Security and Privacy Perspectives on Using ChatGPT at the Workplace: An Interview Study

Angelika Kimbel[0009−0007−1111−6091], Magdalena Glas*[0000−0003−0239−7526], and Günther Pernul[0000−0003−1338−9003]

University of Regensburg, Universätsstr. 31, 93053 Regensburg
{firstname.lastname}@ur.de

Abstract. The emergence of the artificial intelligence (AI) tool ChatGPT has created great excitement and unprecedented potential in various fields. Users are increasingly recognizing its benefits in aiding with work-related tasks and are incorporating it into their work routines. However, unconscious use of ChatGPT poses a risk to an organization if employees inadvertently disclose sensitive information. To date, there is a lack of research examining individuals' perceptions of the security and privacy implications of ChatGPT use in organizational contexts. To bridge this gap, this study examines employees' perceptions of security and privacy-related risks of using ChatGPT for work-related tasks and their strategies to mitigate these risks. Employing grounded theory, we conducted semi-structured interviews with 17 participants from 15 organizations across a range of professions and industries. Our findings indicate that employees have a general awareness of security and privacy-related risks, albeit with some uncertainties and misconceptions. While organizational guidelines for managing these risks are largely absent, participants describe that they employ self-determined strategies to avoid sharing sensitive data.

Keywords: ChatGPT · LLM · Generative AI · Chat Bot · Security · Privacy · Workplace · Employee Behavior

1 Introduction

Since its release in late 2022, ChatGPT[1], an AI-based chatbot developed by OpenAI[2], has rapidly gained popularity, reaching 100 million weekly users in November 2023 [11]. Based on a Large Language Model (LLM), ChatGPT is capable of interacting with users in natural language and offers various applications, such as text and code generation, modification processes, and text summaries. ChatGPT falls under the category of generative AI tools and currently stands as the most widely utilized tool within this category [18]. Individuals not only use ChatGPT for private tasks, but also to help them accomplish job-related tasks

* Corresponding author
[1] https://chat.openai.com/
[2] https://openai.com/

more efficiently. Prior works already investigated the potential of the chatbot for work environments in various domains such as finance [16], healthcare [8,6], and IT [23,9], highlighting its utility in streamlining tasks and facilitating workflows. Despite its advantages, using ChatGPT carries inherent security and privacy risks [27]. When users prompt potentially confidential data into ChatGPT, this data is stored and processed to enhance the underlying AI model, which carries the risk of data being inadvertently disclosed to unauthorized parties. This is particularly concerning in a professional context, as it might jeopardize the confidentiality of organizational data, such as sensitive customer data. As a recent example, Samsung blocked their employees' access to ChatGPT after it became evident that employees prompted internal source code and confidential meeting notes into ChatGPT [21]. Individuals who use ChatGPT to support their work tasks are not necessarily aware of those risks. While previous studies investigated individuals' perceived benefits and challenges when using ChatGPT at their schools or workplaces [20], those studies did not examine individuals' security and privacy perceptions as part of their usage behavior. To this end, this study raises the following question:

RQ. How do individuals perceive and handle security and privacy-related risks when using ChatGPT at work?

Contribution. To address our research question, we conducted semi-structured interviews with 17 participants who use ChatGPT to assist them with work-related tasks. The participants come from 15 organizations of different sizes and industry sectors in Germany. In our interviews, we investigated the participants' awareness and concerns regarding security and privacy-related risks when using ChatGPT.

The rest of this work is structured as follows. Section 2 provides background on the GPT model and associated security and privacy challenges, before giving an overview of related work in Section 3. In Section 4, we outline the method of our study. In Sections 5 and 6, respectively, we present our research findings and discuss their practical implications before concluding our work in Section 7.

2 Background

In the following, we provide an overview of ChatGPT's functionality and discuss potential security and privacy issues that arise when using ChatGPT in professional environments.

