Who is the IT Department Anyway: An Evaluative Case Study of Shadow IT Mindsets Among Corporate Employees

Jan-Philip van Acken and Floris Jansen, *Utrecht University;*
Slinger Jansen, *Utrecht University and LUT University;*
Katsiaryna Labunets, *Utrecht University*

https://www.usenix.org/conference/soups2024/presentation/van-acken

This paper is included in the Proceedings of the Twentieth Symposium on Usable Privacy and Security.

August 12–13, 2024 • Philadelphia, PA, USA

978-1-939133-42-7

Open access to the Proceedings of the Twentieth Symposium on Usable Privacy and Security is sponsored by USENIX.

Who is the IT Department Anyway: An Evaluative Case Study of Shadow IT Mindsets Among Corporate Employees

Jan-Philip van Acken[1], Floris Jansen[1], Slinger Jansen[1,2], and Katsiaryna Labunets[1]

[1]Utrecht University, the Netherlands
[2]LUT University, Finland

Abstract

This study aimed to explore the factors influencing employees to deploy what can be classified as shadow IT in a corporate context. Shadow IT denotes unofficial, unsanctioned forms of IT. We employed a mixed-methods approach, consisting of a survey and follow-up interviews with employees from a large professional services company. The survey yielded 450 responses, uncovering different types of shadow IT within the company. The follow-up interviews with 32 employees aimed to uncover their perceptions of shadow IT, related risks, and their attitudes towards shadow IT usage. The survey and interviews revealed various types of shadow IT and showed a dichotomy of risk-averse and risk-tolerant mindsets. We found that participants employed a combination of these mindsets. Despite being aware of significant risks, gaps exist in acting upon this awareness, leading to an awareness-action gap. Closing this gap can be facilitated through factors that change these mindsets, such as the consequences of previous shadow IT choices, risk discussions, or training.

1 Introduction

Shadow IT occurs when employees bypass official channels "*to get the IT services they want on their own*" [39]. It appears in the form of hardware, software, or services that are *"built, introduced, and/or used for the job without explicit approval or even knowledge of the organisation"* [31]. This confronts any organisation with the challenge of managing a potentially *unknown* threat introduced by well-meaning employees. Note insights from a 2021 Forbes survey, where 46% of the executives surveyed reported that "shadow IT makes it impossible to protect all of their data, systems, and applications all the time" [23]. The questions we strive to answer here are:

RQ1: *How does shadow IT usage differ between departments and ranks?*
RQ2: *What is the employee's perception of shadow IT and risks associated with its usage?*
RQ3: *Which mindset motivates employees to opt for (or against) shadow IT usage in an organisational context?*

In this paper, we conducted a mixed-method evaluative case study in one of the largest professional services organisations' branches in the Netherlands, which reports 5000+ employees, to respond to the research questions. We find that shadow IT is intertwined within the organisation's IT landscape; all types of shadow IT appeared across departments and ranks. We elicited a total of 10 risk-related mindsets that influence the shadow IT behavior of employees.

Summary of contributions: Our main contributions are:

- We present the first mixed-method study of shadow IT usage patterns, perceived implications, and specific mindsets influencing shadow IT usage.
- We quantitatively analyse the scale of shadow IT usage across different departments and ranks in a large corporate organisation through a large-scale survey of 450 employees.
- We identify four risk-averse and six risk-taking mindsets through interviews with 32 employees; combinations of these mindsets might influence shadow IT usage decisions of employees within an organisational context.
- We outline actionable recommendations for security practitioners, to improve cyber risk management in light of shadow IT based on our findings.
- By offering our aggregated survey results, interview transcripts, and codebooks as open data to the research community, we lay the foundation for future studies on shadow IT and related mindsets.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

Unapproved cloud services	Use of Internet-based Software and Software as a Service (SaaS) that are not approved or unknown by the IT department. Also known as 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. (Excel spreadsheet, application developed by employees, ...)
Self-installed applications	Use of software installed by employees on the company's computers to perform their work tasks. (Download & installation of free of charge software from the internet, ...)
Self-acquired devices	Use of devices owned by employees, purchased from retail rather than ordered through the official catalogue of the IT department. It includes the use of applications in the employee's personal devices at the workplace. (cf. BYOD)

Table 1: Shadow IT topology (cf. Mallmann et al. [48])

2 Background and Related work

2.1 Shadow IT Background

Shadow IT was initially viewed as an extension or support to existing IT systems [42, 73], but the misuse of official IT received attention as well [41]. Past systematic literature studies found various definitions [30, 37, 41, 42, 48]. All but one of them at least mention the definition we gave earlier by Haag & Eckhardt: *"Shadow IT is hardware, software, or services built, introduced, and/or used for the job without explicit approval or even knowledge of the organisation"* [31].

According to this definition, an employee using non-company cloud storage solutions because the client wanted the files transferred that way, or an employee building a website to help with client projects that are not officially company-supported, would thus use shadow IT.

We employed the shadow IT topology by Mallmann et al. [48], which suggested a division into four distinguished types of shadow IT to further differentiate (see Table 1).

2.2 Usable Security and Mental Models

Organisations need the ability to detect shadow IT/security and its causes. Managing cybersecurity risks should be guided by involving users rather than deploying standard solutions. Kirlappos et al. [40] and Brandon et al. [13] define actual security as *"the security provided by a system in practice, determined by (1) the security of the underlying technologies and (2) the extent to which users adopt the intended secure behaviour,"* but note that clear directives are missing.

Mental models shape behavior in specific situations. To synthesize some key findings from [66], a 'mental model' was defined as some functional internal construct that operates similarly to the process it represents [17]. According to Johnson-Laird [36], it constitutes a framework based on life experiences, perceptions, and understanding of the world.

Mental Models of Security: Given the difficulty of defending against unknown threats, it is presumably crucial for users to stay informed about potential vulnerabilities, thus reducing the probability of a threat actor exploiting them. Researchers in the fields of usable security and human-computer interaction increasingly rely on users' mental models to comprehend user reasoning and engagement with complex security technology. We identify two main categories in the related work.

Mental models of general security and privacy knowledge have been studied in multiple works [6, 7, 14, 49, 51, 53, 67, 69]. They highlighted that a difference in knowledge/mental models between laypeople and experts makes communication between the two groups inefficient [7]. Models are linked to metaphors and heuristics to explain said differences. While they can be useful shorthand approaches, this also explains the shortcomings: depending on the underlying simplifying heuristic, different aspects of the more complex real-world scenario are left out, in turn leaving different gaps [15]. Wash [67] showed potential dangers of security threats abusing such gaps but pointed out that "even *wrong* mental models produce good security decisions" [68]. Similar to the laypeople/experts differences, we expect different branches in the organisation to hold different mental models. Blythe & Camp [12] postulated an implementation approach for security mental models that aimed to allow for predictions of user behaviour; a valuable stepping stone when developing end-user-focused training. However, one would not need to enforce *correct* models if the mental models already present lead to *usable* security models [68].

Besides the mental models on general security aspects, multiple research works explored **mental models of specific security concepts and technologies** [1–3, 11, 19, 20, 27, 43, 46, 60, 63, 72]. They range from a study of VPN usage habits and preferences among students and general VPN users [20], over exploring adversarial machine learning mental models among practitioners [11], to examinations of the mental models of German office workers' privacy perceptions [63]. Similar to [20], we adopted a mixed-method approach to explore the shadow IT usage patterns in a quantitative survey and interviewed a diverse set of employees to gain insights into their shadow IT perceptions and related mindsets. In line with [63], we targeted the corporate population because the shadow IT phenomenon is specific to the organisational context.

Differences in Mental Models: A study by Staggers and Norcio [61] illustrated that there are big differences in the mental models of experts and non-experts, confirmed by multiple later studies [7, 25, 45]. Moreover, [7] illustrated that there is a link between the mental models of security risks and expertise in security. All these publications reported discrepancies between the mental models of participants in different groups. While previous studies indicated that non-expert would tend to be more careless and ignore warnings [14, 24, 38, 71], more recent studies showed that expertise also lead to ignored warnings, but for different reasons [54], turning security effort and potential harm into a cost-benefit consideration [5].

We explore how groups of practitioners regard cybersecurity concepts, implying differences in mindsets depending on

group composition. Understanding how to influence behavior based on a groups prevalent mindsets may facilitate protecting all end-users.

3 Research methods

To answer our research questions, we conducted a mixed-method case study. We conducted an exploratory survey to gain quantitative insights into the current shadow IT situation in the organisation (RQ1), followed by semi-structured interviews to get a qualitative understanding of survey results (RQ1) and employees' in-depth experience with shadow IT (RQ2 and RQ3). White [70] recently advocated for this integration. The benefit of doing both was that we could potentially show *if* any shadow IT was present through the survey and then follow up with an interview to assess *why* this was potentially the case and how the participants thought about the matter. Due to the anonymous nature of the survey, we could not directly link a participant's survey responses to their interview. The survey was conducted in English; interviews were in Dutch or English, depending on participant preferences.

