An Investigation of Roles, Backgrounds, Knowledge, and Skills of U.S. Government Security Awareness Professionals

Julie M. Haney, Jody L. Jacobs, Susanne M. Furman
National Institute of Standards and Technology
Gaithersburg, MD, 20899, USA
{julie.haney, jody.jacobs, susanne.furman}@nist.gov

ABSTRACT

Security awareness professionals are tasked with implementing security awareness programs within their organizations to assist employees in recognizing and responding to security issues. Prior industry-focused surveys and research studies identified desired skills for these professionals, finding that many are ill-prepared due to gaps in professional skills (e.g., communication, interpersonal) and a lack of recognition of the unique awareness role. However, it is unclear if these findings are similar for security awareness professionals in the United States (U.S.) federal government sector in which awareness plays an important part in teaching employees how to protect sensitive national and citizen data. To identify the current roles, professional backgrounds, and desired knowledge and skills for government security awareness professionals, we conducted a two-phase research study that leveraged focus group and survey methodologies. Insights gained from these results can inform guidance and other initiatives to aid organizations in building security awareness teams with the appropriate competencies. While focused on the U.S. government, findings may also have implications for other sectors and countries.

CCS CONCEPTS

• **Social and professional topics** → **Professional topics** → **Computing profession** → **Computing occupations**

KEYWORDS

security awareness; professionals; work roles; knowledge; skills

ACM Reference format:
J. M. Haney, J. L. Jacobs, and S. M. Furman. 2022. SIG Proceedings Paper in Word Format. In *Proceedings of ACM SIGMIS Computers and People Research, Atlanta, GA USA, June 2022 (SIGMIS CPR'22)*, 4 pages. https://doi.org/XXX.

1 INTRODUCTION

Security awareness programs aim to help employees recognize and respond to security issues, with a goal of achieving long-term behavior change [22]. *Security awareness professionals* are tasked with implementing these programs within their organizations. Prior industry-focused studies [17] [23] identified desired knowledge and skills among security awareness professionals, finding deficiencies in professional skills (e.g., communication, interpersonal). Additionally, a lack of recognition of the unique awareness role and frequent relegation of security awareness duties to be part-time have often led to ill-prepared security awareness professionals.

The development of professionals equipped to implement successful awareness programs is especially critical within national government organizations given the sensitivity and importance of the services these organizations provide for citizens and the frequent cyber-targeting of government employees [12]. However, it is unclear if industry-focused findings about skills apply to the experiences of security awareness professionals in the U.S. government [2] since government hiring requirements for cybersecurity positions may differ from those in private industry [14]. Moreover, there have been questions about whether the "Work Roles" defined in the widely-adopted and U.S. government-mandated National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework) [15] fully capture the security awareness role [19].

To close these gaps, we conducted a two-phased research study. We first collected qualitative data via focus groups of 29 government employees who had security awareness duties or oversaw the programs within their organizations. Focus groups provided an understanding of current awareness teams and the skills-based concepts viewed as most important by participants. These insights then informed a second phase consisting of an online survey with 96 responses. We aimed to answer the following research questions:

> **RQ1:** What NICE Framework Work Roles do U.S. government security awareness professionals currently have?

> **RQ2:** What are the backgrounds of these professionals?

SIGMIS CPR'22, June 2022, Atlanta, GA USA
ACM ISBN XXXX. . . $15.00
https://doi.org/10.1145/XXXX

[2] Throughout this paper, the term "government" signifies the U.S. federal (national-level) government.

RQ3: What are the desired knowledge and skills of government security awareness professionals and teams?

RQ4: Do these professionals feel their security awareness teams have the right mix of knowledge and skills?

Our study makes several contributions. We provide unique insights into the U.S. government security awareness workforce. This understanding can serve as a resource for security awareness professionals, managers, organizational decision makers, and policy makers to improve professional development activities for those with awareness duties and inform hiring decisions for awareness positions. Study results are informing the development of guidance and workforce development efforts [9] to aid organizations in building security awareness teams with the appropriate skillsets. While focused on the U.S. government, findings may also be transferable to security awareness professionals in other sectors and countries.

2 RELATED WORK

2.1 NICE Framework Work Roles

One of our objectives was to identify commonalities in NICE Framework Work Roles assigned to government security awareness professionals. By identifying these roles, we begin to uncover current potential gaps in fit and interpretation for the awareness role.

The widely-adopted NICE Framework provides a common language to define cybersecurity work [15]. The Framework's Work Roles consist of tasks, knowledge, and skills. Private and public sector organizations have utilized these Work Roles to hire cybersecurity workers, build teams to achieve specific objectives, shape career paths, and discover critical gaps in cybersecurity employment [10]. In fact, a 2018 Office of Personnel Management (OPM) memo mandated that federal government agencies "identify and code Federal positions performing information technology, cybersecurity or other cyber-related function…based on the work roles described in the NICE Framework" [13].

