Challenges and Threats of Mass Telecommuting: A Qualitative Study of Workers

Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov,
University of British Columbia

https://www.usenix.org/conference/soups2021/presentation/obada-obieh

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

August 9–10, 2021

978-1-939133-25-0

Open access to the Proceedings of the Seventeenth Symposium on Usable Privacy and Security is sponsored by

Challenges and Threats of Mass Telecommuting: A Qualitative Study of Workers

Borke Obada-Obieh Yue Huang Konstantin Beznosov

University of British Columbia
Vancouver, Canada
{borke,huang13i,beznosov}@ece.ubc.ca

Abstract

This paper reports the security and privacy challenges and threats that people experience while working from home. We conducted semi-structured interviews with 24 participants working from home in the three weeks preceding the study. We asked questions related to participants' challenges with telecommuting. Our results suggest that participants experienced challenges, threats, and potential outcomes of threats associated with the technological, human, organizational, and environmental dimensions. We also discovered two threat models: one in which the employer's asset is at stake and another in which the employee's privacy is compromised. We believe these insights can lead to better support for employees and possibly reduce cyber-attacks associated with telecommuting during the pandemic and beyond.

1 Introduction

Our research aims to provide insight into the security and privacy concerns associated with telecommuting to help employees safely work from home while protecting organizations' confidential information. Our investigation into telecommuting challenges is a response to a clear need for safer work-from-home practices as the rise in telecommuting has led to an increase in cyber-attacks [6, 31, 37, 44].

The global COVID-19 pandemic has resulted in the world's largest telecommuting situation [5]. In 2018, the U.S. Bureau of Labor Statistics report showed that only 8% of all employees work from home at least one day of the week, while 2% worked fully from home [7, 45]. However, most employees now work from home. Recent research from Stanford indicates that as of June 2020, 42% of the labor force was telecommuting (with 33% unemployed and 26% working in essential services) [8, 78]. Researchers estimate that employers plan to keep 20% of their workers continue working from home after the pandemic ends, mainly to reduce costs [41]. Another recent survey shows that 47% of the respondents aim for their workers to telecommute full-time [24]. Further, some major tech companies have already switched to either long-term or permanent work-from-home model [15, 16, 32, 55].

With a remote workforce and everyone working digitally, the threat landscape increases. Research shows that 91% of respondents experienced an increase in cyber-attacks as a result of employees telecommuting [6]. Further, the Canadian Press reported a 1,350% increase in cloud-related attacks and a 4,000% increase in ransomware emails [40]. Remote working can also be problematic when employees' personal computers are not updated with the most recent security protocols and software. Employees risk exposing the entire system to various types of cyber-attacks. Major organizations have suffered data breaches targeted at employees. For instance, the World Health Organization reported a fivefold increase in cyber-attacks, with the most recent attack targeting their employees [77]. There has been a spike in phishing attacks in Italy as a result of people teleworking [33]. In addition, the threat model in a home environment differs from that seen in the physical office workplace. For instance, some company devices used in teleworking are linked to home or less secure Wi-Fi networks. These company devices may not have the physical security provided in the workplace.

To address the security and privacy concerns of working from home, research is needed to understand the specific challenges and threats that employees experience while telecommuting. Several telecommuting research projects compared workers' productivity while working from home and in physical office locations [2, 4, 9, 51, 60]. Some research on working from home also provides tips and strategies for securing the home internet network for employees while telecommuting [21, 35, 43]. However, to the best of our knowledge, no

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Virtual Conference.

research has focused on employees' security and privacy concerns with telecommuting.

To this end, our objective is to address the following research question: *What are employees' security and privacy challenges, threats, and perceived outcomes of threats when working from home?*

For the sake of clarity, we define some terms. Challenges and threats are often used interchangeably; however, they do not necessarily mean the same thing. In this paper, we define a threat as "an event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss" [59]. A challenge is a circumstance that could lead to a threat. And an outcome of a threat is "an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result" [64]. These outcomes could be loss of organizational data confidentiality, integrity, and availability or the loss of personal privacy. We define confidentiality as "the property of non-public information remaining accessible only to authorized parties" [72]. Privacy "more narrowly involves *personally sensitive* information, protecting it, and controlling how it is shared. ... What information should be private is often a personal choice, depending on what an individual desires to selectively release." Integrity is defined as "the property of data, software or hardware remaining unaltered, except by authorized parties" [72].

We addressed our research question by conducting semi-structured interviews with 24 participants. They were employees who had been working from home in the three weeks preceding the study. We asked questions relating to their challenges with telecommuting and analyzed the results using thematic analysis.

Our study makes two major contributions. First, we performed the first qualitative study on employee security and privacy concerns when telecommuting. Furthermore, we identified the perceived outcomes of threats associated with these concerns. We grouped our findings into four categories of challenges and threats: technological, human, organizational, and environmental. We further grouped our findings into the identified outcomes of threats to security and privacy and created threat models that emerged from our results.

Second, we discovered concerns that need to be addressed to protect employee privacy while telecommuting. Many employees felt that they had to sacrifice some privacy to get their work done, such as revealing their personal phone number or street address to clients. Participants feared that clients could locate their home or that they could suffer a break-in. Therefore, there is a need for discussion of how employees and organizations can protect their privacy and security while telecommuting.

Our contributions provide insights into the security and privacy gaps that exist with regard to employees telecommuting. We are optimistic that these insights can lead to changes in the way telecommuting is currently being carried out. These changes will be helpful during the current pandemic and in other situations where employees need to telecommute.

2 Related Work

Telecommuting and telework are similar but different. Whaley [75] defines telecommuting as "using information and communications technologies (ICTs) to bring work to the worker, rather than require them to go to the work." In telecommuting, the employee does not commute to get to work. Examples of telecommuting could be working in the home office or working out of the office in the home environment, for example, the guest house. On the other hand, telework refers to work that is done somewhere that is a distance from one's office. Examples of teleworking could be working at another branch of an office or working at a telework center with other colleagues. While some types of telework are telecommuting, not all types of telecommuting are telework [58, 75].

Many previous papers focused on teleworking benefits and aimed to understand problems that stop its widespread adoption by organizations. For instance, Pyöriä [53] conducted a literature review on the advantages of distributed work, which the author refers to as telework. Similarly, Kintner [34] conducted surveys with 1,002 respondents to determine how receptive businesses were to telework and identify ways to encourage managers to telework. The respondents were workers in various organizations who were not teleworkers. The author identified issues that prevented telework adoption, such as inadequate security for protecting transmitted information while teleworking, the high cost of buying the needed equipment, and the lack of staff available to aid telework transition, among others. Our study builds on previous research and conducts qualitative research with telecommuters. We chose to interview telecommuters to understand their security and privacy challenges and threats when working from home.

Some papers explored the reasons behind the low adoption of telework before the pandemic. One of the reasons for low adoption was poor data security. Clear and Dickson [17] for instance, studied whether telework adoption was influenced more by levels of worker autonomy, employment flexibility, and management attitudes than technology provision. The authors conducted 303 surveys and 58 interviews with representatives of small and medium enterprises (SMEs). In discussing their results, the authors remarked that data security is "a major disadvantage to the adoption of telework." However, the authors did not explain why this was the case. Spinellis et al. [66] also hypothesized that SMEs lacked the potential to have good technical expertise to maintain an adequate security level in teleworking. The work of Pyöriä [52] is closest to ours. This author conducted a survey and interviews with employees to understand the low adoption of telework even in big organizations. The participants, however, were not teleworkers. The authors categorized their findings into those relating to the individual, the organization, and the community. They

described the pros and cons of telework at each level. The findings relating to the organization level are closest to our findings. The author found that some of the drawbacks of teleworking include the problem of employers seeking new means to surveil and control employees, poor data security, and disruption of privacy in employees' homes. Our work differs from Pyöriä's [52] in two major ways. First, we interview employees who are currently telecommuting. Our focus on telecommuting employees helped us to understand the specific challenges these people are facing. Further, building on Pyöriä's study, we focus on telecommuters' security and privacy concerns and find more challenges and threats. Because of the potential for a number of telecommuters to continue for the long term, our research becomes even more critical.

Several papers focus on the security and privacy challenges of telecommuting. However, these papers are not based on empirical data but on hypothetical situations. For instance, one of the earliest papers on telecommuting was written by Sturgeon [67]. The author used a hypothetical case study to highlight vulnerabilities. The author predicted threats and risks to organizations' confidential data when telecommuting using the Simplified Threat and Risk Assessment Process [67]. A more recent paper by Okereafor and Manny [46] provides an overview of security issues that are related to telecommuting and videoconferencing apps. The authors predicted issues related to workers' geographic location such as workers' telecommuting in locations with poor Wi-Fi networks and workers being distracted while working from home, which could lead to dangerous errors. The authors also highlighted other general issues such as telecommuting devices using a lot of bandwidth and reduction in employees' productivity while working from home.

Our paper is the first to provide a qualitative study on telecommuters to understand their security and privacy challenges, threats, and perceived outcomes of threats. We chose to conduct a qualitative study to understand *why* people face some of the predicted challenges and *how* they experience them. Qualitative studies help answer "why" questions and provide an in-depth understanding of what is being studied [54]. We believe that a more in-depth analysis of these concerns will help researchers better understand the challenges and start a discourse on the ways of addressing them.

