

# Data Guardians’ Behaviors and Challenges While Caring for Others’ Personal Data

Julie M. Haney<sup>1</sup>[0000–0002–6017–9693], Sandra Spickard Prettyman<sup>2</sup>, Mary F. Theofanos<sup>1</sup>[0000–0002–3209–6807], and Susanne M. Furman<sup>1</sup>[0000–0002–7013–6603]

<sup>1</sup> National Institute of Standards and Technology, Gaithersburg MD 20899, USA

{julie.haney, marytheo, susanne.furman}@nist.gov

<sup>2</sup> Culture Catalyst, Chicago, IL USA

sspretty@icloud.com

**Abstract.** Many professional domains require the collection and use of personal data. Protecting systems and data is a major concern in these settings, making it necessary that workers who interact with personal data understand and practice good security and privacy habits. However, to date, there has been little examination of perceptions, behaviors, and challenges among these professionals. To address this gap, we conducted an interview study of 19 individuals working in the education, finance, and health fields. We discovered an overarching theme centered on caring in relation to how these professionals feel responsible for protecting other people’s personal data and take on a “data guardian” role. The identification of the experiences and challenges of data guardians can aid organizations in recognizing and supporting this critical role. Study insights can also help designers of systems that process personal data to better align with the needs and constraints of data guardians.

**Keywords:** cybersecurity · privacy · personal data.

## 1 Introduction

Many professional domains – such as health, finance, and education – require the collection and use of sensitive personal data<sup>3</sup>, which, if compromised, could result in significant harm to patients, clients, or organizations. Protecting systems and data is a major concern in these settings, making it imperative that workers who interact with personal data understand and practice good security and privacy habits.

There are often rules and policies that govern workers’ use of personal data. For example, in the United States (U.S.), the Health Insurance Portability and

---

<sup>3</sup> The terminology used to describe sensitive, personal data varies within different laws, e.g., personally identifiable information (PII) in the Privacy Act [2], personal health information (PHI) in the Health Insurance Portability and Accountability Act [11], personal data in the General Data Protection Regulation [12], and personal information in the California Consumer Privacy Act [30]. For simplicity, within this document, we standardize on the term personal data.

Accountability Act (HIPAA) Privacy Rule [11] establishes standards for protecting personal health data. The Financial Privacy and Safeguards Rules under the Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999) [1] govern how financial institutions collect, disclose, and protect personal financial data. Organizations may also enact their own policies or communicate expectations of how data and systems should be protected.

Despite its importance, the protection of personal data can be complicated, especially given the range of people and devices that may have access to this data. Organizational security and privacy rules and policies may not be attuned to occupational workflows or the ramifications on the workers and their primary duties. A common result is the development of circumventions and workarounds to security and privacy practices [28,18]. It may also be that the cost of adhering to security and privacy advice for an individual is greater than the benefit they receive, so they rationally choose to reject it [15,6]. Ultimately, the lack of compliance with organizational security and privacy policies in professional environments can put stakeholders, including clients, at risk.

While prior research investigated security and privacy practices and perceptions of experts and the general public (e.g., [34,7]), there has been little focused examination of professionals in work contexts that require them to regularly interact with and safeguard the personal data of others. To address this gap, our exploratory study examines a group of workers who are responsible for protecting the confidentiality of other people’s personal data as part of their work responsibilities.

With a goal of developing a deeper understanding of the security and privacy beliefs, behaviors, and challenges of these professionals, we conducted an interview study of 19 individuals working in the U.S. who have responsibilities for protecting the confidentiality of personal data in their daily jobs. Specifically, we interviewed professionals in three sectors that involve significant collection and use of personal data: education, finance, and health. We sought to answer the following research questions about these professionals:

- RQ1:** What are the professionals’ beliefs about and experiences with security and privacy in relation to their work?
- RQ2:** What motivating constructs guide the professionals’ security and privacy understandings, beliefs, and behaviors in their daily work?
- RQ3:** What barriers or facilitators exist for these professionals in their protection of personal data?

We identified an overarching theme centered on “caring” in relation to interactions with personal data in the context of work. This caring was exemplified by a deep sense of personal responsibility for safeguarding others’ personal data, motivated by ethical, legal, and organizational expectations. However, the security and privacy-protecting actions they take vary in sophistication and are undertaken with differing levels of diligence as these workers encounter multiple challenges.

Our research makes several contributions. Based on our analysis, we coined the term *data guardians*<sup>4</sup> in recognition of how our participants spoke about their roles and responsibilities. Beginning to uncover the definitional boundaries of the role and associated work practices allows organizations to recognize the importance of this group of professionals and consider how to best support them. Our findings, though focused on professionals in only three domains, may also be transferable and adapted to other populations of workers responsible for personal data. Study insights can also help designers of systems that store, process, and protect personal data to better understand the perspectives of prospective system users (the data guardians) so that interfaces, applications, and tools can be adapted to user needs and constraints. Furthermore, findings can help security and privacy champions and advocates (those who promote good security and privacy practices in professional settings) better address the needs of their target audiences.

## 2 Related Work

To provide a basis of comparison for our findings, we summarize prior work on security and privacy perceptions and behaviors of both experts and non-expert (general public) users of online technologies.

### 2.1 Experts

Multiple researchers examined the practices and perceptions of security and privacy experts (those who work in and are knowledgeable about security and privacy fields). Compared to non-experts, experts generally exhibit more sophisticated and accurate mental models of security and privacy [16,34,7,26]. They are able to comprehensively identify security and privacy risks and are less trusting of the online environment. However, because of their own expertise, they feel confident that they can avoid or recover from risks since they proactively implement protections [34]. Experts display a command of and familiarity with security and privacy tools and employ mitigations considered to be more robust, such as using a password manager, using two-factor authentication, encrypting sensitive communications, and using anonymization tools [7,16,26,34].