To differentiate shadow IT types, we relied on the topology by Mallmann et al. [47] (cf. Table 1). In consultation with cybersecurity experts at the organisation, we created the following scenarios where shadow IT might occur:

S1: *(Shadow IT occurring in)* Specific client projects;
S2: *(Shadow IT occurring in)* General work tasks, so not for specific projects;
S3: *(Shadow IT occurring in)* Personal use.

The taxonomy and scenarios serve as the backbone of the survey and guide the structure and content of the questions.

Case Organisation Context: At the organisation where we conducted our study, most employees are academically trained (cf. Table 2) and work on client projects or long-term deployments, supported by the back office. Data security is crucial since the consultancy tasks they perform touch sensitive data daily.

Despite a well-defined information security policy for responsible software and hardware use (covering shadow IT management), employees enjoy some freedom to use solutions beyond the organisation's default list. These default tools are promoted through the acceptable use policy and available via the organisation's *app store*. Additional software can be downloaded, but installation requires justification through a prompt. Software usage is regularly compared against a blocklist and violations result in email notifications; we lack information on subsequent escalation steps.

Both laptops and mobile phones are managed; phones without the company portal installed on them (i.e., without an endpoint management tool) are denied access. Employees receive *cybersecurity training* during onboarding, which covers the aforementioned acceptable use policy; it states that work tasks should be performed using tools provided by the organisation. They also receive training on phishing, including campaigns targeted at spotting and reporting attempts.

The second author was an intern at the organisation during the project, but he conducted this research independently. Besides providing input to the research team, the organisation's employees did not significantly bias the study's design or implementation, and the research team ensured the scientific rigour of the project. The organisational affiliation and internship status of the researcher were primarily logistical. They did not affect the integrity of the research process. The remaining authors have no ties to the organisation.

3.1 Survey

Design & Implementation: The core of the survey contained four main sections: the first three sections each contained three questions specific to types of shadow IT in specific scenarios (cf. Section 3). The types were *Cloud services*, *Self-installed applications*, and *Self-made solutions*, which fall outside the scope of their organisation. The fourth section covers the *Self-acquired devices* and the use of *personal emails* as types of shadow IT. These sections were refined through pilot testing, with an *Other* option provided for unlisted application types. The survey's final format emerged from an iterative feedback process. We performed three pilot rounds, each involving two new participants. Following this, we conducted a split test with a within-subjects design, comparing the two most promising survey versions. For an anonymised copy of the final survey questionnaire, see dataset. The survey was administered through the Qualtrics platform of Utrecht University[1].

In addition to the core questions, the survey included supplementary sections on informed consent, demographics and background (cf. Table 2), detailed survey instructions, and the opportunity for participants to leave their email addresses to enter a raffle and opt-in for follow-up interviews.

Recruitment: Data collection took place in April and May 2023, targeting 2000 potential participants via mailing lists, which included detailed study information, a survey link, and a flyer with a QR code. Additional printed flyers were placed in the organisation's offices, supported by direct explanations of the study's aim. Participants could win one of four prizes (two gift cards and two goodie bags), with winners announced in early June 2023.

Out of 638 initial responses, 458 were complete. To ensure data reliability, 8 outliers in completion time were excluded because their time fell beyond $\mu \pm (2\sigma)$ [35]. Overall, 70% of respondents fully completed the survey.

Participant Demographics: Table 2 provides a summary of demographics and background. Our survey's gender distribution mirrors that reported in the organisation's annual report. The hierarchical rank structure in our data reflects the pyramid shape seen in similar organisations; more lower ranks

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

and fewer higher ranks. The spread across departments aligns with the organisation's internal distribution (cf. Table 3).

Data Analysis: Our survey included multiple-choice questions with the option for multiple answers. To analyse patterns of shadow IT usage across departments and ranks, we applied χ^2 if we had 80% of cells with values ≥ 5. Otherwise, we used Fisher's exact test, requiring the tested variables to be mutually exclusive. For this, we added a value indicating the absence of a particular shadow IT type in a group, ensuring exclusivity with instances where shadow IT was reported. We then conducted the statistical tests for each shadow IT type, answer option, scenario, and group individually. We adopted 5% as a threshold for α (i.e., the probability of committing a Type-I error). To report the effect size of observed trends, we used ϕ value, categorising the effect as *negligible* for $|d| < 0.2$, *small* for $0.2 \leq |d| < 0.5$, *moderate* for $0.5 \leq |d| < 0.8$, and *strong* for $|d| \geq 0.8$ [22]. To identify specific groups contributing to significant differences, we conducted post-hoc analyses using *residuals* for the χ^2 test [58] or *pairwise comparison* with the Bonferroni correction for Fisher's test results [59].

3.2 Interview

Interview Protocol: We followed the recommendations by [64] to create our interview protocol. The interview questions covered: (i) understanding of shadow IT, (ii) reasons for using shadow IT, (iii) perception of shadow IT usage implications, (iv) awareness of relevant organisational policies, (v) how shadow IT is discussed amongst colleagues, and (vi) how well-informed the participant feels about shadow IT.

Following Castillo-Montoya's guidelines [16], we designed our interview questions to align with our research goals. Topics were introduced before asking the main questions, and specific probes were prepared to elicit in-depth discussions on the perceived risks and implications of shadow IT. We conducted six pilot interviews with practitioners to refine our interview protocol, ensuring clarity and preventing misinterpretation. These led to only minor adjustments in question sequencing and phrasing, allowing us to include them in our final data set. For the interview guide cf. Appendix Section B.

Interviews were conducted in participants' native languages – predominantly Dutch, with two in English. Interviews were held in person; alternatively, we used Microsoft Teams, chosen for its sector popularity and its support for privacy-compliant recording.

Participants Recruitment and Demographics: We invited interview participants through an opt-in question in our survey, conducting the recruitment in two phases. Initially, we employed a dual sampling strategy for a balanced sample. *Cluster sampling* grouped participants by department (cf. department row in Table 2), while *stratified sampling* within these clusters aimed to include all ranks (cf. ranks row in Table 2). This led to 15 interviews across four departments, covering all ranks. Following an analysis of this first phase, we sought additional participants to address gaps, such as the absence of the IT department. In the second phase, we managed to include two more from management and 15 from client-facing roles. Table 4 presents the distribution.

The 32 interviews each lasted 20-35 minutes. Limited by time and resources, we engaged with only four members of the management staff and were unable to recruit participants from the IT department. See Table 5 for participant demographics and background information.

Codebook Creation and Analysis: We used Atlas.ti [2] for open and axial coding to explore shadow IT's facets, using the interview guide to define codes and link quotes to concepts. To ensure the reliability of the results, we followed Barbour's multiple-coding approach [8], refining the codebook over six initial interviews until achieving consistent agreement between the two researchers (Krippendorff's alpha > 0.9). With this codebook, one researcher coded the remaining interviews,and the results were validated by the second researcher. All conflicts were discussed and resolved. Discussions with a third researcher in cases where the prior two could not come to an agreement ensured a correct frame of reference and minimized potential bias [28].

3.3 Ethical considerations

The Ethics Review Board of the authors' institution approved the study protocol and data management plan under reference Bèta S-23055. Participants were informed about the study details, risks, and our use of collected information before obtaining their consent (cf. Appendix Section B). Access to the survey platform was restricted to the research team and was set to exclude personal identifiers like IP addresses. Due to the sensitivity of raw survey data, only aggregated results will be published in agreement with the organisation. Interview transcripts were anonymised, participants reviewed these before final consent for publication was obtained. All personal data and raw sources were deleted post-study. Participants are referred to by numerical codes (e.g., "P03") with quotes used only from those who provided explicit consent.

4 Results & Discussion

For qualitative codes, we provide illustrative statements systematically representing corresponding themes identified across multiple interviews. These statements provide grounding for each code across all groups of participants. Section A in the Appendix provides detailed results from our qualitative analysis of the interviews. To answer RQ1, we combined the quantitative findings from the survey with qualitative insights relevant to this question identified in the interviews. The interview results covered RQ2 and RQ3.

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

Gender		Age	32.7 ±9.4	Work experience	8.74 ±9.0	Rank		Education	
Male	56%	[18-25]	22%	≤5 years	45%	junior	39%	University education (WO)	86%
Female	43%	[26-30]	36%	6-10 years	24%	senior	24%	Higher Professional	
N.A.	1%	[31-40]	22%	11-20 years	15%	manager	15%	Education (HBO)	10%
		[41-50]	13%	21-30 years	11%	senior manager	12%	PhD	1%
		[50+]	7%	30+ years	5%	management	9%	Other	3%

Table 2: Summary demographics of survey participants, n=450

	Survey	Organisation*	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%

Note: a minor random noise has been introduced to the numbers in the "Organisation" column to prevent guessing the organisation's identity.

Table 3: Department Distribution Comparison

	Jun.	*Sen.*	*Mngr*	*Sen. mngr*	*Mngmnt**	**Total**
Client-fac.	6	4	5	6	-	21
Support	1	2	3	1	-	7
Mngmnt	-	-	-	-	4	4
IT	0	0	0	0	-	0
Total	7	6	8	7	4	**32**

* according to the organisational structure, all employees in the management (Mngmnt) department also holds management rank and no management employees work in other departments.