2.1 Generative Pre-Trained Transformer (GPT) Models and ChatGPT

ChatGPT, in its current version, builds upon the generative pre-trained transformer (GPT) models GPT-3.5 and GPT-4 developed by OpenAI. GPTs represent a subtype of LLMs, artificial neural networks that are used for natural

language processing (NLP) [28]. GPTs use large sets of unlabeled data for self-supervised pre-training to create human-like content by predicting the next word in a textual context. These predictions are refined through a transformer architecture that weighs the importance of different words in a sentence to more efficiently consider the context of the prediction [26]. To improve the models' performance for conversational usage in ChatGPT, e.g., to ensure compliance with OpenAI's ethical standards, GPTs are fine-tuned using a combination of supervised learning and reinforcement learning techniques, which leverage human feedback [13]. With ChatGPT, OpenAI made its models GPT-3.5 and, later, GPT-4 available to the public. Due to its context-aware use of natural language, users can employ ChatGPT for a plethora of applications that can help them simplify work-related tasks. To name just a few possible applications, ChatGPT can be utilized to retrieve information, discuss a topic, generate and summarize text, and create, optimize, and debug source code. For a comprehensive overview of application domains, we want to refer to the work of Ray [17].

2.2 Security and Privacy Challenges of ChatGPT

Despite the indisputable advantages that ChatGPT offers users in completing work-related tasks, using ChatGPT comes with certain risks regarding security and privacy that users are not necessarily aware of. Besides personal data such as names, mail addresses, or billing information associated with a user's account, ChatGPT also stores user conversations [15]. OpenAI retains the authority to internally process conversation data, e.g., to review user prompts for compliance violations. Furthermore, conversation data is used by OpenAI to further train their GPT models, making user inputs part of their training base. Data that users input into ChatGPT to complete a work task might contain confidential data that should not be accessed by an unauthorized party. However, the way OpenAI processes the user data makes the user input in conversations available to OpenAI and, thus, violates the confidentiality of this data. Cases of data disclosure by employees have been reported not only at Samsung [21], but also at several Australian hospitals [24], where staff prompted patient data into ChatGPT to write medical reports without the patients' consent.

In addition to the risks associated with OpenAI's deliberate processing of user data, the confidentiality of processed data can also be harmed by technical errors or deliberate attacks of malicious parties [10]. In 2023, a security incident became public, revealing a vulnerability in an open-source library used by OpenAI. This vulnerability resulted in the disclosure of users' chat titles, names, and banking details to other active users [14]. Moreover, the user data stored and processed by OpenAI is susceptible to malicious attacks that aim to extract information. This can happen, e.g., over applications, which apparently offer convenient ways to access ChatGPT, however, with the malicious intent to intercept the traffic between a user and ChatGPT [1]. As another example, Nasr et al. [12] demonstrate how specific input prompts could compel ChatGPT to output parts of training data sets that contained confidential user data.

3 Related Work

Prior works have investigated how individuals use ChatGPT to improve tasks at their workplace. Skuvje [22] conducted an online survey asking ChatGPT users about their experience with using ChatGPT in their daily lives, including tasks at their workplace. Chu [4] analyzed the influencing factors of ChatGPT's quality aspects on user satisfaction, utility, and organizational performance through an online survey of employees within different industries. Temsah et al. [25] focused on the healthcare sector and conducted a survey among medical workers regarding their attitudes and willingness to use it in healthcare. The studies explore the opportunities and implications of ChatGPT in professional settings. They also examine the potential barriers users perceive, such as ChatGPT sometimes providing inaccurate or incorrect information. However, concerns about security and privacy as obstacles to adopting ChatGPT for work-related tasks are only discussed in passing. Three prior studies have explicitly examined users' perceptions regarding the security and privacy risks of using ChatGPT. Sebastian [19] and Alawida et al. [2] conducted online surveys in which participants were asked to indicate which security issues respectively attack scenarios they perceived as a risk when using ChatGPT. Thus, the studies provides information on which of the given scenarios users consider to be particularly relevant. However, the authors did not capture user perceptions of risks beyond those specified scenarios. Choudhury and Shamszare [3] conducted an online survey to investigate the impact of users' trust in ChatGPT on their intent and actual use of the chatbot. The study shows that trust has a significant effect both on the intentional and actual use of ChatGPT. Perceived security and privacy were specified as one aspect of user trust, assessed by two items within the seven-item questionnaire.