3 Methods

3.1 Participant Recruitment

We recruited participants by advertising on Facebook, LinkedIn, and Kijiji using the platforms' paid advertisement functionalities. Potential participants filled out an eligibility survey. To be eligible to take part in the study, participants had to be 19 years or older. Participants had to have worked full-time physically in an office space in the year preceding the study. Participants had to have been working with computers for at least three days a week, so that we could explore current challenges they might be facing with the technology. Further, participants had to have been working remotely full-time in the last three weeks preceding the study. The latter inclusion criteria was to ensure that participants would remember recent experiences with working from home.

3.2 Interview Procedure

We proceeded with the interviews after the participants gave informed consent to participate in the study. To avoid priming, we told participants that the aim of the study was to understand their experiences working from home.

We asked participants for demographic information and about their general experiences working from home. Based on these experiences, participants were asked further questions regarding what they enjoyed about working from home and what they would love to change about their experience (if anything). Participants were also asked to list new technologies that they had been using to work from home. We asked further questions about participants' thoughts about using the technologies (see appendix D). Afterward, we compensated the participants. One or two researchers took part in each interview session. All interview sessions were audio recorded.

3.3 Data Collection

We piloted our study procedure with two participants. Based on the feedback from the pilot interviews, we improved the clarity of the questions. All other instruments in the main study remained the same as those used in the pilot.

We carried out semi-structured individual interviews with all recruited participants. This allowed them to express their thoughts in their own way and to add information as they saw fit, without the restrictions of structured interviews [19].

All interviews were conducted either via Skype or Zoom, based on participants' choice. We chose to conduct online interviews due to the restrictions placed on in-person meetings resulting from the COVID-19 pandemic. Participants were compensated with CAD $20, sent via e-transfer. Data collection was done from March to September 2020. Our university's Behavioural Research Ethics Board (ID: H20-01219) approved the research before any data collection took place.

3.4 Data Analysis

Two researchers transcribed and coded more than 18 hours of recorded interview sessions, each an average of 44 minutes long. Interviews were analyzed using thematic analysis [27], a "set of procedures designed to identify and examine themes from textual data in a way that is transparent and credible" [26]. We followed the data analysis steps outlined

by Guest et al. [26]. Two researchers segmented and coded the transcribed interviews into categories, types, and relationships to develop the codebook. Afterward, three researchers identified the themes that emerged from the data. In addition, four researchers engaged in a code and theme sorting exercise to come to a consensus on the identified themes. We conducted data analysis concurrently with the collection and reached theoretical saturation after 21 interviews, as no new codes emerged from the last three data collection sessions (see saturation graph in Figure C.1).

4 Results

We present our findings in the form of the challenges and perceived threats, which we categorized into technological, human, organizational, and environmental dimensions. We also link them to perceived outcomes of threats.

4.1 Participants

We recruited a diverse set of 24 Canadian participants. They were 19 to 64 years old (mean 41 and median 38), with 14 of them identified as men. Table A.1 shows the demographics of the participants regarding age, gender, educational level, place of work and job, as well as size of the employer and geographic region (when available).

4.2 Technological Dimension

Challenges related to technological dimensions are due to the use of technology while telecommuting. These challenges could result in threats to the security and personal privacy.

4.2.1 Sharing work information in unauthorized ways

Some participants used unofficial online communication channels to share work-related information. This action was a security concern as it was unclear whether these unauthorized technological solutions satisfied employers' data security requirements. Since different communication solutions have varying degrees of compliance with organizations' security and privacy requirements, using these solutions could lead to various security and privacy threats for both the organization and its employees. This action could also lead to the outcome of threat of the loss of the data *confidentiality*.

One reason for using unauthorized channels was **low usability of the authorized channels**. For instance, P15 (customer service representative) was supposed to use Bell Total Connect (BETC). However, he found it unusable: *"[To use BETC] you've got to request access, then you download it, and then you've got to have your credentials in place. ... It's a complicated program."* P15 ended up using Facebook and sometimes text messages to communicate work-related information with his boss and colleagues while telecommuting.

Another reason for the use of alternative communication channels was because **most of our participants' colleagues were already using them.** It was therefore easier to reach colleagues there. P14 (call center representative) explained: *"We do have a chat [function] in our [official] program, [but it's] just that everybody's on Facebook Messenger. So whether you like Facebook or not, you're kind of forced to use Facebook. And so I [use Facebook since] everybody's there."*

4.2.2 Sacrificing personal privacy and security

There were many instances where participants sacrificed their privacy or security to telecommute. We discuss these instances below.

The tension between professionalism and privacy on video calls. Many participants experienced tension and uncertainty around the use of their webcams during work meetings. For the sake of personal privacy, participants wanted to keep their video cameras off during some periods of work calls. However, they were uncertain whether doing so made them appear less professional or serious about their job. For P16 (planning department director), having the webcam on during work meetings was a necessity, although his colleagues did not necessarily agree: *"People should be available on video if they're doing work during the workday. [However,] that [is] a concern for some people. I have a colleague, and today she said, 'I can't show you my video because my hair is in an Afro.' ... Maybe she didn't want people to say something, or to notice, or to make a case out of it."*

P21 (senior project manager) also explained the dilemma: *"I can't force [people to turn their video on]. It's their home, so I can't really force them; I can only insist. I know that some of the managers in our organization make [a] point of telling [employees to] turn [their video] on during the meeting, [because the employees] have to be paying attention."*

Some participants felt that having the video camera on was an invasion of their privacy. Participants feared that people could take screenshots of them without their consent. P18 (executive director), explained this concern: *"I've thought about [people taking screenshots during video meetings], 'cause I know people who have [done that]. I have a call every two weeks, and there's usually about eight or nine of us [on the call], and I know that they're taking screenshots of the video [meeting], but I wish ... a part of me feels like, there should be a notification feature [on the teleconferencing app that shows] if somebody's doing a screenshot [during meetings] or if they save an image. My preference is that people ask if they're going to do a screenshot for whatever reason."* Having webcams on also virtually invited co-workers into participants' homes, which was seen as a privacy invasion. P5 (sales director) explained: *"[Through video calls,] you're inviting a lot of people into [your] home that [you] wouldn't have otherwise. So you're here [on the video call], your kids are walking by, or other family members or your dog or whatever the case*

may be, [and] you may not want people to see [all of that]." P3 (research assistant) further explained: *"[Work video meetings] certainly blur that line between your home life and your workplace. Like right now, you're in my kitchen with me. Normally co-workers wouldn't necessarily be inside the house, which is sort of a weird ... it changes that relationship [with my co-workers].*" Having webcams on during work meetings leads to the loss of employee's *privacy*.

While some of these challenges can be solved using virtual backgrounds [65, 68, 80], participants had issues with the availability and usefulness of virtual backgrounds. First, not all videoconferencing apps fully support virtual backgrounds [39]. Second, not all participants liked the idea of using a virtual background as they found the concept of virtual backgrounds to be too dull or unexciting. Third, virtual backgrounds do not guarantee that people walking by will not pop up on the screen [57].

The design of some tools made it difficult for employees to maintain security while working from home. This challenge sometimes led to the organizational outcome of threat of the loss of the data *confidentiality*. For instance, phones that used the same port for charging and connecting headphones were a challenge in case of long and frequent calls: *"I think the biggest issue [with working from home] for me is [my phone]. If I've got a day that is heavily focused on a lot of client stuff, then I have to continue using my work phone, which can be problematic ever since they've got rid of the bloody plugin that you can put your headphones in and [replaced] it with [one port], because that's [the port] I need to charge my damn phone with. So I have, on occasion, had it plugged in [to charge] and used it without headphones. And technically, depending on the voice tones of the other person [on the other end of the phone], somebody may have [over]heard our conversation.*" [P11 (health director)]. This was a security concern because housemates could overhear confidential information (§4.3.1). The participant sacrificed the confidentiality of his work calls to get the job done. In some cases, to use headphones and maintain security, P11 switched from taking calls on his work phone and used his personal phone instead. However, our results also suggest that using personal phones to manage work conversations could be a security and privacy concern, as we explain below.

Employees share their personal information to aid telecommuting. Some participants shared personal phone numbers or home addresses with colleagues and clients. In some cases they used their personal devices to work from home. These actions sometimes made it difficult for participants to draw the line between their personal and work lives. P8 (accounting supervisor), for instance, could not "move" his work landline home. So he gave the clients his personal phone number. Prior to working from home, P8 never picked up calls from unknown numbers because he was afraid of being scammed. That changed after giving his personal number to work clients: *"[Recently I received a call from an unknown number.] First ... I wasn't going to answer [but] then I [decided to] answer [and] I was really lucky that I took the call because it was [from] the government. And [the government] was just verifying information so that they could pay [my organization] the subsidy. So if I'd refused that call, it would have really slowed down the payment, and then my boss would have been mad at me, because we were rushing around to submit our application. So of course now I'm answering more calls on my [personal phone], and I don't screen it as closely as I [used to do] before. If I'm going to work from home, that's part of working from home. I'm going to pick up the phone for numbers that I don't know.*" P8 sacrificed his privacy and precautionary safety measure to continue his regular work activities at home.