Table 4: Participant Cohort Matrix for the Interviews

ID	Rank	Department	Degree	Age	Experience
P1	Junior	Client-facing	MSc (University)	18-25	0-3
P2	Senior	Client-facing	Postmaster	26-30	3-6
P3	Junior	Client-facing	MSc (University)	18-25	0-3
P4	Junior	Support	MSc (University)	18-25	0-3
P5	Manager	Support	Applied MSc (HBO)	51-59	30+
P6	Manager	Support	*MBO**	51-59	26-30
P7	Management	Management	MSc (University)	51-59	26-30
P8	Manager	Support	MSc (University)	36-40	16-20
P9	Senior Manager	Client-facing	Postmaster	41-50	16-20
P10	Manager	Client-facing	MSc (University)	26-30	3-6
P11	Senior Manager	Support	Applied MSc (HBO)	41-50	21-25
P12	Senior	Client-facing	MSc (University)	26-30	3-6
P13	Senior	Support	MSc (University)	18-25	0-3
P14	Management	Management	Postmaster	51-59	30+
P15	Senior	Support	PhD	41-50	16-20
P16	Manager	Client-facing	MSc (University)	31-35	7-10
P17	Junior	Client-facing	MSc (University)	26-30	3-6
P18	Junior	Client-facing	MSc (University)	18-25	0-3
P19	Senior	Client-facing	MSc (University)	26-30	0-3
P20	Senior	Client-facing	MSc (University)	31-35	3-6
P21	Senior Manager	Client-facing	MSc (University)	51-59	30+
P22	Manager	Client-facing	MSc (University)	31-35	7-10
P23	Manager	Client-facing	Applied MSc (HBO)	41-50	21-25
P24	Manager	Client-facing	MSc (University)	41-50	16-20
P25	Senior Manager	Client-facing	MSc (University)	36-40	11-15
P26	Junior	Client-facing	MSc (University)	26-30	0-3
P27	Junior	Client-facing	MSc (University)	26-30	0-3
P28	Senior Manager	Client-facing	Postmaster	41-50	11-15
P29	Senior Manager	Client-facing	BSc (University)	60+	30+
P30	Management	Management	Postmaster	51-59	16-20
P31	Management	Management	Postmaster	41-50	26-30
P32	Senior Manager	Client-facing	Applied MSc (HBO)	51-59	26-30

* - MBO stands for Secondary Vocational Education in the Netherlands

Table 5: Interview participant demographics

4.1 RQ1: Shadow IT usage

Employees often use unauthorised external tools for work and personal tasks, with limited awareness of organisational policies. This highlights the need for cybersecurity education and communication. Self-installed applications and cloud services are extensively used, driven by the need for specific functionalities, ease of use, and overcoming IT limitations, especially in client projects.

Survey Results: Usage by Shadow IT Types Figure 1 shows the self-reported usage rate of the software-related shadow IT types across scenarios and the overall personal device usage rate. We could expect the corporate sector to be doing better; however, our survey showed a high level of shadow IT presence (up to 63%). Similarly, Gomez et al. [52] revealed a high level of shadow IT usage in US higher education in a survey of IT professionals.

Self-installed applications have a significant role in the project workflow across departments and ranks. We discovered a statistically significant use of remote workspaces ($Fisher's\ p(Fp) = 0.035$ with a small effect size (ES) ($\phi = 0.34$) for departments), conferencing tools ($\chi^2 p = 0.0025$ with a small ES ($\phi = 0.30$) for departments and $\chi^2 p = 0.00024$ with a small ES ($\phi = 0.37$) for ranks), screen capture ($Fp = 0.037$ with a small ES ($\phi = 0.35$) for departments), and the "other" tools ($\chi^2 p = 0.0032$ with a strong ES ($\phi = 0.82$) for ranks) in *client-specific projects*.

Further analysis using residuals revealed that the support department uses statistically fewer **conferencing tools** ($true\ residual = -2.03$) compared to the other departments, while the management department used statistically more conferencing tools ($true\ residual = 2.02$). When looking at the nature of their work, this makes sense. *Support*, focused on internal tasks, does not need external conferencing tools beyond what the organisation provides. In contrast, the *management* is involved in landing new projects and often requires various conferencing tools like WebEx, Zoom, or Skype.

A similar test for ranks shows the lack of conferencing tools usage amongst the *junior* group ($true\ residual = -2.63$) and the extra presence amongst the *senior manager* group ($true\ residual = 2.13$). Junior employees tend to handle more hands-on work, while the latter are more involved in managing

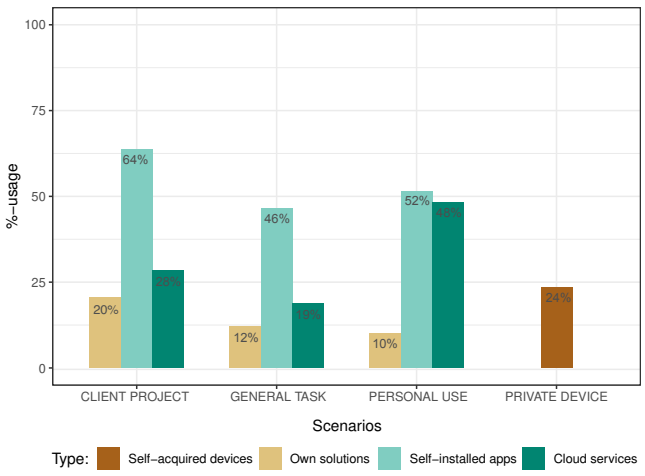


Figure 1: Rate of participants using at least one form of shadow IT. Grouped by scenarios, plus the rate of reported private device usage overall. (n=450)

projects and more frequent communication with clients.

For the *"other"* category, the post hoc test returned a residual value = 2.56, indicating statistically significant use of this category by managers. The reported examples for this category can be further categorised as: (i) data analysis tools (e.g., Azure Data Studio and R Studio) and (ii) networking and remote access tools (e.g., FileZilla, PuTTY, WinSCP, and Wireshark). The post hoc analysis did not confirm statistical significance for the rest of the types. At large, the client-facing department is mainly involved in client projects, demonstrating the biggest variability in shadow IT types used.

In general working tasks, conferencing tools ($\chi^2 p = 0.0033$ with a small ES ($\phi = 0.44$) for ranks) and streaming services ($Fp = 0.0017$ with a moderate ES ($\phi = 0.70$) for ranks) stand out. For personal tasks, streaming services demonstrated statistically significant results ($\chi^2 p = 0.0072$ with a small ES (with $\phi = 0.33$) for ranks).

We find an apparent decrease in the use of self-installed applications in general work tasks vs. 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, thus mitigating risks and preventing occurrences like the QQ Browser in the *management* group.

Cloud services were mostly reported for personal use. Among participants, 38-55% of the responses reported using some cloud services. *"Cloud storage"* was well represented throughout both departments and ranks. We find very high occurrences of Google Drive, Dropbox, WeTransfer, and OneDrive. This might explain why the external cloud storage services are very high in the first two work-related scenarios. If employees are used to storing and sharing files in a certain solution, they might be prone to use these in a work setting, even though the organisation has well-supported cloud storage services. In addition to the larger cloud service providers, we see a few specialised cloud storage applications in the IT staff, like NAS solutions, with several extensions to manage and support this. Initial statistically significant results for browser extensions ($Fp = 0.022$ with a small ES ($\phi = 0.35$) for departments) and browser tools ($Fp = 0.053$ with a moderate ES ($\phi = 0.66$) for ranks) were not confirmed by the post hoc analysis.

Self-made solutions: Employees find the need to *create their own solutions* sometimes, indicating a gap between their unique needs and the tools provided by their organisations. They demonstrate resourcefulness and creativity in using their own software, websites, external spreadsheets, and system couplings, among other solutions. Solutions span from niche calculations to tracking spreadsheets, forecasting models, and task automation. Across all roles, we find that self-built solutions are lower in personal contexts, suggesting that they are driven by work-related needs rather than personal preferences. The patterns imply that all employees, regardless of role, encounter tasks for which existing systems do not offer standard solutions. However, the statistical tests did not reveal any significant differences across cohorts.

Private devices/emails: We do not observe a lot of usage of private devices or personal emails (76% of participants reported no usage), and it is well spread across different ranks and departments. Among users, we identified two prevalent cases: using private devices/emails for 'mailing and communication', including emailing colleagues, forwarding emails to personal accounts, and calling clients and candidates, and 'calendars and reminders', where work and private calendars are sometimes merged, and private reminders can be set for work. Statistical tests did not reveal any significant differences across cohorts.

Interview Results To complement the survey findings, we conducted semi-structured interviews and analysed the reasons behind shadow IT usage and usage-related patterns. We now discuss our qualitative findings.