Some experts serve in educational and advocacy roles to impart security and privacy best practices and values to employees and build security and privacy culture within organizations. Examples include security champions [13], cybersecurity advocates [14], and privacy champions [33]. These experts employ a variety of persuasive techniques and communication channels to reach their target audiences. *Privacy champions* [33] are of special interest to our area of

---

<sup>4</sup> The term “data guardian” does not describe a formalized cybersecurity or privacy work role (e.g., like those described in the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity [22]), but rather encompasses a range of professionals using large amounts of personal data as part of their jobs.

investigation since our targeted study population is on the receiving end of champions' privacy awareness and advocacy efforts. Champions view privacy as being a multi-faceted concept that involves aspects of data protection and control, transparency, trust, legal compliance, and ethics. Despite good intentions, privacy champions encounter numerous challenges that threaten the success of their work, including negative attitudes or misunderstandings about privacy among their stakeholders and difficulty communicating the importance of privacy to audiences with diverse backgrounds and roles. To combat these challenges, privacy champions employ a variety of strategies to promote privacy, frequently emphasizing the need to take a "collaborative tone." They regularly engage in efforts to improve their organizations' privacy culture, develop guidance, policies, and tools to help stakeholders build privacy into their processes and products, and take on training and mentoring roles.

While the privacy champions study was focused on individuals in software teams, many of the findings may be applicable to those working in other privacy contexts within organizations, including our target population within the education, health, and finance domains. We envision that insights into challenges faced by our participants can aid privacy champions in adjusting their tactics to be more effective and responsive to these workers' needs.

## 2.2 Non-expert General Public Users

Non-expert general public users (individuals who do not have specialized security or privacy knowledge or responsibilities) operate with a different set of assumptions and mental models than experts. Prior research findings demonstrate that these users rely on multiple mental models about security and privacy that are often incomplete or incorrect and tend to not be proactive in their approach to online security and privacy [25,17,36,16].

Non-expert users can experience a form of security fatigue: feelings of resignation, complacency, and a loss of control [29]. Fatigue and frustration can then result in a decrease in desired security behaviors [10]. In the privacy context, people often are resigned to disclosing data and rationalize their use of privacy-invasive technologies despite their own discomfort [27]. The tendency to satisfice, cognitive biases, time pressures, lack of knowledge, and desensitization contribute to users often making poor security and privacy decisions [23,37]. In organizations, non-expert employees may view stringent security measures as counterproductive and stressful since these measures impede their ability to be flexible in their day-to-day operations [24,19]. Therefore, in what is known as "shadow security," users may circumvent or devise their own security measures to counter practices perceived as overly-burdensome [28,18,3]. Furthermore, employees may view organizational security awareness training as boring, with little relevance to their day-to-day work [4].

Our target population of data guardians (those are responsible for interacting with personal data on a regular basis) is different from both the security/privacy expert and non-expert populations. However, little is known about their practices and challenges. Our study begins to address this gap.

### 3 Methodology

We conducted an exploratory, semi-structured interview study to investigate the security and privacy perceptions and practices of professionals who regularly interact with personal data. The NIST Research Protections Office reviewed the protocol for this research project (ITL-0010) and determined it meets the criteria for “exempt human subjects research” as defined in 15 CFR 27, the Common Rule for the Protection of Human Subjects.

#### 3.1 Sample and Recruitment

We purposefully recruited professionals in education, finance, and healthcare domains whose jobs necessitated frequent interactions with other people’s personal data but who were not privacy and security experts. Working with three domains allowed us to focus the data collection and analysis on a bounded case and permitted more thorough exploration of potential domain-related differences in worker beliefs, behaviors, and experiences.

Initially, we used both personal and professional contacts to generate names of potential participants from each of the three domains. This purposeful sampling [21] was combined with convenience sampling, in which access, availability, and willingness to participate played a role in recruitment. Twelve participants came from this initial outreach to contacts. Subsequently, seven additional participants were recruited through snowball sampling in which participants suggested others who might be willing to participate. Participants were from two regions in the U.S.: 14 from four different states in the Midwest, and five from Mid-Atlantic states and Washington, D.C.

#### 3.2 Data Collection

We developed a semi-structured interview protocol that included questions designed to elicit information about participants’ beliefs, behaviors, and challenges related to online security and privacy in their work. The protocol was largely based on a prior study that investigated expert and general public perspectives [34], with adjustments for our specific population. Several professional colleagues who work in positions similar to those of our sample reviewed the protocol for language, content, and flow. We used their feedback to revise the protocol, then conducted two pilot interviews with representative participants to gain additional feedback that resulted in minor adjustments to clarify language.

After finalizing the protocol, we conducted 19 interviews. The in-person interviews averaged about 30 minutes and took place in a location convenient for the participant. Participants were compensated with a \$50.00 gift card.

Prior to beginning each interview, the research team provided participants with an information sheet and talked to them about the purpose of the study and how their data would be collected, used, and protected. Participants then completed a short demographics questionnaire. All but one session were audio-recorded and transcribed. Participant H05 requested not to be recorded, but

agreed that the interviewer could take notes. To protect confidentiality, we assigned reference codes to participants: a letter indicating the participant's work domain (E = education; F = finance; and H = healthcare) is followed by the interview number (e.g., H04).

