Lessons Learned and Suitability of Focus Groups in Security Information Workers Research

Julie M. Haney[0000−0002−6017−9693], Jody L. Jacobs[0000−0002−6433−884X], Fernando Barrientos, and Susanne M. Furman[0000−0002−7013−6603]

National Institute of Standards and Technology, Gaithersburg MD 20899, USA
{julie.haney,jody.jacobs,susanne.furman}@nist.gov, fbarrie4gmu@gmail.com
https://csrc.nist.gov/usable-cybersecurity

Abstract. Security information workers (SIW) are professionals who develop and use security-related data within their jobs. Qualitative methods – primarily interviews – are becoming increasingly popular in SIW research. However, focus groups are an under-utilized, but potentially valuable way to explore the work practices, needs, and challenges of these professionals. Based on our experience with virtual focus groups of security awareness professionals, this paper documents lessons learned and the suitability of using focus groups to study SIW. We also suggest ways to alleviate concerns SIW may have with focus group participation. These insights may be helpful to other researchers embarking on SIW research.

Keywords: security information workers · focus groups · methodology · security · usability.

1 Introduction

Security information workers (SIW)[1] are professionals who develop and use security-related data within their jobs. Some SIW are employed in largely technical roles, such as: IT professionals who implement and manage security systems and processes; developers who build software that implements security mechanisms; analysts who collect and investigate security data; Chief Information Security Officers (CISOs) and other security managers; and consultants who facilitate the adoption of security best practices and technologies [?]. Other SIW may have less-technical roles, for example, security policy makers, security communicators, or educators who instruct their students about safe online practices.

Conducting research with SIW participants allows for discovering work practices, challenges, and needs to aid in the development of tools, techniques, and other support mechanisms that are usable and valuable to SIW and their stakeholders. Qualitative methods – largely interviews – have become increasingly

[1] The term "security information worker" does not describe a formalized cybersecurity work role (e.g., like those described in the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity [?]), but rather encompasses a range of professionals handling security information.

popular when studying these workers [?]. Focus groups are a less-frequently used qualitative method but can be valuable for studying SIW (e.g., as employed in [?,?]). While other cybersecurity researchers have shared lessons learned in their experiences with surveys, interviews, and field observations of SIW (e.g., [?,?,?]), none have discussed how *focus groups* might be appropriate for studying SIW.

In this paper, we document lessons learned from our experiences with virtual focus groups of United States (U.S.) government security awareness professionals – those tasked with training their organization's workforce on security best practices – as part of a mixed-methods research project. We then discuss the suitability of using focus groups to study SIW, including potential benefits, disadvantages, challenges, and recommendations for offsetting hesitations SIW may have with focus group participation. These insights may be helpful to other researchers embarking on SIW research.

2 Background

2.1 Focus Groups

Focus groups are a research methodology typically having five characteristics: "(1) a small group of people, who (2) possess certain characteristics, (3) provide qualitative data (4) in a focused discussion (5) to help understand the topic of interest" [?]. Differing from other group interactions (e.g., meetings or a single group interview with a project team) in which consensus or recommendations are the goal, *multiple* focus groups are conducted to discover a range of perspectives. Data from the groups are then compared and contrasted. Although often conducted similarly, we also differentiate academic research focus groups (the topic of this paper) from marketing focus groups in which the goal is to understand people's behaviors and preferences related to consumer products.

Common Uses and Benefits. Focus groups are especially useful in exploratory research to discover people's perceptions and feelings about a topic of interest [?]. Focus group data can be used for a variety of purposes, including guiding program or policy development, gaining an understanding of behaviors, and capturing organizational concerns and issues.

Focus groups can also be valuable in mixed-methods research when used as either a precursor to quantitative surveys of larger samples [?] or as an aid in the interpretation of data collected in a survey [?]. When used as a precursor (as is this case in our experience), the interactive nature of focus groups can facilitate the development of survey questions and procedures by providing an understanding of how people think and talk about specific topics, identifying concepts that are of particular importance to participants, and soliciting ideas for survey recruitment [?,?,?].

Criticisms. Despite their strengths, several criticisms have been directed at focus groups. Because focus groups bring participants together in a non-probabilistic, artificial setting, focus group participants may intellectualize and present themselves as rational and thoughtful. However, in reality, behaviors may be unconscious, irrational, or driven by emotion [?,?]. Participants' responses may also be influenced by group dynamics and pressure to conform to the opinions of others [?]. Moreover, in cases in which groups are too large and the topic is complex, there is a fear of discussions becoming superficial [?].