Reasons for using shadow IT: The main reason, reported by 10 out of 32 (10/32) participants, was the *need for specific functionality* since a participant seeks a certain functionality not covered by the approved solutions: *"Well, it is often for work-related matters that there is no such thing within the current tools [...]"* [P3] Another top reason is *client requirements* (4/32) when the participant had to use a certain shadow IT application because of a client project. On installing unofficial programs, the system prompts for a justification, aiming for conscious decisions as to why users install unsupported 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]

The other reasons are related to the employees' *habits* (8/32) when they work with a certain software for years: *"[. . .]I have worked with it for years, so then it also becomes a habit, and I'm happy with it"* [P5] or because *these tools allow me to do it quickly and easily."* [P3]

A *workaround* (5/32) as a means to get some tasks finished is also mentioned: *"[. . .] 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]

Among the less frequent reasons, we found *insufficient standard solutions*, *time constraints*, *financial feasibility*, and overcoming a *language barrier*. Our findings are aligned with [50] and [18], who emphasised the occurrence of shadow IT to address deficiencies in official IT systems and provide additional reasons for these occurrences.

Policy/awareness/usage gap: Despite the organisational policy forbidding external tools for business-related tasks, Figure 1 shows that employees use them a lot for both work and personal tasks. Implicitly, the policy allows using external tools for private tasks, placing trust in the employee adherence. Monitoring can only detect the tools' usage *in general*, unable to tell private or business tasks apart. These services are used across all job levels and situations, aggregated by ranks and departments. We asked our interviewees what shadow IT means to them and how aware they are of the related organisational policy. Only six participants (6/32), all from the *client-facing department*, were able to define what shadow IT is, while 15 participants demonstrated familiarity with the related policy: *"You may only use applications that are approved by [organisation]. 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]

Participants generally felt informed about shadow IT implications, yet their actions sometimes contradicted this knowledge, highlighting an *awareness-action gap*. Hielscher and Parkin [34] found that effective security awareness programs are often constrained by a lack of clear goals and communication between managers and employees. Shadow IT usage decisions involved evaluating both internal (company-provided) and external (shadow IT) solutions, often requiring consultation with IT teams and higher-ranked individuals, reflecting the organisation's hierarchical structure.

Among the policy-aware participants, we saw that even though there are ways to turn shadow IT into *accredited* IT[3], those seem to be taken only rarely: *"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 needing the functionality. So by approaching IT, you enter a negotiation you need to win [. . .]"* [P22]

A clear split emerges among those *unfamiliar* with the policy (17/32). Some openly admit they do not know it, while others list their cybersecurity courses to prove their knowledge. Some talk about different policies or show other proof of their cybersecurity know-how. It appears cybersecurity is perceived to be crucial in the workplace, and not being up to speed can lead to significant consequences: *"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] One participant had a moment of realisation 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]

Most of our participants believed that they are reasonably (14/32) or well-informed (7/32) about the use of technology: *"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] Some demonstrated adequate knowledge of how to act but did not always follow through: *"I have a good idea of what I should and should not do. However, I do not always fully act like it [. . .]"* [P16]

Shadow IT Perspective: The *"perspective"* of shadow IT refers to a viewpoint shift when working on a client project using client-provided resources: *"So that would mean we would need an environment at the client. This can be a client laptop or environment through [remote workspace]. Both with the tools installed so that the client pays for licenses and puts the responsibility for updating on the client. Moreso to put the risk of these applications in their shoes."* [P22]

This shift places all applications on the client's system outside the organisation's purview. It is commonly observed among employees engaged in client-facing roles, with examples including the use of client laptops, remote workspaces, and client licenses to create distinct work environments.

We observe that participants doing longer projects for a single client often get a physical device in the form of a *client laptop* (7/21)[4]. They need to do a mini-onboarding process to install all relevant software, but in doing so, they mitigate any shadow IT threats for their own organisation:

"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]

In other cases, the employees might get access to a *remote workspace* (4/21) or the client shares the *licenses* for the necessary applications (3/21): *"The client uses a certain ap-*

[3]Present the application to an online service desk, once it passes checks (licenses used, vendors, compliance, etc.), it counts as accredited.

[4]Here we report code grounding within the client-facing group as this observation is specific to this group.

plication, we will copy that and just work from their accounts in those systems." [P10]

4.2 RQ2: Shadow IT Perception

We observed a complex interplay between perceived risks, benefits, and mitigation strategies in shadow IT usage. Shadow IT is used for efficiency gains and cost savings despite awareness of cybersecurity risks like malware and data leaks. Usage strategies seem influenced by participants' mindsets.

Perceived Benefits: Across cohorts, we find a nuanced perception of shadow IT. Participants discussed perceived benefits, noting that certain tools allow them to work more *efficiently* (8/32): *"[Tool] can be used for a variety of things. For example, [. . .] I had to do [working task], I then used that tool, and it just saves me so much time"* [P27] This observation aligns with Pinto et al. [18], who demonstrated that both workaround behavior and shadow IT usage positively impact individual performance.

Participants also consider financial feasibility (*cost benefit*; 3/32) as a reason to use shadow IT: *"[. . .] the costs for the organisation. I mean, if everyone went to IT for every small thing, that would not work [. . .]"* [P16]

Perceived Risks: Our participants frequently related *data leaks* (23/32) to the use of shadow IT: *"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]. Sometimes, they described the concept rather than explicitly naming it: *"In general, it is quite hard to find out who is behind the tool and what exactly they do to your data [. . .]"* [P25]

As a precursor to data leaks, the participants often mentioned the *malware* threat (14/32). The only specific type of malware that was mentioned is a virus. However, some participants described infected or malicious programs:

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

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

Next to malware, *unauthorised access* (10/32) was perceived as possible risk due to shadow IT. Some participants explicitly state a threat actor, while others simply focus on unauthorised access by *some entity*:

"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 [and] exploit this data." [P15]

Non-central governance (8/32) concerns the principle at the core of the potential threats related to shadow IT, even preceding the malware and unauthorised access. Namely, shadow IT instances fall outside of the scope of the organisation, and therefore, the organisation can not perform standardised cybersecurity checks on these instances:

"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 [organisation], even if there might be very evident risks, they will not be aware of this" [P19]

As expected, managers prioritise the organisation's reputation (5/32): *"The biggest risk of all is the reputation damage for [organisation] due to data breaches. Since all the work we do is confidential, and sometimes even holds price-sensitive information"* [P14] It is noteworthy that even junior employees show a high level of awareness about *reputation risk*, suggesting widespread awareness: *"So if we do something that makes [organisation] untrustworthy, this can impact the name and therefore everyone in the organisation"* [P4].

Among the less evident risks of shadow IT, we also encounter *ransomware* (3/32) and *misinformation* (2/32). The latter is mentioned in light of the recent rise of generative Large Language Models: *"[. . .] 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].

Contradictions: We observed several examples where participants illustrated risk comprehension, yet rationalised their own use of shadow IT instances. Specifically, we encountered two situations where participants (identifiers changed) realised that paradox and figured that their behavior was in conflict with the organisation's protocols:

"Yes, you should always be careful with these things. [. . .] We might be already crossing a line here. [. . .] Now, thinking about it this way, I do not think it is allowed. Because it is not a [organisation] tool." [P11]

"We just need to put this into practice. So perhaps I should ask my supervisors about our usage of tools outside the [organisation] toolbox" [P15]

4.3 RQ3: Mindsets of shadow IT usage

Our study revealed a dichotomy in attitudes towards shadow IT, with four mindsets favouring risk aversion and six inclined towards risk tolerance. Individuals' approaches to shadow IT are influenced by evolving mindsets, contexts, and experiences, highlighting the complexity of decision-making in this area and the impact of external factors like discussions or awareness-raising initiatives.

When coding interview transcripts, we noted instances where participants subtly illustrated their conceptualisation of shadow IT. We identified codes representing various mind-

sets and their interplay, reflecting internal drivers influencing participants' attitudes towards shadow IT usage. We found ten distinct mindsets: four risk-averse (35 coded statements among 23 participants), promoting cautious behaviours when dealing with shadow IT, and six risk-taking (37/22), increasing individuals' risk appetite with regard to shadow IT.

4.3.1 Risk-Averse Mindsets

RA1. Consequence-Avoidance Orientation is a mindset where individuals prioritise steering clear of negative outcomes or consequences when making decisions and taking action. We found 17 participants demonstrated a high awareness of various consequences and are therefore cautious to avoid 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]
This is potentially related to prolonged exposure to a tool/service that was perceived as 'bad' by users, thereby lessening their well-being score [21], with the extreme case arguably being complete avoidance.
RA2. Knowledge-Based Conservatism mindset (8/32) is defined by a preference for using established knowledge and wisdom as a basis for decision-making. We noticed that a specific group of participants showed a notably higher level of awareness regarding the concept of shadow IT. They also demonstrated a deeper understanding of the associated risks and implications, thanks to their extensive expertise in information technologies. This equipped them with the knowledge to navigate the challenges posed by shadow IT effectively. We related this mindset to participants' expertise in technology, which influenced more secure behaviour in the context of shadow IT: *"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 that the average Joe here won't think of"* [P7]
RA3. Risk Transfer Mindset (8/32) is characterised by a tendency to transfer risks to external/other entities. In our study, 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 makes it more convenient for clients and helps to mitigate potential shadow IT threats for the organisation.

"I would 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." [P22]
RA4. Cautious Seasoned Judgement mindset (4/32) reflects a thoughtful decision-making approach informed by broad experience, similar to but distinct from *Knowledge-based Conservatism*, which relies on specific expertise. This mindset is not consciously used to guide shadow IT actions, but it manifests in individuals who, similar to a 'cautious seasoned judge', encourage colleagues to appreciate the value of accumulated wisdom and experience in making well-thought-out decisions. Our observations suggest that individuals' combinations of mindsets, incl. learning from past shadow IT usage outcomes, can evolve over time. This mindset can be compared to the practice of introducing security and privacy champions [9, 62] who care about security and might act as those "seasoned judges".