When asked if he still had a fear of picking up a call from a scammer, P8 replied: *"I'm afraid if I pick up [a] call from a scammer, that somehow they are going to know that there is a live person at the end of the line and then they're going to get me more scam calls. [But] I'm afraid that if I miss a business call, then I'm going to get criticized by my boss because it affects my work, [and] I [end up not] do[ing] something [at work] fast enough. And the boss will be mad, because I didn't pick up a phone call.*"

P23 (school secretary) further remarked: *"I had to use my own personal cell phone to communicate with parents. That part of [telecommuting] was awkward ... because now I find the parents text me or leave me a message to get information. For me [giving out my phone number] does cross the boundary. I always have tried to separate as much as I could, my private life from my work life ... it was basically just assumed upon us [by the organization] when [the organization] decided they were going to [send us home to work]. ... I probably could have done [the call blocking code], but I didn't do that. I do believe you get charged for [doing that] so I didn't want to have that fee on top of other fees.*"

In some cases this challenge included giving coworkers participants' home addresses. P3 further explained: *"So if I asked my coworker to pick something up from my office, then probably he might drop it off at my house. So then he would know where I live. So I feel like it starts to open up some kind of personal privacy [issue].*"

The use of some technological tools in telecommuting made it easy to monitor participants' activities. For example, the User Presence feature [70] in Microsoft Teams makes it easy to determine a user's activities online. Some participants were concerned of their *privacy* being further reduced by this feature, as illustrated by P16: *"I notice that you can tell who is on their computer and who is not, [using Microsoft Teams]. For example, now I can type any name, and I can see [who is online and who is not]. [The] red [button] means that they're on a [Microsoft Teams] call or [in] a meeting; green means that they're on their computer, but not in a meeting. And yellow means that they've walked away from their computer and the little X means the computer's turned off. I*

find that [that] can be used to monitor whether people are at their desk or not. So, for example, a manager can check whether their employee is yellow, green, or red, and they could be green and surfing the 'net, and they could be yellow and reading a document [on] the computer. ... [Managers] might jump to conclusions [in] thinking that an employee should be either green or red, but not yellow, because yellow means that they're not [at] the computer."

Unauthorized people controlling participants' computer remotely. The possibility that people's computers could be remotely controlled was a privacy and security challenge for participants. Some jobs require participants to give their employers or customers remote access to their computers. However, in giving employers remote access, participants feared that their employer would be able to access other parts of their computers remotely which could lead to *unauthorized access to data* and loss of *privacy*. When teaching students online, the job of P17 (education assistant) requires her to give her students remote access to her computer so that they can play an educational game: *"When we are sharing the screen with [another] person, we ... give [remote] control to the other person, [and] that was [a] concern because that person can go on your computer and probably check anything on your desktop. [For example, after giving remote control to a student], then that student can control my screen ... or can check anything."*

4.2.3 Reducing security for usability

To make some technological tools usable, security was sometimes sacrificed. We discuss some instances where security and privacy were sacrificed for usability while telecommuting.

Employees bypassed organizations' security measures to make use of technological tools. As a security measure, some work-from-home phones were too locked down, and participants did not find them usable enough. Participants sometimes came up with workaround solutions that were less secure. These workarounds would result in even higher consequence of threat to the *confidentiality* of the organization's data than the task they were trying to accomplish, as illustrated by the story of P6 (senior staff): *"The [work] iPhone that I [use] is so well locked down that I cannot copy and paste from an email into a text message. [If I try to do that, the work iPhone] says 'You cannot paste your organization's data here,' and it's a complete pain because there are times when [I'm] communicating with my boss by text message where she says, 'Can you just send me that phone number?' [or] like an email address or something like that. [I] can just type [the information my boss is asking], but my memory is terrible. I would always copy and paste something rather than [type] it. [It's] a particularly annoying feature and so I found a workaround: If I had something that I needed to text to my boss, I [would] actually send the email from my work email address to my home email address, then use my [personal] iPhone to cut and paste the information into a text and send."*

Reduced security of technology to aid usability. To enable employees to work effectively from home, sometimes IT personnel reduced the security of some organizations' devices. Such compromises could reduce organizational data *confidentiality* and *integrity* and violates organization's security control rules and policies. P8 narrated a related experience: *"[I] brought [a second] monitor home when I first remote accessed [in to work]. The second monitor did not work, and so I complained to the IT manager, and [the IT manager] said [that] for security purposes the standard remote logging software simply does not allow two monitors. So the IT manager said, '[P8's name], don't tell anybody else this because it's not good control, but I made you a special URL, and now you can access [the work computers remotely with] two monitors.' I'm guessing that by giving me this special URL [designed just] for me, I have more access to the [organization's] information... . So I think it's weaker control over the security of [people's] information.' And [the IT guy] did tell me, 'Don't tell anyone else; I'm just doing this as a favor for you,' because IT [has] to maintain the security of the computer network. And if there was a hack or break-in, [the IT manager] would get blame[d]. So I have not told anyone else, but really I should tell my colleagues because it would speed up their work, [but] I'm afraid I'll lose the special favor with the IT manager if I tell anybody else."*

4.3 Environmental Dimension

There were threats specific to the home work environment. They were mostly expressed as fears and concerns. We describe these threats below.

4.3.1 Household members can access the organization's confidential information

There were concerns about others in the household overhearing the organization's confidential information. This was a particular concern for participants with housemates. In some cases, participants shared office space with their housemates. In other instances, the house had thin walls, and the house occupants and guests could overhear conversations held in various locations within the house. Some participants' jobs included handling confidential information; therefore, a security threat was that others could overhear these conversations. This led to the organizational outcome of threat of the loss of data *confidentiality*. For instance, P15, who had three roommates and worked from the dining area of his house, explained: *"If [clients are] giving me [their] credit card information, and I'm reading [the credit card details] back to [them, I would be] around people [in the house while reading the details]. Frankly, I don't think I'll be able to avoid [my roommates' overhearing] until I go back to the office. ... Right now, if somebody comes into the kitchen [to] make food, I could be*

on a call, [and] that makes things a little awkward at times."

Participants feared that their customers and colleagues could overhear private conversations from participants' homes. They were concerned with the loss of their and other housemates' *privacy*. P9 (call center agent), explained this concern: *"We have very thin walls in my house, and my room is right beside the bathroom. And a lot of times when my parents are calling [for] my brothers' [attention], I can hear [my parents] through the wall. Sometimes I have text[ed] my brothers [saying], 'Hey, can you please keep it down? I'm on the phone with a taxpayer. And they may be able to hear you through my headset.' [At] home you can almost hear everything that goes on."*

There was also the possibility of unauthorized people viewing employer's confidential data. For instance, P11, who worked from his dining room, explained: *"[I] had multiple eye surgeries last year, so I don't really see out of this [eye]. So I have a big screen in our dining room, which is completely open to our kitchen. And then [on] another side, it's kind of an open concept: living room, dining room, [and] kitchen. If anybody was coming in and walking around, they could have seen documents that I was working on the large screen, because it blows it up quite large, so it's quite legible to anybody that wanted to read it."* This is a security threat, as P11 sometimes works on clients' confidential information.

4.3.2 Employee's location could be traced

Some participants feared that some of the work calls made from home could be traced back to their location. This would result in the loss of their *privacy*. To illustrate, P9 works with the government and sometimes takes phone calls from angry citizens. While telecommuting, P9 uses her work mobile phone to make and receive calls from clients at home. P9 remarked: *"Sometimes, I wonder if [clients] are able to trace my phone calls. I know they're not [able to] because my [work] phone number doesn't pinpoint the exact location I am in. I work with [people's social insurance/security] numbers [and] addresses [on my system, and] a lot of the times when I get calls, some of them I realized have been close to my neighborhood. There was one call I received that was actually two streets down from where I was staying. And I [thought], '[What] if this person knew where I was located?' Sometimes I wonder, 'Oh, man, like if they knew where I was located, would they come to my house and ask me to do stuff?"* While this threat may be improbable, this fear made the participant anxious about handling work phone calls from home.

4.3.3 People might break into employee's house

There was a fear that someone could break into participants' houses to steal the company's equipment. This was a security concern and a constant fear for few participants who took home expensive work devices to aid telecommuting. If realized, this consequence of threat could result in the violation of participants' *privacy* and safety, loss of system *availability*, as well as data *confidentiality* and *integrity*, and, in extreme cases, the loss of *life*. For instance, P11 explained: *"My only other massive fear is, what if I had a break-in and somebody stole my [work] laptop? I mean, I have great confidence that that wouldn't happen, but it absolutely has been a fear. I think that's probably [the] only sort of ... situation that genuinely creates the occasional bit of anxiety for me ... 'Jesus, how do I know I am [secure]?' [Someone breaking in] seems like one of those improbable situations, but not impossible. So, even saying it out loud makes me nervous that somehow I am creating that reality now, because we certainly have people [in my neighborhood] with addictions who sooner or later need to feed their addictions and need to get money and sometimes get desperate."*

4.4 Human Dimension

These are challenges that were specific to individuals and their varying capabilities or limitations. We explain these challenges below.