Several measures can be taken to counter these potential pitfalls [?,?]. Focus groups can be paired with other methodologies (e.g., field observations or surveys) to capture real-world behaviors and validate findings. Furthermore, moderators have an important role in creating an open, welcoming environment in which participants feel safe to express their true thoughts. Moderators also should carefully monitor group dynamics to ensure a small number of individuals do not dominate the conversation. Limiting group size can help to ensure participants have adequate opportunity to express their thoughts.

It also should be noted that group dynamics and influence may not necessarily be a negative aspect of focus groups. Rather, observations of these interactions can actually be quite insightful as they may mimic participants' daily conversations with others [?].

2.2 Focus Groups in Security Information Workers Research

Focus group methods are infrequently found in formal, academic cybersecurity research. Fujs et al. [?] identified 160 papers describing qualitative research related to cybersecurity (not limited to studies involving SIW) from 2017-2019, classifying only 11 as using focus groups. However, the authors' definition of focus group is arguable in that they binned group interviews with only two individuals and workshops into the focus group category. Therefore, there may have been fewer focus group studies than the 11 reported.

Fewer examples can be found when applied specifically to research involving SIW. Bada et al. [?] conducted focus groups of security professionals to better understand the relationship between cybersecurity awareness-raising campaigns and the cybersecurity capacity maturity of six African nations. Kumar et al. [?] conducted focus groups with primary school teachers to identify, in part, how educators could best communicate security and privacy information to students. Gorski et al. [?] utilized four in-person focus groups of software developers in a participatory design study related to security warnings for cryptographic libraries. This was the only paper related to focus groups and SIW we found that described the methodology and focus group protocol development in detail. However, we discovered no papers that discuss lessons learned after the use of focus groups to study SIW.

3 Study Methodology

As a basis for our lessons learned and position on suitability for SIW research, we first provide an overview of how focus groups were employed in our research study. The study protocol was reviewed by the National Institute of Standards and Technology (NIST) Research Protections Office and determined to be exempt human subjects research.

3.1 Study Overview

Security awareness training can be a first step towards helping employees recognize and appropriately respond to security issues, with a goal of achieving long-term behavior change [?]. However, security awareness programs may face a multitude of challenges, including lack of resources and appropriately trained staff, a poor reputation among the workforce for training being a boring, "check-the-box" exercise, and a tendency to measure success based on training completion rates rather than workforce behavior change [?,?,?]. Moreover, it is unclear if these challenges apply to U.S. government (federal) organizations. To address this uncertainty, we conducted a two-phased, mixed-methods study leveraging both qualitative and quantitative methods to better understand the needs, challenges, practices, and necessary competencies of federal security awareness teams and programs.

Focus groups of 29 federal security awareness professionals were a first phase that informed a follow-on, predominantly quantitative survey completed by 96 security awareness professionals. A focus group methodology was selected as our qualitative phase for several reasons. Beyond the utility of informing the survey, since one of the goals of our study was to identify potential ways in which information could be shared more effectively across the community, we believed it would be valuable to observe how ideas emerged during group discussion. Focus groups would also serve a practical purpose as we had an abbreviated timeline in which to collect and analyze data. Our study results were going to inform the revision of a government security awareness guidance document set to commence around the same time as our study. Wanting to provide input earlier rather than later in the revision process and factoring in the time to design and execute a follow-on survey, we saw focus groups as being more efficient as compared to individual interviews.

3.2 Focus Group Design

When designing the study, we consulted seven subject matter experts (SMEs) who were veteran security awareness professionals or past and current coordinators of federal security collaboration forums that address security awareness topics. The SMEs provided input into the study's overall direction, focus group questions, and participant recruitment strategies.

We selected a multiple-category design for the focus groups, which involved focus groups with several types of participants to allow for comparisons across or within categories [?]. Based on SME discussions, we decided on three categories: 1) department-level organizations (e.g., U.S. Department of Commerce), 2) sub-component agencies, which are semi-autonomous organizations under a department (e.g., NIST is a sub-component under Department of Commerce), and 3) independent agencies, which are not in a department (e.g., General Services Administration). In the Executive Branch of the U.S. government, there are 15 departments, over 200 sub-components, and just over 100 independent agencies.

In deciding how many groups to conduct, we consulted the focus group methodology literature. In a multiple-category design, it is suggested that 3-4 focus groups per category are usually sufficient to reach data saturation, but there may be categories consisting of small populations for which fewer groups may suffice [?]. As such, we aimed for three groups each for the independent and sub-component categories. Since there are only 15 government departments from which to recruit, having two groups of those working at the department level was deemed to be acceptable. Furthermore, Guest et al. [?] found that about 80% of all data saturation occurs after 2 - 3 focus groups, with 90% occurring after 3 – 6 groups. Because we observed that many of the same themes identified during analysis occurred regardless of organization category, we felt relatively confident that we had likely reached a high level of data saturation with our eight groups.

