Beyond the Office Walls: Understanding Security and Shadow Security Behaviours in a Remote Work Context

Sarah Alromaih, *University of Oxford and King Abdulaziz City for Science and Technology;* Ivan Flechais, *University of Oxford;* George Chalhoub, *University of Oxford and University College London*

https://www.usenix.org/conference/soups2024/presentation/alromaih

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.

Beyond the Office Walls: Understanding Security and Shadow Security Behaviours in a Remote Work Context

Sarah Alromaih[1,2], Ivan Flechais[1], George Chalhoub[1,3]
[1]*University of Oxford, Oxford, UK*
[2]*King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia*
[3]*University College London, London, UK*
[1]*{sarah.alromaih, ivan.flechais}@cs.ox.ac.uk,* [3]*g.chalhoub@ucl.ac.uk*

Abstract

Organisational security research has primarily focused on user security behaviour within workplace boundaries, examining behaviour that complies with security policies and behaviour that does not. Here, researchers identified shadow security behaviour: where security-conscious users apply their own security practices which are not in compliance with official security policy. Driven by the growth in remote work and the increasing diversity of remote working arrangements, our qualitative research study aims to investigate the nature of security behaviours within remote work settings.

Using Grounded Theory, we interviewed 20 remote workers to explore security related practices within remote work. Our findings describe a model of personal security and how this interacts with an organisational security model in remote settings. We model how remote workers use an appraisal process to relate the personal and organisational security models, driving their security-related behaviours. Our model explains how different levels of alignment between the personal and organisational models can drive compliance, non-compliance, and shadow security behaviour in remote work settings. We discuss the implications of our findings for remote work security and highlight the importance of maintaining informal security communications for remote workers, homogenising security interactions, and adopting user experience design for remote work solutions.

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

1 Introduction

Organisational security research has primarily focused on user security behaviour within workplace boundaries [42]. User behaviour typically falls into two categories with regard to security policies: those who comply with security policies and those who do not [33]. Within the non-compliant space, researchers have identified shadow security behaviour [38]—where security conscious users come up with their own security practices when they cannot comply with the official security policy.

Along with improvements in collaborative work technologies, the global COVID-19 pandemic pushed individuals outside of organisational perimeters and established remote work as the "new normal". The 2022 workplace trends and insights report [2] revealed that 73% of employees now operate in a hybrid or fully remote setting and nearly half work entirely from home. Interestingly, a third of workers expressed their preference to continue working in a fully remote capacity.

Yet, despite the growing interest in remote working, the existing literature on user security-related behaviour has mostly focused on contexts where remote work is not so prevalent (e.g. [39], [34], [10]). Furthermore, to our knowledge, no user study has been conducted to explore users' security behaviour and shadow practices entirely in the context of remote work. To explore this gap, our overarching research question is: *What are the current security and shadow security practices in remote work?*

To address our research question, we used Grounded Theory [13, 16, 23] to conduct and analyse a qualitative semi-structured interview study with 20 participants engaged in remote work, each employed by a single employer (i.e., an external organisation and not their own business), aiming to explore security related practices within remote work.

Our findings describe three different models which interplay with one another and help describe security practices in remote work. The first consists of a personal security model driven by a variety of external factors, including past experiences, past incidents, qualifications, external advice, and in-

teractions with online services and technologies. The second consists of the current organisational security model which significantly influences the personal model, and consists of security rules and tools disseminated formally through security awareness and training, and informally through interaction with colleagues and the security culture. The third is a model of an appraisal process which individuals use to relate the personal and organisational security models to help them decide which security practices they should follow. This model explains how different levels of alignment between the personal and organisational models can drive compliance, non-compliance, and shadow security behaviour in remote work settings.

In helping to explain security behaviour in remote work, our findings support prior research that notes that shadow security practices can arise from perceptions of inappropriate organisational policies and rules [6, 39]. We discuss the implications of our findings for remote work security, highlighting the challenge of maintaining informal security communications for remote workers to help foster a strong security culture, the need for greater consistency in the experience of security interactions across devices and services, and the wider value of considering the user experience of remote work security in the design of new technology and in the operation of remote work organisations.

The rest of the paper is organised as follows: In Section 2, we give a background overview of related topics. We elaborate on our research methodology in Section 3. We present and discuss our results in Sections 4 and 5, respectively. Finally, we conclude our paper in Section 7.

2 Background

In this section, we will review security compliance and shadow practices within the workplace, followed by an overview of remote work as the context of our research study. Lastly, we will discuss remote work security.

2.1 Security Compliance and Shadow Practices

Security in its simplest form can be described as "*things that should happen, do, and things that shouldn't happen, don't.*" [54]. Therefore, organisations implement various controls and measures to ensure effective security within the workplace. These controls and measures range from technical and non technical solutions to organisational security awareness and training. Among these controls, the information security policy is the most important, since it indicates how workers should behave in order to mitigate security risks [33].

User behaviour typically falls into two categories with regard to security policies: those who comply with security policies and those who do not [29]. Since 1999, Adams and Sasse [3] have noted that for some users it is impossible to meet both security policy requirements and complete their main work task in a timely manner, leading to further studies to suggest a third category, which is shadow security behaviour [38]— where security conscious users come up with their own security practices when they cannot comply with the official security policy.

Shadow security practices have the same characteristics as shadow Information Technology (IT) phenomenon in that they are both covert and unofficial. Shadow IT refers to any hardware, software, and other solutions employed by users without explicit approval or knowledge from their organisations [30, 31]. There are many terms used in the literature to describe this phenomenon, including shadow IT, shadow systems, rogue IT, workaround systems, grey IT or feral systems [52, 56]. Shadow IT solutions can take the form of a simple Excel spreadsheet [52] or a complex application integrated with the official systems [57]. The proliferation of portable devices, cloud technologies, and subscription-based software or services have transformed traditional IT management and contributed to shadow IT becoming more prevalent [44].

Kirlappos et al. [38] investigated security policy non-compliance by interviewing employees within a large organisation. This study revealed instances of shadow security in which employees create workarounds that try to achieve reasonable security goals as a more suitable alternative to prescribed security policies. The researchers suggested that security experts should take cues from these shadow security practices, given that these practices offer a basis for workable security protocols better aligned with employees' workplace goals [39].

2.2 Remote Work As Context

Remote work, also referred to as telecommuting, telework, flexible work arrangements, distributed work and virtual teams [5], is the ability to work outside of an organisation's physical workplace as part of a flexible working arrangement [1]. With respect to location and time, remote work encompasses various modalities, enabling individuals to work from nearly anywhere—primarily from home, but also from other locations such as communal spaces (e.g., libraries, coffee shops) or co-working environments. This flexibility sometimes includes the option for asynchronous work, allowing employees to select their working hours based on their productivity peaks and personal commitments [27]. Additionally, there is the hybrid working model, where employees blend office days with remote workdays as part of their working arrangement to combine the best of both settings [58].

The concept of remote work, whether from home or while on the move, has been in existence for some time [49]. However, with the improvements in information and communication technologies (ICT), the global COVID-19 pandemic pushed individuals outside of organisational boundaries and established remote work as the "new normal" [53]. As a result, remote work has boomed since the COVID-19 pandemic, in contrast to the steady increase observed between 1980 and

2019 [47]. Furthermore, this trend reflects a growing acceptance among employers in allowing employees to work remotely. According to Hansen et al. research [32], from 2019 to early 2023, the proportion of job postings offering new employees the option to work remotely increased by more than threefold in the U.S. and by a factor of five or more in Australia, Canada, New Zealand, and the UK. This growth has significantly expanded knowledge workers' access to job opportunities and better incomes but also posed cybersecurity challenges, despite security not being a frequent priority in this context [22].

2.3 Security of Remote Work

In 2021, a study by Bispham et al. [9] found a lack of research on cybersecurity in remote work and distance education, despite the extensive use of internet and computing technologies in these domains. The authors conducted exploratory in-depth interviews with cybersecurity experts and remote work support staff. The interviews revealed several security challenges associated with remote work, including an uptick in phishing attacks, a higher number of compromised accounts, and an increase in ransomware attacks.

Researchers and industry experts have proposed various solutions to address cybersecurity risks in this context, such as scaling up the use of virtual private networks (VPNs) and Multi-Factor Authentication (MFA), implementing endpoint protection, providing user education on phishing scams, implementing zero trust model [60], establishing robust policies for mobile device management (MDM), and considering cloud migration strategies to protect organisational assets [20, 43, 51]. Nevertheless, as indicated by the exploratory interviews conducted by Bispham et al. [9], "the best approaches to security are unsettled and evolving".

Godlove [25] provided insights for organisations with remote workers regarding data security attitudes and compliance. A survey of 150 remote workers revealed that personal attitude, social pressure, sense of control, and responsibility moderately explain their willingness to follow security guidelines. Yet, despite the growing interest in remote working, the existing literature on user security-related behaviour has mostly been investigated in contexts where remote work was infrequently practised by only a few employees (e.g. [39], [34], [10]), with no focus on shadow security. Our goal is to address this gap by exploring user security behaviour and shadow practices in the context of remote work.