While these studies provide initial insights into the security and privacy perceptions of ChatGPT users in general, they do not examine the specific risks associated with storing and processing potentially confidential information in professional settings. This study aims to bridge this gap by conducting interviews with individuals who utilize ChatGPT for work-related tasks. The objective is to explore users' awareness of security and privacy risks associated with ChatGPT in a professional context and examine their strategies to cope with these risks.

4 Method

This study employed a qualitative research design, conducting semi-structured interviews with participants who use ChatGPT in a professional context. In this section, we outline the method we employed for conducting these interview, following the grounded theory method by Corbin and Strauss [5]. This approach was chosen due to its suitability for establishing new theories based on qualitative data on topics that lack existing theories, as is the case for our topic. The application of this exploratory method allows for a thorough analysis of participants' subjective perceptions and experiences without specifying predefined options to choose from that influence or limit the participants in their statements.

4.1 Interview Guide

We structured the interview around three main topics:

1. **Guidelines:** Within this topic, we inquired participants about any existing organizational policies or guidelines governing the use of AI technologies within their respective organizations.
2. **Awareness:** In this topic, we aimed to explore participants' awareness of security and privacy-related risks associated with using ChatGPT in a work context and the privacy settings that ChatGPT provides.
3. **Security and privacy-related behavior:** During the final part of the interview, we engaged participants in discussions about their strategies for addressing perceived security and privacy risks when using ChatGPT for work-related tasks.

To identify possible obstacles in understanding the topics, a pilot study was conducted with two participants prior to the data collection of the main study. The results of the pilot study were solely used to refine the interview guide and are not presented as part of the study results.

4.2 Recruiting and Data Collection

We recruited 17 participants from 15 organizations across different industry sectors in Germany. The organizations' sizes ranged from three very small (1-9 employees), three small (10-99 e.), eight medium (100-999 e.), one large (1000-5000 e.), to two very large (>5000 e.). Participants were recruited over the authors' personal networks and social media. They voluntarily signed up for the interview study out of personal interest and did not receive any compensation for their participation. The main criterion for the selection of participants was the usage of ChatGPT as part of their job routines. This was clearly communicated to potential participants, emphasizing that using ChatGPT for private purposes alone was not sufficient to be selected for the study. We explicitly also included participants who indicated to use ChatGPT only infrequent, i.e., less than once a week. This approach allowed for an exploration of the reasons for occasional use and possible associations with security and privacy perceptions. The interviews were conducted between September and November 2023 by the first author and held either virtually over a video conferencing tool or in person. With the participants' consent, the interviews were recorded for transcription. The interviews lasted, on average, 15:38 minutes (SD = 4:49). Regarding background variables, 35% (6) of participants identified as female, the remaining as male. Participants ranged in age from 22 to 43 years ($M = 27.3, SD = 4.3$). An overview of participants' occupations, industry sectors, and size of organizations, as well as the frequency of ChatGPT usage, is presented in Table 1. Until the time of the interviews, all participants but one were using the GPT3 model over the free version of ChatGPT, U17 was using GPT4 over ChatGPT Plus.

Table 1: Participant Overview

ID	Job Title	Industry Sector	Org. Size	Usage
U1	Configuration Manager	Technology	medium	infr.
U2	Business Dev. Manager	Professional services	very large	daily
U3	Marketing Specialist	Finance	medium	infr.
U4	Research Assistant	Research and education	medium	weekly
U5	Occup. Safety Specialist	Automotive	medium	weekly
U6	Head of Digital Marketing	Consumer goods	small	weekly
U7	Application Developer	Technology	medium	weekly
U8	Software Developer	Automotive	large	daily
U9	Digital Project Manager	Consumer goods	very large	daily
U10	Management Assistant	Automotive	medium	infr.
U11	Engineer	Manufacturing	very small	daily
U12	Engineer	Automotive	medium	infr.
U13	Consultant	Professional services	medium	weekly
U14	CEO	Professional services	very small	daily
U15	Elementary Teacher	Research and education	small	daily
U16	Software Developer	Automotive	small	weekly
U17	CEO	Technology	very small	daily

Note. **Organization sizes:** very small: 1-9 employees, small: 10-99 emp., medium: 100-999 emp., large: 1000-4999 emp., very large: >5000 emp.; **Usage:** Infr. (infrequent): less than once a week