To develop the focus group instrument, we followed the suggested process for creating a questioning route outlined in Krueger and Casey [?]. This route includes: an easy-to-answer, opening question; an introductory question that gets people thinking about the topic; a transition question that prompts participants to go into more detail about their experiences with the topic; key questions, which are the core of the discussion; and ending questions that allow participants to voice their thoughts on critical aspects of the topic and suggest other significant topics related to but not explored during the group. Appendix A contains the focus group script with labels for each type of question.

3.3 Data Collection

Focus group participants were selected to represent the diversity of federal agencies. We identified prospective participants via several avenues: recommendations from the SMEs; researchers' professional contacts; an online cybersecurity mailing list of small federal agencies; speakers and contest participants/winners from the last three years of the Federal Information Security Educators (FISSEA) conference [?]; and LinkedIn and Google searches. Invitations were sent via email. Participants had to be federal employees and have knowledge of the security awareness programs in their organizations either because they had security awareness duties or oversaw the programs.

We held the focus groups in December 2020 and January 2021. While focus groups are often conducted in-person, because of the pandemic and distributed locations of federal security awareness professionals across the U.S., we ran all focus groups using a virtual meeting platform. To maximize discussion time during the actual focus groups, we held a 15-minute meeting with each participant individually in the days preceding their focus group to test and troubleshoot their meeting connection and review the informed consent form. Participants were also provided the opportunity to ask questions. Prior to the focus group, each participant had to return their digitally signed consent form via email to the research team.

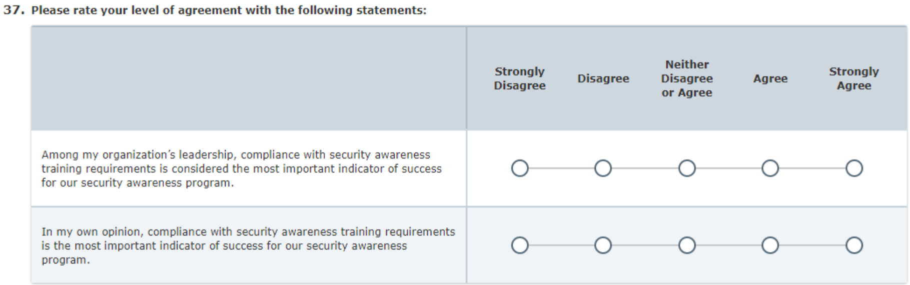
In all, we conducted eight focus groups with 29 total participants. Focus group sessions lasted 60-75 minutes, with each having 3-5 participants. Three focus groups consisted of 12 representatives from independent federal agencies. Two focus groups (each with 3 people) were with representatives from department-level agencies. The third set consisted of three focus groups with 11 representatives from 10 department sub-component agencies (in one group, two individuals from the same agency attended).

Three research team members managed the focus groups. The principal investigator served as the moderator for all groups. The moderator shared a slide presentation that displayed questions as they were being asked. To begin the focus groups, she welcomed participants and briefly discussed tips to help the conversation (e.g., "This is a confidential discussion," "There are no wrong answers" and "When not talking, please mute yourself."). Then she asked each question, probed further to clarify or get more details on responses as appropriate, and facilitated discussion. Another team member acted as the assistant moderator and helped participants with technical issues via chat and email. Finally, a note taker captured the main points of the groups' conversations as a backup in the event that the recording failed or was corrupted.

All focus groups were audio recorded and transcribed. Participants also completed an online survey to gather demographic and organizational information. To ensure anonymity and to be able to confidentially link data between the focus groups and demographic survey, each participant was assigned a reference code, with individuals from independent agencies identified as N01 – N12, department-level organizations as D01 – D06, and sub-components as S01 – S11.

3.4 Data Analysis

Data analysis started with coding [**?**], which involved categorization of focus group data. Initially, each of the four members of the research team individually coded a subset of three transcripts (one from each category of focus group) using an *a priori* code list based on the focus group questions and then added new codes as needed. The research team met several times to discuss codes and develop a codebook (a list of codes to be used in analysis). As part of the final codebook, all codes were "operationalized," which involves formally defining each code to ensure understanding among all coders. Coding continued until all transcripts were coded by two researchers, who met to discuss code application and resolve differences. The entire research team convened to discuss overarching themes identified in the data and areas of interest to include in the subsequent survey.