3 Methodology and Research Question

For this exploratory research study, we adopted a qualitative research design, guided by the constructivist approach to Grounded Theory proposed by Charmaz [13] to address our research question: *What are the current security and shadow security practices in remote work?*

Originally proposed by Glaser and Strauss [24], Grounded Theory has shown to be a well-established methodology for exploring security research [19, 50], and is particularly suited to areas of inquiry that have not been widely researched. Also, it allows examining topics and situations from several perspectives, which can lead to comprehensive and deep explanations. It can uncover underlying perspectives, perceptions, and beliefs that influence behaviours, practices, and incidents by examining both rational and irrational aspects [61]. We designed and conducted semi-structured interviews with 20 participants who were working remotely, either fully remote or in a hybrid mode, and we employed the constructivist approach to Grounded Theory by Charmaz [14] as a data analysis method aiming to construct substantive theory through a structured, flexible, iterative and comparative process of analysing the data [15]. An overview of the research process and applied methods is shown in Figure 1.

3.1 Recruitment and Sampling

To recruit our participants, we adopted purposive sampling to initially identify our target participants. This method was complemented by snowball sampling to further expand the participants group [48]. We advertised the study on online platforms, such as LinkedIn and X (formerly Twitter), aiming to recruit individuals working remotely for a single employer (i.e., an external organisation and not their own business), either fully remote or in a hybrid mode. Also, we expanded our pool of participants by encouraging interested individuals to refer us to suitable contacts from their networks, employing a snowball sampling approach [26].

Interested individuals who met our criteria received a study information sheet and a consent form. Upon signing the consent form, they were requested to complete an online questionnaire regarding their demographic information. The demographic information includes participant age, gender, education, location, organisation business domain, current job role, work settings and level of technical competency in computer security. We defined different levels of technical competence (novice, competent, and expert) using a simplified version of Dreyfus' skill acquisition model that has been widely used to define levels for assessing individual competency [18]. Our demographic information questionnaire can be found in Appendix A.

We interviewed 20 participants: 11 reported working fully remotely, while 9 worked in a hybrid mode. A detailed overview of our sample demographics is presented in Table 1.

3.2 Interview Procedure

We conducted semi-structured interviews with 20 remote workers. We designed and structured our interview guide according to the funnel technique [11], starting with general open-ended questions and gradually moving to specific ones. Using this approach helps build rapport with the participants to clarify and obtain more specific information about their

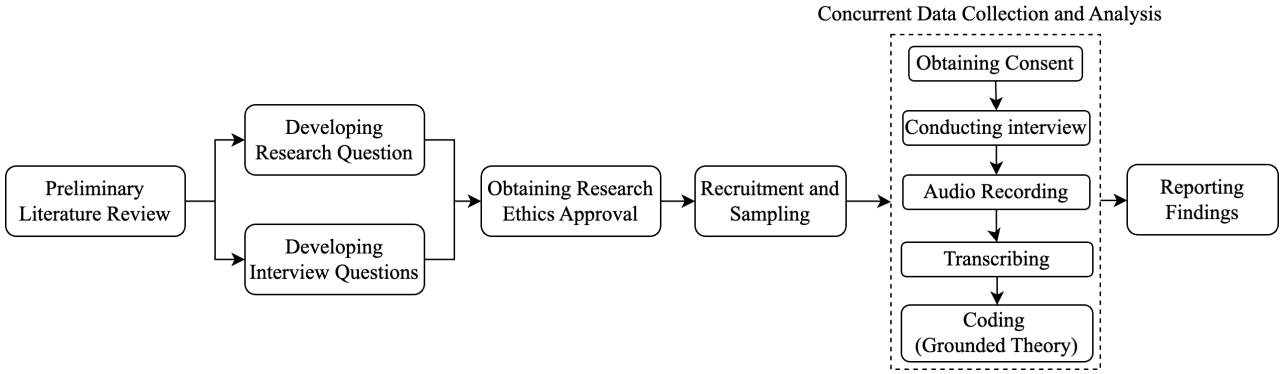

Figure 1: An overview of the research process

P#	Age (M/F)	Degree	Location	Domain	Role (Work Setting)	Competence
P01	25-34 (M)	Postgrad	UK	Tech/IT	Researcher (Remote)	Competent
P02	25-34 (M)	Undergrad	USA	Tech/IT	Products Consultant (Hybrid)	Competent
P03	25-34 (M)	Grad	USA	Tech/IT	Cybersecurity Professional (Hybrid)	Expert
P04	25-34 (F)	Grad	UK	Tech/IT	Product Manager (Remote)	Competent
P05	25-34 (M)	Grad	UK	Consulting	Director (Hybrid)	Competent
P06	25-34 (M)	Grad	UK	Consulting	Associate Software Consultant (Hybrid)	Competent
P07	25-34 (M)	Postgrad	Germany	Tech/IT	Security Awareness Advocate (Remote)	Expert
P08	25-34 (M)	Undergrad	UK	Tech/IT	Full-Stack Developer (Remote)	Expert
P09	35-44 (F)	Grad	UK	Retail	Finance (Remote)	Expert
P10	25-34 (M)	Postgrad	USA	Tech/IT	Editor (Remote)	Novice
P11	35-44 (M)	Undergrad	UK	Consulting	Strategist (Remote)	Competent
P12	35-44 (F)	Undergrad	UK	Energy/Utilities	Head of Operations (Hybrid)	Competent
P13	18-24 (M)	Grad	UK	Education	Research Assistant (Hybrid)	Competent
P14	25-34 (F)	Postgrad	UK	Tech/IT	UX Consultant (Remote)	Expert
P15	25-34 (M)	Undergrad	UK	Tech/IT	Software Engineer (Remote)	Novice
P16	25-34 (M)	Postgrad	UK	Education	Researcher (Hybrid)	Expert
P17	25-34 (F)	Undergrad	UK	Consulting	Lawyer (Remote)	Novice
P18	35-44 (M)	Grad	UK	Tech/IT	Proposition Manager (Hybrid)	Competent
P19	25-34 (M)	Postgrad	UK	Tech/IT	Software Engineer (Hybrid)	Expert
P20	18-24 (M)	Undergrad	UK	Tech/IT	Consultant (Remote)	Novice

Table 1: Participants Demographic Information.

remote work security behaviour. We adopted this approach to help overcome potential reluctance from participants who might be concerned about the consequences of answering such questions honestly or giving answers that are regarded as socially undesirable [7] (i.e. under-reporting undesirable behaviours such as workarounds or non-compliant security behaviour).

The interview was designed to begin by asking general questions about the participant's background, job responsibilities, and remote work experience. Then, questions moved on to security. Participants were asked about whether their remote work has any security or privacy implications, security policies, awareness of security measures, and adherence to security policies, as well as security training for remote work. Lastly, participants were asked questions about their experience with incident reporting and views on security culture at their organisation. Our interview questions can be found in Appendix B.

Prior to each interview, participants were provided with a study information sheet and asked to sign a consent form if they agreed to participate. Subsequently, they completed a demographic information questionnaire. The interviews were conducted virtually by one of the researchers via Zoom or Microsoft Teams, based on the participant's preference. All interviews were audio-recorded, transcribed, and anonymised. The study exclusively recruited volunteers, who were free to withdraw at any time and for any reason, and no compensation was provided to participants.

3.3 Pilot Study

Prior to conducting the main study, we carried out a pilot study to test our semi-structured interview script with 3 researchers from our institution who have experience with remote work. [64]. The pilot study helped to ensure the clarity of questions and to identify any issues, limitations, or other weaknesses in the interview script beforehand [41].

Based on the pilot study results, we were better informed of the average duration of our interviews at 51 minutes. Moreover, further refinements were made by identifying sensitive questions where participants might be concerned about the consequences of answering honestly or might give answers that are perceived as socially undesirable (i.e. breaching security policy). By rephrasing those sensitive questions as indirect questions [21], participants could then answer from the perspective of another person. This method was found to be effective at minimising social desirability bias [7]. The pilot interviews were not included in the analysis of the research study.

3.4 Data Analysis

Following the Constructivist Grounded Theory procedure of systematically collecting, coding, analysing and theoretically categorising data [13,63], the conducted interviews were audio-recorded, transcribed, and anonymised by the primary researcher. Then, we analysed the interview transcripts using Nvivo, a qualitative data analysis software. The primary researcher and a second researcher iteratively performed open coding by analysing each interview line by line in accordance with the Constructivist Grounded Theory approach [63], and

compared the new codes to the growing collection of codes (i.e., constant comparison). Researchers met with the principal investigator regularly during the analysis to discuss and refine the identified codes, then shifted more toward categorising codes (i.e., focused coding). We established links among different codes, based on an intense analysis focused on observing the categories and their interconnections. We began theoretical coding by iteratively rearranging our categories until they stabilised and confirming the connections built among them. The researchers generated a codebook of 217 codes.

Data saturation [16, 28, 55] was observed between the 18th and 20th interviews in which no significant new codes emerged from those interviews, and we stopped interviewing. In total, the study material analysed consisted of 16 hours and 58 minutes of recorded interviews (~81,420 words), each on average 52 minutes long (~4,771 words).

To verify the credibility of the codebook, the third researcher cross checked the codes against the interview transcripts. Additionally, we tested for inter-rater reliability and found that the average Cohen's kappa coefficient for all codes was 0.85, which is over 0.80 indicating strong agreement [46]. We also assessed the reliability and credibility of the findings through a complementary triangulation method, specifically member checking [35], in which we randomly selected three participants and asked for their feedback on our findings. All participants confirmed the identified categories and themes, without providing any comments that would introduce new themes. The Codebook is available in Appendix C.