4.4.1 Challenges with using the technology

Some participants were not tech-savvy, which made it harder for them to switch to full-time telecommuting. P7 (network engineer), for instance, remarked: *"The human aspect of security is always the biggest problem. [The IT personnel] are not there to monitor what everyone does at home on their computers all the time. Users don't know how to properly explain what their [technological] issue is; they use end-user terminology instead of technical terminology. So trying to translate the communication with the users was the biggest challenge. [When users had a technical issue,] trying to get them to explain to us what the problem [was challenging]."*

Lack of technical knowledge could lead to dangerous errors. This outcome of threat was particularly a concern when there was a disconnect between the participants' knowledge and what the organization expected them to do. For instance, some participants could fail to install security-critical software updates on their work systems while telecommuting, due to the lack of the technical capacity to do so. This challenge could lead to the loss of *integrity* and *confidentiality* of the organizational data, should employees' computers become targets of cyber-attacks.

The lack of technological competence was also reflected in poor understanding of security. For example, when discussing virtual private networks (VPNs), P1 (digital communications specialist) remarked: *"VPN, is ... something that secures your laptop. I just know [VPN] makes everything safe. You can't get hacked. You can't [have] none of that [hacking]. Everything's secured."* In this particular case, P1 assumed that once she connected to her employer's network using a VPN, everything

on her laptop was secure.

4.4.2 The challenge of distinguishing real organizational emails from phishing ones

Participants had difficulty distinguishing between real organizational emails and phishing ones. Sometimes, employees had been so much sensitized about phishing emails that they would classify real organizational emails as phishing. P7 shared an illustrative story: *"[Prior to working from home, my organization had [a] service that would do hands-on training [and send] out test fake emails to [employees]. If anyone clicked on [one of these fake emails], they'd get a warning, that [said], 'By the way, this is not real; this is a phishing email.' Now, [while employees have been working from home], we were sending out updates regarding viruses and anti-viruses and then people were reporting [them] as [phishing emails], not realizing it was a legitimate board email. [People have become] too paranoid."*

It was hard for some participants to recognize legitimate work-from-home precautions and apply them as needed. Some of these precautions are required to protect the confidentiality and integrity of work data. Therefore, similar to the challenges of using technology (§4.4.1), this challenge could lead to the loss of *confidentiality* and *integrity* of organizational data.

4.5 Organizational Dimension

The major challenge was that organizations sometimes provided few or no guidelines on how to telecommute. We define telecommuting guidelines as a set of instructions for employees about what to take home from work, how to set up their home office, and how to ensure the security and privacy of work-related information. We discuss this challenge below and explain how it led to other security and privacy issues for participants.

Many participants received little or no guidance on telecommuting. P15, for instance, was handling financial information while working from home. However, it was unclear to him how he would do that safely. When asked about guidelines regarding working from home, he explained: *"We barely get told anything [regarding telecommuting]. ... There hasn't been any communication with regard to how to handle confidential conversations over the phone. We just use our discretion [in handling financial] matters [over the phone].*

Telecommuting violates the organizations' work policies. For some organizations, working from home violates the organization's policies, and therefore, there are no guidelines for employees. When P11 was asked about the work-from-home guidelines instituted by his organization, he remarked: *"There were no guidelines [for telecommuting;] in fact, ... [working from home] is breaking [the] guidelines. ... We had just recently completed a very thick policy manual about data protection, information, privacy, [and] security ... that indicated [that] you don't take anything [from] work [to] home. All work will be done from the office. So in fact, having to respond to the pandemic created a conflict with recent policies around the security of information."* As such, people in some organizations had no guidelines on how to work from home.

Participants, therefore, came up with their own norms of working from home. They used their own understanding and interpretation of security and privacy best practices. For instance, when asked about her work-from-home practices, P3 explained: *"[Be]cause I'm working on my personal computer, [I'm] not saving anything on my actual computer a whole lot. ... I save everything on my [USB] stick. It's not too hard [to remember to save files on my USB stick] because I just leave the stick plugged into my computer ... so it's right there."* P3 further explained that she secured her laptop by using a password, though her USB stick was not encrypted or password protected. Since P3's USB stick was always plugged into the computer, the information saved on the USB stick was only as secure as the information saved on her personal computer or even less. The concern is that attackers (who could be household members) need a password to access the files saved on P3's laptop, but attackers can easily access the USB stick files. This challenge could lead to the organizational outcome of threat of the loss of data *confidentiality* if attackers had access to the USB stick.

5 Discussion

Our findings point to the security and privacy challenges, threats, and potential outcomes of threats that participants perceive while telecommuting. Figure 1 illustrates the consequences of a threat that could arise due to the identified challenges and threats with telecommuting, which we described in the previous section. In this section, we generalize discussion of the results in the form of perceived outcomes of threats to telecommuters and their employers. In Table 1 and Table 2, we present the challenges and threats, as perceived by participants, and show how they could lead to various outcomes of threats. We identified participants' perceived outcome of threat in which the organization's assets are at stake (Table 2). In contrast with office work, mass telecommuting introduces additional consequences of threats. The participants' privacy, data, and in some cases, well-being are at stake (Table 1). In the rest of the discussion section, we describe both types of these outcomes of threats and discuss options for mitigating some of them. It should be noted, however, that proper evaluation of these countermeasures is subject to future research.

While some of the challenges and threats are not unique to telecommuting, the issues are amplified in scale and severity when workers solely rely on telecommuting. The severity of the challenge gets intensified due to the lack of physical proximity among the coworkers for many weeks, if not months.

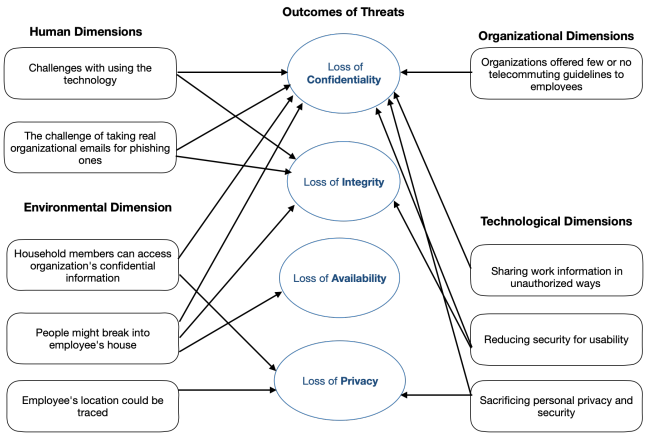

Figure 1: The relationship between challenges, threats, and the outcomes of threats. Arrows link challenges\threats to the outcomes of the threat.

For example, confidential information may have never been shared through unauthorized means (§4.2.1), because employees would meet in person. However, mass telecommuting takes away that opportunity, leaving employees with nothing else but to rely solely on online solutions, some of which (in isolation or in combination with other technologies) turned out to be over-restrictive or otherwise have less than acceptable usability (§4.2.3). Another example is the possibility of using technological tools to monitor employees' activities, which could result in an invasion of their privacy (§4.2.2). This challenge could lead to bigger issues, such as monitoring employees' or coworkers' daily routine even during weekends. These privacy issues became much more of a concern when long-term mass telecommuting became widespread overnight and might even remain so after the pandemic [15, 16, 32, 55]. Identifying and addressing these challenges, therefore, would go a long way toward improving telecommuting beyond the pandemic. Further, mass telecommuting could also happen in emergency situations such as power outages, earthquakes, and other natural and human-made disasters. In the rest of this section, we categorize recommendations into three types, according to the intended audience: organizations (R-O), employees (R-E), and those working with telecommuters (R-T).

5.1 Perceived Outcome of Threat Toward Workers

Telecommuting elevates the outcomes of threats to personal safety for employees and their households. Some participants worried that angry clients could locate their homes and terrorize them (§4.3.2). Other participants were anxious that criminals could break into their homes and steal their organizations' expensive work devices while also putting participants' privacy and safety at risk (§4.3.3). These anxieties could negatively affect employees' productivity, job satisfaction or employee retention while telecommuting [22, 38, 50]. Physical security at work is the responsibility of the employers and is commonly implemented by monitoring and controlling access to the office space and parking lots, and by stationing security personnel in the office buildings [10, 25, 63]. In the telecommuting scenario, however, the expensive work equipment now resides in the employees' homes, and there is no physical security provided. Organizations could implement encryption of the computer's hard drive to safeguard their data [29, 36, 61, 73]. However, the safety of the employees and the household members is also at risk due to telecommuting. Therefore, telecommuting produces a negative externality [30], as it is the employer that benefits from the employee being able to telecommute, but it is the household members who have to mitigate the elevated risk to physical safety and the psychological trauma that comes with it.

Employers can put measures in place to manage the safety of the telecommuters and their households **(R-O)**. Organizations need to be sensitive to the employees' physical security and consider the reality that different employees live in neighborhoods with varying safety levels (§4.3.3). Organizations can be mindful of this threat and manage it as part of their policies or processes for handling work from home. For long-term (and full-time) telecommuting, the employers could consider setting up home alarm systems for their employees. The employers could also look into setting up work hubs where the organization's devices could be set up and the employee's safety is protected. Further, employers can educate employees about security measures at the work hub to allay their fears. We also suggest that organizations provide clear guidelines on managing the home-work environment to optimize employees' physical safety. For instance, similar to on-site organizational security measures, employers could develop processes for physical security while telecommuting, such as help lines or safety routines that employees could use if the organization's clients/customers misuse employees' personal data.