37. Please rate your level of agreement with the following statements:

	Strongly Disagree	Disagree	Neither Disagree or Agree	Agree	Strongly Agree
Among my organization's leadership, compliance with security awareness training requirements is considered the most important indicator of success for our security awareness program.	○	○	○	○	○
In my own opinion, compliance with security awareness training requirements is the most important indicator of success for our security awareness program.	○	○	○	○	○

Fig. 1. Survey question about compliance as an indicator of success for a security awareness program

3.5 Informing a Survey

Focus group data informed the development of a predominantly quantitative survey that was distributed to a larger number of security awareness professionals. The following describes several ways in which the survey was influenced.

We discovered areas of particular importance or divergence among focus group participants that were incorporated as questions in the survey. For example, we observed a tension among participants with respect to the success of the security awareness program being determined by compliance with training mandates (measured by training completion rates) versus actual impact on employees' behaviors. Thus, we developed a question to gauge this sentiment among surveyed organizations (see Fig. 1). As another example, focus group participants identified several significant challenges their security awareness programs face. In the survey, we developed corresponding questions that asked participants to rate the level of challenge they encountered (5-point Likert scale ranging from "Very challenging" to "Not at all challenging") for each of those challenge items (see Fig. 2 for an example).

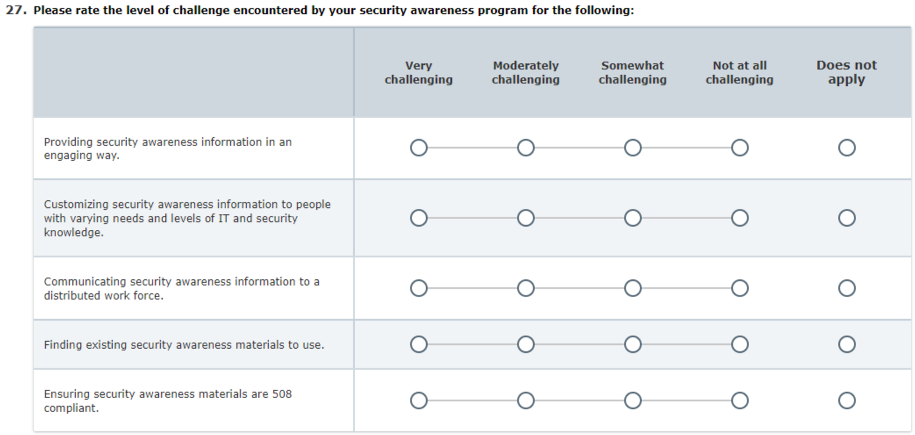
Focus group data also informed possible answer choices for a number of questions. For instance, when asking what happens when employees do not complete their awareness training on time, we included answer options based on examples provided to us by focus group participants (see Fig. 3).

4 General Lessons Learned

Before addressing the suitability of focus groups for SIW research, we first discuss general lessons learned in our experience with virtual focus groups.

4.1 Differences from Interviews

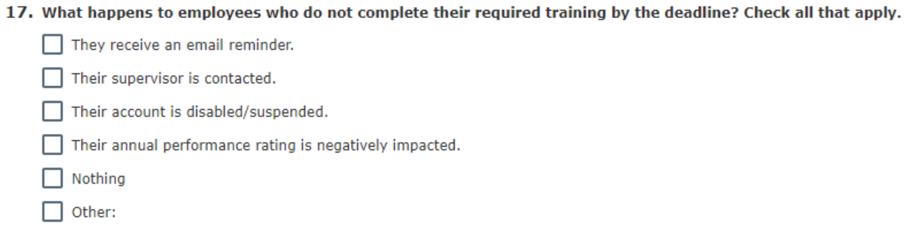
Given that the moderator utilizes a semi-structured questioning approach, one might think that focus groups are similar to interviews. However, even though



27. **Please rate the level of challenge encountered by your security awareness program for the following:**

	Very challenging	Moderately challenging	Somewhat challenging	Not at all challenging	Does not apply
Providing security awareness information in an engaging way.	○	○	○	○	○
Customizing security awareness information to people with varying needs and levels of IT and security knowledge.	○	○	○	○	○
Communicating security awareness information to a distributed work force.	○	○	○	○	○
Finding existing security awareness materials to use.	○	○	○	○	○
Ensuring security awareness materials are 508 compliant.	○	○	○	○	○

Fig. 2. Example survey question about challenges encountered in the security awareness program



17. **What happens to employees who do not complete their required training by the deadline? Check all that apply.**

□ They receive an email reminder.
□ Their supervisor is contacted.
□ Their account is disabled/suspended.
□ Their annual performance rating is negatively impacted.
□ Nothing
□ Other:

Fig. 3. Survey question about consequences for not completing training

our research team had extensive prior experience with interviews, we discovered that focus groups were quite different than interviews in several respects.