3.5 Research Ethics

Our institution's research ethics committee reviewed and approved the study. A study information sheet, along with a consent form, was presented to participants prior to each interview. This sheet explained the purpose of the study and how the collected data would be handled. Each participant confirmed that they had understood the information provided and agreed to participate by filling out a consent form, retaining the right to withdraw from the study at any time. No participants withdrew from the study. All interview transcripts were completely anonymised and stored securely.

3.6 Limitations

Our study has some limitations common to qualitative research: First, our qualitative study is limited by our sample size and diversity. According to prior work recommendations [13], we interviewed between 12 and 20 remote workers until no significant new codes emerged. Furthermore, we recruited a diverse group of participants from different industries and job roles to increase the likelihood of at least one participant mentioning relevant findings. However, it is important to note that our sample is relatively young. Additionally, our qualitative study seeks to explain and understand a phenomenon rather than surveying or generalising from a sample.

Second, researchers' skills and personal biases can influence qualitative research quality [40]. To overcome this limitation, the primary researcher who conducted all interviews was trained in designing and conducting interviews, since the quality of the questions asked [8] and the skill of the interviewer [36] determine the depth of the data collected.

Third, our study is based on interviews where participants self-reported their own behaviour, and it is common to have social desirability bias in self-reporting studies [7]. To minimise social desirability bias, open-ended and indirect questions were used instead of leading questions and participants were encouraged to provide in-depth answers in their own words.

Fourth, a limitation of our study is the potential discrepancy between participants' beliefs about their organisation's security policies and the actual policies in place. Participants may misunderstand official policies due to factors such as poor wording, incomplete knowledge, or changes in policy over time. While we acknowledge this limitation, the self-reported views of participants remain relevant to understanding the motivations behind their actions. Future research may benefit from strategies aimed at validating participants' perceptions against documented security policies.

4 Results

In this section, we present the findings of our study and discuss our key findings organized according to the main themes of our analysis, noting that no significant differences were observed between fully remote and hybrid employees during the analysis. The main themes are: Personal Security Model (Section 4.1), External Security Influences (Section 4.2), Organisational Security Model (Section 4.3), and Personal-Organisational Security Appraisal in Remote Work (Section 4.4).

4.1 Personal Security Model

A Personal Security Model is one of the dominant emergent themes from our study. It is composed of an individual's attitude, perception, knowledge, concerns, beliefs and practices related to personal security. Our data analysis showed that this model is constantly shaped and influenced by an individual's experiences and interactions with their environment, as illustrated in Section 4.2. Furthermore, it guides their personal behaviour in safeguarding both their home and remote work security.

Based on our findings, participants whose personal security models are focussed on productivity regard security as a lesser priority, while participants whose personal security models are aligned with strong security beliefs will prioritise proactive security practices regardless of what is stated in the policy. P14 who works as UX consultant with a productivity mindset said "*It's in this day and age where all that you are forced to think about is hustling and productivity and kind of producing, producing, producing every day. Security takes*

a back step, you would not mind ignoring security rules if it means that you can get things done faster if it will help you that day, if it will help you for the next 5 minutes.". Our analysis identifies the following sub-themes within the personal security model: proactive personal security practices (Section 4.1.1) and faulty security practices (Section 4.1.2).

4.1.1 Proactive Personal Security Practices

Several participants mentioned proactive security practices for protecting either their work-related or personal online activities at home. These included, but not limited to, rules of thumb for checking email legitimacy (i.e., checking email headers, looking up unknown email addresses on Google, scrutinising email content), website authentication (i.e., accessing websites from bookmarks, checking security certificates, inspecting website URLs), and installing new software for both work and personal use (i.e., installing software from the original or trusted source, testing untrusted software on a dedicated machine). P03 explained testing new software on a dedicated machine "*what I used to do is exactly before I installed it and started using it, I used to test it on a different machine just to understand clearly what it was doing and then see what it was doing in the background as well and then start using it.*" P16, who works as a researcher, mentioned checking email legitimacy: *"I think I'm more cautious than others because I'm usually validating the e-mail headers."* While P17, a lawyer at a consulting company, stated: "*I probably just copy paste the e-mail into Google and just check if it's legitimate or spam.*"

A timely response to security updates was mentioned as a practice by P18, a proposition manager, who noted:"*I just do it because that's what you're supposed to do. I don't know fundamentally why, but I just know because it's cybersecurity. Whatever security patch exists now, they're going to figure it out. It will be a vulnerability that appears at some point, so they detect it, and they create a patch you have to download.*". Driven by their personal privacy concern, P15, a software engineer, mentioned the practice of using separate browsers for work and personal use. P04, a Product Manager, mentioned using complex passwords and changing them frequently as a personal security practice, even though it is not mandated by their startup company. They said, *"I make sure to have complex passwords and change them every so often even though I am not asked by my company."* Other participants mentioned using personal MFA (N=3), VPN (N=3), and a password manager (N=2).

4.1.2 Faulty Security Practices

Some participants reported faulty security practices stemming from misconceptions or incorrect beliefs. For instance, P17 perceived public WiFi in reputable places as secure, which led them to connect without a VPN. They said, "*I try to go to places that are reputable like Starbucks or those kinds of coffee shops that are chains, and I know they have probably got good, secure WiFi in place for their customers*." Additionally, P08 conveyed another false perception about the safety of public WiFi of the hotel or cafeteria, stating: *"...in my opinion, these places just want to cater to people's needs, which is WiFi. I don't think they have the intention to steal people's data or whatever."* However, it is worth noting that public or open WiFi networks are often unsecured and can be vulnerable to malicious attacks such as 'Evil Twin' attacks [59], making them an easy target for hackers looking to steal data. Both participants mentioned the existence of policies that restrict the use of public WiFi for work. Therefore, good security practices advise using a secure WiFi network or VPN when connecting to public networks.

4.2 External Security Influences

A set of influencing factors on the personal security model was identified during the analysis, as depicted in Figure 5. This model of external security influences plays an important role in shaping aspects of the personal security model, including knowledge, attitudes, concerns, and beliefs. These factors consequently affect the personal security decision-making process for both work and non-work contexts. These influences stem from various sources. The diverse nature of influences on the personal security model, in terms of how and from where individuals are influenced, alters the type of influence. For instance, while knowledge serves as a fundamental influencer, providing individuals with the necessary information to assess risks and adopt protective measures, skills represent a distinct category of influence. Skills encompass the practical abilities individuals possess to implement security practices effectively. This could include proficiency in using security tools or navigating digital environments securely.

The identified sources of influence are: online services and technologies, qualifications, external advice, past incidents, past work experiences, and the current organisational security model. In the remainder of this section, we will describe each source of influence.

External advice is sought by individuals such as P18, a Software Engineer, who seeks guidance from a friend skilled in security, complementing their novice competency in security skills. Additionally, others, like P06, an Associate Software Consultant, noted seeking advice from experienced coworkers or IT staff members. P06 expressed, "*I would just pretty much piggyback on everything that more experienced people have done.*"

Past incidents, such as the breach involving unauthorised access to patient information, as reported by P15, and an incident where P10's colleague's laptop was stolen from their car, underscore the importance of protecting personally identifiable information and work devices for them. Additionally, fraudulent banking transactions experienced by P09 led them to close all tabs when accessing their bank accounts and sometimes only use the bank-associated app, as additional measures they take to enhance security and minimise risks.

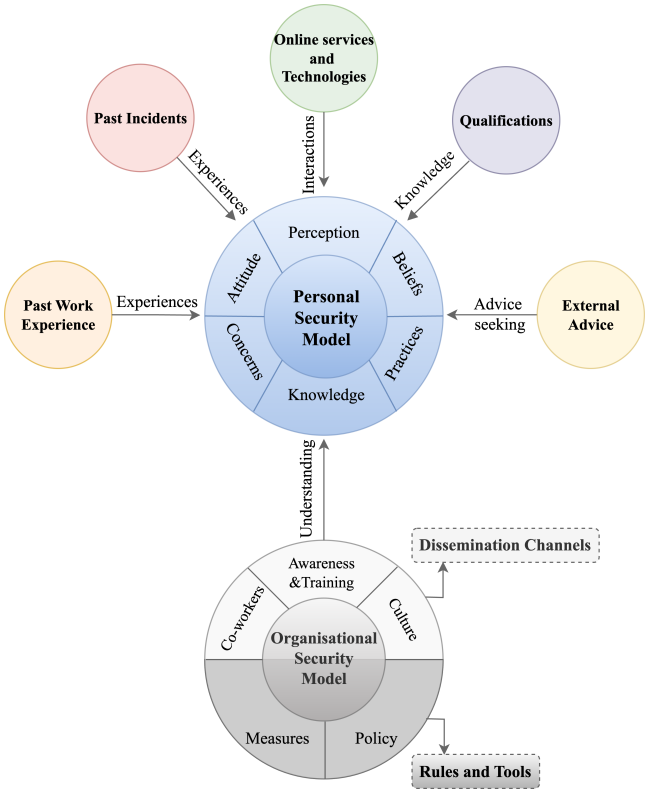

Figure 2: A model of external security influences.