"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]

4.3.2 Risk-Taking Mindsets

RT5. Common Sense Fallacy mindset, prevalent among our participants (11/32), revolves around the idea that discussions about shadow IT and cybersecurity, in general, should be minimal due to an assumed baseline of 'common sense' understanding. Those holding this view believe that individuals should already grasp fundamental cybersecurity concepts.

Individuals with this mindset intuitively know what is acceptable or not within a given context. It is crucial to recognise that not everyone possesses this basic cybersecurity knowledge. Assuming universal understanding can reduce important team discussions, a drawback when dealing with shadow IT. While 'common sense' facilitates decision-making, it can also sideline critical conversations, adversely impacting overall shadow IT behaviour: *"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]
RT6. Illusion of Sufficiency mindset (6/32), wherein an individual erroneously believes they do not require any shadow IT applications, under the assumption that all necessary tools are already provided by their organisation. This notion is exemplified by citing instances of shadow IT, effectively illustrating the 'illusion'. Consequently, individuals with this mindset tend to perceive themselves as immune to related risks, assuming all solutions are sanctioned by their organisation. This misbelief diminishes their vigilance towards potential cybersecurity threats.

It is noteworthy that all participants holding this mindset exhibited a lack of familiarity with shadow IT. This knowledge gap perpetuates the misconception that all the tools they employ are officially endorsed, which may not be the case. This attitude characterises the essence of this mindset: *"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]
RT7. Misguided Sense of Protection (6/32) Individuals hold a false or erroneous belief in their own protection. This mindset is noticeable in our participants, many of whom manifest insecure norms. Participants often recount their experiences with other security measures, such as those addressing phishing and viruses, and consequently, they extrapolate that these

protections extend to safeguarding them against shadow IT.

Consequently, these individuals possess a sense of invincibility, perceiving that the organisation's protection shields them from harm. In the realm of cybersecurity, this excessive perception of invulnerability influences participants' behaviour concerning shadow IT usage. They operate under the false premise that any unauthorised usage or installation would trigger alerts, creating 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 [organisation] if you have something on your system which is not good [. . .]" [P5]

Behaviour akin to this mindset has been pointed out as potentially dangerous [46], citing that erroneous user mental models of systems "*expose users to security and privacy risks.*"

RT8. Performance-Driven Rule Bending mindset (5/32) centred on achieving specific outcomes, even at the expense of adhering to established rules and guidelines. Participants occasionally demonstrate a readiness to disregard or actively circumvent standard cybersecurity protocols to meet work deadlines. This negatively impacts the overall shadow IT behaviour of individuals:

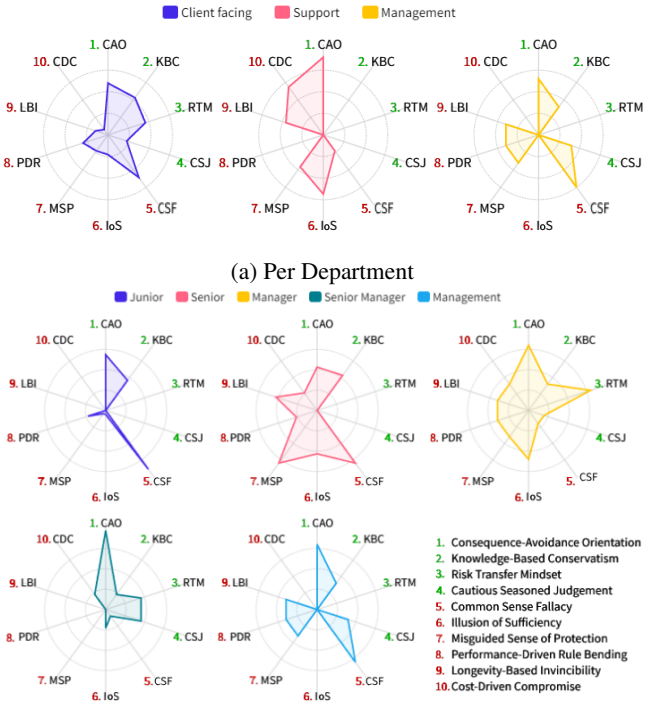
"I cannot explain to a client that certain tasks have not been completed. This means that sometimes employees enter a grey area, perhaps even cross it by doing what they shouldn't. I think everyone is aware of this [. . .]" [P20]

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

RT9. Longevity-Based Invincibility (5/32) Individuals believe that the extended presence of a concept grants them a sense of immunity from adverse effects. This form of survivorship bias leads participants to disregard potential negative outcomes associated with shadow IT, mainly due to their positive long-term experiences with these solutions, fostering a perception of 'invincibility.'

We have observed instances where entire teams have adopted specific shadow IT solutions for an extended period, fostering an illusion of safety among them. Consequently, new employees, introduced to these tools as a longstanding practice, may not fully grasp the associated risks. The attitude of *"we've used it for so long without any issues"* represents this mindset and erodes their vigilance in managing shadow IT instances effectively: *"[. . .] 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]

RT10. Cost-Driven Compromise (4/32) Individuals make decisions based on financial considerations. We have observed a clear pattern among participants, wherein cost savings are explicitly prioritised in their shadow IT decisions. The *"we use it because it is free"* attitude represents this mindset, and it significantly undermines the shadow IT behaviour 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] Security mindsets and organisational security culture are shaping employee behaviour and adopted practices [32]. Schoenmakers et al. [57] revealed that the security mindset involves aspects like proactive monitoring, investigating, and evaluating potential security threats. In our study, we focused on risk-taking and risk-averse mindsets, but similarly to those aspects, our mindsets can potentially manifest at different levels and combinations in employees. Moreover, Ryan et al. [55] identified four security archetypes that are similar to our RA1 and RA3 (or "pragmatics"), RA4 (or "champions"), RT9 (or "optimist"), RT7 and RT8 (or "heroes").



(a) Per Department

(b) Per Rank

Figure 2: Relative Occurrence of Mindsets

4.3.3 Mindset Patterns

We explored the occurrence patterns of certain mindsets across departments and ranks. Figure 2 visualise two cohorts through radar graphs, with different mindsets per axis. The data is normalised to account for varying cohort sizes, focusing on relative occurrences (denoted by the rings in the figures) to identify patterns across different groups.

Departments: Across different departments, we observe distinct patterns of mindset presence, as illustrated in Figure 2a. While four mindsets (RA1, RT5, RT7, and RT9) are prevalent across all departments, most are of a risk-taking nature, suggesting a lack of a general organisation-wide risk-averse mindset. Notably, the *client-facing* and *management* groups exhibit similarities in the combination of risk-averse (RA1,

RA2, RA3) and risk-taking mindsets (RT5, RT7, RT8) due to their overlapping work responsibilities. A mild distinction arises when comparing these two groups with the *support* department, mainly attributable to the absence of risk-averse mental models (except RA1) in the latter.

Ranks: Regarding employee ranks, we identify a few light trends (see Figure 2b). Notably, the risk-averse mindsets RA1 and RA2 are consistently present across all ranks, indicating a widespread awareness of potential shadow IT consequences and expertise that positively influence shadow IT behaviour. Moreover, the risk-averse mindsets RA3 and RA4 were found to be prevalent among higher ranks, such as *manager*, *senior manager*, and *management*. These mindsets align well with the responsibilities and challenges these employees face, suggesting that individuals in higher-level roles adopt a more risk-conscious approach to shadow IT decision-making. This highlights the importance of involving these groups in work scenarios.

5 Implications of Findings & Limitations

In this section, we discuss the implications of the findings reported in Section 4 and provide recommendations for practitioners. Moreover, we discuss the limitations of the study.

Research Implications: Our study explored shadow IT usage and employees' perceptions and attitudes within a large corporate setting. It identified ten key mindsets affecting employees' perceptions of and decisions for shadow IT. The results reveal how these mindsets affect shadow IT behaviours, resulting in risk-averse or risk-taking behaviours in employees.

While no major patterns linked specific cohorts to particular mindsets, the variation across employee groups highlighted the need for broader research across diverse populations to capture the full spectrum of mindsets present. Our portfolio of mindsets can inform future qualitative and quantitative research among various populations and contexts, serving as a foundational framework.