### 3.3 Data Analysis

The research team iteratively coded and analyzed the data for this study. Data analysis began with the development of an *a priori* code list based on research questions and related literature. Initially, the researchers independently read and coded the same three transcripts to determine how they were using and applying codes. Subsequently, each of the researchers read two additional transcripts and met again to identify any ongoing issues with the code list, including the need for more specific operationalization (definition) of a code or the creation of emergent codes. Subsequently, the two researchers split the remainder of the transcripts to complete the coding. See Appendix C for the final codebook.

We continued to meet regularly during this process to discuss our coding. We focused not just on agreement but also on where and why there were differences in our coding and the insights afforded by subsequent discussions [5,20]. Once coding was completed, subsequent analysis included organizing the data into higher-level codes (axial coding) and discussing relationships in the codes and the data (selective coding) [21]. This process allowed us to discuss our emergent ideas and refine our interpretations as we moved from concrete codes to more abstract constructs and themes. What emerged was an overarching sense of care on the part of data guardians in relation to their access to and protection of other people's personal data.

## 4 Participants

Of the 19 participants, there were eight participants who worked in education, six in finance, and five in healthcare. All participants directly supported others, whether that be students and their families in the education domain, clients in the finance domain, or patients in the healthcare domain. They also all held positions requiring professional licenses or certifications within their domains (e.g., teacher, realtor, nurse).

Table 1 provides an overview of participant demographics, including self-reported security knowledge. There were similar numbers of male (9) and female (10) participants, ranging in age from 20–29 years old to 60+. Only three participants indicated a high level of security knowledge, over half ( $n = 10$ ) rated themselves as having a moderate amount of knowledge, and just under a third ( $n=6$ ) said they had little or very little knowledge.

In their daily work, these professionals often interacted with a wide range of personal data. A school social worker regularly encountered student data consisting of: “date of birth, residence, grades, parent names. . . When I have access to IEPs [individualized education program] that often includes some medical, . . . social-emotional level of mental health” (E04). An accountant enumerated

**Table 1.** Participant Demographics

Domain	ID	Occupation	Gender	Age Range	Security Knowledge
<i>Education</i>	E01	School administrator and teacher	F	30-39	moderate
	E02	Special education teacher	F	40-49	little
	E03	High school teacher	F	50-59	very little
	E04	School social worker	F	20-29	little
	E05	High school counselor	F	30-39	moderate
	E06	Elementary school teacher	F	30-39	moderate
	E07	High school counselor and data analyst	F	30-39	moderate
	E08	University administrator and faculty	M	40-49	high
<i>Finance</i>	F01	Finance banker	M	50-59	high
	F02	Accountant	M	20-29	little
	F03	Realtor	M	30-39	little
	F04	Accountant	F	40-49	moderate
	F05	Investment banking intern	M	20-29	high
	F06	Realtor	F	60+	moderate
<i>Health</i>	H01	Mental health professional	M	60+	moderate
	H02	Physical therapist	M	30-39	moderate
	H03	Nurse	F	50-59	moderate
	H04	Doctor	M	30-39	moderate
	H05	Nurse	M	30-39	little

the type of client data he interacts with: “date of birth, social security number, age, address,... children, children’s social security numbers,... bank information” (F02). A doctor discussed the personal data he has access to: “medical records... name, address, phone number,... insurance information,... financial information” (H04).

## 5 Results

Today, the work of many professionals necessitates a high degree of dependence on computers and working online. The individuals we interviewed further depended on having access to personal data necessary for them to provide support and services to their students, patients, and clients. Overall, we found that these professionals recognized and exhibited care when interacting with other people’s data, essentially operating as data guardians. In the following sections, we discuss this emerging theme of *care* in the context of participants’ perceptions, behaviors, and challenges related to the protection of personal data.

### 5.1 Privacy and Security Conceptualizations

To first understand perceptions of privacy, we asked participants what they thought privacy means in the context of their work. Privacy was frequently

expressed as the protection of personal data, most commonly by limiting who has access. For example, a high school counselor said, “privacy would be having that [student and parent] information, making sure that it’s protected, if we have it on our computers, that we’re not sharing it outside of just the small circle that needs to know that information” (E05).

Privacy was also described in general terms of what might happen if sensitive data got into the wrong hands. A participant remarked, “It’s about information that’s personal that, if released, could do damage of a multitude of types” (F04).

Other participants characterized privacy as following a set of procedures dictated either by the organization or regulation. For example, a school administrator stated, “Privacy to me is a lot of there being rules and then there being people who are aware of what the rules are because I think having the rules isn’t really enough” (E01).

Participants were also asked about the relationship between privacy and security. Overall, they understood that the two concepts, though not the same, were strongly related. For example, both deal with protection and controlling access. Beyond that, security was perceived as being an enabler of privacy in an *active* sense: “Privacy is kind of the goal and security’s the way to get there” (F05). One participant viewed privacy as protecting data in a physical format and security as protecting digital data:

“Privacy is more making sure that somebody’s not watching what you’re doing when you’re on the computer so that they’re not able to view something they shouldn’t view when they’re standing there. Whereas security is a little bit more in-depth than that, making sure somebody else can’t hack into that system and access that without your being there” (H03).

## 5.2 What It Means to Care

Across the three domains, participants spoke about a sense of personal responsibility related to protecting others’ personal data. In part, this was because their work today necessitates a different type of interaction with client data. Taking care of others (students, clients, or patients) now also means taking care of their data online. A doctor spoke specifically about this responsibility: “It’s my responsibility to make sure I follow the rules, make sure I do everything in my power to keep people’s information safe and make sure that I don’t do anything that could lead to somebody’s information getting out there” (H04).