These events serve as valuable lessons that influence the personal security model. In particular, the first two cases emphasise the significance of being vigilant and proactive in safeguarding data and devices to mitigate potential risks and protect oneself from future security breaches.

Online service and technologies, online services encompass various categories, including social media platforms, cloud computing services, financial services, and more. Each category provides a unique user experience and implements distinct security policies and measures. Our analysis revealed evidence suggesting that users can be influenced by their interactions with any type of online service. For example, P20, a Client Solutions Manager, emphasised the impact of encountering policies such as password complexity frequently on their practice in creating personal account passwords. Furthermore, our findings suggest that individuals' perceptions of technology security are often shaped by their interactions with and the popularity of these technologies. P09, for instance, expressed a preference for Apple products, citing their strong reputation for security and consistent security patches, as well as their user-friendly prompts for updates. This consistent approach has significantly influenced P09's attitude toward purchasing their products and installing security updates, despite their limited technical understanding.

Qualifications, our analysis revealed a multifaceted aspect to this source of influence, encompassing differing socioeconomic statuses as a factor alongside educational backgrounds that range from the quality of education to technical specialty, and their relationship to security. Additionally, other factors include digital access to technology, which shapes individuals' personal security models for action in specific situations. For instance, P12 noted that the great job opportunities they experienced strongly shaped their security-related behaviour. P03, a Security Professional by degree, also commented on their practice of testing unknown tools in different virtual machines and related that to their skills and educational background. Moreover, P01's skill in using video editing tools helped them in cropping identifiable elements of patient video while working remotely with a research partner who has a strict policy regarding data privacy.

Past work experience is a source of influence that shares similar characteristics with organisational security influences. Individuals' personal security models are shaped by the skills and knowledge they acquired through their past work experiences, which can manifest as security practices for personal matters, such as adopting a personal password manager, as noted by P04, as well as for managing their work accounts' passwords with their current employer, who does not provide a password manager.

Organisational security model is the final source of influence on the personal security model, and represents how the current organisation tackles remote work security: both by communicating what employees should be doing, and by providing security rules and controls for them to implement (see Section 4.3). The organisational security model relates to the personal security model in a number of different ways. described in more detail in Section 4.4.

4.3 Organisational Security Model

The organisational security model is another emerging theme from our data analysis. Most organisations define security through a combination of rules and tools (i.e., security policies and security measures) that describe what individuals should and should not do, and provide them with the technical means of doing so (e.g., VPN, endpoint management, MFA). These rules and tools are communicated to remote workers by direct and indirect dissemination channels (i.e., security awareness and training, security culture and co-workers). Security culture is defined as a set of collective norms and values, developed through employee interaction with security elements or experience of the behaviour of their colleagues [17, 62].

As illustrated in Figure 5 , individuals develop a personal understanding of security rules and tools. This understanding is significantly shaped by formal initiatives implemented for disseminating information about these rules and tools, such as security awareness and training programmes. However, personal understanding is also influenced indirectly by co-worker dynamics, organisational security culture, and their personal background. Within this theme, our analysis captured how participants relate to elements of the organisational security model for remote work, as will be illustrated in the

following two sub-themes: tools and rules (Section 4.3.1) and dissemination channels (Section 4.3.2).

4.3.1 Rules and Tools

Security Policies: participants reported different perceptions and attitudes towards security policies, ranging from a lack of clear security policy for remote work. P12, when asked about their familiarity with the policy and guidelines for remote work, said "*there is nothing specifically for remote work.*" P03 confirmed that, "*...most companies do not have a policy. They are just sending emails, giving you guidelines. I don't think they developed policies per se.*" On the other hand, with the existence of policies, P05 mentioned accessibility issues related to policy content, saying "*policies are written in such a way that no one wants to read them because they're written in kind of legal jargon, and no one wants to read through 10 pages of legal jargon just to be told that you shouldn't visit bad websites.*" While P14 remarked, "*..these rules are not for everyday people, it's for computer scientists.*"

Participants (N=6) expressed difficulty in remembering the policies. For example, when asked about their familiarity with the security policy and guidelines provided by their organisation for remote work, P04 responded, "*I don't fully remember what it says.*" In addition, participants (N=5) commented on the lack of policy flexibility. P13 expressed, "*I think it is just done more as a blanket, everyone this is the security; this is the restrictions you will have; you are not allowed to download anything, whereas I think it needs to be done on a more specialised basis.*" Meanwhile, P07 referred to the policy as one-size-fits-all.

Participants were asked about what motivates them to follow policy rules. P05 prioritised job performance in terms of efficiency and effectiveness, they commented, "*I think if the policies match how I need to do my job or make my job easier and protect it.*" While privacy concerns were the driver for policy adherence for P8, a Full-Stack Developer. When asked about what motivates individuals to follow policy rules, they said, "*...as long as they can work productively and not be tracked.*"

Security Measures, along with the provided software and hardware for remote work, are essential for upholding adherence to remote work security policies. Participants have varied understanding, perceptions, and attitudes towards remote work facilities and the security measures in place. Some participants perceived the security measures for remote work as heightened (N=6), where the complexity of security protocols can sometimes clash with practical work demands, prompting the adoption of workarounds. Based on participants' statements when asked about the motivations behind adopting workarounds, P06 mentioned, "*... definitely comfort. Honestly, it's because the procedures are very painful.*" And P7 stated, "*the fact that if something is still too difficult, people will find another way that's probably outside policy to make things happen.*"

Additionally, P13 commented on the contrast between heightened security measures in remote work and office settings, suggesting,"*I just think it's because the hardware they give you to try to be more secure because they know you're not in the office space.*" Furthermore, P15, a Software Engineer at a startup company, highlighted the absence of proactive security measures, pointing out a tendency to neglect certain security aspects under the assumption that negative events will not occur while working remotely.

4.3.2 Dissemination Channels

Security Awareness and Training Programs are considered key components of organisational security initiatives, providing essential knowledge and skills to enhance overall security. Conceptually, this aims to influence the knowledge, practices, and concerns of participants to improve their competence and awareness and to align their concerns with those of the organisation (see Figure 5).

Participants have varied attitudes and perceptions toward the security training provided by their organisation. Participants have reported a lack of quality content (N=3), fatigue from training duration (N=3), repetitive training material (N=4), and questioning the necessity to repeat the same training again and again, resulting in a lack of training efficacy. Using aeroplane safety announcements as an analogy, P15 explained that repetition of basic training content decreases attention and engagement. Other participants reported the lack of comprehensive formal security training (N=5). P08 said, "*We haven't really received any sort of security training.*"

Furthermore, a number of participants proposed ideas to improve the efficacy of the training (N=7). P03 suggested that the training should be chunked, focused, and theme-based training sessions. Moreover, their expertise as a security professional enabled them to recognize specific instances that could impact the security practices of others. P03 proposed utilising hypothetical security scenarios as a means to educate employees.While P18 suggested signposting the new training content so workers are aware of what is new and different from the previous training, which would increase their attention and enhance their learning experience. Also, P18 suggested that security training should be customised based on the worker's background and experience, taking into account their familiarity with previous training and relevant knowledge.

The frequency of the training was discussed by several participants (N=5), with participants proposing monthly, bimonthly, or every four months as a suitable frequency. P07 mentioned that, "*basically anything you do less than quarterly in terms of training will be forgotten.*" P06 suggested, "*Something like an hour every 3 or 4 times a year that would be helpful.*" While P03 suggested 15 minutes training that is very well focused and to be done monthly or bimonthly.

Security Culture and Co-workers act as indirect channels through which employees perceive the security rules and

tools, consequently impacting the overall security posture of the organisation. The absence of immediate in-person support while working remotely can significantly impact how employees approach security. P06 highlighted this by saying, "*I think you are a bit more self-reliant when you are on your own. In theory it's the same as in the office you can always reach someone on the company's chat and then you would get help. That's the theory, right? And in practice, you're more on your own when you're working alone, and you try to do workarounds that you wouldn't necessarily try on your own if you were in the office.*" This sentiment underscores the importance of fostering a supportive security culture, especially in remote work settings, where employees may feel isolated and more inclined to find insecure shortcuts to complete their tasks.

Moreover, interaction with co-workers has multiple influences, which could have a positive or negative outcome. One example noted by P18 is the use of WhatsApp by their co-workers to share work documents as an informal communication channel, ignoring the policy rule prohibiting it. As stated by P18, their behaviour was influenced by interactions with other co-workers, leading them to use unauthorised communication channels for work.

4.4 Personal-Organisational Security Appraisal in Remote Work

Our analysis has shown that user security-related behaviour in remote work is influenced by an appraisal process, as depicted in Figure 3. This process occurs between the users' personal security model and their understanding of the organisational security model rules and tools. The understandings of the rules and tools are gained through dissemination channels, collectively forming the organisational security model, as explained in Section 4.3.

We captured various types of alignments between the personal security model and the organisational security model, characterised by the size and extent of their overlap. These alignments have been summarised into three representative models of alignments, as illustrated in Figure 4. These three models reflect how remote workers subjectively understand and interact with the rules and tools of the organisational security model for remote work. Therefore, our assessment of reported security-related behaviour is not grounded in objective truth, but rather in participants' justification and interpretation of these elements.