Recommendations for Practitioners: To address the challenges related to shadow IT, based on our findings, we suggest:

- **Transparent Communication:** By fostering an environment where employees feel safe and comfortable discussing their technology needs, organisations can identify and address potential shadow IT instances. Not only can this approach mitigate usage risks of shadow IT, it also builds trust between the IT department and other employees, creating a more cooperative and secure digital work environment.
- **Targeted Shadow IT Awareness Training:** The interviewees often related the knowledge of potential negative consequences of shadow IT to recurring mandatory training. While we did not quantify this trend, the consistent focus on threats and repercussions positively affected employee behaviour, particularly reflected in *Consequence-Avoidance Orientation* and *Knowledge-Based Conservatism* mindsets (see Section 4.3). To foster awareness of shadow IT consequences, we recommend maintaining a training initiative. Previous work [33] suggests an untapped benefit here: educating users about the capabilities of a tool could increase usage, thus potentially boosting the usage of official tools. However, 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. Thus, we recommend tailoring training content to align with the specific needs of various roles, departments, and mindsets, ideally tapping into existing functional models or using functional metaphors, as has been suggested [56, 72].
- **Shadow IT Protocols:** For the employees with *Performance-Driven Rule Bending* mindset, we suggest creating protocols supporting individuals in navigating rule-bending situations while making it as safe as possible. This approach is supported by Pinto et al. [18], who argue that while shadow IT poses certain risks, it also provides significant benefits to individual performance.
- **Track Long-term Instances:** To manage the *Longevity-Based Invincibility* mindset, the IT team could track down the use of long-term-adopted shadow IT tools and uncover their adoption reasons. From there, an informed decision about phase-out, replacement, or take-over can be taken, as per Fürstenau et al. [26].

Finally, we stress the significance of transparent communication regarding information security policies. We emphasise the need to accommodate employees' perspectives and needs in the supplied software, hardware, and training opportunities.

Future work: Given the number of interviewees and the specific organisation targeted here, replicating our research to confirm our findings is viable. We encourage further exploration into how different mindsets converge in decision-making, potentially through a controlled game-like scenario for rich data collection. Understanding how combinations of mindsets impact the resulting shadow IT behaviour would prove valuable to boost overall secure behaviour. This could theoretically be achieved by either hampering risk-taking mindsets or strengthening the risk-averse mindsets.

We assume that individuals can hold a combination of various mindsets related to shadow IT. We apply the '*theory of planned behaviour*' [4] and assume that for users to have the intention to display safe security behaviour, there are three main contributing factors. In no particular order, we have first the subjective norm regarding the behaviour, the pressure by one's surroundings to engage in or abstain from a behaviour. Secondly, there is the perceived behavioural control; and lastly, the mindset towards the behaviour (called attitude in [4]). We have yet to uncover to what extent certain mindsets are present or how these are influenced by differing situations.

We observed that shadow IT instances are not limited to individual users but also involve departments or smaller groups

within an organisation (e.g., *Longevity-Based Invincibility* mindset). While we have taken certain cohorts to horizontally and vertically divide the employee group for analysis, we have not seen obvious patterns of shadow IT instances across the chosen cohorts. Future research might uncover what different cohorts provide the most optimal division of individual groups, such that clear patterns of combinations of shadow IT mindsets in certain groups become apparent.

Limitations: To support our readers in an appropriate contextualisation of our results, we discuss the key limitations and describe how we reduced their impact. The survey's respondent composition mirrors the larger organisation, leading to a prevalence of *client-facing* group responses and fewer from other groups. This difference in group sizes may challenge the χ^2 test's validity, which requires over 80% of cells to have values above 5. Thus, we adopted Fisher's exact test for scenarios where the χ^2 test's assumptions were not met.

Our survey design might be lengthy and holds some nuances. We split the survey into four shadow IT types and set it in three scenarios. Thus, if respondents do not read the explanation and context carefully enough, the responses can be prone to errors. To prevent errors, we placed clear instructions after the demographics part, emphasising the focus on applications beyond the organisation's norm and clarifying scenario contexts, and validated these changes in a pilot test.

Another limitation of the survey was receiving challenging explanations, such as *support* department participants, who mainly deal with internal tasks, answering sections on client-specific projects—possibly indicating misunderstandings or inattention. However, given the support group's small portion (7.8%) of our sample, its impact seems minimal, aside from their notably lower use of conferencing tools (see Section 4.1).

Given the sensitivity of the shadow IT topic, our study might be prone to social desirability bias (SAB), prompting participants to provide socially acceptable rather than truthful responses. To mitigate it, the survey was anonymous [29], the interview was kept confidential, indirect questioning was used [44]. Our interviewees expressed freedom to express "undesirable" opinions without withdrawing from the interview (see P25 at Section 4.1), proving that the researcher was able to establish trusting rapport with the participants [10]. For this, we developed a uniform protocol to probe participants' shadow IT perceptions, observing varied question comprehensions among participants from different groups. To maintain the interview flow, we sometimes provided application examples, which may have influenced responses.

A significant limitation is our failure to interview IT department staff, although some were surveyed. Future research should bridge this by interviewing IT professionals to understand their shadow IT mindsets, similar to what has been done regarding 'the' security mindset [57]. While our study reflects large corporate environments, broader validation across different organisational contexts is recommended.

Our study did not examine the impact of the growing trend towards remote work on shadow IT. This evolving work dynamic calls requires further investigation to understand its effects on shadow IT practices within organisations, offering important insights for both academia and industry.

6 Conclusion

This work investigated the perception of the shadow IT concept: the occurrences of shadow IT, how its usage varies across different cohorts in a large organisation, and the mindsets associated with it. We find that shadow IT is an intertwined part of the organisation's IT environment, observing all types differentiated by [47]: *cloud services*, *self-installed applications*, *self-built solutions*, and *personal devices*. We notice that users opt for familiar tools and services to meet work or personal needs; if these tools are not provided by default in the organisation then users tend to opt for shadow IT.

Most threats associated with shadow IT are perceived differently across cohorts, reflecting varying degrees of risk awareness and differing risk-mitigating approaches. Despite this awareness, we found inconsistencies and gaps in acting upon this awareness, resulting in an *awareness-action gap*.

The understanding and perception of shadow IT across cohorts are conceptualised through ten different mindsets. We differentiate *risk-averse* mindsets from *risk-taking* mindsets and propose that individuals typically hold a combination of these based on several personal and work-related factors and their current context. We consider that a combination of these mindsets influences individual shadow IT behaviour.

This research provides comprehensive and practical insights into employee perceptions of shadow IT. It points towards 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 recommend the following measures: (i) fostering an environment where employees can openly discuss their technology needs, (ii) maintaining high awareness through tailored training, (iii) creating shadow IT protocols for certain scenarios, and (iv) tracking long-term shadow IT instances and conducting their risk assessment. This investigation of shadow IT, while providing practical insights and recommendations, also identifies the need for future work in understanding the behavioural impact of the combination of shadow IT mindsets. By exploring these implications, organisations can better manage shadow IT, minimising potential risks while maximising the benefits.

Data Availability: Data (incl. survey and interview questionnaires, aggregated survey results, summarized demographic information, and de-identified transcripts) is made available via Utrecht University data publication platform Yoda for a minimum period of 10 years [65].

Acknowledgements: We would like to thank all the reviewers for their insightful, constructive, and supportive comments. Their valuable feedback has significantly enhanced the quality of this research.

References

[1] Noura Abdi, Jose M. Such, and Kopo M. Ramokapane. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In Heather Richter Lipford, editor, *Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS)*, pages 451–466, Santa Clara, CA, USA, 2019. USENIX Association.

[2] Ruba Abu-Salma, Elissa M Redmiles, Blase Ur, and Miranda Wei. Exploring User Mental Models of End-to-End Encrypted Communication Tools. In Lex Gill and Rob Jansen, editors, *Proceedings of the 8th USENIX Workshop on Free and Open Communications on the Internet (FOCI)*. USENIX Association, 2018.

[3] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the Adoption of Secure Communication Tools. In Úlfar Erlingsson and Bryan Parno, editors, *Proceedings of the 38th IEEE Symposium on Security & Privacy (S&P)*, pages 137–153. IEEE, 2017.

[4] Icek Ajzen. The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(2):179–211, 1991.

[5] Devdatta Akhawe and Adrienne Porter Felt. Alice in warningland: A Large-Scale field study of browser security warning effectiveness. In *22nd USENIX Security Symposium (USENIX Security 13)*, pages 257–272, Washington, D.C., August 2013. USENIX Association.

[6] Bilal Al Sabbagh and Stewart Kowalski. Developing social metrics for security modeling the security culture of it workers individuals (case study). In *Proceedings of the 5th International Conference on Communications, Computers and Applications (MIC-CCA)*, pages 112–118. IEEE, IEEE, 2012.

[7] Farzaneh Asgharpour, Debin Liu, and L. Jean Camp. Mental models of security risks. In Sven Dietrich and Rachna Dhamija, editors, *Proceedings of the 12th International Workshop on Usable Security (USEC)*, volume 4886 of *Lecture Notes in Computer Science*, pages 367–377. Springer, 1 edition, 2007.

[8] Rosaline S Barbour. Checklists for improving rigour in qualitative research: a case of the tail wagging the dog? *British Medical Journal*, 322(7294):1115–1117, 2001.

[9] Ingolf Becker, Simon Parkin, and M Angela Sasse. Finding security champions in blends of organisational culture. *Proc. USEC*, 11:124, 2017.

[10] Nicole Bergen and Ronald Labonté. "everything is perfect, and we have no problems": detecting and limiting social desirability bias in qualitative research. *Qualitative health research*, 30(5):783–792, 2020.