Loss of workers' privacy is the major theme that emerged in the interviews. As can be seen in the rightmost column of Table 1, every type of concern is related to this theme. The main reason for its omnipresence, we believe, is that telecommuting is a hybrid work situation, where employees are at home but expected to carry out the organization's activities. Therefore, employees must behave in a specific way, which comes at the cost of their privacy. For instance, employees gave clients and coworkers (and even sometimes customers) their own phone numbers and other personal information (§4.2.2). The participants had other privacy boundaries (e.g., by answering phone calls from unknown numbers) compromised to facilitate telecommuting (§4.2.2). Workers were also worried about others taking screenshots of them without their consent during video calls (§4.2.2) and others feared that their clients and colleagues could overhear personal conversations taking

Table 1: Perceived Outcome of Threat Toward Workers

Asset	Employee's behavior	Threat agents	Reason for concern	Threat	Outcome of threat
1. Employee's personal phone number and home address	Employee giving coworkers their personal information to aid telecommuting	Coworkers	a. Violation of personal boundaries b. Less control over who has access to personal information	a. Coworkers could use employee's personal information for purposes other than initially declared b. Sharing of personal information without permission from the subject of the information	**a. Misuse and unauthorized sharing of shared personal data** **b. Loss of privacy** (§4.2.2)
2a. Employee's money b. Employee's privacy	Employee picking up calls from unknown numbers, not screening phone calls	Phone scammers	Reduced protection from scam calls	a. Phone scammers could obtain employee's financial information b. Increase in scam calls	**a. Abuse of personal data** **b. Becoming a victim of scams** **c. Loss of privacy** (§4.2.2)
3a. Employee's private home setting b. Housemates' privacy c. Employee's privacy	Employee forced to turn on their video camera during telecommuting	Coworkers	a. Personal environment of the employee is exposed to coworkers b. Lack of privacy in the home environment VS the work environment	a. Coworkers seeing employee's private environment and housemates b. Employee's improper disclosure of themselves	**a. Accidental disclosure** **b. Loss of privacy** (§4.2.2)
4. Employee's routine	Using technological tools that make it easy to monitor employees	Coworkers, managers	Coworkers and managers can monitor employee's activities and routine	Coworkers and managers could use this information to predict employee's routine	**Loss of privacy** (§4.2.2)
5. Employee's personal data	Giving students remote access to the employee's computer	Students	Due to a lack of computer knowledge, there is uncertainty about what students can do on the employee's laptop when given remote access via videoconferencing	Students could control the computer of a non–tech-savvy employee and access personal data	**a. Abuse of personal data** **b. Loss of privacy** (§4.2.2)
6. Employee's safety	Calling customer/client from home	Customer/client	Unmasked work phone number	An angry customer/client could locate employee's home by tracing phone calls made to the customer/client	**a. Abuse of personal data** **b. Loss of life** **c. Loss of privacy** (§4.3.2)
7. Employee's safety	Distributing care packages from home	Criminals present in neighborhood	Physical harm by intruders during a break-in to the house	Physical harm and injury	**a. Loss of life** **b. Loss of privacy** §4.3.3)

place at the workers' homes (§4.3.1).

There are various ways for employers to aid their employees in maintaining privacy while working from home. Organizations can provide some form of phone number masking (which prevents others from knowing the actual phone number of the caller) or VoIP solutions [42] to employees who have to use their personal phones for work [23] **(R-O)**. Further, we suggest technology support for alerting participants of video calls when screenshots are taken, to help employees maintain awareness of their privacy violations and to deter abuse of such capabilities by others (§4.2.2) **(R-E)**. To prevent clients and colleagues from hearing personal conversations happening in the household, teleconferencing software and phones could have a feature where the microphone is automatically muted when employees are not talking. Using voice recognition, the microphone automatically unmutes when the employee starts talking to the client or coworker **(R-T)**. There could also be directional microphones on phones and videoconferencing apps, whereby the technology only picks up the voice of the person in front of the computer or phone **(R-T)**.

Furthermore, there seems to be a conflict between employees maintaining their privacy and doing their job. Our findings confirm Pyöriä's work, as this author predicted disruption to privacy in employees' homes as a challenge that could arise in teleworking [52]. Our participants experienced a dilemma around whether to turn on their webcams during work meetings. For some, turning on the webcams was an invasion of privacy, as it welcomed coworkers into their private homes and lives. On the other hand, employers expected participants to always have their webcams on during work meetings as these meetings are done within work hours (§4.2.2). Further, some employees also had to give clients remote access to their personal computers while telecommuting (§4.2.2). In addition, some telecommuting solutions could aid with monitoring employees' activities and detect when employees were at or away from their desks (§4.2.2). Research shows that such online status indicators or presence sharing applications leads to privacy concerns for users [12,18,28,56]. Other features of videoconferencing apps raise further concerns about employees' privacy during telecommuting. For instance, Microsoft Teams and Zoom allows meeting participants to livestream a meeting without getting consent from the participants [69,81]. Therefore, employees' work meetings in their personal spaces can be livestreamed on Facebook Live and YouTube without the employees' knowledge. All of these situations raise questions about employers' rights over employees privacy in their own homes. Palen et al. discussed the issues surrounding privacy in a technologically connected world. Because privacy is personal, people set various boundaries in their everyday life to maintain their privacy [3,49,71]. However, the use of information technology disrupts or demolishes those boundaries. The authors explain the challenge further: "problems emerge when participation in the networked world is not deliberate, or when the bounds of identity definition are not within one's total control. [49]" As seen in our results, employees do not have full control over their privacy, which is a challenge. There is also the issue of content collapse in telecommuting. "The concept of context collapse describes the process by which connections from various aspects of individuals' lives become grouped together under generic terms [1,11,74]." Similarly, in

telecommuting, workers experience context collapse and are faced with the dilemma of how to draw boundaries between their personal and professional lives. This leads to privacy issues for participants (§4.2.2).

To help create a balance between privacy and doing one's job, organizations can have discussions and transparency on how much privacy employees are entitled to when telecommuting **(R-O)**. It may be helpful for organizations to clearly state what they expect from employees regarding having the camera on or off while working from home, dress code while telecommuting, or giving clients their personal phone numbers. There might, however, be no clear-cut answers to these questions. Moreover, they raise bigger questions that future research could look into. For example, can employees maintain their privacy while working from home? If yes, how can privacy boundaries be maintained while respecting organizational cultures, social norms, and work policies? Does the use of technologies that monitor employees' routines (mostly during work hours) violate their privacy? Should technological tools be allowed to monitor workers' activities during and after work hours when they work from home? How can employees give or withdraw their consent for recording, screenshots, or livestreaming during online work meetings without feeling stigmatized or fearing repercussions? How can organizations and technologists make sure employees are not putting their physical safety at risk when working from home (§4.2.2)? Employers and employees need to consider these different scenarios when making telecommuting arrangements.

5.2 Perceived Outcome of Threat Toward Organizations

The outcomes of threats related to the confidentiality and integrity of the organization's assets were the most common theme in this category (see Table 2). Kintner et al. and Spinellis et al.'s participants also predicted inadequate security for protecting transmitted information in teleworking as a potential challenge [34, 66]. In some cases, the organization's assets were at risk because the official work communication platforms' were not usable (§4.2.3). Therefore, participants used other insecure but usable and familiar technological solutions to talk to coworkers and share clients' confidential information. Since participants no longer had the luxury of talking in person to their colleagues about work-related matters, participants were looking for technology support closest to in-person interactions. Such support made communication with coworkers easy without unnecessary setup or complicated authentication procedures (§4.2.1 & §4.2.3). Employers need to ensure that work communication platforms are very intuitive and easy, if they want to address this issue **(R-O)**. These work communication platforms could also be linked to other popular social communication channels. For example, organizations could work toward having a secured platform on Facebook to discuss work-related information. One of the principles of secure systems design is the path of least resistance [79]. This principle states that "to the greatest extent possible, the natural way to do any task should also be the secure way" [79]. Since employees are already using these social platforms anyway, employees are most likely to follow the path of least resistance. Such types of platforms are subject to future research and development.

The inability to distinguish between phishing and real emails rendered employers' announcements ineffective. Some organizations asked their employees to use their personal devices to work and expected employees to use the organization's software on those devices. Because IT personnel didn't have control or access to the employees' devices, IT personnel had to send emails to the employees with system updates required to maintain the organization's software while telecommuting. Because employees found it challenging to distinguish between fake and real emails, employees ignored important system updates sent through emails (§4.4.2). Organizations could make use of already existing solutions to digitally sign and encrypt official emails from the organizations [47] **(R-O)**. Employees would, however, need to learn and understand how these solutions work because, as previous research shows, people find it difficult to use encrypted and signed emails correctly [76]. Apart from email, we suggest that other communication platforms could be used, such as a usable official messaging platform to relate work information **(R-O)**.

There was also the outcome of threat of household members overhearing confidential work discussions. In real-life situations, these confidential conversations are mostly held in offices, which are considered safe enough for those conversations to happen. However, in the context of telecommuting, home environments do not necessarily provide sufficient sound insulation. While this might not be an acute issue for traditional households with one family, cohousing [13], collective housing, and similar arrangements that are increasingly common in urban areas where housing is expensive significantly decrease control and awareness of who might be in a household and possibly overhear discussions at any given moment.