Recruitment Effort. We found that recruitment and scheduling were more labor-intensive as compared to interviews. There were significant challenges coordinating the schedules of participants to find blocks of time in which at least three people (plus the researchers) were available, especially since some participants had demanding jobs (e.g., CISO). When prospective participants responded affirmatively to our email invitation, to determine availability, we sent them a link to an online scheduling application with several possible dates and times for the focus groups. However, less than half used the application, resulting in our research team having to follow up with additional emails to coordinate.

Level of Detail. Focus groups do not afford the in-depth data often collected via individual interviews. Because more people have to provide input in an allotted time frame, fewer questions can be asked, and follow-on probes to gather more information may be limited. For example, in several of our focus groups, we had to skip a question due to time constraints, forcing us to follow up with participants via email to obtain responses. Therefore, there should be careful consideration on whether focus groups can provide the level of detail required for the study investigation and how many questions can be answered to the desired depth. In our case, because of the abbreviated timeline and main intent of data informing a follow-on survey that could validate initial findings, we felt that the data we collected was sufficient, especially with the five focus groups that were able to be scheduled for more than one hour. However, if conducted as a standalone study, the data might not have been enough to reach solid conclusions.

Group Dynamics. Unlike individual interviews, focus groups require careful moderation to navigate group dynamics and ensure all participants have an opportunity to share. We did indeed encounter dominant personalities whose responses had to be politely curtailed and more passive participants who had to be encouraged to offer input. In one of our early focus groups, we observed the participants falling into a round-robin pattern with one participant frequently going last and often agreeing with prior responses, e.g., "Similar to what others say, we do the same within our phishing program" (N01) and "I agree with both of those points" (N01). Therefore, we tried to encourage that participant to answer first in subsequent questions.

Despite several challenges, we discovered benefits of the group format. Participants became fellow questioners when someone would say something that piqued interest or needed clarification. During one of the independent agency focus groups, a participant posed a question to another based on a prior comment: "When you disable people [for not completing their training on time], is that done automatically or is that a manual process at your agency?" (N09). During another focus group, several participants said that they track user incidents as a way to measure the effectiveness of their programs. However, S04 said that he was struggling to understand how they relate incidents to training and asked his fellow participants for clarification. One participant provided an explanation and examples of what his organization does. Not only did this explanation aid the questioner, but it contributed additional data for our research purposes.

Comments could also aid in recall or trigger additional comments that might not have otherwise come out in individual interviews. For example, in one focus group, even though N01 had already provided a response to a question, another participant's comment about "stars" being awarded to employees who demonstrate good security behaviors prompted her to interject and spend an additional minute and a half sharing her organization's approach to incentives.

4.2 Virtual Focus Groups

We found that *virtual* focus groups necessitated adjustments to address challenges arising beyond those typically encountered in traditional, in-person groups.

Less is Better. Because of shorter attention spans and competing distractions when engaging in virtual meetings [?], it is recommended that virtual focus groups should involve fewer participants (as compared to the 5-8 people typical for in-person groups) as well as shorter blocks of time (60 - 90 minutes versus two hours when in-person) [?]. To that end, we scheduled focus groups of 3-5 participants lasting at most 75 minutes. The short, individual meeting with each participant prior to their group allowed us to proactively address administrative and logistical items, freeing up time for more discussion during the actual focus groups.

Selecting a Usable Meeting Platform. We gave careful consideration to the selection of a virtual meeting platform. We desired an application that would be either familiar to most participants or easy-to-learn, required minimal set up (e.g., quick installation of a client) or could be accessed via a browser, allowed for recording, permitted participants to be viewed anonymously (e.g., by changing their display name and turning off the camera), and offered alternative connection options (e.g., dial-in by phone). We also wanted a platform in which we could share presentation slides to serve as a guide and reminder to participants about the current question being discussed. We ultimately selected Webex given that this platform was widely used within the government and met our criteria.

Expecting the Unexpected. In-person focus groups tend to be held in more controlled, predictable settings. However, the online aspect of virtual focus groups introduces new, and sometimes unexpected, challenges. Pre-group meetings with participants afforded an opportunity to guide participants through the use of the platform and troubleshoot technical difficulties. We also encouraged participants to join the group several minutes early in case extra help was needed. However, due to busy schedules, many participants were not able to join early, and several participants still encountered technical issues such as poor connections or speakers or microphones failing to work. To aid these participants, the assistant moderator acted in a troubleshooting role, conversing privately with participants experiencing issues using the meeting chat function or, in some cases, via email.