[11] Lukas Bieringer, Kathrin Grosse, Michael Backes, Battista Biggio, and Katharina Krombholz. Industrial practitioners' mental models of adversarial machine learning. In Apu Kapadia Sonia Chiasson, editor, *Proceedings of the 18th Symposium on Usable Privacy and Security (SOUPS)*, pages 97–116. USENIX Association, 2022.

[12] Jim Blythe and L Jean Camp. Implementing mental models. In Lorrie Faith Cranor, editor, *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS)*, pages 86–90. USENIX Association, 2012.

[13] Merel Brandon, Hanna Kathrin Schraffenberger, Wouter Sluis-Thiescheffer, Thea van der Geest, Daniel Ostkamp, and Bart Jacobs. Design principles for actual security. In *Proceedings of Nordic Conference on Human-Computer Interaction (NordiCHI)*. ACM, 2022.

[14] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2010.

[15] L Jean Camp. Mental models of privacy and security. *IEEE Technology and society magazine*, 28(3):37–46, 2009.

[16] Milagros Castillo-Montoya. Preparing for interview research: The interview protocol refinement framework. *The qualitative report*, 21(5):811–831, 2016.

[17] Kenneth James Williams Craik. *The nature of explanation*, volume 445. CUP Archive, 1967.

[18] Aline de Vargas Pinto, Iris Beerepoot, and Antônio Carlos Gastaud Maçada. Encourage autonomy to increase individual work performance: the impact of job characteristics on workaround behavior and shadow it usage. *Information Technology and Management*, 24, 2023.

[19] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. Investigating system operators' perspective on security misconfigurations. In Michael Backes and XiaoFeng Wang, editors, *Proceedings of the 25th ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1272–1289. ACM, 2018.

[20] Agnieszka Dutkowska-Zuk, Austin Hounsel, Amy Morrill, Andre Xiong, Marshini Chetty, and Nick Feamster. How and Why People Use Virtual Private Networks. In Kurt Thomas Kevin Butler, editor, *Proceedings of the 31th USENIX Security Symposium (USENIX Security)*, pages 3451–3465. USENIX Association, 2022.

[21] Sindhu Kiranmai Ernala, Moira Burke, Alex Leavitt, and Nicole B. Ellison. Mindsets matter: How beliefs about facebook moderate the association between time spent and well-being. In *Proceedings of the 2022 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2022.

[22] Christopher J Ferguson. *An effect size primer: A guide for clinicians and researchers.* American Psychological Association, 2016.

[23] Forbes Insights. Perception gaps in cyber resilience: Where are your blind spots? *Forbes*, 2021.

[24] Batya Friedman, David Hurley, Daniel C Howe, Edward Felten, and Helen Nissenbaum. Users' conceptions of web security: a comparative study. In Dennis Wixon, editor, *Proceedings of the 2002 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 746–747. ACM, 2002.

[25] Steve M Furnell, Peter Bryant, and Andrew D Phippen. Assessing the security perceptions of personal internet users. *Journal of Computer Security*, 26(5):410–417, 2007.

[26] Daniel Fürstenau, Hannes Rothe, and Matthias Sandner. Leaving the Shadow: A Configurational Approach to Explain Post-Identification Outcomes of Shadow IT Systems. *BUS INF SYST ENG*, 63, 2020.

[27] Kevin Gallagher, Sameer Patil, and Nasir Memon. New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. In Sonia Chiasson and Matthew Smith, editors, *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS)*, Santa Clara, CA, USA, 2017. USENIX Association.

[28] Lucia Garcia and Francis Quek. Qualitative research in information systems: time to be subjective? In Janice I. DeGross Allen S. Lee, Jonathan Liebenau, editor, *Proceedings of the 8th International Federation for Information Processing (IFIP)*, pages 444–465. Chapman & Hall, Ltd., 1997.

[29] Ahmad Nauman Ghazi, Kai Petersen, Sri Sai Vijay Raj Reddy, and Harini Nekkanti. Survey research in software engineering: Problems and mitigation strategies. *IEEE Access*, 7:24703–24718, 2018.

[30] Marie-E. Godefroid, Ralf Plattfaut, and Björn Niehaves. IT Outside of the IT Department: Reviewing Lightweight IT in Times of Shadow IT and IT Consumerization. In Frederik Ahlemann, Reinhard Schütte, and Stefan Stieglitz, editors, *Innovation Through Information Systems*, pages 554–571, Cham, 2021. Springer International Publishing.

[31] Steffi Haag and Andreas Eckhardt. Shadow IT. *BUS INF SYST ENG*, 59(6):469–473, 2017.

[32] Julie M. Haney, Mary Theofanos, Yasemin Acar, and Sandra Spickard Prettyman. "we make it a big deal in the company": Security mindsets in organizations that develop cryptographic products. In William Enck and Adrienne Porter Felt, editors, *Proceedings of the 27th USENIX Security Symposium (USENIX Security)*. USENIX Association, 2018.

[33] Maximilian Häring, Eva Gerlitz, Matthew Smith, and Christian Tiefenau. Less about privacy: Revisiting a survey about the german covid-19 contact tracing app. In *Proceedings of the 2023 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2023.

[34] Jonas Hielscher and Simon Parkin. "What Keeps People Secure is That They Met The Security Team": Deconstructing Drivers And Goals of Organizational Security Awareness. In Patrick Gage Kelley Kelley and Apu Kapadia, editors, *Proceedings of the 20th Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, 2024.

[35] Ihab F Ilyas and Xu Chu. *Data cleaning*. Morgan & Claypool, 2019.

[36] Philip-Nicolas Johnson-Laird. *Mental models: Towards a cognitive science of language, inference, and consciousness*. Harvard University Press, 1983.

[37] Sebastian Käss, Marie Godefroid, Vincent Borghoff, Susanne Strahringer, Markus Westner, and Ralf Plattfaut. Towards a taxonomy of concepts describing it outside the it department. In *Proceedings of the 32nd Australasian Conference on Information Systems (ACIS)*, 2021.

[38] Michaela Kauer, Florian Kiesel, Felix Ueberschaer, Melanie Volkamer, and Ralph Bruder. The influence of trustworthiness of website layout on security perception of websites. In *Current issues in IT security*. Duncker & Humblot, 2012.

[39] Iacovos Kirlappos, Simon Parkin, and M Angela Sasse. Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective Security. In *Proceedings of the 2014 Network and Distributed System Security (NDSS) Sympsoium*, 2014.

[40] Iacovos Kirlappos, Simon Parkin, and M Angela Sasse. "shadow security" as a tool for the learning organization. *ACM SIGCAS Computers and Society*, 45(1):29–37, 2015.

[41] Andreas Kopper and Markus Westner. Towards a taxonomy for shadow IT. In *Americas Conference on Information Systems*, 2016.

[42] Martin Kretzer and Alexander Maedche. Generativity of Business Intelligence Platforms: A Research Agenda Guided by Lessons from Shadow IT. In *Proc. of MKWI*, pages 207–229, 2014.

[43] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. "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)*, pages 246–263. IEEE, 2019.

[44] Dong-Heon Austin Kwak, Xiao Ma, and Sumin Kim. When does social desirability become a problem? detection and reduction of social desirability bias in information systems research. *Information & Management*, 58(7):103500, 2021.

[45] Debin Liu, Farzaneh Asgharpour, and L Jean Camp. Risk communication in security using mental models. In Sven Dietrich and Rachna Dhamija, editors, *Proceedings of the 12th International Workshop on Usable Security (USEC)*, volume 4886 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2007.

[46] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. User Mental Models of Cryptocurrency Systems-A Grounded Theory Approach. In Heather Richter Lipford and Sonia Chiasson, editors, *Proceedings of the 16th Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, 2020.

[47] Gabriela Labres Mallmann, Aline de Vargas Pinto, and Antônio Carlos Gastaud Maçada. Shedding light on shadow it: Definition, related concepts, and consequences. In Paulo Silva Isabel Ramos, Rui Quaresma, editor, *Proceedings of the 18th Conference of the Portuguese Association for Information Systems*, pages 63–79. Springer, 2018.

[48] Gabriela Labres Mallmann, Aline de Vargas Pinto, and Antônio Carlos Gastaud Maçada. Shedding Light on Shadow IT: Definition, Related Concepts, and Consequences. In *Information Systems for Industry 4.0*, Lecturenotes in information systems and organisation, pages 63–79. Springer International Publishing, Cham, 2019.

[49] Heike Märki, Miriam Maas, Michaela Kauer-Franz, and Marius Oberle. Increasing software security by using mental models. In D Nicholson, editor, *Advances in Intelligent Systems and Computing*, pages 347–359. Springer, 2016.

[50] Frauke Mörike, Hannah L Spiehl, and Markus A Feufel. Workarounds in the shadow system: An ethnographic study of requirements for documentation and cooperation in a clinical advisory center. *Human factors*, 66(3):636–646, 2024.

[51] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration. In Rachel Greenstadt, Damon McCoy, and Carmela Troncoso, editors, *Proceedings of the 18th Privacy Enhancing Technologies Symposium (PETS)*, pages 5–32, Barcelona, Spain, 2018. De Gruyter Open.