However, participants drew a distinction between protecting their own versus others’ data, often being more attentive to security in their work context as compared to their personal context. An educator said:

“If it’s my information, I can make a decision about what to send and when to send it and how to send it and if I care. But when I have other people’s information, . . . I think I have to be a little bit more careful because, well, it’s not mine. So, it shouldn’t be up to me about whether or not that’s put in danger” (E01).



### 5.3 How Participants Care

We asked participants what actions they took to safeguard personal data. Specific actions included having strong passwords, encrypting sensitive emails, and using secure wireless connections or virtual private networks (VPNs). However, some participants were vague in their articulation of actions they take. For example, an educator noted that “I’m just really super cautious” (E03), and a healthcare worker said it was about “being mindful” (E06).

Beyond their own actions, participants also relied heavily on others – service providers or Information Technology (IT) professionals within their organizations – to provide oversight and keep the data they work with safe. A high school counselor said, “I just am trusting that the makers of the software that we use... know that this information has to be protected or that there’s some sort of regulation about it that keeps that information safe. But I don’t know that for a fact” (E05). This reliance was often based on blind trust since data guardians did not see themselves as experts in this area, as expressed by one participant: “I’m not a cyber tech guy at all, so I just kind of take what we’re given and roll with it” (F02).

### 5.4 Motivations for Caring

The caring that participants articulated was connected to ethical, legal, and organizational expectations. Not meeting those expectations could result in negative consequences.

**Ethical Obligations** Almost all participants spoke about having an ethical obligation to protect personal data. A financial and wealth advisor said, “It’s a trust factor and one that’s an ethical issue too. When somebody submits their personal information, you’re saying, ‘Yeah. Okay. I’ve got it, and I’ll protect it to make sure it doesn’t leak out’ ” (F01). Participants often related ethics to what would happen if trust was lost due to a privacy/security breach. An owner of an accounting firm talked about potential loss of company reputation:

“As a small company, it’s often word of mouth. We need our clients to trust us. We need them to trust that we will keep their data and information safe, that nothing will happen to it, that others will not be able to access it, and that we are doing everything in our power to ensure that. Without that trust and without that relationship, we do not have the potential to grow as a firm. We, I believe, would suffer financially tremendously if we had a breach in that trust relationship” (F04).

Beyond reputation, other participants articulated potential consequences to those they supported. An accountant discussed financial consequences for clients should their data be breached: “Their information could be out there, and their investment portfolio could be accessed” (F02). An educator described potential dangers for students and their families:

“Many students’ families and sometimes students are undocumented. And in this particular political moment, that could be really dangerous. We have really sensitive information that matters, I think, for our students’ lives, for their families’ lives, for their siblings’ lives” (E02)

**Legal Obligations** Some participants were familiar with applicable laws governing the use and protection of personal data in their domain, while others were not. Healthcare workers all mentioned HIPAA; however, their comments did not always specifically address legal obligations related to *online* privacy and security. Educators rarely noted legal obligations, with only two participants providing vague references to mandated reporting laws that do not mention online privacy and security specifically. Of the three domains, those who worked in finance articulated legal responsibilities and consequences the most clearly. An accountant identified legal consequences should a breach occur by citing a U.S. Internal Revenue Service code: “Section 7216 imposes criminal and financial penalties on tax preparers when they have knowingly or recklessly disclosed return-related information, so we take that very seriously” (F04).

**Organizational Expectations** Participants were often motivated by organizational security and privacy expectations. Oftentimes, these expectations were customized to the domain and organizational needs, as noted by a small business owner: “We’re a very small firm. What works for us may not work for a large, multinational corporation, but certainly, what works for a large, multinational corporation is not going to work for us” (F04).

Participants generally recognized the importance of following organizational rules and policies, even if doing so required extra effort. For example, a doctor commented on his view of the importance of following organizational rules:

“Sometimes there are things we don’t want to have to do and it would be faster to do it a different way, but less secure. And so I’m always going to opt on the side of being more secure. But that might mean it takes me longer. That might mean the next patient has to wait an extra five minutes, but those are things I think we’ve got to do if we want things to be safe” (H04).

Most participants received some type of training or written guidance about organizational expectations. For some, training took place when they first joined the organization. A few participants said they receive training constantly throughout the year. However, more often, training was a once-a-year activity.

Even though training was common, the *importance* placed on training and communicating expectations varied. Some organizations viewed ongoing training as essential, as expressed by a small business owner: “In our field, even today, folks receive very little training on cybersecurity, on how to keep information safe, on what to do, and how to do it. And so I think the first thing is educate yourself” (F04). She continued, “We have clear policies around that, and we do try to ensure that everyone follows those. I would say that I think, for the most

part, folks do" (F04). However, other organizations, especially in the education domain, were less clear about their expectations or did not communicate those in terms understandable to their employees, leaving workers unsure about how to keep data safe. E04, a teacher, said that she had received "no training" about security and privacy. In some cases, data guardians received a handbook with a long list of guidelines. This large volume of information could be overwhelming, so workers may not retain the information, as expressed by a teacher:

"There's a whole list of things that we're supposed to do. Do I know this list? No. So it must not be that important. And we have to sign a contract or some sort of legal document that says that we read those and that we will follow those rules, but I don't know if anyone really knows what they are" (E03).

Further contributing to confusion, some organizations' actions were inconsistent with their own rules. For example, one participant discussed the contradictory ways in which his university dealt with a security issue:

"They say we're always supposed to be using not the public, unsecure network, but the secure network. But... when tech support can't figure out how to get you onto the secure WiFi when you're actually on the premises, then they're like, 'Oh well, just use unsecure. It's not that big of a deal' " (E08).