We also experienced two instances in which unexpected guests initially joined the meeting. In both cases, focus group participants had invited other coworkers to observe. However, because these coworkers had not signed the informed consent, we had to politely ask them to leave the meeting. Although we had previously mentioned that all participants had to sign the informed consent prior to the focus groups, in retrospect, we should have emphasized that the form covered the individual, not the organization.

Moderating Differently. The moderation of virtual focus groups can be especially challenging. Since most of our participants opted to not turn on their cameras, the lack of visual cues and delays in audio or video made turn-taking more difficult for participants and put the moderator at a disadvantage. For example, the moderator could not tell when someone gave an indication they wanted to say something and could not gauge participants' reactions to questions or others' responses. To address these issues, the moderator kept her camera on so as to allow participants to see her own visual cues. She also demonstrated patience when waiting for participants to respond, allowing for several seconds of silence to provide participants adequate time to think through their responses.

5 Suitability for Studying Security Information Workers

In addition to providing general lessons learned, we contribute a discussion on virtual focus group benefits and disadvantages that may be unique to studying SIW or similar populations.

5.1 Benefits

Overcoming Recruitment Challenges. Security information workers are traditionally difficult to recruit [**?**,**?**,**?**]. However, focus groups may provide some benefits that help overcome recruitment challenges.

Accommodating time and environment constraints. SIWs are often overworked with busy schedules and may be part of a specialized and distributed workforce [**?**,**?**]. Although full ethnographic, in situ investigations (e.g., [**?**]) may provide the most comprehensive insights into the work of SIW, these types of studies may be impractical or impossible for a number of reasons, including resources required (for both the research team and the workers) and the sensitivity of SIW work environments that may necessitate significant relationship and trust building to access [**?**,**?**,**?**].

We found that shorter, virtual focus groups (versus in-person sessions) were less intrusive and more palatable considering these workers' time and location constraints. Given our own externally-driven time constraints, the focus groups allowed for gathering input from participants much more efficiently than would have been the case with interviews, allowing us to develop and launch our follow-on survey within our targeted time frame.

Information sharing as an incentive to participate. Given their constraints, SIW must also be properly incentivized to participate. When discussing the challenge of recruiting security professionals, researchers have emphasized the importance of demonstrating the value of participation and addressing reciprocity (what the participant receives in return) [**?**,**?**]. It is common for researchers to extol the value of their research for the social good in recruitment materials, e.g., "Results will inform security awareness training program guidelines to aid federal organizations in the development of effective security awareness programs." However, a more individualized benefit should also be provided.

Offers of monetary compensation for those who participate, though common, may not be enough. Research institutions typically offer smaller amounts (e.g.,

$20 - $25 for an hour-long interview [?]) not commensurate with the $50+ an hour earned on average by SIW in the U.S. [?,?]. In our situation, since we work for a government agency and recruited government employees, we were not able to offer any monetary incentive.

Instead, we found that the very nature of focus groups provided a personal, and perhaps more attractive, incentive to participate. Since information sharing is a natural and important way of working in the security community [?,?], the opportunity to hear about others' experiences during a focus group provided immediate benefit to participants and their organizations versus waiting for results to be captured in a report that may be published many months later.

In our study, we observed multiple participants commenting on the value of hearing what other organizations were doing. For example, at the end of their respective focus groups, a security awareness program lead of a large independent agency stated, "I've picked up some good tidbits from everybody else in the phone call today that I can go back and probably implement immediately" (N08), and a trainer in a sub-component agency remarked, "It's been very interesting to hear everyone's perspectives" (S06). After one participant talked about his organization's security day events in which they bring in external speakers, a CISO complimented the approach: "I'm totally borrowing that idea" (N06). Several participants even exchanged email addresses after their focus groups to continue their discussions.

Navigating a Specialized Field. The security community has its own specialized language, acronyms, and jargon, even more so for specialties within the field and certain sectors like the government. This language may be unfamiliar to researchers with no first-hand experience in the particular security field under investigation. Because of this lack of familiarity, researchers may find it difficult to sort through large amounts of data to find what will be of greatest interest to the community under study [?]. However, focus groups may be particularly valuable in countering this SIW research challenge as they allow experts in the field to self-identify areas of interest. What matters most to SIW comes out naturally and with more passion in group discussions.

We experienced these benefits first-hand. Although two members of our research team had security backgrounds, neither were overly familiar with the terminology used to describe federal security awareness programs and policies nor the unique challenges faced by these programs. We found that the focus groups aided our understanding of the specialized language of federal security awareness professionals, helped us identify areas of interest and particular challenge, and allowed us the opportunity to observe how professionals working in this field interact and communicate. These insights were vital to the creation of the follow-up survey and will greatly inform recommendations resulting from the study as well as how and where we present our findings to be of most value to the federal security awareness community.