4.4.1 Personal and Organisational Security Models are Well Aligned (Figure 4A)

This case represents an well integrated situation where users perceive no limitations in the provision of remote work facilities (i.e., software, hardware, security policies, and measures). Participants reported compliant behaviours with security policies (e.g., performing work tasks on organisation-provided devices, refraining from USB usage, using VPN, using recommended tools only, using multi-factor authentication, and using complex passwords). P07 pointed out that the satisfaction of all their needs motivated them to follow company security policies to perform work tasks on organisation-provided devices, stating "*...the hardware I have been given is very powerful and easily does all of the things I need to do. So from that perspective I do not need to look for other devices...*"

4.4.2 Personal and Organisational Security Models are Partially Aligned (Figure 4B)

In this case, the two models are partially aligned, where users are mindful of security to varying extents based on both their personal security understanding and on their perception of organisational security. This led to the emergence of three distinct behavioural patterns: poorly compliant security behaviours, proactive security behaviours in the absence of policy, and non-compliant security behaviours driven by security. Notably, the latter two behaviours are instances of shadow security, where users may resort to their own methods of ensuring security, either because they perceive gaps in organisational security or because they feel the need to take additional precautions beyond what is officially mandated.

Poorly compliant security behaviours: In this case, the participants do not behave according to the desired security behaviour. Instead, they comply with the policy but disagree with it, leading to less secure behaviour driven by compliance. This included sporadic VPN usage for work and password reuse. Participants discussed the influences behind such poor behaviour. P08, a Full-Stack Developer, stated that personal privacy concerns and VPN drawbacks are the main reasons behind occasional VPN usage for work, saying, "*They provide the VPN from Cisco and it's kind of slow and laggy and I kind of don't like it... Well, they give us the VPN for security, but you know they're in fact monitoring me. So no, I don't really use it on a daily basis. I just use it occasionally.*"

A stated need for convenience and memorability led P19, a Software Engineer, to reuse one password for their work device and the password manager, in addition to laptop login constraints that prevent the use of PIN – a set of numbers – over passwords. P19 said "*...I am reusing one password for logging on to Windows as well as the password manager, they're the same password. Usually I don't do that, but for work I needed a password to remember, and I wasn't going to make more than one...*" Furthermore, P19 added, "*...it's because they're forcing me to use a password, not a PIN on my laptop. I can't log in with the pin. I need the full password. So, I just use the same one I used for my password manager as well. I think it's a strong password.*"

Proactive security behaviours in the absence of policy: In this case, several behaviours aimed at improving participants' remote work security were reported when formal security policies are not in place, including: enhancing home WiFi security (e.g., changing WiFi password regularly, monitoring

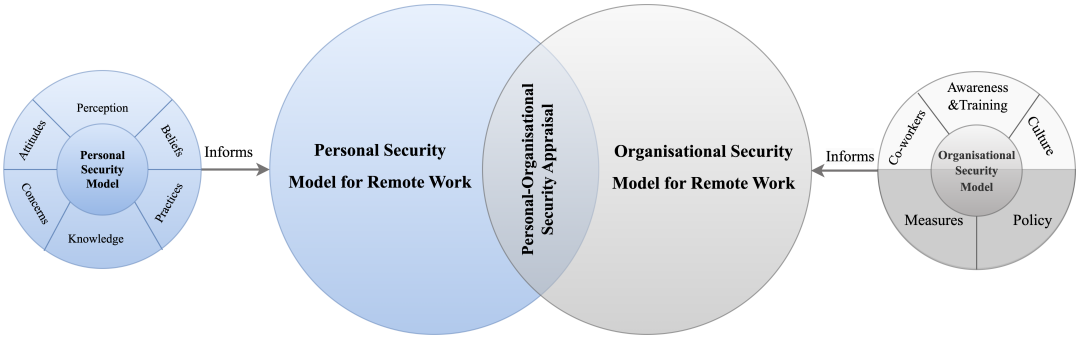

Figure 3: A model of alignment between personal and organisational security models for remote work

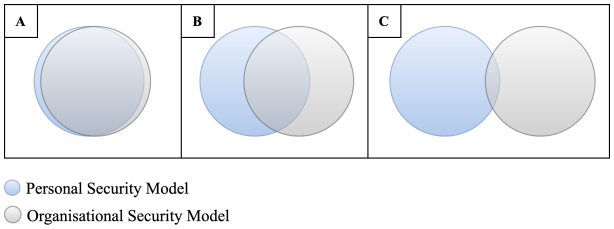

Figure 4: Different modalities of alignments between personal and organisational security models for remote work

and controlling connected devices), daily laptop shutdown, installing software only from trusted sources, segregating work and personal devices, using complex passwords, using a shredder at home, using secure file sharing, and avoiding suspicious websites on work laptops.

Non-compliant security behaviours driven by security, involve users' behaviours that deviate from established security policies but still consider security with alternative means. For instance, P02 mentioned using a secure file sharing platform like Secure Dropbox as an alternative due to limitations with the cloud service provided by their company, despite the policy prohibiting such action. P02 prioritised security and sought out a solution that better met their needs, stating, "*I primarily use Dropbox just because you need to log in and there are some security measures there.*"

4.4.3 Personal and Organisational Security Models are Poorly Aligned (Figure 4C)

In this case, participants reported instances of non-compliant behaviours that could undermine their remote work security. These behaviours are driven by various factors other than their interpretation of security policies. These include connecting to public WiFi without VPN, substituting the recommended software or tools without permission, transferring data between personal and work device, sharing work documents via WhatsApp, using insecure file sharing service (WeTransfer), sharing account passwords with co-workers, and bypassing print restriction by sending work documents to personal email.

All reported behaviours here were perceived by participants to be in breach of an underlying policy rule and mainly driven by convenience. P05, commented on sending work documents to personal email due to restrictive printing policy that does not align with their work. Admitting the behaviour to be risky, they said "*...there's a lot of restrictions over what can be printed or sent and at the end of the day if someone needs to print something. It means they have to share it to their personal e-mail and then print it. So, that's where the policies don't match the work and the workaround is where the risk is.*" Also, they commented on using insecure file sharing service (WeTransfer) over the company recommended solution (SharePoint),"*...our company is taking a policy that we can't do or download from WeTransfer so that makes it just an extra hassle for people's work... I think consumer solutions like WeTransfer solves that as the easiest case whereas SharePoint there's just so many more extra steps to get what you need done and it's so easy to forget.*"

Other participants reported workarounds driven by productivity such as creating backdoors to access internal resources remotely, replacing the hard drive on the work device, or performing work on personal devices in order to eliminate restrictions. We did not expect our participants to discuss their own personal and deliberate breaches of policy. However, when asked why someone would make use of workarounds in remote work settings, they provided several justifications. These included beliefs about limited organisational monitoring in remote work, human nature preferring ease of use, privacy invasion concerns, slow or relaxed IT response, productivity reasons, and underestimation of the security threat posed by the workaround.

5 Discussion

As traditional organisational boundaries become less tangible, more flexible, and more porous, our results show that shadow security practices continue to evolved to match.

Remote Work Security Policies: Our study highlights that shadow security in remote work encompasses behaviour that aims to improve, extend, or remediate the perceived limitations of existing security policies. A number of these limitations were directly tied to the security policies themselves. The first policy limitation was that some participants could not remember the details of security policies or felt that these policies were not clearly written and communicated. This limitation is relatively straightforward, centred broadly on problems with the timeliness, language and communication of the policies themselves.

A second policy limitation is more subtle and our participants articulated this as policies that were not suited to their needs, leading to frustration, friction or other impediments. These problems arise from an individual's subjective assessment of the security policies, looking at the perceived need, effectiveness, and cost/benefit of following the policy. These findings aligns with previous studies [6, 39] which highlight how shadow security practices can emerge due to perceptions of inappropriate organisational policies and rules. We describe this as the personal-organisation security appraisal, and note that there are commonalities between the personal security model and the Theory of Planned Behaviour (TPB) [4], one of the most widely used theories for studying user attitudes as an influence on human behaviour. TPB defines four factors that underlie the decision toward certain behaviours: attitudes, subjective norms, perceived behavioural control, and intentions. Since shadow security is highly tied to the user's personal security model, which comprises their attitudes, perceptions, knowledge, concerns, beliefs, and practices related to personal security, it encompasses all the elements that can influence a person's decision to behave in a certain manner.

We believe that policy authors, such as CISOs, need to be particularly aware of the content, delivery, and uptake of remote work security policies, as compliance, non-compliance and shadow practices may be harder to determine.

Organisational Security Awareness, Training, and Education (SATE): Our results also suggest that while the personal security model is strongly tied to individual attitudes, perceptions and beliefs, it is also shaped by previous and ongoing SATE efforts. As mentioned in Section 4.3.2, SATE targets individuals to improve their knowledge, upskill their practices, and influence their concerns to be better aligned with the needs of the organisation that employs them. We believe that there are interesting implications arising from the fact that high quality SATE can benefit future employers of existing employees. Put another way: current employers benefit (or suffer) from the SATE efforts of previous employers. Organisations directly benefit from improving the security knowledge and skill of their employees, however there are also positive externalities for other employers who benefit when those trained employees are then recruited. With the rise of the gig economy [37], this has particular implications on the economics, delivery, and alignment of SATE in the context of employees that have multiple employers.