Not following organizational policies could have consequences for employees. One educator said she is "nervous... that I could maybe... get disciplined for being careless" (E03). A financial participant commented, "some of these are fireable offenses" (F01). Another said, "Our employees know what the consequences will be by not following those policies and procedures, and it would be termination. We take this seriously" (F04).

## 5.5 Challenges to Caring

While participants acknowledged that they have a responsibility to protect the personal data of their students, clients, and patients, they often encountered a number of challenges that impeded their ability and willingness to do so.

**Attitudes and Biases** A majority of participants – including all education participants – expressed personal attitudes that may interfere with their willingness to take protective actions. These attitudes were often rooted in the availability heuristic, in which people assess the probability of a security or privacy breach occurring based on recent events, and the optimism bias, in which people believe they are less likely to experience a negative event. For example, showing an optimism bias, a high school art teacher opined, "the chances of anybody really targeting me are so low that as long as I don't make silly mistakes and just give out my passwords, I'll probably be fine, statistics show" (E01).

While they may be diligent about protecting others' data, some participants expressed attitudes that impacted their personal practices, suggesting that their

good security and privacy habits may not persist outside of the work context. A physical therapist was not as worried about his own online privacy because “I don’t feel like I’m doing anything that the police would be coming to me for” (H02). Others expressed resignation that there was not much they could do to protect themselves online because giving up some privacy is “just a way of life today” (E02).

**Lack of Knowledge** Participants cited their lack of security and privacy knowledge as an impediment to their behaviors. Although our participants regularly accessed and interacted with personal data, security and privacy were not their areas of expertise nor their primary focus while on the job. A health care provider remarked that security can be a burden because “it’s another thing to learn. . . That was not something that I went to nursing school to figure out” (H03). While more than half of participants rated their level of security knowledge as moderate or high, their responses and behaviors did not always reflect this. F06, a realtor, rated her security knowledge as moderate, but made comments demonstrating that she did not understand technology or security. For example, she recounted how she had fallen prey to an online scam, expressed confusion about how her computer works, and said “I don’t know that I’m qualified or smart enough to figure it out” when asked what might help her stay safe online.

**Not understanding risks.** Participants knew that bad things can happen but could not always articulate specific risks. An educator commented, “Whatever it is it could hurt people. . . I’m not even sure what the risks are. I just know they’re out there” (E03). Since they did not fully understand the risks, they did not know if their actions were appropriate or effective, leaving them feeling uncertain, frustrated, and anxious. For example, when talking about how to protect private data, a school social worker commented, “I have no idea how people hack into that. . . And so when I don’t understand something, I don’t think that I’m able to feel confident that I’m accurately protecting myself” (E04). When asked what emotions online security and privacy invoke, she said, “I would say frustration. I would say helplessness. . . Feeling like it’s something that I could never get on top of given that it’s not my job. I’m not in internet security” (E04).

**Difficulty in keeping knowledge current.** The pace of change in technology and security/privacy threats, mitigations, and regulations further contributed to participants’ lack of understanding and feelings of powerlessness. A realtor said:

“I don’t know all the ways things could happen, so how could I take precautions to protect myself and my clients from those things? I’ve taken classes on computer security. . . But that can only do so much, and these hackers are coming up with. . . more and more clever ways to get around all sorts of firewalls” (F03).

Adapting to and educating employees about security and privacy changes was a particular challenge to organizations. H04 mentioned that his healthcare

employer has to continually update training to keep up. The owner of a small accounting firm recognized the importance and complexity of keeping pace: “We need to continually update our skills, update our tools and resources, update the way we do things, update our policies and procedures. Without that, I don’t think we can have real privacy” (F04).

***Need for improved training.*** To address the perceived lack of security and privacy knowledge, several participants thought that they should be provided more or better training or resources at work. A nurse expressed a desire for more guidance on how to protect patient data, saying, “It’d be nice, though, if there is... some easily accessible resource out there that talks about what needs to be done and the easiest way to do it” (H03). To address the unknowns of how to best protect counseling notes, a school social worker thought that standard, secure procedures should be communicated throughout the organization: “I think it would be something good for all social workers in the network or something to have a training on security or to be told... ‘This is how we’re all going to track our confidential meeting notes’ ” (E04).

**Complexity** Even though participants recognized that protecting personal data is part of their job, they often found it to be complex, difficult, and taking time away from their primary tasks. A finance banker, F01, summed up the complexity he encounters: “Lots of procedures, lots of security issues, a lot of bank regulation issues.” Several mentioned that there are multiple systems and software applications they need for their jobs, which adds time and difficulty in keeping track of sometimes conflicting system security requirements. Passwords were repeatedly mentioned as an example of a burdensome security mechanism, especially when having to maintain different passwords on multiple systems.

Even though participants often articulated the importance of following organizational rules, they did not always follow prescribed practices due to complexity. To cope, they sometimes found workarounds. However, these workarounds often negated the intent of the rule. One participant thought that workarounds were inevitable: “Human nature often defaults to the easiest possible scenario and the fastest possible scenario and maybe not necessarily the safest possible scenario” (H04). Because of the desire to do what is easiest, H05 said that he rarely sees people following security and privacy procedures at work. A university educator recognized the value of security and privacy, yet “I haphazardly practice good behavior. My first emotion is just being annoyed. One more thing to deal with” (E08). In the case of passwords, participants admitted to less-secure practices, including choosing a simple password, using the same password for multiple systems, or writing their passwords down.