5.2 Disadvantages and Challenges

There are also potential downsides to using focus groups with SIW and situations in which they are not appropriate.

Sensitive Topics. Some security topics may not be appropriate for group sharing, or SIW may be reluctant to share information that may reflect poorly on their organizations or themselves [?,?]. For example, in their work studying security practitioners, multiple research groups found that disclosure of organizational security procedures and tools was viewed as being sensitive since these were often proprietary or related to vulnerabilities that are usually closely-held secrets [?,?,?]

Security Mindsets. Security information workers often possess a "security mindset" in which they tend to think like a cyber attacker or adversary [?]. This "peculiar mix of curiosity and paranoia that turns life into a perpetual game of 'what if' questions" [?] may result in SIW being hesitant to participate in recorded virtual meetings or trust other focus group participants. Moreover, SIW may be wary of the researchers or the legitimacy of the study invitation. For example, in our study, despite sending our recruitment invitations from a government email address, one individual requested we send a digitally signed email from our institution to prove that we were not scammers before he would respond any further.

5.3 Mitigating Concerns

There were several mitigations we found effective in alleviating SIW concerns about participating in focus groups.

Establishing Credibility and Rapport. In countering potential mistrust of researchers among SIW, participation rates have been found to rise with the authority and credibility of the requestor [?]. In our experience, our affiliation with an institution having a positive reputation in the security field was helpful for persuading security awareness professionals to participate. The researchers' own security backgrounds further aided in putting people at ease as they believed they were talking to others with similar mindsets. This was also observed in Botta et al. [?] in which the lead researcher had experience as a security practitioner.

Efforts to build rapport with our participants were also valuable in creating a safe, open environment in which participants felt comfortable sharing their honest thoughts and experiences. We began these efforts during the individual, pre-focus group meetings described earlier that allowed us to meet participants before the group. We found that participants were more willing to turn on their cameras for these shorter meetings than in the actual focus groups, providing the opportunity to match names to faces. We were also able to communicate what participants should expect given that many had never participated in a focus group and were not sure what other types of people would be participating. Participants could also ask questions, which assured them that they and their concerns were important to the research team. Rapport-building continued during the focus groups, as the moderator encouraged and thanked participants for their responses throughout the sessions, and followed up afterwards with another "thank you" via email. Overall, the study afforded a way to network and establish relationships that continued after the focus groups, as demonstrated by several participants continuing communications with the research team in the months following.

Demonstrating Protective Measures. To encourage participation in virtual SIW studies, researchers need to explicitly address participant concerns when collecting data online, including how they are protecting security and confidentiality and minimizing harm to participants [**?**].

Clearly communicate protective measures. Details about how participant identities and data will be protected should be included in the informed consent form. In countries or institutions in which informed consent is not required, researchers should still take care to clearly communicate these protections in writing. The importance of this communication was highlighted in other SIW studies. For example, Botta et al. [**?**] discussed their rigorous data protection procedure and how they relayed that to their interview participants. In their focus groups, Gorski et al. [**?**] described how they required focus group participants to sign a consent form detailing data protection practices that included anonymization of identities and destruction of audio recordings and personally identifiable information at the close of the study.

We followed a similar approach. As described previously, the informed consent was reviewed thoroughly during the pre-group meetings, and each participant had to sign and return the consent prior to their focus group. In the informed consent, we were specific about the measures we were taking, which included:

- the use of participant codes (e.g., D04) to link data
- our practice of redacting all names of people and organizations from the transcripts should they accidentally be mentioned
- at the end of the study, destruction of recordings and documents linking participant names and participant codes
- how and where data would be securely stored and transmitted (e.g., on a secured government server, transmitted via an encrypted, secure file transfer application)
- who has access to study data
- the voluntary nature of participation and the participant's right to withdraw from the study at any time
- a participant's right to ask that certain comments they made be removed from the research record

- how data would be reported in aggregate with care not to identify any individuals or organizations

At the conclusion of the pre-focus group meetings, multiple participants commented that they felt more comfortable with the study due to our discussion about the security and privacy procedures.

Use secure technologies that support participant preferences. Using a secure virtual meeting platform that allows for individual privacy is another important mitigation to alleviate SIW concerns. We selected a platform that had no known vulnerabilities or privacy concerns at the time and which would allow participants options for anonymity, such as turning off cameras or changing display names. Most participants elected to keep their cameras off, and several changed their display names to be first name only. Furthermore, introductions at the beginning of the focus groups were not recorded, and participants could choose to not reveal their names or organizations to others during that time. This anonymity option was employed by one participant, who wished for her organization to remain anonymous due to political sensitivities.