There is no easy way to address this problem. The solution is not as simple as telling employees to take work calls where other household members cannot overhear the conversation. By default, there seems to be an assumption that the employee's home environment is a typical family setting with father, mother, and child(ren) and an office space with a closed door where the employee can conveniently take work calls. In reality, employees have a wide variety of cohabitation arrangements and environments and for some, it is simply impossible to avoid working in a space shared with the housemates. Further, in some cases working in a separate room doesn't solve the problem of poor sound insulation (§4.3.1). Organizations **(R-O)** need to be sensitive to the fact that employees' living situations vary and should be mindful of the corresponding

Table 2: Perceived Outcome of Threat Toward Organizations

Asset	Employee's behavior	Threat agents	Reason for concern	Threat	Outcome of threat
1. Confidential information	Putting organizations' and customers' confidential information on social media platforms	Employees of social media platforms, cybercriminals	Lack of confidentiality on social media platforms	a. Employees of the social media platform could spy on the organization's confidential data b. Cybercriminals could exploit the vulnerabilities of social media platforms and obtain confidential information	**Loss of confidentiality** (§4.2.1)
2. Customer/client's confidential information	a. Discussing confidential information through device speakers b. Reading out clients' confidential information	Housemates	Lack of sound insulation	Housemates could overhear confidential information	**Loss of confidentiality** (§4.2.1)
3a. Citizen's information b. Political report that has not been made public	Making use of a less secure personal phone and email software	Social insiders, cybercriminals	Personal phones and email software are not configured to be as secure as work phones and emails	a. Social insiders snooping through employee's phone and accessing their text messages b. Hijacking personal email account and obtaining copies of the work emails	**Loss of confidentiality** (§4.2.3)
4. Organization's accounting information	Reducing the security of systems to aid telecommuting	Cybercriminals	Reduced security of remote desktop server	Cybercriminals could compromise the security of the system and access organization's data	**a. Loss of confidentiality** **b. Loss of integrity** (§4.2.3)
5. Confidential information	Giving students remote access to employee's personal computer	Students	Due to a lack of computer knowledge, there is uncertainty about what students can do on the employee's laptop when given remote access via videoconferencing	Student could control the computer of a no–tech-savvy employee and access confidential data	**a. Loss of confidentiality** **b. Loss of integrity** §4.2.2)
6. Client's health information	Displaying confidential information on big screens, in large font sizes, while telecommuting in the kitchen area	Housemates	Housemates could read confidential information off the screen	Housemates could view confidential health information	**Loss of confidentiality** (§4.3.1)
7. Organization's confidential information	Unable to troubleshoot work devices from home	Cybercriminals	Reduced security of work devices for telecommuting	Cybercriminals could exploit vulnerabilities in work devices	**Loss of confidentiality** (§4.4.1)
8. Organization's confidential information	Using expensive organizational work devices to aid telecommuting	Criminals present in neighborhood	Lack of physical security of work devices and recent break-in	Neighbors could break into employee's home and steal work equipment	**a. Loss of confidentiality** **b. Loss of integrity** **c. Loss of availability** (§4.3.3)

outcomes of threats to the confidentiality of work calls.

There is a need for discourse in the research community on the possible solutions to these problems. Table 1 and Table 2 present a comprehensive illustration of possible outcomes of threats to organizations and employees while telecommuting. As telecommuting becomes more full-time and long-term [15, 16, 24, 32, 41, 55], the topics and issues surrounding organizational data security and employees' safety and privacy need to be discussed and addressed. The main topic is that there is a dilemma around employees maintaining their privacy and safety while telecommuting and employers ensuring that employees carry out their work from home and safeguard their organization's data. With the increase in successful cyber-attacks on telecommuters [6, 33, 40, 77], addressing the identified security and privacy challenges and threats encountered by employees may go a long way in reducing cyber-attacks related to telecommuting. We believe our study provides insights into these challenges and serves as a basis for possible solutions to be explored and discussed and will ultimately lead to better work-from-home practices for both employees and employers.

5.3 Limitations

Our sample could have been more balanced and diverse. It had more male (56%) participants, though statistics show that more men are employed than women [48]. The average and median age were 41 and 38, respectively. We could have recruited more older participants. However, the oldest participant was 64, and statistics show that on average the age of retirement is 62 [14, 62]. Further, we do not have enough data about the context (e.g., participant's environment) to determine whether each threat is realistic or probable. As with most qualitative research, the data were self-reported and may have been affected by several systematic biases such as social desirability, halo effect, and acquiescence response bias [20]. Nonetheless, we believe that our study results can serve as a background for further research and discourse on how to improve the security and privacy of telecommuters.

6 Acknowledgements

This research has been supported in part by a gift from Scotiabank to UBC. We thank Larisa Lensink for having brainstorming sessions with the lead author on the idea of doing this study. We appreciate all participants involved in the study. We thank members of the University of British Columbia's Laboratory for Education and Research in Secure Systems Engineering, which provided feedback on the reported research and the earlier versions of the paper. We thank our anonymous reviewers for their feedback and suggestions for improving the paper. Stylistic and copy editing by Eva van Emden helped to enhance the readability of this paper.

References

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[2] Abi Adams-Prassl, Teodora Boneva, Marta Golin, and Christopher Rauh. Work tasks that can be done from home: Evidence on variation within & across occupations and industries. *CEPR Discussion Paper No. DP14901*, 2020.

[3] Irwin Altman. The environment and social behavior: privacy, personal space, territory, and crowding. *ERIC*, 1975.

[4] John Ameriks, Joseph Briggs, Andrew Caplin, Minjoon Lee, Matthew D Shapiro, and Christopher Tonetti. Older americans would work longer if jobs were flexible. *American Economic Journal: Macroeconomics*, 12(1):174–209, 2020.

[5] Shelly Banjo, Livia Yap, Colum Murphy, and Vinicy Chan. Coronavirus forces world's largest work-from-home experiment. https://www.bloomberg.com/news/articles/2020-02-02/coronavirus-forces-world-s-largest-work-from-home-experiment, 2020. Accessed: 2020-09-11.

[6] Carbon Black. Global threat report extended enterprise under threat. https://www.carbonblack.com/wp-content/uploads/VMWCB-Report-GTR-Extended-Enterprise-Under-Threat-Global.pdf, 2020. Accessed: 2020-09-11.

[7] Nicholas Bloom. The bright future of working from home. https://siepr.stanford.edu/research/publications/bright-future-working-home, 2020. Accessed: 2020-09-11.

[8] Nicholas Bloom. How working from home works out. https://siepr.stanford.edu/research/publications/how-working-home-works-out, 2020. Accessed: 2020-09-11.

[9] Nicholas Bloom, James Liang, John Roberts, and Zhichun Jenny Ying. Does working from home work? evidence from a chinese experiment. *The Quarterly Journal of Economics*, 130(1):165–218, 2015.

[10] Security Boulevard. Best practices: 6 physical security measures every company needs. https://securityboulevard.com/2019/03/best-practices-6-physical-security-measures-every-company-needs/, 2019. Accessed: 2021-02-1.

[11] Danah Boyd. Taken out of context: American teen sociality in networked publics. *Available at SSRN 1344756*, 2008.

[12] Andreas Buchenscheit, Bastian Könings, Andreas Neubert, Florian Schaub, Matthias Schneider, and Frank Kargl. Privacy implications of presence sharing in mobile messaging applications. In *Proceedings of the 13th international conference on mobile and ubiquitous multimedia*, pages 20–29, 2014.

[13] Cohousing Califonia. Cohousing califonia. https://www.calcoho.org, 2021. Accessed: 2021-02-24.

[14] Statistics Canada. Retirement age by class of worker. https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=1410006001, 2020. Accessed: 2020-09-11.

[15] CBC. Shopify permanently moves to work-from-home model. https://www.cbc.ca/news/canada/ottawa/shopify-pandemic-staff-ottawa-1.5578614, 2020. Accessed: 2021-01-18.

[16] Katie Clarey. In the next decade, half of facebook's workforce could be remote. https://www.hrdive.com/news/facebook-remote-workforce-zuckerberg-announcement/578578/, 2020. Accessed: 2021-01-18.

[17] Fintan Clear and Keith Dickson. Teleworking practice in small and medium-sized firms: management style and worker autonomy. *New Technology, Work and Employment*, 20(3):218–233, 2005.

[18] Camille Cobb, Lucy Simko, Tadayoshi Kohno, and Alexis Hiniker. User experiences with online status indicators. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2020.

[19] Deborah Cohen and Benjamin Crabtree. Qualitative research guidelines project. http://www.qualres.org/, 2006.

[20] Diane Dodd-McCue and Alexander Tartaglia. Self-report response bias: Learning how to live with its diagnosis in chaplaincy research. *Chaplaincy Today*, 26(1):2–8, 2010.

[21] Gus Evangelakos. Keeping critical assets safe when teleworking is the new norm. *Network Security*, 2020(6):11–14, 2020.

[22] Michael T Ford, Christopher P Cerasoli, Jennifer A Higgins, and Andrew L Decesare. Relationships between psychological, physical, and behavioural health and work performance: A review and meta-analysis. *Work & Stress*, 25(3):185–204, 2011.

[23] Derek Frome. Masked calling. https://www.twilio.com/docs/glossary/what-is-masked-calling, 2020. Accessed: 2020-01-07.

[24] Ryan Golden. Gartner: Over 80% of company leaders plan to permit remote work after pandemic. https://www.hrdive.com/news/gartner-over-80-of-company-leaders-plan-to-permit-remote-work-after-pande/581744/, 2020. Accessed: 2021-01-18.