To address complexity, participants expressed a need for usable security and privacy solutions that could seamlessly integrate into the work environment. A participant commented, “What really is needed are tools and mechanisms that are not cumbersome and that allow us to get on with our work while at the same time protecting privacy and providing security” (F04). Another said that, although he has a duty to make good choices, the onus is not just on him:

“I think that the people who develop these tools, I think the people who come up with these programs, I think they have a responsibility, too, and their responsibility is to make sure that it’s not too cumbersome on me. . . If you want me to be safe and secure, you need to find ways to help me do that” (H04).

**Inevitability of Security Problems** Participants were often realistic in their expectations of security and their own limitations. For example, a participant said, “We know that nothing is ever 100% safe. That’s true whether we’re talking about handwritten records and physical files, or we’re talking about things that are kept online” (H04). Even when they followed best practices and organizational procedures, they thought it may never be enough to adequately protect the personal data with which they are entrusted. A financial sector participant commented, “Our responsibility is to make sure that we’re following best practice and that we do everything we can, knowing that maybe we can’t do everything and that something might still happen” (F04). A realtor said, “I don’t feel confident that anything is safe enough” (F06).

Because of their deep sense of responsibility for protecting others’ data, the concern that, no matter what they do, personal data could still be compromised resulted in participants experiencing emotions such as frustration, anxiety, stress, and fear. F04 acknowledged that anyone can make an error that puts personal data in jeopardy: “One mistake, one click – and sometimes it’s very easy to click by mistake – and who knows where you’ll be, who knows what will happen, and who knows what then happens in terms of clients’ data and information.” As a result, F04 said:

“I feel fear and that bothers me. I don’t think I should have to feel fear in my work, . . . but I think that it’s the fact that it seems at least to be out of my control. I can put mechanisms in place and policies in place and tools in place and still we get phishing emails and still we can be hacked and sometimes we might not even know it.”

Similarly, when asked what emotions he feels when thinking about online privacy and security, a doctor said:

“I’d say I’m worried, always worried. There’s that level of stress I think anytime you’re in charge of or have other people’s information and other people’s lives, if you will, in your hand. . . While I’d like to save that stress for saving people’s lives, I think sometimes this might, in fact, be just as serious to them in some cases” (H04).

## 6 Discussion

In this section, based on our bounded case of the education, finance, and health domains, we compare data guardians to previously identified user populations, finding them to be a group with special needs. We then suggest ways in which organizations can better support their own data guardians.

## 6.1 Between Two Worlds

In their critical role in the protection of personal data, data guardians are a unique population of workers who, at times, are between two worlds: those of security/privacy experts and general public users. Like experts, data guardians are expected to know online security and privacy best practices and consistently make good choices to protect personal data. However, these workers often think and behave more like non-expert, general public users.

We observed a marked tension between data guardians *wanting* to protect personal data and *being able* to protect. Like the experts represented in prior studies [34,7], data guardians exhibit a sense of responsibility about keeping personal data secure and private, and they generally understand that negative consequences could result if they fail in those duties. However, in contrast to experts, their primary education and training are focused on roles that support people rather than systems. Their lack of security expertise may result in them not feeling empowered to protect personal data, whereas experts have confidence in their own abilities [34].

Unlike general public non-experts who often are resigned about their inability to protect their own data [27,34], data guardians have a greater sense of duty since they are stewards of others' personal data. Moreover, they may have strict organizational procedures they must follow or may be subject to significant consequences for violating national or state laws. However, despite this extra burden of responsibility, similar to general public users (e.g., as identified in [25,16,17]), data guardians may have limited understanding of security and privacy risks, technologies, and mitigation strategies and have inconsistent security/privacy experiences as they navigate different applications. Complexity and conflict with their primary tasks result in the security workarounds and justifications that exemplify the shadow security phenomenon found in prior studies [3,18]. Some participants are further unsure of organizational or legal expectations about desired security and privacy practices beyond general platitudes. These uncertainties result in data guardians often taking limited actions on their own and largely depending on others, as also reflected in prior work [16,25]. In addition, our participants clearly exhibit the "security fatigue" previously noted among the general population [29] in their expression of biases that lead to less vigilance, frustration with complex and unusable security mechanisms, and a sense of powerlessness that no matter what they do, something bad may still happen [23,37].

## 6.2 Domain Differences

Although our sample size was not large enough to definitively identify contrasts among data guardians in the education, finance, and healthcare domains, we offer preliminary thoughts about observed differences.

Overall, participants in the education domain had the least amount of formal security training, often saying that they did not remember much of the guidance provided by their institutions, if provided at all. These participants often

did not know about applicable laws governing the protection of data in educational institutions and seemed to be more naive about the likelihood of a privacy or security breach. Education participants also were more likely to see security as complex and admit their lack of understanding. These findings suggest potential reasons behind susceptibility of education organizations to attack and the poor evaluations states received regarding their ability to protect student records [31,35].

In contrast, finance and healthcare participants received more focused security and privacy training, often on a continuous basis. These participants also exhibited a deeper understanding of the harmful repercussions of security or privacy compromises. In particular, healthcare participants worked in a high-stakes environment in which their patients' health and lives may depend on the security of personal and medical data. In general, finance and healthcare participants, although recognizing that safeguarding data could be time-intensive, often placed its importance above convenience. They were also more knowledgeable about applicable regulations and organizational policies, likely because of clearer regulations and harsher consequences for not following those [11,9]. Finance participants working in banking or accounting were most able to articulate how they could safeguard personal data in their care.

### 6.3 Practical Implications for Supporting Data Guardians

Our study identifies a class of employees who work with and are expected to protect online personal data but may not be adequately equipped to do so. The following are actions organizations can take to better support data guardians.