4.3 Data Analysis

The raw interview data included 265 minutes of audio material that was transcribed to 36955 words. MAXQDA[3] was used for data analysis. Following the steps suggested by Corbin and Strauss [5], we first used open coding before applying axial coding, including the use of graphical representations. Selective coding was then used to create codes. Throughout the process, constant comparisons were made between existing codes, and ongoing thoughts and reflections were documented in memos. After the first round of coding was performed by the first author, the second author conducted a subsequent analysis of the codes and categories to check their validity and iteratively refine the codes. In a joint discussion, existing codes were combined for better presentation. The final codebook consists of 32 codes categorized into ChatGPT applications and the three main interview topics. The final codebook is made available on GitHub[4].

4.4 Limitations

The findings of this study must be considered in light of certain limitations, which we acknowledge in this section. First, our study explicitly focuses on individuals who actively use ChatGPT as part of their work routines. To this end,

[3] https://www.maxqda.com/
[4] https://github.com/ChatGPTInterviewStudy

the security and privacy perceptions of those individuals who do not use ChatGPT, whether due to personal choice or because its usage is restricted within their organization, are not considered. Investigating perspectives from non-users will be subject to future research. Secondly, it's important to note that this study only includes participants from Germany, possibly limiting the generalizability of our findings to other geographical regions. However, the study participants cover a wide array of positions and industry sectors. As a result, we believe our study's findings still offer valuable perspectives and behavioral strategies despite the regional focus. Lastly, the nature of qualitative interviews introduces the possibility of response bias. Participants may be influenced by social desirability, leading them to tailor their responses to fit perceived expectations rather than accurately reflecting their real behavior [7]. For instance, individuals may report privacy-related behaviors during interviews due to social norms, even if their actual behaviors differ. Awareness of this potential bias is essential when interpreting the findings of this study.

5 Findings

In the following section, we describe the findings of the 17 conducted interviews in relation to the three interview topics introduced in Section 4.1. An overview of our findings is presented in Table 3.

To understand the context of privacy awareness and its impact on ChatGPT, we initially discussed with the participants what type of work-related tasks they use ChatGPT for. We identified six codes of applications in which the participants used ChatGPT for work-related tasks. Notably, the majority of participants reported using ChatGPT for more than one application (rf. Table 2). The two most frequently mentioned applications were content generation and information retrieval. Content generation refers to use cases in which users use ChatGPT to generate a document based on semi-structured input, e.g., for generating emails (U9, U17), articles for external communication (U3, U13, U17), meeting agendas (U2) or student reports (U15).

Table 2: ChatGPT Applications: A majority of participants employ ChatGPT across diverse applications.

Code	**Participants**	$\sum$
Content generation	U2 - U7, U9 - U13, U15, U16	13
Information retrieval	U1, U4 - U6, U9, U11 - U14, U16	10
Programming	U1, U4, U7 - U9, U11, U16	7
Brainstorming	U9, U10, U15	3
Language processing	U11, U14, U17	3
Data Analysis	U17	1

Information retrieval encompasses use cases in which users seek to get information about a certain subject, e.g., about which legal and regulatory requirements apply to the participant's organization (U5, U14). Seven participants mentioned using ChatGPT for programming or further code-related tasks, such as creating source code based on natural language specifications (U1, U4, U7-U9, U16), debugging (U8), or creating software documentation (U11). Four participants described using ChatGPT to discuss ideas and seek inspiration for creative tasks, which we summarized under the codes brainstorming. Further applications mentioned were using ChatGPT for refining and modifying existing texts (language processing), e.g., for summarizations (U17), grammar checks (U11) or translations (U14), and using ChatGPT for data analysis (U17) on uploaded datasets with ChatGPT Plus.

5.1 Guidelines

Only two (U9, U17) participants reported on guidelines regarding the usage of ChatGPT in their organizations. U9 mentioned that in their (very large) organization, employees are provided with a catalog detailing ChatGPT usage recommendations, including handling sensitive information and formulating prompts. Conversely, U17, CEO of a small company, indicated the absence of explicit policies, with only informal guidelines due to the small number of employees in the company. U4 and U15, both teachers, reported receiving information about how ChatGPT can be integrated with teaching, however, with no information about possible security and privacy risks. The majority of participants stated the absence of organizational guidelines, which they partly attributed to ChatGPT's novelty.

