoted by a false sense of security due to the belief that if something goes wrong, the IT department will fix this for you. While this does not have to be the case
Performance-driven rule bending	This mental model is denoted by adopting shadow IT instances due to a time constraint or some other form of pressure to finish work-related tasks faster or more efficiently.

TABLE H.1: The codebook with descriptions of codes