[25] Greetly. Workplace security & access control - the fundamentals. https://www.greetly.com/blog/workplace-security-access-control-the-fundamentals, 2020. Accessed: 2021-02-1.

[26] Gregory Guest, Kathleen M MacQueen, and Emily E Namey. *Applied thematic analysis*. Sage Publications, 2011.

[27] Gregory Guest, Kathleen M MacQueen, and Emily E Namey. Introduction to applied thematic analysis. *Applied thematic analysis*, 3:20, 2012.

[28] Roberto Hoyle, Srijita Das, Apu Kapadia, Adam J Lee, and Kami Vaniea. Was my message read? privacy and signaling on facebook messenger. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 3838–3842, 2017.

[29] Huridocs. 5 steps to protect your data in case of computer theft. https://huridocs.org/2015/12/steps-to-protect-your-data-computer-theft/, 2015. Accessed: 2021-02-1.

[30] Corporate Finance Institute. What are negative externalities? https://corporatefinanceinstitute.com/resources/knowledge/economics/negative-externalities/, 2021. Accessed: 2021-02-24.

[31] INTERPOL. Interpol report shows alarming rate of cyberattacks during covid-19. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19, 2020. Accessed: 2021-01-18.

[32] Jack Kelly. Twitter ceo jack dorsey tells employees they can work from home 'forever'—before you celebrate, there's a catch. https://www.forbes.com/sites/jackkelly/2020/05/13/twitter-ceo-jack-dorsey-tells-employees-they-can-work-from-home-forever-before-you-celebrate-theres-a-catch/?sh=771246c82e91, 2020. Accessed: 2021-01-18.

[33] Yiftach Keshet. Recent escalations in cyberattacks in italy prove the coronavirus impact on cybersecurity – acting as a warning for cisos worldwide. https://www.cynet.com/blog/recent-escalation-in-cyberattacks-in-italy-prove-the-coronavirus-impact-on-cybersecurity-acting-as-a-warning-for-cisos-worldwide/, 2020. Accessed: 2020-09-11.

[34] Susan Kintner. Preliminary report telework/telecommuting: Employers' perspectives and perspectives of service members and veterans with disabilities. *e-Networks in an Increasingly Volatile World*, page 204, 2006.

[35] D Richard Kuhn, Miles C Tracy, and Sheila E Frankel. Security for telecommuting and broadband communications. *NIST Special Publication*, 800:46, 2002.

[36] Micah Lee. Encrypting your laptop like you mean it. https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/, 2021. Accessed: 2021-02-1.

[37] Dan Lohrmann. 2020: The year the covid-19 crisis brought a cyber pandemic. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html, 2020. Accessed: 2021-01-18.

[38] Julie M McCarthy, John P Trougakos, and Bonnie Hayden Cheng. Are anxious workers less productive workers? it depends on the quality of social exchange. *Journal of Applied Psychology*, 101(2):279, 2016.

[39] Google Meet. Change your background in google meet. https://support.google.com/meet/answer/10058482?co=GENIE.Platform%3DDesktop&hl=en&oco=1#zippy=%2Cwhy-dont-i-have-the-change-background-option, 2021. Accessed: 2021-02-19.

[40] Ezequiel Minaya. 4,000% increase in ransomware emails during covid-19. https://www.nationalobserver.com/2020/04/14/news/4000-increase-ransomware-emails-during-covid-19?utm_source=National+Observer&utm_campaign=71c5787b54-EMAIL_CAMPAIGN_2020_04_14_12_21&utm_medium=email&utm_term=0_cacd0f141f-71c5787b54-276991505, 2020. Accessed: 2020-09-11.

[41] Ezequiel Minaya. Cfos plan to permanently shift significant numbers of employees to work remotely — survey. https://www.forbes.com/sites/ezequielminaya/2020/04/03/cfos-plan-to-permanently-shift-significant-numbers-of-employees-to-work-remotely---survey/#11bc806575b2, 2020. Accessed: 2020-09-11.

[42] Nextiva. Protect your number with call masking. https://www.nextiva.com/features/voip/call-masking.html, 2021. Accessed: 2021-02-24.

[43] Marian Niedźwiedziński and Anna Bąkała. Telework and security. *Systems: journal of transdisciplinary systems science*, 12(1), 2007.

[44] Insurance Bureau of Canada. Cyber risks: An increased threat during covid-19. http://www.ibc.ca/on/business/risk-management/cyber-risk/an-increased-threat-during-covid-19, 2020. Accessed: 2021-01-18.

[45] U.S. Bureau of Labour Statistics. Economic news release. https://www.bls.gov/news.release/flex2.htm, 2020. Accessed: 2020-09-11.

[46] Kenneth Okereafor and Phil Manny. Solving cybersecurity challenges of telecommuting and video conferencing applications in the covid-19 pandemic. *Journal Homepage: http://ijmr. net. in*, 8(6), 2020.

[47] OpenPGP. Openpgp about. https://www.openpgp.org, 2021. Accessed: 2021-02-1.

[48] International Labour Organisation. The gender gap in employment: What's holding women back? https://www.ilo.org/infostories/en-GB/Stories/Employment/barriers-women#intro, 2018. Accessed: 2020-09-11.

[49] Leysia Palen and Paul Dourish. Unpacking" privacy" for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 129–136, 2003.

[50] I Plaisier, ATF Beekman, R De Graaf, JH Smit, R Van Dyck, and BWJH Penninx. Work functioning in persons with depressive and anxiety disorders: the role of specific psychopathological characteristics. *Journal of affective disorders*, 125(1-3):198–206, 2010.

[51] Choudhury Prithwiraj, Cirrus Foroughi, and Barbara Larson. Work-from-anywhere: The productivity effects of geographic flexibility. *Strategic Management Journal*, 42(4):655–683, 2021.

[52] Pasi Pyöriä. Knowledge work in distributed environments: issues and illusions. *New Technology, Work and Employment*, 18(3):166–180, 2003.

[53] Pasi Pyöriä. Managing telework: risks, fears and rules. *Management Research Review*, 2011.

[54] André Queirós, Daniel Faria, and Fernando Almeida. Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies*, 2017.

[55] Miguel Quiroga. Visible's shift to a permanent work from home model. https://www.linkedin.com/pulse/visibles-shift-permanent-work-from-home-model-miguel-quiroga/?trackingId=28Ku%2F%2Ft4b5g4PVyiJ9PBsA%3D%3D, 2020. Accessed: 2021-01-18.

[56] Yasmeen Rashidi, Kami Vaniea, and L Jean Camp. Understanding saudis' privacy concerns when using whatsapp. In *Proceedings of the Workshop on Usable Security (USEC'16)*, pages 1–8, 2016.

[57] Reddit. Black screen or entire screen flickering. https://www.reddit.com/r/Zoom/comments/fyi2ip/black_screen_or_entire_screen_flickering/, 2020. Accessed: 2020-09-17.

[58] Brie Weiler Reynolds. Differences between teleworking and telecommuting. https://www.flexjobs.com/blog/post/telecommuting-or-telework-whats-the-difference/, 2020. Accessed: 2020-09-17.

[59] Ron Ross, Michael McEvilley, and Janet Oren. Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems. Technical report, National Institute of Standards and Technology, 2016.

[60] Katrin Schmelz and Anthony Ziegelmeyer. Reactions to (the absence of) control and workplace arrangements: experimental evidence from the internet and the laboratory. *Experimental economics*, pages 1–28, 2020.

[61] Jack Schofield. How can I protect my data if my laptop is stolen. https://www.theguardian.com/technology/2016/jul/07/how-can-i-protect-my-data-if-my-laptop-is-stolen, 2016. Accessed: 2021-02-1.

[62] USA Social Security. Retirement benefits. https://www.ssa.gov/benefits/retirement/planner/agereduction.html, 2020. Accessed: 2020-09-11.

[63] Hashim Shaikh. The importance of physical security in the workplace. https://resources.infosecinstitute.com/topic/importance-physical-security-workplace/, 2018. Accessed: 2021-02-1.

[64] R. Shirey. Rfc 4949-internet security glossary, version 2. https://tools.ietf.org/html/rfc4949, 2007. Accessed: 2021-02-24.

[65] Skype. How do i customize my background for skype video calls? https://support.skype.com/en/faq/fa34896/how-do-i-customize-my-background-for-skype-video-calls, 2021. Accessed: 2021-02-19.

[66] Diomidis Spinellis, Spyros Kokolakis, and Stefanos Gritzalis. Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management & Computer Security*, 1999.

[67] Alice Sturgeon. Telework: threats, risks and solutions. *Information Management & Computer Security*, 1996.

[68] Microsoft Teams. Change your background for a teams meeting. https://support.microsoft.com/en-us/office/change-your-background-for-a-teams-meeting-f77a2381-443a-499d-825e-509a140f4780, 2021. Accessed: 2021-02-19.

[69] Microsoft Teams. How to live stream microsoft teams meeting to youtube, facebook live & others. https://www.youtube.com/watch?v=fGMYvHrIB6M, 2021. Accessed: 2021-02-1.

[70] Microsoft Teams. User presence in teams. https://docs.microsoft.com/en-us/microsoftteams/presence-admins, 2021. Accessed: 2021-02-1.

[71] Zeynep Tufekci. Can you see me now? audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1):20–36, 2008.