5.2 Awareness and Perceived Concerns

Within the second topic, participants not only explained what they explicitly knew about security and privacy risks regarding ChatGPT but also expressed their personal and subjective apprehensions or worries that participants have regarding the security and privacy of their data when using ChatGPT. To this end, this topic was refined to *Awareness and Perceived Concerns* to describe both the participant' explicit awareness and their subjective concerns.

Processing of Data. Regarding the processing of data, most participants were aware that their data was used to improve the GPT model. In this regard, some participants explicitly mentioned the "thumbs up - thumbs down" function for giving feedback to output prompts as a clear indicator of data processing. However, the statements on how the data may be specifically processed remained very vague overall. Apart from using customer data to improve the GPT model, participants made only indefinite assumptions about how their data is (or might be) used. Only two participants (U1, U14) mentioned the potential of access to deanonymized data, suggesting that OpenAI staff can access and review the data. Participant U14 expresses his concerns by stating: *"Because you know it is stored*

Table 3: Summary of the interviews' key findings per topic.

Topic	Key Findings
Guidelines	• Majority of participants' organizations lack guidelines on security and data protection recommendations for using ChatGPT
Awareness/Concerns	• Participants are generally aware of data processing of ChatGPT chat and user data for model improvement • Assumptions vary about OpenAI server locations and GDPR compliance • Awareness about privacy settings is limited • Some participants express concern about data leakage, also with regard to the potential sale of their data for advertising or other purposes
Security/Privacy-related behavior	• Participants show consensus on avoiding sensitive data input, identifying various types of sensitive data • Participants either restrict their use to non-sensitive applications or anonymize input prompts, despite challenges like occasional lapses in removing sensitive information

[...] and if it is stored, you can imagine there's a guy sitting behind it reading all your conversations." Four participants (U7, U10, U11, U15) presumed that OpenAI might monetize data, e.g., for user profiling and targeted advertising: *"[...] I can imagine there's also a monetization opportunity for the company if they also learn more about users, like now in Instagram, for example, that you create profiles [...]. So, I think that's the case. From that perspective, that's another point for me, not to enter too personal data, [...]."* (U15).

Some participants (U6, U8, U11) perceived the processing for improving the GPT models as explicitly positive as they would benefit from improvements: *"[...] I think it's very good if it gets better, because I want to use it. And I get something out of it, so why not give them something in return?"* (U11). Two participants (U4, U11) additionally noted that their indifference to the use and storage of their data stems from the fact that other platforms are already collecting data: *"So I'm already aware that there's some processing going on. But I don't care. Google also knows all my interests based on my search history. So, I don't care if ChatGPT knows that I'm interested in science or programming or learning. I don't care."* (U4). A majority of participants, however, raised concerns about the processing of data. Some explicitly expressed concerns about potential information leaks to unauthorized individuals. U1 addressed queries from other users in this context, highlighting the potential seriousness of such incidents in corporate settings: *"In the corporate world, sharing sensitive data with the public can be a serious problem. If other users submit queries to ChatGPT and it processes them accordingly, then the problem is very serious and should be avoided."*

Storage of Data. Our participants held varying assumptions regarding OpenAI's data storage practices. Some speculated that servers were located in the EU, while others believed they resided in the United States (US). Among those who assumed EU servers, one participant (U1) expected that data would need to be stored anonymously to comply with the General Data Protection Regulation (GDPR). Conversely, those assuming US servers perceived the GDPR might be circumvented due to data storage location. However, U11 linked this circumvention to perceived benefits, stating: *"With laws and policies held there [US] that are arguably incompatible with the GDPR, but you can waive it if you want to take advantage of it."* Regarding the types of data stored, some participants were aware that personal data and all conversation data were stored, while others assumed that only "relevant data" was retained. Finally, three participants (U1, U6, U14) emphasized the opacity surrounding ChatGPT, expressing uncertainty about the storage mechanisms. *"What is anonymous data? To what extent is it anonymous? What can really be allocated? What statistics are extracted from ChatGPT? This is why I'm very careful and ask myself, 'What information do I want to put in ChatGPT?'"* (U1).