Informal Communications: In tandem with SATE, we also found that remote employees rely on indirect channels to learn and share security know-how with other employees. Our findings suggest that remote workers are more isolated from their peers and the security culture of their employing organisation. This may undermine information sharing between colleagues about security practices and rules, leading to poor understanding of rules and fewer opportunities to learn how to use tools correctly. These informal dissemination channels are much less developed in remote work settings, and our findings indicate this is likely to contribute to poor or non-compliant security behaviour.

Usability of Remote Work Security: Finally, we note that shadow security practices can arise from technical limitations in the provision of remote work facilities. Our participants mentioned that some of the controls they had to use (e.g. access control) were complex and constraining, leading to difficulties in achieving their work objectives. In addition, participants also noted that there was a lack of available support options, meaning they felt more isolated and had to solve problems themselves. Both of these issues are indicative of the need for greater consideration of usability and the wider security user experience for remote workers.

Further research into shadow security practices for remote work can provide a fruitful source of inspiration and innovation, helping to shape new ways of working remotely and securely. Our recommendation are consistent with the approach taken by Kirlappos et al. [39], which aims to learn from shadow practices to improve overall organisational security. As Kirlappos et al. [39] aptly state, "*shadow security existence should not be treated as a problem, but as an opportunity to identify shortfalls in current security implementations that can be leveraged in providing more effective security solutions for organisations.*" By embracing this perspective, organisations can address the gaps in their current security measures and develop more effective and user-friendly security solutions for remote work environments.

6 Recommendations

Based on our findings, we discuss the following recommendations:

6.1 Developing Informal Security Channels

A key finding from our study is the important role of colleagues as a source of security information. An organisation whose employees access shared spaces and communicate

face-to-face can expect informal and private communications to happen spontaneously. However in a remote work environment, such communications need to be a) mediated technologically, b) initiated deliberately, and c) responded to purposefully. One problem arising from a) is that employees feel that communications are more difficult in remote work settings, and we also noted some concerns about companies monitoring their remote employees, both of these concerns can hinder the open discussions about security rules and tools among colleagues. Furthermore, b) and c) both create barriers to spontaneous or opportune discussions that can occur outside of a deliberately initiated interaction. As a result, we argue that remote workers need better technology to help them connect with co-workers about security issues and to share their concerns and solutions, and that more research is needed to determine how and when informal security discussions can be supported to improve security culture among remote workers.

6.2 Homogenising Security Interactions

Individuals are often influenced by their interactions with various platforms such as devices and services, particularly regarding security protocols and practices, which may vary across platforms. This variability can either foster secure habits over time through consistent exposure to the same protocols or lead to confusion and resistance when changes occur, potentially resulting in actions that could pose security vulnerabilities. A key finding from our study is that habit and convenience were among the factors considered during the personal-organisational security appraisal, leading to poor compliance behaviour, shadow security, and even non-compliance with security policies. It is also worth noting that a corollary to this is that innovation and change are particularly difficult in security, as this aims to break previous modes of interaction and familiarity in favour of new ones. Particular attention should therefore be placed on exploring how and when change is necessary, together with suitable strategies for introducing and managing change.

These insights underscore the necessity for standardising security tools and regulations, especially in remote work, which is increasingly prevalent across diverse industries, each facing unique requirements security challenges. To tackle this complexity, we propose implementing security style guides specifically tailored for remote work environments, aiming to homogenise security interactions across platforms and industries.These guides will serve as comprehensive resources outlining best practices, policies, and procedures for ensuring the security of remote work setups. By integrating insights from various industries, security practitioners can develop comprehensive guidelines addressing a wide range of security concerns, fostering knowledge sharing and collaboration across industries.

6.3 Adopting User Experience Design for Remote Work Solutions

Our study identifies that poorly designed remote work solutions can significantly hinder productivity, increase frustration, and elevate security risks. These frustrations often compel employees to create workarounds and shadow security practices. By prioritising user experience (UX) design [12, 45] in the development of remote work solutions, organisations can create intuitive interfaces and streamline workflows that encourage compliance with security measures. UX not only enhances user satisfaction but plays a critical role in ensuring adherence to security protocols. This involves conducting user research, gathering feedback from remote workers, and iteratively refining the design of remote work tools and platforms to prioritise usability and security simultaneously. By adopting a user-centred design approach and aligning user experience with security objectives, organisations can foster a culture of compliance and reduce the prevalence of workarounds and shadow security practices among remote workers.

7 Conclusion

Our exploratory study of security and shadow security practices in the context of remote work was motivated by the prevalence of remote work in the knowledge economy and the lack of research in this context. Based on our analysis of 20 semi-structured interviews with remote workers, our findings complement and extend prior research, which found that shadow security practices can arise from perceptions of inappropriate organisational policies and rules [6, 39].

Our analysis proposes three models for describing security practices in remote work: the first is a personal security model influenced by external factors (e.g. past experiences, knowledge of technology, or qualifications). The second comprises the current organisational security model for remote work, which includes security rules and tools disseminated through awareness and training, interaction with colleagues, and the overall security culture. The third is an appraisal process individuals use to relate the personal and organisational security models, driving compliance, non-compliance, and shadow security behaviour in remote work settings.

This opens up opportunities for future research in remote work security, for example exploring the delivery and long term effects of security awareness, training, and education for remote work in the gig economy; tackling the challenge of improving and harmonising security user experiences across different device and service providers; or exploring how informal communications can be facilitated in remote work settings. It also allows for the investigation of different interventions, such as persuasive techniques or digital behaviour interventions, as a means to enhance user security behaviour in remote work settings.

Acknowledgments

The authors would like to thank all the participants in this research study for their perspectives and valuable insights. We also thank the anonymous SOUPS reviewers for their constructive feedback. Sarah Alromaih is funded by a graduate scholarship from King Abdulaziz City for Science and Technology.

References

[1] Definition of remote work - gartner information technology glossary. https://www.gartner.com/en/information-technology/glossary/remote-work.

[2] 2022 workplace trends & insights report. https://www.beezy.net/2022-workplace-report, January 2023. Retrieved on 2023-01-24.

[3] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[4] Icek Ajzen. The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2):179–211, 1991.

[5] Tammy D Allen, Timothy D Golden, and Kristen M Shockley. How effective is telecommuting? assessing the status of our scientific findings. *Psychological science in the public interest*, 16(2):40–68, 2015.

[6] Adam Beautement, M Angela Sasse, and Mike Wonham. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 new security paradigms workshop*, pages 47–58, 2008.

[7] 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.

[8] Peter Birmingham and David Wilkinson. *Using research instruments: A guide for researchers*. Routledge, 2003.

[9] Mary Bispham, Sadie Creese, William H Dutton, Patricia Esteve-Gonzalez, and Michael Goldsmith. Cybersecurity in working from home: An exploratory study. In *TPRC49: The 49th Research Conference on Communication, Information and Internet Policy*, 2021.

[10] John M Blythe, Lynne Coventry, and Linda Little. Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, pages 103–122, 2015.

[11] Charles F Cannell, Peter V Miller, and Lois Oksenberg. Research on interviewing techniques. *Sociological methodology*, 12:389–437, 1981.

[12] George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom. Factoring user experience into the security and privacy design of smart home devices: A case study. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–9, 2020.

[13] Kathy Charmaz. *Constructing grounded theory: a practical guide through qualitative analysis*. Introducing qualitative methods. Sage, London, 2006.

[14] Kathy Charmaz. *Constructing grounded theory*. Introducing qualitative methods. SAGE Publications Ltd, London, 2nd edition edition, 2014.

[15] Kathy Charmaz. Constructivist grounded theory. *The Journal of Positive Psychology*, 12(3):299–300, May 2017.

[16] Juliet Corbin and Anselm Strauss. *Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, California, 2008.

[17] Adéle Da Veiga and Jan HP Eloff. A framework and assessment instrument for information security culture. *Computers & security*, 29(2):196–207, 2010.

[18] Stuart E Dreyfus and Hubert L Dreyfus. A five-stage model of the mental activities involved in directed skill acquisition, 1980.

[19] Durga Prasad Dube and Rajendra Prasad Mohanty. Application of grounded theory in construction of factors of internal efficiency and external effectiveness of cyber security and developing impact models. *Organizational Cybersecurity Journal: Practice, Process and People*, 3(1):41–70, 2023.

[20] Yogesh K Dwivedi, D Laurie Hughes, Crispin Coombs, Ioanna Constantiou, Yanqing Duan, John S Edwards, Babita Gupta, Banita Lal, Santosh Misra, Prakhar Prashant, et al. Impact of covid-19 pandemic on information management research and practice: Transforming education, work and life. *International journal of information management*, 55:102211, 2020.

[21] Robert J Fisher. Social desirability bias and the validity of indirect questioning. *Journal of consumer research*, 20(2):303–315, 1993.

[22] Steven Furnell and Jayesh Navin Shah. Home working and cyber security–an outbreak of unpreparedness? *Computer fraud & security*, 2020(8):6–12, 2020.

[23] Barney G. Glaser. *Basics of Grounded Theory Analysis*. Sociology Press, Mill Valley, CA, 1992.

[24] Barney G Glaser, Anselem L Strauss, and E Strutzel. The discovery of grounded theory: Strategies for qualitative research new york aldine de gruyter. *GlaserThe Discovery of Grounded Theory: strategies for qualitative research1967*, 1967.

[25] Timothy Godlove. Examination of the factors that influence teleworkers' willingness to comply with information security guidelines. *Information Security Journal: A Global Perspective*, 21(4):216–229, 2012.