2.2 Security Awareness Professionals

Prior research on security awareness professional skills provide a basis for contextualizing our study results. Several groups surveyed security awareness professionals, discovering that the majority performed security awareness duties on a part-time basis without a job title that reflects their duties [17] [23]. Security awareness was viewed as an interdisciplinary role, requiring a mix of technical and professional skills, which are those used by individuals to relate to their environment and the people around them [7].

These observations mirror findings in related research on cybersecurity advocates, those who promote and educate about security best practices [5] [6]. Advocates are grounded in the multi-faceted "change agent" role defined in Diffusion of Innovations Theory [16]. Change agents must be able to effectively communicate and relate to their target audience to encourage adoption of a new technology or process. Likewise, as a type of cybersecurity advocate and change agent, security awareness professionals need to take both technical and non-technical approaches to connect with and empower their audience to make good security choices [5].

Unfortunately, technical specialists who are often assigned security awareness responsibilities may lack professional skills necessary for the job. For example, these individuals may struggle in tailoring security communications to their largely non-technical audiences [17] [20]. Furthermore, a lack of understanding within the security community that awareness is a unique discipline may lead to ill-prepared awareness professionals [1].

While these prior efforts identify issues within the general security awareness workforce, none before us have specifically looked at the U.S. government population.

3 METHODOLOGY

We conducted a mixed-methods research study with two sequential phases from December 2020 to July 2021. Our study is exploratory in that it applies an existing area of study (industry security awareness) to a new context (U.S. government). Exploratory research is meant to produce new ideas but not to test hypotheses or come to concrete conclusions [21]. As such, we identify potential areas of interest and gaps that may require future research.

Our institutional research protections office approved the study. To ensure anonymity, we assigned each participant's data a reference code.

3.1 Focus Groups

We first collected qualitative data via focus groups of government employees knowledgeable about their organizations' security awareness programs either because they had awareness duties or oversaw the programs. The focus groups provided an understanding of how people think and talk about awareness topics and what concepts participants viewed as important.

3.1.1 Design. In developing the focus group protocol, we consulted seven subject matter experts (SMEs), including veteran security awareness professionals and past and current coordinators of government security collaboration forums. The final protocol is included in Appendix A.

We selected a multiple-category design [8] with participants from three categories of organizations: 1) department-level organizations (e.g., U.S. Department of Labor), 2) sub-component agencies, which are semi-autonomous organizations under a department (e.g., Bureau of Labor Statistics under Department of Labor), and 3) independent agencies, which are not in a department (e.g., Federal Trade Commission).

3.1.2 Data Collection and Analysis. We recruited potential focus group participants to represent the diversity of government agencies. We identified participants via: recommendations from the SMEs; our professional contacts; online security-focused government mailing lists; and LinkedIn and Google searches.

We conducted eight virtual focus groups with 29 total participants, representing 28 unique government organizations (one focus group had two individuals from the same organization). Each focus group had 3-5 participants. Two focus groups were with individuals working in departments, three with sub-components, and three with independent agencies. Participants provided informed consent and completed an online survey to collect demographic and organizational information. Focus group sessions lasted 60-75 minutes and were audio-recorded and transcribed.

Data analysis started with coding, which involves categorization of qualitative data [2]. Initially, each member of the research team independently coded a subset of three transcripts (one from each category of focus group) using a preliminary code list based on the focus group questions. We added new codes as needed and met several times to discuss codes and develop a codebook. 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.

3.2 Survey

3.2.1 Design. We developed survey questions and answer options based on focus group data. Five SMEs reviewed an initial draft of the survey, and three security awareness professionals from the focus groups piloted the survey. Subsequently, we made minor adjustments to the survey formatting and wording to improve clarity. The final survey included questions about Work Roles, educational and professional backgrounds, and desired knowledge and skills for awareness teams (Appendix B).

3.2.2 Data Collection and Analysis. Recruitment methods and participation criteria mirrored those in the focus groups. We also sent the survey invitation to prior focus group participants and asked them to forward it to eligible colleagues within and outside their organizations. The survey was open for 18 days, with 96 survey responses in the final dataset. Survey participants represented a diverse range of organizations of different types and sizes. Appendix C contains details on the represented organizations and programs for both the focus groups and survey. Because multiple participants from the same organization may have completed the survey, we cannot ascertain how many unique organizations were represented.

For analysis, we calculated descriptive statistics of quantitative responses using Stata statistical software. Because participants had the option of skipping questions, we include the number of responses (n) for each question. Two researchers performed coding for open-ended responses.