Privacy Settings. Regarding the participants' privacy settings, only three (U12, U13, U17) participants were aware of the option to limit the storage of their data and prevent its use for system improvement. However, none of these participants claimed to use it. Instead, they mentioned that locating this setting was challenging or that although they were aware of its existence, they had not explored it thoroughly. Among the other 14 participants, this setting was initially unfamiliar. Upon being informed about it, they expressed different reactions. Only two participants (U3, U10) showed interest in the possibility of adjusting the privacy-enhancing setting. The rest of the participants showed no inclination to activate this setting for enhanced privacy. Some reasoned that they preferred to retain their chat history, while others expressed skepticism about the effectiveness of the setting. As articulated by one participant (U6): *"Whether that's really the case in the end [...] when I say don't do it [the processing], whether they really stop, I don't know. I think there are many cases [...] where it happens anyway, so it's not as I turn it off and then I say, now I have the 100% feeling that it's not happening. I don't trust it anyway, I just leave it on."*

5.3 Security and Privacy-related Behavior

Finally, we present our findings on how the participants' describe to handle security and privacy-related risks when using ChatGPT in the context of their respective organization. All participants agreed on the importance of avoiding inputting potentially sensitive data into ChatGPT. They primarily associated sensitivity with personal data, including information about internal employees and customers. Moreover, participants noted different types of sensitive data related to their respective organizations, such as cost statistics (U5), as well as internal source code (U8, U16, U11), particularly when containing access

credentials. In addition, two participants indicated that they avoid prompting the names of their organizations (U13, U17) in interactions with ChatGPT. Our observations revealed two distinct strategies employed by the participants to ensure the security and privacy of data they perceived as sensitive: Firstly, some participants opt to use only non-sensitive applications, while others describe anonymizing input prompts as an additional measure.

Restricting to non-sensitive applications. Seven participants explained not to employ any specific security and privacy-preserving strategies for using ChatGPT as they only use it for applications that do not involve any potentially sensitive data, e.g., when using ChatGPT for creating documents that will be published as part of the organization's external communication. Thereby, some of the participants explained they would use ChatGPT in the same way they use search engines for information retrieval: *"So I haven't really had that case yet. Personally, I wouldn't know when I would have to enter such data, I mean, comparing it to Google. Let's just say that I've never had a situation where I've had to give out personal information when I was doing a normal search. So I'm not really worried about it."* (U12).

Anonymization of input prompts. The second group of participants uses ChatGPT for a broader range of applications, e.g., generating emails, that involve the processing of potentially sensitive data (like the names of email recipients and business data as the content of such emails). To ensure confidentiality in those cases, participants reported adopting an additional step to anonymize or replace potentially sensitive data before inputting it into ChatGPT. They describe this process as initially considering what information to share, mindful of potential implications of data leakage, and then constructing their inputs accordingly. This approach allows them to use ChatGPT across a broad spectrum of applications while ensuring security and privacy. One participant (U1) elaborated: *"In order not to give ChatGPT any internal information or anything like that, I write the entire inputs with dummy text, dummy variables..., and then just replace the variables and the dummy text."*. U7 admits that despite her awareness of not sharing sensitive data, she occasionally forgets to remove sensitive information, such as customer names, from prompts. Overall, participants input information into ChatGPT based on their own convictions while being aware of the potential risk of data leakage and employ various strategies to mitigate this risk while leveraging the benefits. However, as noted by U2, perceptions of risk may change with long-term use: *"It's only when you've been using it for a long time that a problem like this comes up, and then you stop thinking about it. In the beginning you always think, what can it do? But at some point you say, you use it every day anyway, it doesn't matter. I think the problem is yet to come."*

6 Practical Implications

At the time of our study, ChatGPT had been available for nearly a year, bringing generative AI technology to a broad public. Our study aimed to qualitatively investigate how individuals and their organizations address the security and

data challenges posed by integrating this tool in their work routines. In the subsequent section, we analyze the insights gleaned from our study findings and, on this basis, provide practical recommendations for organizations.