[72] Paul C van Oorschot. *Computer Security and the Internet*. Springer, 2020.

[73] VeraCrypt. Veracrypt about. https://www.veracrypt.fr/en/Home.html, 2021. Accessed: 2021-02-1.

[74] Jessica Vitak, Cliff Lampe, Rebecca Gray, and Nicole B Ellison. "why won't you be my facebook friend?" strategies for managing context collapse in the workplace. In *Proceedings of the 2012 iConference*, pages 555–557, 2012.

[75] Natalie Whaley. Surveillance in employment: The case of teleworking. *Technical Communication*, 47(2):260–260, 2000.

[76] Alma Whitten and J Doug Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX Security Symposium*, volume 348, pages 169–184, 1999.

[77] WHO. Who reports fivefold increase in cyber attacks, urges vigilance. https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance, 2020. Accessed: 2020-09-11.

[78] May Wong. Stanford research provides a snapshot of a new working-from-home economy. https://news.stanford.edu/2020/06/29/snapshot-new-working-home-economy/, 2020. Accessed: 2020-09-11.

[79] Ka-Ping Yee. User interaction design for secure systems. In *International Conference on Information and Communications Security*, pages 278–290. Springer, 2002.

[80] Zoom. Virtual background. https://support.zoom.us/hc/en-us/articles/210707503-Virtual-background, 2020. Accessed: 2020-09-17.

[81] Zoom. Live streaming meetings or webinars using a custom service. https://support.zoom.us/hc/en-us/articles/115001777826-Live-Streaming-Meetings-or-Webinars-Using-a-Custom-Service, 2021. Accessed: 2021-02-1.

Appendices

A Participants' Demographics

ID	Age	Gender	Educational level	Place of work	Position at work	Number of employees	Location
P1	24	F	Bachelor's	University	Digital communications specialist	-	Montreal, Quebec
P2	32	F	Master's	Library	Manager of marketing and communications	-	Montreal, Quebec
P3	31	F	Master's	University	Research assistant	14	Kitchener, Ontario
P4	36	F	Master's	Community organization	Occupational therapist	2,000+	Mount Pearl, Newfoundland
P5	49	F	Master's	IT firm	Sales director	10,000+	Caledonia, Ontario
P6	51	M	Bachelor's	Provincial government	Senior staff	-	Halifax, Nova Scotia
P7	47	M	High school	High school	Network engineer	11,000	Mono, Ontario
P8	61	M	Bachelor's	Children's science museum	Accounting supervisor	101	Vancouver, British Columbia
P9	24	F	Bachelor's	Federal tax agency	Call center agent	40,000	Ottawa, Ontario
P10	38	M	Bachelor's	Realtor	Mortgage broker	11,000	Mono, Ontario
P11	52	M	Bachelor's	Community center	Health director	85	Port Hardy, British Columbia
P12	31	M	College	Telecommunications	Account manager	-	-
P13	25	F	Bachelor's	Car sharing service	Business operations manager	22,000	Vancouver, British Columbia
P14	64	M	Bachelor's	Cannabis producer	Call center representative	37,000+	New Maryland Parish, New Brunswick
P15	31	M	Bachelor's	Telecommunications company	Customer service rep	37,000+	New Maryland Parish, New Brunswick
P16	47	M	Master's	Public transport services	Director in the planning department	4,000	Toronto, Ontario
P17	38	F	Master's	Elementary school	Education assistant	-	Dawson Creek, British Columbia
P18	38	M	College	Arts and culture management organization	Executive director	3	Vancouver, British Columbia
P19	43	M	Bachelor's	University	Business support analyst	10,000+	Vancouver, British Columbia
P20	30	M	Bachelor's	College	Assistant registrar systems and reporting	-	-
P21	53	M	Master's	Securities commission	Senior project manager	-	-
P22	48	M	College	Telecommunications provider	Customer service call agent	-	-
P23	59	F	College	High school	School secretary	-	-
P24	24	F	College	High school	School teacher	35	Halifax, Nova Scotia

Table A.1: **Demographics of participants.**

B Summarized Recommendations to Organizations (R-O), Employees (R-E), and Those Working with Telecommuters (R-T)

Table B.1: Summarized recommendations.

Recommendations	R-O, R-E, R-T
1. Organizations could make use of already existing solutions to digitally sign and encrypt official emails from the organizations	R-O
2. Apart from email, we suggest that other communication platforms could be used, such as a usable official messaging platform to relate work information	R-O
3. Organizations need to be sensitive to the fact that employees live in various living conditions and mindful of the corresponding outcomes of threats to the confidentiality of work calls	R-O
4. Employers can put measures in place to manage the safety of the telecommuters and their households	R-O
5. Organizations can provide some form of phone number masking (which prevents others from knowing the actual phone number of the caller) or VoIP solutions to employees who have to use their personal phones for work	R-O
6. To help create a balance between privacy and doing one's job, organizations can have discussions and transparency on how much privacy employees are entitled to when telecommuting	R-O
7. Employers need to ensure that work communication platforms are very intuitive and easy, if they want to address this issue	R-O
8. Technology support for alerting participants of video calls when screenshots are taken, to help employees maintain awareness of their privacy violations and to deter abuse of such capabilities by others	R-E
9. To prevent clients and colleagues from hearing personal conversations happening in the household, teleconferencing software and phones could automatically mute the microphone when employees are not talking; using voice recognition, the microphone automatically unmutes when the employee starts talking	R-T
10. There could also be directional microphones on phones and videoconferencing apps, whereby the technology only picks up the voice of the person in front of the computer or phone	R-T

C Saturation Graph

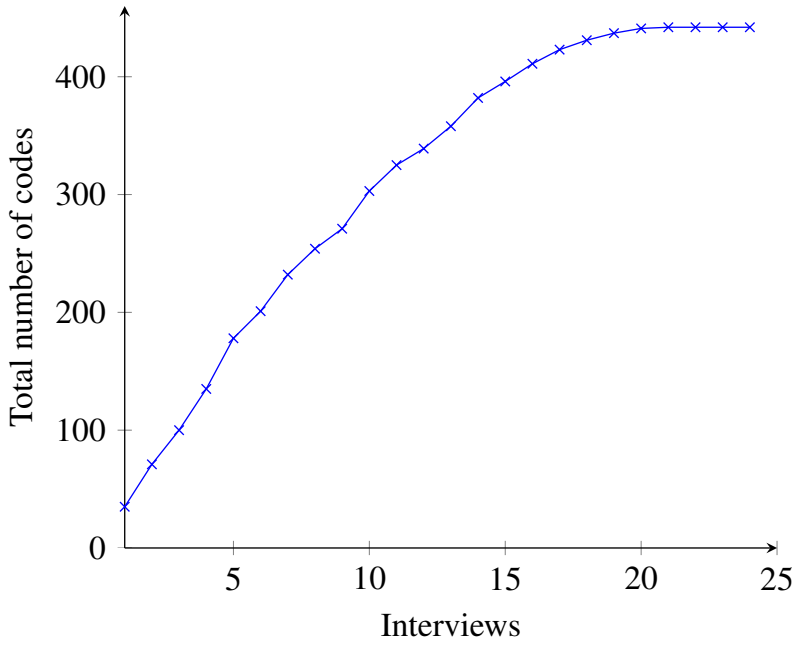

Figure C.1: Total number of codes after each interview.

D Interview Guide

Demographic questions

1. Age
2. Gender
3. Educational level
4. Place of work
5. Position at work

Interview questions

1. How has the pandemic affected your life?
2. How has it changed your life?
3. How has it changed your life in relation to others living with you?
4. Describe your typical work day before the pandemic
5. How many hours do you work?
6. Did you work remotely from home before the pandemic? If yes, how frequently?
7. How long have you been working from home?
8. If yes to the above question, how does your current remote work differ from previous experiences?

9. What is your experience working from home?
10. Describe your day-to-day work activities from home?
11. How does your current work activities differ from working in your physical office space?
12. What technology (or software, machines, devices) did you use to work with in the physical office space?
13. How do you handle/work with confidential communications in your work environment?
14. How do you manage confidential documents in your work environment?
15. What, if anything, is your workplace's guide on handling confidential communications and documents from home?
16. What, if anything, are the measures taken to comply with the organization's work-at-home rules?
17. What makes it easy to comply with these rules?
18. What makes it difficult to comply with these rules?
19. What motivates you, if anything, to be secured when you work from home?
20. What are your concerns, if any, with working from home as opposed to working in the office?
21. List the new technologies or software used specifically to work from home
22. What software or technologies have you explored since working from home?
23. If not mentioned ask, what video conferencing softwares have you been using to work from home?
24. If not mentioned ask, do you use VPNs to access your organization's resources?

For each technology used for remote working, ask:

25. Why did you choose this technology?
26. What if anything makes it easy to use the software? Why?
27. What if anything makes it difficult/complex to use the software?
28. If any complexity is discussed: How do you mitigate the complexities of using these technologies?
29. How does the technology assist you in securing your organization's confidential documents and communications?
30. How does the technology assist you in complying with your company's guide on protecting confidential documents and communications?
31. If you could change how the technology currently works, what would you change and why?
32. How do you handle concerns related to people in the household?
33. How is your current work environment?
34. What, if anything, would you like to change about your current work environment?
35. What other information do you think will be useful for this research?