3.3 Limitations

Our study has several limitations. Focus group data may have been impacted by the influence of group dynamics [3]. To mitigate this concern, the moderator tried to ensure that all participants were afforded the opportunity to share their thoughts. In actuality, group dynamics and influence may not necessarily be detrimental. Rather, observations of these interactions can be insightful as they may mimic participants' daily conversations with others [3]. Additionally, pairing focus groups with a survey of a larger population helped validate findings [8].

We also acknowledge that our participants may not represent the full range of government security awareness professionals. However, participants were from a wide range of organizations of varying sizes, types, and programs. Finally, both the focus groups and survey populations largely involved those performing security awareness duties, with fewer managerial positions represented. Therefore, it is difficult to determine the perspectives of those who make workforce hiring or development decisions.

4 PARTICIPANT ROLES AND BACKGROUNDS

In this section, we describe findings for research questions 1 and 2 (**RQ1, RQ2**).

4.1 Current Roles

4.1.1 Security Awareness Duties. We asked participants several questions related to their security awareness duties, including what roles they serve in relation to the security awareness program, how much work time they spend on security awareness duties, and the number of years they have worked in security awareness. Table 1 shows the results. Almost all participants were part-time on security awareness: 93% in the focus groups and 90% in the survey. Overall, 39% of focus group participants and 56% of survey participants spent less than half their time on security awareness.

4.1.2 NICE Framework Work Roles. In the survey, we asked if participants were assigned a NICE Framework Work Role. Half said "Yes," 29% said "No," and 21% responded "I don't know." Those answering affirmatively were then asked which Work Role(s) they were assigned, with 45 responses (Figure 1). Forty-four percent selected two or more Work Roles. Information Systems Security Manager (ISSM) was the most common role but was still held by less than half. Cyber Policy and Strategy Manager and Cyber Workforce Developer and Manager were the next most-selected roles.

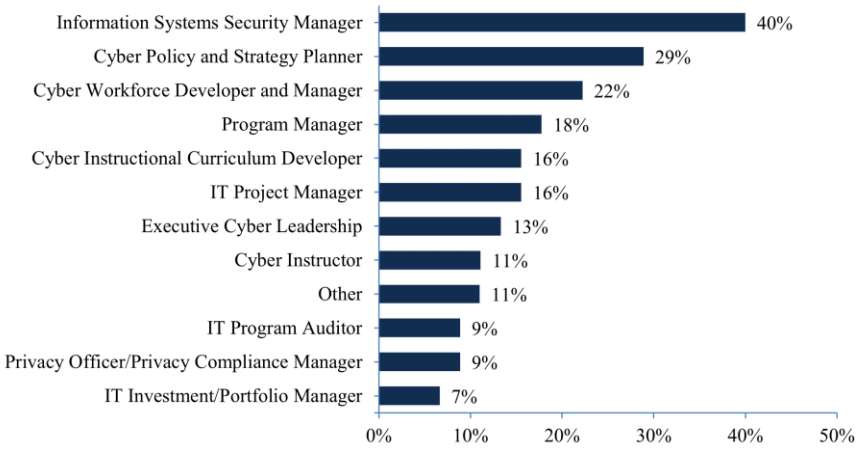

Figure 1: NICE Framework Work Roles (n=45)

Table 1: Participant Demographics Related to Security Awareness Duties

		Focus Groups (n=29)	Survey (n=96)
Security awareness role	Program lead	55.2%	33.3%
	Team member	10.3%	35.4%
	Manager/executive	13.8%	9.4%
	Lead & manager	20.7%	10.4%
	Other	0.0%	11.5%
% work time spent on security awareness duties	Full time	7.1%	10.4%
	75%	17.9%	12.5%
	50%	35.7%	21.9%
	25%	21.4%	17.7%
	Less than 25%	17.9%	37.5%
Security awareness experience	Less than 1 year	0.0%	1.0%
	1 – 5 years	31.0%	25.0%
	6 – 10 years	31.0%	32.3%
	11 – 15 years	27.6%	16.7%
	16 – 20 years	6.9%	14.6%
	20+ years	3.4%	10.4%

We additionally examined which Work Roles were assigned to those holding each security awareness role (lead, member, manager). We found that 40% of those with program lead responsibilities (including those who were both managers and leads) reported as having the ISSM role, one third had the Cyber Workforce Developer and Manager role, and 27% held the Cyber Policy and Strategy Planner role. ISSM was also the predominant Work Role among security awareness team members (61%), followed by Cyber Policy and Strategy Planner (33%) and Program Manager (22%). Note that, given most participants only work part-time on security awareness, some of these Work Roles may not be directly associated with security awareness duties, but rather participants' other duties.