[26] Leo A Goodman. Snowball sampling. *The annals of mathematical statistics*, pages 148–170, 1961.

[27] Lynda Gratton. How to do hybrid right. *Harvard Business Review*, 99(3):66–74, 2021.

[28] Greg Guest, Arwen Bunce, and Laura Johnson. How many interviews are enough? an experiment with data saturation and variability. *Field methods*, 18(1):59–82, 2006.

[29] Ken H Guo. Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, 32:242–251, 2013.

[30] Andreas Györy, Anne Cleven, Falk Uebernickel, and Walter Brenner. Exploring the shadows: It governance approaches to user-driven innovation. In *ECIS 2012 - Proceedings of the 20th European Conference on Information Systems*, 2012.

[31] Steffi Haag and Andreas Eckhardt. Shadow it. *Business & Information Systems Engineering*, 59:469–473, 2017.

[32] Stephen Hansen, Peter John Lambert, Nicholas Bloom, Steven J Davis, Raffaella Sadun, and Bledi Taska. Remote work across jobs, companies, and space. Technical report, National Bureau of Economic Research, 2023.

[33] Karin Höne and Jan H. P. Eloff. Information security policy—what do international information security standards say? *Computers & security*, 21(5):402–409, 2002.

[34] Allen C. Johnston, Barbara Wech, Eric Jack, and Micah Beavers. Reigning in the remote employee: Applying social learning theory to explain information security policy compliance attitudes. In *16th Americas Conference on Information Systems 2010, AMCIS 2010*, volume 3, pages 2217–2230, 2010.

[35] Karsten Jonsen and Karen A Jehn. Using triangulation to validate themes in qualitative studies. *Qualitative research in organizations and management: an international journal*, 4(2):123–150, 2009.

[36] Annabel Kajornboon. Using interviews as research instruments. *E-journal for Research Teachers 2.1*, page 1–9, 2005.

[37] Otto Kässi and Vili Lehdonvirta. Online labour index: Measuring the online gig economy for policy and research. *Technological forecasting and social change*, 137:241–248, 2018.

[38] Iacovos Kirlappos, Simon Parkin, and M Angela Sasse. Learning from "shadow security". In *NDSS Workshop on Usable Security*, 2014.

[39] 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.

[40] Benjamin Koskei and Catherine Simiyu. Role of interviews, observation, pitfalls and ethical issues in qualitative research methods. *Journal of Educational Policy and Entrepreneurial Research*, 2(3):108–117, 2015.

[41] Steinar Kvale and S Brinkmann. Introduction to interview research. *Doing interviews*, pages 2–11, 2007.

[42] Ying Li and Mikko Siponen. A call for research on home users' information security behaviour. In *PACIS 2011 Proceedings*, page 112, 2011.

[43] Florian Malecki. Overcoming the security risks of remote working. *Computer fraud & security*, 2020(7):10–12, 2020.

[44] Gabriela Labres Mallmann and Antonio Carlos Gastaud Maçada. Behavioral drivers behind shadow it and its outcomes in terms of individual performance. In *AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems*, 2016.

[45] Aaron Marcus. *HCI and user-experience design*. Springer, 2015.

[46] Mary L McHugh. Interrater reliability: the kappa statistic. *Biochemia medica*, 22(3):276–282, 2012.

[47] Ferdinando Monte, Charly Porcher, and Esteban Rossi-Hansberg. Remote work and city structure. *American Economic Review*, 113(4):939–981, 2023.

[48] Albine Moser and Irene Korstjens. Series: Practical guidance to qualitative research. part 3: Sampling, data collection and analysis. *European journal of general practice*, 24(1):9–18, 2018.

[49] JM Nilles, FR Carlson, Paul Gray, and Gerhard Hanneman. Telecommunications-transportation tradeoffs. *Final report*, 1974.

[50] Norbert Nthala and Ivan Flechais. Informal Support Networks: an investigation into Home Data Security Practices. pages 63–82, 2018.

[51] Savvas Papagiannidis, Jonathan Harris, and David Morton. Who led the digital transformation of your company? a reflection of it related challenges during the pandemic. *International journal of information management*, 55:102166, 2020.

[52] Lazar Raković, Marton Sakal, Predrag Matković, and Mirjana Marić. Shadow it–systematic literature review. *Information Technology and Control*, 49(1):144–160, 2020.

[53] Jason Sabin. The future of security in a remote-work environment. *Network Security*, 2021(10):15–17, 2021.

[54] Martina Angela Sasse, Debi Ashenden, D. Lawrence, L. Coles-Kemp, I. Fléchais, and P. Kearney. Human vulnerabilities in security systems. *Human Factors Working Group, Cyber Security KTN Human Factors White Paper*, 2007.

[55] Clive Seale. The quality of qualitative research. *The Quality of Qualitative Research*, pages 1–224, 1999.

[56] Mario Silic and Andrea Back. Shadow it–a view from behind the curtain. *Computers & Security*, 45:274–283, 2014.

[57] Mario Silic, Jordan B Barlow, and Andrea Back. A new perspective on neutralization and deterrence: Predicting shadow it usage. *Information & management*, 54(8):1023–1037, 2017.

[58] Darja Smite, Nils Brede Moe, Jarle Hildrum, Javier Gonzalez-Huerta, and Daniel Mendez. Work-from-home is here to stay: Call for flexibility in post-pandemic work policies. *Journal of Systems and Software*, 195:111552, 2023.

[59] Yimin Song, Chao Yang, and Guofei Gu. Who is peeping at your passwords at starbucks?—to catch an evil twin access point. In *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, pages 323–332. IEEE, 2010.

[60] VA Stafford. Zero trust architecture. *NIST special publication*, 800:207, 2020.

[61] Anselm Strauss and Juliet Corbin. *Basics of Qualitative Research Techniques*. Sage Publications, Thousand Oaks, CA, 1998.

[62] Kerry-Lynn Thomson, Rossouw Von Solms, and Lynette Louw. Cultivating an organizational information security culture. *Computer fraud & security*, 2006(10):7–11, 2006.

[63] Robert Thornberg, Kathy Charmaz, et al. Grounded theory and theoretical coding. *The SAGE handbook of qualitative data analysis*, 5(2014):153–69, 2014.

[64] III Turner, Daniel W. Qualitative interview design: a practical guide for novice investigators. *Qualitative report*, 15(3):754–, 2010.

A Demographics Questionnaire

1. Select your age group:
    - 18-24
    - 25-34
    - 35-44
    - 45-54
    - 55-64
    - 65-74
    - 75 or older
    - Prefer not to answer
2. Select your gender:
    - Male
    - Female
    - Other
    - Prefer not to answer
3. Where do you live?
    - —
    - Prefer not to answer
4. What is your work setting?
    - Remote: Fully remote work.
    - Hybrid: A combination of remote work and working from a designated office space.
5. Which of the following best describes your organisation's business domain?
    - Manufacturing
    - Retail
    - Technology/IT
    - Healthcare
    - Finance
    - Hospitality
    - Education
    - Consulting
    - Real Estate
    - Transportation and Logistics
    - Entertainment and Media
    - Non-profit/NGO
    - Government/Public Sector
    - Energy and Utilities
    - Other —
6. What best describes your role within your organisation?
7. What is the highest level of school you have completed?
    - No schooling completed
    - Nursery
    - High School
    - Trade/technical/vocational training
    - Undergraduate studies
    - Graduate studies
    - Postgraduate studies
8. How would you rate your technical skills in computer security and privacy (e.g. understanding threats, vulnerabilities, and countermeasures)?
    - Novice
    - Competent
    - Expert

B Interview Questions

B.1 Remote Work Experience

1. Can you tell us a bit about yourself and your background?
2. Can you tell me about your experience working remotely?
3. How long have you been working remotely?
4. Can you share any specific examples of remote work tasks you have successfully completed in the past?
5. Did you work remotely from home before the pandemic?
   (a) If yes, how frequent?
6. How does your current remote work differ from your previous experiences before the pandemic?
7. Have you faced any challenges while working remotely?
   (a) If so, how did you overcome them?

B.2 Introductory to Security in Remote Work

1. How does cybersecurity fit into your day?
2. Do you think your remote work has any security or privacy implications?
   (a) If yes, what would be your concerns? (Prompt: dealing with confidential information)

B.3 Security, Awareness and Training

1. How familiar are you with the security policies and guidelines provided by your organisation for remote work?
2. Have you received any security training recently?
   (a) If yes, how long ago?
   (b) What was it like? (Prompt: Training format, sessions length)
   (c) Do you think it is helpful?
3. Do you receive reminders about security? (Prompt: Emails, nudges)
   (a) If yes, what do they ask/prompt you to do?

B.4 Personal vs Work Protection

1. Is there anything you do at home to protect remote work over and above what you would normally do for other online activities at home? (Prompt: securing your home WiFi network or using a VPN to access remote resources)

B.5 Remote Work Setup (Equipments and Tools)

1. What devices do you use for remote work?
2. Are they your personal devices or provided by your organisation?
3. Are you ever worried about the possibility of them being lost or stolen?
4. Do you have a routine for regular backups?
5. Are there any specific communication or productivity tools recommended by your organisation?
   (a) If yes, what are they?
   (b) Are they good enough?
6. Do you use other tools?