[52] Selma Gomez Orr, Cyrus Jian Bonyadi, Enis Golaszewski, Alan T Sherman, Peter AH Peterson, Richard Forno, Sydney Johns, and Jimmy Rodriguez. Shadow it in higher education: Survey and case study for cybersecurity. *Cryptologia*, pages 1–65, 2022.

[53] Celeste Lyn Paul and Kirsten Whitley. A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. In Louis Marinos and Ioannis Askoxylakis, editors, *Proceedings of the 1st International Conference on Human Aspects of Information Security, Privacy and Trust (HAS)*, pages 145–154. Springer, 1 edition, 2013.

[54] Robert W. Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. An experience sampling study of user reactions to browser warnings in the field. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18. ACM, April 2018.

[55] Ita Ryan, Utz Roedig, and Klaas-Jan Stol. Understanding developer security archetypes. In *2021 IEEE/ACM 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS)*, pages 37–40. IEEE, 2021.

[56] Leonie Schaewitz, David Lakotta, M Angela Sasse, and Nikol Rummel. Peeking into the black box: Towards understanding user understanding of e2ee. In *Proceedings of the 2021 European Symposium on Usable Security*, pages 129–140, 2021.

[57] Koen Schoenmakers, Daniel Greene, Sarah Stutterheim, Herbert Lin, and Megan J Palmer. The security mindset: characteristics, development, and consequences. *Journal of Cybersecurity*, 9(1), 2023.

[58] Donald Sharpe. Chi-square test is statistically significant: Now what? *Practical Assessment, Research, and Evaluation*, 20(1):8, 2015.

[59] R John Simes. An improved bonferroni procedure for multiple tests of significance. *Biometrika*, 73(3):751–754, 1986.

[60] Eric Spero, Milica Stojmenovic, Zahra Hassanzadeh, Sonia Chiasson, and Robert Biddle. Mixed Pictures: Mental Models of Malware. In Ali Ghorbani, editor, *Proceedings of the 17th International Conference on Privacy, Security and Trust (PST)*, Fredericton, NB,Canada, 2019. IEEE.

[61] Nancy Staggers and Anthony F. Norcio. Mental models: concepts for human-computer interaction research. *International Journal of Man-machine studies*, 38(4):587–605, 1993.

[62] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2021.

[63] Jan Tolsdorf and Florian Dehling. In our employer we trust: mental models of office workers' privacy perceptions. In *Proceedings of the 24th Financial Cryptography and Data Security*, pages 122–136. Springer, 2020.

[64] Daniel W Turner. Qualitative interview design: A practical guide for novice investigators. *The Qualitative Report*, 15(3):754–760, 2010.

[65] Jan-Philip van Acken, Floris Jansen, Slinger Jansen, and Katsiaryna Labunets. Data underlying the research of case study of shadow it mindsets among corporate employees, 2024. Available at https://doi.org/10.24416/UU01-WEIBJU.

[66] Melanie Volkamer and Karen Renaud. Mental models–general introduction and review of their application to human-centred security. *Number Theory and Cryptography: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday*, pages 255–280, 2013.

[67] Rick Wash. Folk models of home computer security. In Lorrie Faith Cranor, editor, *Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS)*, pages 1–16. USENIX Association, 2010.

[68] Rick Wash and Emilee Rader. Influencing Mental Models of Security: A Research Agenda. In Sean Peisert, Richard L. Ford, Carrie Gates, and Cormac Herley, editors, *Proceedings of the 2011 New Security Paradigms Workshop (NSPW)*, pages 57–66. ACM, 2011.

[69] Rick Wash and Emilee Rader. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In Lorrie Faith Cranor, Robert Biddle, and Sunny Consolvo, editors, *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS)*, pages 309–325. USENIX Association, 2015.

[70] Martin S. White. Workarounds and shadow it - balancing innovation and risks. *Business Information Review*, 40(3):114–122, 2023.

[71] Wu, L Min, Robert C Miller, and Garfinkel. Do security toolbars actually prevent phishing attacks? In Robin Jeffries, editor, *Proceedings of the 2006 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 601–610. ACM, 2006.

[72] Justin Wu and Daniel Zappala. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In Sonia Chiasson and Rob Reeder, editors, *Proceedings of the 14th Symposium on Usable Privacy and Security (SOUPS)*, pages 395–409, Baltimore, MD, USA, 2018. USENIX Association.

[73] Stephan Zimmermann and Christopher Rentrop. Schatten-it. *HMD Praxis der Wirtschaftsinformatik*, 49(6):60–68, 2012.

Appendix A Codebook

Codebook levels			Client-facing	Support	Mngmnt	All groups	
Lvl 1	Lvl 2	Lvl 3 / Lvl 4	G	G	G	G	C
Perspective			15	0	0	15	7
	Client laptop		7	0	0	7	7
	Remote workspace		5	0	0	5	4
	Client licenses		3	0	0	3	3
Shadow IT			193	59	19	271	32
	Definition		19	5	4	28	28
		Unfamiliar	13	5	4	22	22
		Familiar	6	0	0	6	6
	Reasons for shadow IT		32	15	1	48	20
		Need for functionality	7	3	0	10	10
		Client requirement	8	0	0	8	4
		Habit	2	3	0	8	8
		Ease of use	4	2	0	6	5
		Workaround	4	1	0	5	5
		Insufficient standard	1	3	0	4	3
		Time constraint	4	0	0	4	3
		Financial feasability	0	2	0	2	2
		Language barrier	1	0	0	1	1
		Personal preference	1	1	1	3	3
	Implications of shadow IT		53	17	10	80	32
		Benefits	7	4	2	13	11
			Efficiency	6	2	2	10	8
			Cost efficiency	1	2	0	3	3
		Risks	46	13	8	67	32
			Data leak	16	4	3	23	23
			Malware	11	2	1	14	14
			Unauthorized access	8	2	0	10	10
			Non-central governance	7	0	1	8	8
			Reputation risk	2	2	1	5	5
			Ransomware	1	1	1	3	3
			Outdated software	1	1	0	2	2
			Misinformation	0	1	1	2	2
	Scenario		22	3	0	25	11
		Approach IT team	6	2	0	8	8
		Approach manager	5	0	0	5	5
		Autonomous due dilligence	5	0	0	5	5
		Approach client	3	0	0	3	3
		Check internal store	1	1	0	2	2
		Discuss with team	2	0	0	2	2
	Types		68	19	4	91	28
		Cloud services	26	8	1	35	17
			Generative LLM	10	1	0	11	10
			Online collaboration	6	2	0	8	5
			Translate tools	3	4	0	7	7
			Cloud storage	3	1	1	5	5
			Browser extension	4	0	0	4	4
		Self-installed applications	36	11	3	50	24
			Streaming services	8	0	0	8	8
			Code editor	5	2	0	7	7
			Other browser	4	3	0	7	7
			Network tool	3	1	0	4	4
			Remote workspace	4	0	0	4	4
			Mobile application	1	1	1	3	3
			PDF reader	3	0	0	3	3
			Conferencing tool	2	0	0	2	1
			File reader	1	1	0	2	2
			Automation software	0	1	1	2	2
			Password manager	1	1	0	2	2
			Version control app	1	1	0	2	2
			Screencapture tool	1	0	1	2	2
			Design tool	1	0	0	1	1
			Virtual machine	1	0	0	1	1
		Self-made solutions	4	0	0	4	2
			Own software	2	0	0	2	1
			External spreadsheet	1	0	0	1	1
			System coupling	1	0	0	1	1
		Private devices	2	0	0	2	2
			Network device	1	0	0	1	1
			Personal laptop	1	0	0	1	1
Policy & Awareness			63	15	9	87	32
	Policy awareness		21	7	4	32	32
		Unfamiliar	9	6	2	17	17
		Familiar	12	1	2	15	15
	Use of technology discussion		26	3	3	32	32
		Formal	11	2	2	15	15
		Informal	10	0	1	11	11
		No discussion	5	1	0	6	6
	Awareness perception		16	5	2	23	23
		Reasonably well-informed	9	4	1	14	14
		Well-informed	6	0	1	7	7
		Not well-informed	1	1	0	2	2
Contradictions			11	7	2	20*	9
Mindsets			46	17	9	72	31
	Risk-averse		25	6	4	35	23
		Consequence-avoidance orientations	9	6	2	17	17
		Knowledge-based conservatism	7	0	1	8	8
		Risk transfer mindset	6	0	0	6	6
		Cautious seasoned judgment	3	0	1	4	4
	Risk-taking		21	11	5	37	22
		Common sense fallacy	8	1	2	11	11
		Illusion of self sufficiency	3	3	0	6	6
		Misguided sense of protection	3	2	1	6	6
		Performance-driven rule bending	4	0	1	5	5
		Longevity-based invincibility	2	2	1	5	5
		Cost-driven compromise	1	3	0	4	4

C abbreviates coverage, the number of different experts mentioning the concept; G abbreviates grounding, the number of times a code occurred in total.. Note: * - the coverage for contradictions occurred at least twice per document; the category was used to code for the two statements that were perceived as being contradictory to each other.

Table 6: Interview Codebook with Coverage and Grounding

Appendix B 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-anonymised transcripts will only be processed by researchers who are collaborating in the study, or who are responsible for assessing its implementation. After analysis, the transcripts will be further anonymised 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.nl 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.....

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.