We also allowed for options for completing the online demographic survey to accommodate participant preferences. The survey was implemented in Google Forms. However, we provided an alternative if a participant's organization blocked access to Google Workspace or if they felt uncomfortable entering their information online. We sent participants a Microsoft Word version of the survey that they could complete and securely transmit back via encrypted email or a secure file sharing application. Four participants took advantage of this option.

6 Conclusion

Focus groups are a rarely-used research method for studying security information workers. While not appropriate in all situations, focus groups can be a valuable way to collect data efficiently while capitalizing on the security community's proclivity to information sharing. Moving from in-person to virtual focus groups can provide even more benefits, as these reduce the time commitment for busy SIW and allow for the inclusion of individuals from multiple locations. When employing focus groups, careful consideration should be made to address potential SIW security and privacy concerns to encourage participation and ensure a positive participant experience.

Appendix A Focus Group Script

Moderator Introduction and Ground Rules

Welcome to our focus group! I'd like to start off by thanking each of you for taking time to participate today. We'll be here for about *[insert time]* at most. It may be less than that, but we want to allow plenty of time for discussion.

I'm going to lead our discussion today. I will be asking you questions and then moderating our discussion. *[Research team members]* are part of the research team and will be assisting me by taking notes and jumping in with follow-up questions when appropriate.

I'd like to go over a few items that will allow our conversation to flow more freely. *[Share PowerPoint presentation that summarizes ground rules.]*

1. This is a confidential discussion without fear of reprisal or comments being taken out of context. We told you how we are going to protect your confidentiality, and we ask the same of you with respect to others in the group here today.
2. If you don't understand a question or need clarification, please ask.
3. You don't have to answer every question, but we'd like to hear from each of you today as the discussion progresses. There are no "wrong answers," just different opinions and experiences.
4. We'll do our best with turn-taking. Unmute and jump in or click the "raise hand" icon next to your name in the Participants panel.
5. When not talking, please mute yourself to cut down on background noise and feedback.
6. Turning on your camera is optional but can help with conversational cues, but there's no pressure to turn it on.
7. Chat is available if you'd like to share a link or resource with the group or have any technical issues. But if you'd like to say something that contributes directly to the conversation, please say it out loud so that we can capture it on the recording.

Introduction of participants
Opening question: First, we'll do some introductions. These will NOT be recorded. I'll go around to each of you. Please tell everyone your name, organization, and your role with respect to security awareness.

Focus Group Questions
I'm now going to start recording this session. *[Advance through slides for each question.]*

1. ***Introductory question:*** When I say "security awareness and training," what does that mean to you? What comes to mind?
2. ***Transition question:*** Tell me about your organization's approach to security awareness and training. This can include general security awareness for the workforce as well as awareness for specialized job roles.
3. ***Key question:*** How do you decide what topics and approaches to use for your security awareness program?
   (a) *[Probe for sub-components]* What kind of guidance/direction, if any, does your department provide? How much leeway do you have to tailor the training to your own organization?
   (b) *[Probe for department-level agencies]* What kind of guidance/direction, if any, do you push down to sub-components within your department?

4. ***Key question:*** What's working well with your program?
5. ***Key question:*** What's not working as well and why? What are your challenges and concerns with respect to security awareness in your organization?
6. ***Key question:*** How do you determine the effectiveness of your program, if at all?
7. ***Key question:*** If you could have anything or do anything for your security awareness program, what would that be?
   (a) *[Probe]* What would you do to solve the challenges you currently experience?
   (b) *[Probe]* What kinds and formats of resources and information sharing would be most beneficial?
8. ***Key question:*** What knowledge, skills, or competencies do you think are needed for those performing security awareness functions in your organization?
9. ***Ending question:*** If you had one or two pieces of advice for someone just starting a security awareness program in an agency like yours, what would that advice be?
10. ***Ending question:*** Recall that the purpose of our study is to better understand the needs, challenges, practices, and professional competencies of federal security awareness teams and programs. This understanding will lead to the creation of resources for federal security awareness professionals.
11. ***Ending question:*** Is there anything else that we should have talked about, but didn't?

Closing
I will now end the recording. That concludes our focus group. Thanks for attending and talking about these issues. Your comments have been very insightful.

Just a few reminders. If you want something that you said removed from the research record, please let us know. Also, if you think of anything else you didn't get a chance to talk about, feel free to email us.

We really appreciate your participation and thank you again for your time. Have a wonderful day!