B.6 Security Policy and Measures

1. Do you think it is important to keep your device and software up to date with the latest security patches and updates?
2. Have you ever installed any software other than that provided by the organisation?
   (a) If yes, why do you do that?
   (b) Did you take any precautions when doing so? (Prompt: verify the source)
3. How do you verify the authenticity of websites or online resources before providing sensitive information, such as login credentials or personal data, while working remotely?
4. What measures do you take to prevent unauthorized access to your remote work device? (Prompt: strong passwords, two-factor authentication, or biometric authentication)
5. Where do you usually perform your job when working remotely? (Prompt: public areas like cafes, at home office)
   (a) If public areas, do you think using public WiFi might pose a threat to the organisation? and how?

6. Do you handle any physical paperwork or print out information related to your work?
    (a) If yes, does any of it include potentially confidential information?
    (b) If it does, how do you dispose of such documents once you're finished with them?
7. Do you share the devices you work on with anyone else in your household?
    (a) If yes, do you believe that this could pose a security threat?
    (b) How do you ensure the protection of your work-related materials?
8. Do you use removable storage devices, such as USB sticks, to store or transfer work-related data?
    (a) If yes, how important is it? Why?
    (b) Is that your own one or was it given to you by the organisation?
    (c) Is any of the stored data in any sense confidential?
    (d) What precautions do you take to protect that data?
9. Is there any situation where you encounter difficulties accessing legitimate resources or platforms?
    (a) If yes, have you ever used a workaround to bypass the restrictions?
    (b) Are you aware if others do the same?
    (c) How frequently does this happen?

B.7 Security Incidents

1. How do you handle unexpected security incidents or potential security threats, such as suspicious emails or notifications, while working remotely?
2. Have you ever come across something that you consider to be a vulnerability that the organisation has not thought of?

B.8 Security Culture

1. To what extent do you believe individuals generally adhere to the policy rules?
2. Can you think of a reason why somebody might not follow one of them?
3. Are there any policies or procedures that you routinely do not comply with? Why do you do this?
4. Does the organisation check whether employees comply with security policies?
    (a) What sanctions or punishments are used against people that get caught?
    (b) Do you think these are appropriate?
5. In general, what do you think of the policies? Do you think they are too strict, too soft, or about right?
6. What is your perception of the overall security culture within the organisation? Would you consider it to be highly security-conscious or not particularly focused on security?

C CodeBook

Theme	Sub-Theme	Category	List of Codes
Personal Security Model	Proactive Personal Security Practices	Personal Security Practices (general)	Using a separate browser for work and personal use; Using separate work and personal password managers; Timely response to security updates; Using complex passwords; Using DNS over HTTPS; Using DNSSEC; Using a password manager; Using personal MFA; Using a personal VPN; Full disc encryption; Keep fully encrypted backup; Locking device screen when away; Never use public WiFi; No sharing devices in the household; Proactive email verification; Safe browsing practices on work device.
		Rules of thumb website authenticity	Access websites from bookmarks list; Avoid sponsored links in search results; Check the security certificate; HTTPS verification; Inspect the website URL; Look for copyright and trust badges; Look for website reviews; Look up IP address using Whois; Selective trust-based website reputation; Trust Google's first link of the website; Verify using Google Search
		Rules of thumb Email legitimacy	Check email header; Look up email address on Google; Scrutinise email content
		Rules of thumb installing new software (work and personal use)	Avoiding untrusted software installation; Installing software from the original source; Installing software from a trusted source; Installing well-known software only; Testing untrusted software on a dedicated machine
	Faulty Security Practices	Faulty Security Practices	Connecting to reputable (public or any) WiFi; Performing personal activities on work devices.
External Security Influences	Online services and technologies	Online services and technologies	interactions with Online services and technologies; technology access
	Past incidents	Past incidents	past incidents
	Past work experience	Past work experience	security measures; security policies; security training
	External advice	External advice	experienced colleague or friend; online forum; Online search for security insights
	Qualifications	Qualifications	Educational background; Access to job opportunities
	Organisational security model	Organisational security model	Co-workers' practices; Current security reminders; Current security training
Organisational Security Model	Remote work challenges	Remote work challenges	Communication issues with other team members; Connectivity and accessibility issues; Creating structured communication; Device restrictions in remote vs. office work; Fear of losing or damaging work devices; Intangible aspects lost in remote work; Lab equipment accessibility; Lack of clear hybrid-remote work policies; Lack of immediate colleague assistance; Lack of security education; Managing prolonged online discussions or arguments; Mixing personal and work activities on work devices; Resource accessibility issues; Risk from international travel; Theory vs. Practice in remote work assistance; Unofficial vs. official communication; Unstable virtual working environment; Using a public network; Varied remote work locations; Visual exposure of work in public areas
	Rules and Tools	Security measures	perception of enforced software update; perception of immunity to risks; desire for effortless security; equating working from home with a physical office; Balancing security measures and usability; Limited proactive security measures; Endpoint management; MFA; VPN; Modem verification; Zero Trust model; VPN issues
		Security policy (attitudes/perceptions)	Adherence to company policy; Absence of remote work security policy; Adherence to technically enforced policy; Challenges in policy compliance; Challenges in policy content accessibility (language or format); Difficulty in remembering policies; Proactive policy familiarization; Productivity-driven mindset; Risk-driven adherence; Shadow IT and policy adaptation; Demand for tailored security policies; No actions above policy when working at home. Make the work environment unusable; Mixed perceptions about the security policies; No one read the policy; One-size-fits-all policy or Lack of flexibility; Perception of policy disregard; Policies as bureaucratic; Policies as facilitators vs. barriers; Policy and guideline flexibility; Policy Complexity based on business size; Policy is for 'Stupid User'; Positive effect of user-centred security design; Positive view of stricter policies; Privacy-driven adherence to policy; Productivity-driven adherence to policy; Lack of policy on installing new software; Lack of informed incident reporting process; Varied policy implementation by industry
	Dissemination Channels	Security Awareness and Training Programs (attitudes & perceptions)	Importance of ongoing training; Knowledge empowerment; Lack of enthusiasm toward training; Resistance to training; Utility of training (trained vs useful); Effectiveness of incentive-based reminders; Shaping user behaviour; Basic training content; Boredom due to training duration; Distraction from meaningful tasks; Emphasis on policy reinforcement; Enforced security training; Focus on GDPR compliance; Inform the incident management protocol; Lack of belief in training efficacy; Lack of company-specific training; Lack of formal security training; Perceived effectiveness of enforced training; Repetitive security training; Sustaining knowledge through training; Training redundancy over time; Variability in security training based on job role; corrective training
		Security Awareness and Training Programs (suggested enhancements)	Hypothetical security scenarios; Informal learning through discussion forums; Interactive training sessions; Leveraging marketing and PR strategies; Scenarios based on previous incidents; Signposting new content; Tailoring security campaigns to different user types; Tailoring training to worker background and experience; Training frequency; Chunked and focused training session (Theme-based); Utilising communication platforms for security; Cyber score metrics
		Security Culture and Co-workers	Absence of immediate in-person support; Implicit trust in the used software (Start-up case); Lack of support in academic institutions; Prioritising efficiency over security; Reduced contextual awareness when working remotely; Lack of guidance and oversight
Personal-Organisational Security Appraisal in Remote Work	Well alignment	Complaint behaviours	Document labelling or classification; Following policies for installing new software; Maintaining secured home workspace; No sharing of work devices; Performing work tasks on company provided devices; Refraining from USB usage; Timely response to software updates; Updating passwords frequently; Using complex passwords; Using MFA; Using a password manager; Using recommended tools; Using thumbprint USB; Using VPN
		Justifications	Seamless remote infrastructure; Lack of necessities
	Partial alignment	Poor complaint behaviours	Occasional VPN usage for work; Password reuse
		Justifications	Faulty beliefs; Ease of use; Lack of policy; Lack of measures
		Proactive security behaviours no policy	Avoiding suspicious websites on work laptops; Daily laptop shutdown; Enhanced home WiFi security; Installing software from a trusted source; Minimizing visibility to others in public areas; Monitoring home network-connected devices; Never working or connecting to public WiFi; Recycling passwords; Segregating internal and external file sharing; Segregating work and personal devices; Strict work laptop usage; Using complex passwords; Using a hotspot through a mobile data plan; Using a password manager for work accounts; Using personal MFA; Using secure file sharing; Using a shredder at home; Using VPN
		Non-complaint behaviours driven by security	Replace official file sharing with secure alternative
	Poor alignment	Non-complaint behaviours (workaround)	Using insecure file sharing service; Disconnecting from the VPN; Installing new tools or software; Sharing account password with co-workers; Substituting the recommended software; Transferring data between personal and work devices; Creating a backdoor; Replacing work laptop hard drive; Using Google Sheets instead of Excel; Using personal email for work; Using a personal laptop; Using WhatsApp to share work documents
		Justification for workarounds	Belief about limited organisational monitoring; Bypassing company restrictions (site blocking); Complexity of organisational security measures; Convenience; Heightened security measures in remote work vs office; Usability issues; Lack of attention; Generic policy rules; Privacy invasion concerns; Productivity reasons; Slow or relaxed IT response; Time constraints and task urgency; Underestimating workaround vulnerability; Underestimation of workers' capability; Cost-benefit analysis

Figure 5: Codebook of Themes and Codes.