***Identify the data guardians in the organization.*** The conceptualization of data guardians and their work practices allows organizations to recognize the importance of the role in the protection of data, their level of responsibility, and how best to support them. In some domains, it is clear which employees operate as data guardians (e.g., health professionals), but it is less clear in others (e.g., realtors). As initial steps in supporting guardians, organizations can: 1) create clear criteria for classifying data guardians (those who use personal data on a regular basis), 2) identify who the data guardians are in the organization; 3) recognize ways in which data guardians interact with other people's personal data; and 4) determine how these interactions support (or interfere with) guardians' primary tasks towards solutions that mitigate interference with primary tasks.

***Work to create a strong privacy and security culture.*** While data guardians recognize their responsibility to care, we found that their organization's culture does not always support them in enacting that care. Therefore, establishing a strong privacy/security culture at all levels of the organization, although non-trivial, is essential for supporting data guardians. This may be especially important in educational institutions, where there are current gaps impacting data guardians. Organizational leadership can outwardly recognize the value of the data guardian role and ensure adequate resources to support these workers. IT and security staff should model desired security and policy behaviors by consistently following organizational policies. Privacy and security champions can



also play a significant role in improving their organization's security and privacy culture, for example, through targeted discussions about the importance of privacy/security, gaining management support for privacy functions and tools, and facilitating communication between teams [33,13,14].

***Communicate expectations.*** Our participants were sometimes uncertain about specific actions they were required to take. To minimize uncertainty, organizational expectations about online security/privacy should be clearly and consistently communicated, including why these policies are in place and the consequences when rules and policies are not followed. In particular, data guardians should understand how their security and privacy actions relate to the ethical and legal responsibilities of their jobs. In this regard, organizations can appeal to data guardians' strong motivation of responsibility to care to impart on them the importance of acting diligently to protect data.

***Provide targeted and ongoing awareness and training.*** We found that security and privacy awareness training varied greatly in quantity and quality. Training and reference documentation should be meaningful for the data guardians and customized to the specific work they do within the organization. For example, training could identify common types of personal data encountered in the daily work, risks, mitigations, misconceptions, and challenges faced by data guardians within a specific domain. Training and documentation should include not just awareness of privacy and security issues, but also actionable and achievable steps to take [14] that empower guardians to engage in best practices while also being successful in their primary tasks. Furthermore, beyond the typical, once-a-year training common in many organizations, training should be engaging, relatable, and reinforced throughout the year via a variety of communication media tailored to the preferences and needs of the data guardians within an organization [4]. Furthermore, providing information that makes a "work-home" connection can encourage the building of sustainable and consistent online security and privacy habits [8].

***Procure and develop usable systems and processes.*** Complexity and lack of usability was a common challenge noted in our interviews, often resulting in frustration or less-secure workarounds. To counter this challenge, organizations should work toward developing or selecting usable systems and processes for use by data guardians. Interfaces, applications, and tools must be adapted to the specific needs and constraints of these workers and avoid placing too great a burden on data guardians as they try to accomplish their primary tasks. There also needs to be greater integration between systems to minimize the burden on data guardians, for example, by enacting single sign-on authentication. Data guardians should be involved in the requirements gathering and piloting of these systems and processes to voice questions or issues they encounter.

#### 6.4 Limitations and Future Work

Our study has several limitations. Participants' self-reported responses might have been influenced by social desirability or recall biases. For example, par-

ticipants may have been hesitant to talk about negative security behaviors or attitudes. Additionally, since the concept of a data guardian role is emergent, we relied on traditional domains where employees typically work with others' personal data, specifically focusing on just three domains as a starting point. Coupled with the smaller number of participants common to qualitative research, the study cannot be generalized to all professional roles and domains. However, unlike quantitative research, generalizability is not the goal of exploratory qualitative work, which strives to provide rich descriptions that allow for understanding of the phenomenon under study, the identification of future research areas, and the transferability of findings to other contexts [32]. Additional research may extend our study to include other domains or do a deep-dive into a particular domain to gather sector-specific insights. Finally, we did not consider the size or type (e.g., private, public) of organizations in the selection of participants. This may be a focus for future research that could explore how data guardians are supported in different categories of organizations.

## 7 Conclusion

Through an interview study of professionals in the education, finance, and healthcare domains, our research identifies the motivations, behaviors, and challenges of taking on a data guardian role. Data guardians, while not security or privacy experts, are unique from general public users in their sense of responsibility and care for safeguarding other people's data. Although this role is in support of their primary profession, it is nonetheless essential for their jobs and supporting their students, clients, and patients. Our identification of current security and privacy misconceptions and the challenges faced by data guardians can aid organizations in the improvement of organizational awareness and training programs. Study insights can also help designers of systems that store, process, and protect personal data to better understand the perspectives of prospective system users (the data guardians) so that interfaces, applications, and tools can be adapted to user needs and constraints. Our investigation, though focused on professionals in only three domains, may also be transferable and adapted to other populations of workers responsible for sensitive data.

## Disclaimer

Certain commercial companies or products are identified in this paper to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the companies or products identified are necessarily the best available for the purpose.