Participants described how they have already integrated ChatGPT, to varying degrees, into their work routines. In line with the results by Alawida et al. [2] and Temsah et al. [25], we found that the ChatGPT users we interviewed are generally aware that chat data is stored and processed. However, there are uncertainties and sometimes erroneous assumptions, like user data being sold for marketing purposes. Furthermore, the large majority of respondents were not aware of the extent to which they could prevent the processing of their data by adjusting privacy-friendly settings. This highlights a notable gap in information among users regarding the extent of data processing and privacy safeguards. Only two of the 15 organizations represented in the study provide employees with guidelines for dealing with security and privacy-related risks associated with using ChatGPT in the workplace. This suggests that the strategies employed by the majority of participants, as detailed in Section 5.3, are self-determined due to the lack of organizational guidance. Thus, using ChatGPT only for applications that do not involve sensitive data or taking an additional step towards anonymization of sensitive data is based purely on the participants' individual awareness and their intrinsic motivation. Such reliance on individual behavior introduces variability and potential errors that can lead to the disclosure of sensitive data.

For this reason, it is essential for organizations to be aware of the security and privacy risks posed by ChatGPT and to develop ways to mitigate these risks. We argue that outright restricting the use of ChatGPT is not a viable solution. With numerous alternatives available and the efficiency gains offered by generative AI tools, employees are likely to seek out similar tools to enhance their work processes. Instead, organizations must adapt to this reality and focus on implementing measures that facilitate responsible usage. Organizations may consider deploying their own instance of ChatGPT to have more control over data handling and security measures. However, this can be cost-intensive and, therefore, not feasible for every organization. To this end, we recommend focusing on raising awareness among employees by providing them with clear best practices for using ChatGPT or other generative AI tools at the workplace, outlining guidelines for data handling, privacy settings, and data anonymization tools such as GPT Privacy[5] or MaskMyPrompt[6]. Furthermore, organizations need to provide ongoing support and assistance to employees in implementing security and privacy-friendly strategies, e.g., offering technical support for configuring privacy settings.

[5] https://gpt-privacy.com/
[6] https://www.maskmyprompt.com/

7 Conclusion

Our qualitative study explores the perceptions of 17 participants regarding security and privacy aspects of using ChatGPT within their organizations. Our findings indicate that organizational guidelines or policies are absent in most of the participants' organizations. To this end, participants pursue individual strategies to counter security and privacy risks. As these strategies highly depend on the awareness and intrinsic motivation of the individual, they might not always be robust. Moving forward, organizations should proactively address security and privacy-related risks of ChatGPT or other generative AI tools by implementing measures to enhance awareness, establish best practices, and support employees in adopting security and privacy-friendly strategies. By doing so, organizations can effectively mitigate the risks associated with generative AI at the workplace while capitalizing on the transformative potential of the technology.

References

1. Security implications of chatgpt. Tech. rep., Cloud Security Alliance (2023)
2. Alawida, M., Abu Shawar, B., Abiodun, O.I., Mehmood, A., Omolara, A.E., Al Hwaitat, A.K.: Unveiling the dark side of chatgpt: Exploring cyberattacks and enhancing user awareness. Information **15**(1), 27 (Jan 2024)
3. Choudhury, A., Shamszare, H.: Investigating the impact of user trust on the adoption and use of chatgpt: Survey analysis. Journal of Medical Internet Research **25**, e47184 (Jun 2023)
4. Chu, M.N.: Assessing the benefits of chatgpt for business: An empirical study on organizational performance. IEEE Access **11**, 76427–76436 (2023)
5. Corbin, J., Strauss, A.: Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Sage Publications, Thousand Oaks, CA, 4. edn. (2015)
6. Dave, T., Athaluri, S.A., Singh, S.: Chatgpt in medicine: an overview of its applications, advantages, limitations, future prospects, and ethical considerations. Frontiers in Artificial Intelligence **6** (May 2023)
7. Furnham, A.: Response bias, social desirability and dissimulation. Personality and individual differences **7**(3), 385–400 (1986)
8. Grünebaum, A., Chervenak, J., Pollet, S.L., Katz, A., Chervenak, F.A.: The exciting potential for chatgpt in obstetrics and gynecology. American Journal of Obstetrics and Gynecology **228**(6), 696–705 (2023)
9. Jin, K., Wang, C.Y., Pham, H.V., Hemmati, H.: Can chatgpt support developers? an empirical evaluation of large language models for code generation. arXiv preprint arXiv:2402.11702 (2024)
10. King, J., Meinhardt, C.: Rethinking privacy in the ai era - policy provocations for a data-centric world. Tech. rep., Human-Centered Artificial Intelligence, Stanford University (2024)
11. Malik, A.: Openai's chatgpt now has 100 million weekly active users. https://techcrunch.com/2023/11/06/openais-chatgpt-now-has-100-million-weekly-active-users/ (2023), accessed: 2024-03-12

12. Nasr, M., Carlini, N., Hayase, J., Jagielski, M., Cooper, A.F., Ippolito, D., Choquette-Choo, C.A., Wallace, E., Tramèr, F., Lee, K.: Scalable extraction of training data from (production) language models. arXiv preprint arXiv:2311.17035 (2023)
13. OpenAI: Introducing chatgpt (2022), https://openai.com/blog/chatgpt, accessed: 2024-03-12
14. OpenAI: March 20 chatgpt outage: Here's what happened (2023), https://openai.com/blog/march-20-chatgpt-outage, accessed: 2024-03-12
15. OpenAI: Privacy policy. https://openai.com/policies/privacy-policy (2024), accessed: 2024-03-12
16. Rane, N.: Role and challenges of chatgpt and similar generative artificial intelligence in finance and accounting. SSRN Electronic Journal (2023)
17. Ray, P.P.: Chatgpt: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope. Internet of Things and Cyber-Physical Systems **3**, 121–154 (2023)
18. Sarkar, S.: Ai industry analysis. Writerbuddy (2023), https://writerbuddy.ai/blog/ai-industry-analysis, accessed: 2024-03-12
19. Sebastian, G.: Do chatgpt and other ai chatbots pose a cybersecurity risk?: An exploratory study. International Journal of Security and Privacy in Pervasive Computing (IJSPPC) **15**(1), 1–11 (2023)
20. Shoufan, A.: Exploring students' perceptions of chatgpt: Thematic analysis and follow-up survey. IEEE Access **11**, 38805–38818 (2023)
21. Singh, P.: Samsung employees accidentally leaked company secrets via chatgpt: Here's what happened. Business Today (2023), https://www.businesstoday.in/technology/news/story/samsung-employees-accidentally-leaked-company-secrets-via-chatgpt-heres-what-happened-376375-2023-04-06, accessed: 2024-03-12
22. Skjuve, M., Følstad, A., Brandtzaeg, P.B.: The user experience of chatgpt: Findings from a questionnaire study of early users. In: Proceedings of the 5th International Conference on Conversational User Interfaces. CUI '23, Association for Computing Machinery, New York, NY, USA (2023)
23. Sridhara, G., G., R.H., Mazumdar, S.: Chatgpt: A study on its utility for ubiquitous software engineering tasks. arXiv preprint arXiv:2305.16837 (2023)
24. Taylor, J.: Ama calls for stronger ai regulations after doctors use chatgpt to write medical notes. https://www.theguardian.com/technology/2023/jul/27/chatgpt-health-industry-hospitals-ai-regulations-ama (2023), accessed: 2024-03-12
25. Temsah, M.H., Aljamaan, F., Malki, K.H., Alhasan, K., Altamimi, I., Aljarbou, R., Bazuhair, F., Alsubaihin, A., Abdulmajeed, N., Alshahrani, F.S., et al.: Chatgpt and the future of digital health: a study on healthcare workers' perceptions and expectations. In: Healthcare. vol. 11, p. 1812. MDPI (2023)
26. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A.N., Kaiser, Ł., Polosukhin, I.: Attention is all you need. Advances in neural information processing systems **30** (2017)
27. Wu, X., Duan, R., Ni, J.: Unveiling security, privacy, and ethical concerns of chatgpt. Journal of Information and Intelligence (2023)
28. Zhao, W.X., Zhou, K., Li, J., Tang, T., Wang, X., Hou, Y., Min, Y., Zhang, B., Zhang, J., Dong, Z., Du, Y., Yang, C., Chen, Y., Chen, Z., Jiang, J., Ren, R., Li, Y., Tang, X., Liu, Z., Liu, P., Nie, J.Y., Wen, J.R.: A survey of large language models. arXiv preprint arXiv:2303.18223 (2023)