## References

1. 106th Congress: S.900 - Gramm-Leach-Bliley Act. <https://www.congress.gov/bill/106th-congress/senate-bill/900> (1999)

2. 113th Congress: S.607 - Electronic communications privacy act amendments act of 2013. <https://www.congress.gov/bill/113th-congress/senate-bill/607/text> (2013)
3. Alotaibi, M., Furnell, S., Clarke, N.: Information security policies: A review of challenges and influencing factors. In: 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST). pp. 352–358 (2016)
4. Bada, M., Sasse, M.A., Nurse, J.R.: Cyber security awareness campaigns: Why do they fail to change behaviour? <https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf> (2019)
5. Barbour, R.S.: Checklists for improving rigour in qualitative research: a case of the tail wagging the dog? *British Medical Journal* **322**(7294), 1115–1117 (2001)
6. Barth, S., de Jong, M.D., Junger, M., Hartel, P.H., Roppelt, J.C.: Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics* **41**, 55–69 (2019)
7. Busse, K., Schäfer, J., Smith, M.: Replication: ‘...no one can hack my mind’ - revisiting a study on expert and non-expert security practices and advice. In: Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). pp. 117–136 (2019)
8. Caldwell, T.: Making security awareness training work. *Computer Fraud & Security* (6), 8–14 (2016)
9. Congressional Research Service: Financial services and cybersecurity: The federal role. <https://crsreports.congress.gov/product/pdf/R/R44429> (2016)
10. D’Arcy, J., Teh, P.L.: Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management* **56**(7), 103151 (2019)
11. Department of Health and Human Services: The HIPAA privacy rule. <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> (2021)
12. European Union: General data protection regulation. <https://gdpr.eu/> (2016)
13. Gabriel, T., Furnell, S.: Selecting security champions. *Computer Fraud & Security* (8), 8–12 (2011)
14. Haney, J.M., Lutters, W.G.: “It’s Scary...It’s Confusing...It’s Dull”: How cybersecurity advocates overcome negative perceptions of security. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). pp. 411–425 (2018)
15. Herley, C.: So long, and no thanks for the externalities: the rational rejection of security advice by users. In: 2009 Workshop on New Security Paradigms. pp. 133–14 (2009)
16. Ion, I., Reeder, R., Consolvo, S.: ‘...no one can hack my mind’: comparing expert and non-expert security practices. In: Eleventh Symposium on Usable Privacy and Security (SOUPS 2015). pp. 327–346 (2015)
17. Kang, R., Dabbish, L., Fruchter, N., Kiesler, S.: “my data just goes everywhere.” user mental models of the internet and implications for privacy and security. In: Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) (2015)
18. Kirlappos, I., Parkin, S., Sasse, M.A.: “Shadow security” as a tool for the learning organization. *Computers and Society* **45**(1), 29–37 (2015)
19. Lee, C., Lee, C.C., Kim, S.: Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security* **59**, 60–70 (2016)
20. McDonald, N., Schoenebeck, S., Forte, A.: Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. In: ACM on Human-Computer Interaction. p. 72. ACM (2019)

21. Merriam, S.B., Tisdell, E.J.: *Qualitative Research: A Guide to Design and Implementation*. John Wiley & Sons, San Francisco, CA, 4th edn. (2016)
22. Petersen, R., Santos, D., Smith, M.C., Wetzel, K.A., Witte, G.: NIST Special Publication 800-181 Revision 1: Workforce Framework for Cybersecurity (NICE Framework). <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf> (2020)
23. Pfleeger, S.L., Caputo, D.D.: Leveraging behavioral science to mitigate cyber security risk. *Computers & Security* **31**(4), 597–611 (2012)
24. Post, G.V., Kagan, A.: Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security* **26**(3), 229–237 (2007)
25. Prettyman, S.S., Furman, S., Theofanos, M., Stanton, B.: Privacy and security in the brave new world: The use of multiple mental models. In: *International Conference on Human Aspects of Information Security, Privacy, and Trust*. pp. 260–270 (2015)
26. Racine, E., Skeba, P., Baumer, E.P., Forte, A.: What are PETs for privacy experts and non-experts. In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (2020)
27. Seberger, J.S., Llavore, M., Wyant, N.N., Shklovski, I., Patil, S.: Empowering resignation: There’s an app for that. In: *2021 CHI Conference on Human Factors in Computing Systems*. pp. 1–18 (2021)
28. Smith, S.W., Koppel, R., Blythe, J., Kothari, V.: Mismorphism: a semiotic model of computer security circumvention. In: *2015 Symposium and Bootcamp on the Science of Security*. pp. 1–2 (2015)
29. Stanton, B., Theofanos, M.F., Prettyman, S.S., Furman, S.: Security fatigue. *IT Professional* **18**(5), 26–32 (2016)
30. State of California: SB-327 Information privacy: connected devices. <https://leginfo.legislature.ca.gov> (September 2018)
31. Stickland, R., Haimson, L.: The state student privacy report card: Grading the states on protecting student data privacy. Tech. rep., Network for Public Education (2019)
32. Swedberg, R.: Exploratory research. In: Elman, C., Gerring, J., Mahoney, J. (eds.) *The production of knowledge: Enhancing progress in social science*, pp. 17–41. Cambridge University Press (2020)
33. Tahaei, M., Frik, A., Vaniea, K.: Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. pp. pp. 1–15 (2021)
34. Theofanos, M., Stanton, B., Furman, S., Prettyman, S.S., Garfinkel, S.: Be prepared: How US government experts think about cybersecurity. In: *Workshop on Usable Security (USEC)* (2017)
35. Verizon: 2021 data breach investigations report. <https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf> (2022)
36. Wash, R.: Folk models of home computer security. In: *Sixth Symposium on Usable Privacy and Security (SOUPS 2010)*. pp. 11–26 (2010)
37. West, R., Mayhorn, C., Hardee, J., Mendel, J.: The weakest link: A psychological perspective on why users make poor security decisions. In: *Social and Human elements of Information Security: Emerging Trends and countermeasures*. pp. 43–60 (2009)