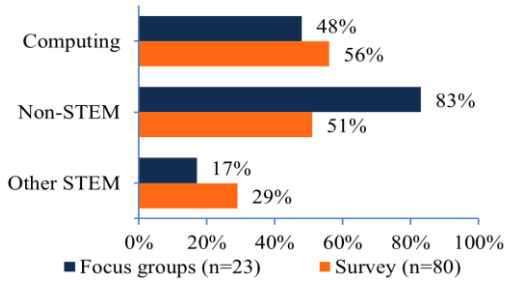

Figure 2: Degree Disciplines

4.2 Professional Backgrounds

4.2.1 Education. We asked participants in which disciplines they held post-secondary school degrees. Because this was an open-ended question, participants may not have entered all their degrees. For example, in some instances, participants only entered an advanced degree (e.g., "MBA") without specifying their bachelor's degree field. Nonetheless, responses provide some insight into formal educational backgrounds. We organized valid responses into three categories:

- **Computing-related fields,** e.g., Computer Science, Computer Engineering, Information Technology (IT), Cybersecurity
- **Other Science, Technology, Engineering, and Mathematics (STEM) fields**, e.g., Chemistry, Mathematics, Mechanical Engineering, Physics
- **Non-STEM fields**, e.g., Business, Psychology, Education

Just under half of focus group participants and a little over half of survey participants listed computing degrees. Over 80% of focus group participants and just over half of survey participants had at least one non-STEM degree (see Figure 2).

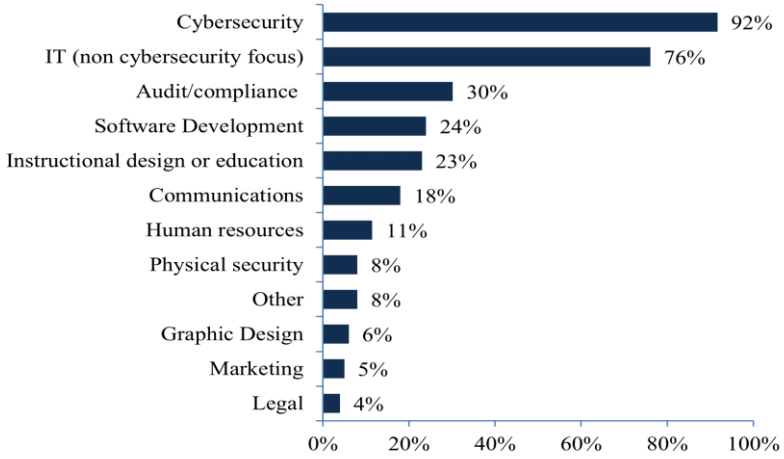

Figure 3: Fields Worked in Professionally (n=96)

4.2.2 Job Experience. In the survey, we asked participants to select fields they had worked in professionally over the course of their career (Figure 3) Almost all participants had worked in cybersecurity and over 75% had worked in other IT jobs. Participants also selected a variety of other non-IT fields, such as instructional design/education, communications, and human resources (HR). Forty percent of respondents had *only* worked in a technical field (cybersecurity, IT, or software development).

5 KNOWLEDGE AND SKILLS

This section describes study results related to **RQ3**, the desired knowledge and skills of security awareness professionals and teams. All statistics are from the survey. Direct quotes from the focus groups and open-ended survey questions are included to further support quantitative results. Quotes from the survey are attributed to individual participants with an anonymous identifier consisting of "Q" followed by the participant number (e.g., Q48). Focus group participants from independent agencies are identified as N01-12, departments as D01-06, and sub-components as S01-11.

5.1 Importance Ratings

We asked participants to rate the importance of their security awareness teams having various knowledge and skills. The specific knowledge and skills included in the survey were identified by participants in the focus groups as being critical to their jobs. The four-point rating scale ranged from "not important at all" to "high importance." In this section, we organize the knowledge and skills into three categories: technical, professional, and contextual.

5.1.1 Technical Knowledge and Skills. Figure 4 shows participant importance ratings for technical knowledge and skills, including cybersecurity, privacy, and IT.

Cybersecurity: Cybersecurity knowledge was rated moderately or highly important by all survey participants. Focus group participants likewise mentioned the need for security awareness professionals to have expertise in cybersecurity. For example, a participant described issues when team members do not have security knowledge:

> "I've had both feds [U.S. federal government employees] and contractors who were great creative content organizers, but they didn't understand enough about cybersecurity to know when they were writing the training. Or even if it was a training session that I wrote and gave it to them, some of it wouldn't make sense to them…It has taken some time to bring non-cybersecurity knowledge individuals up-to-speed." (D06)

Another participant felt that security knowledge was important for collaborating with technical staff: "I think you need someone who is able to converse with network engineers, incident response teams" (S06).

However, not all participants believed deep cybersecurity knowledge was required for their role since they could rely on the expertise of others, such as training vendors or organizational security staff. For example, a program lead said, "I'm not a SME in any of these areas per se. I am more so the coordinator of the training" (S08).

Privacy: Privacy knowledge and skills were rated as moderately or highly important by 96%. Privacy awareness training often was included in annual security awareness training, as discussed by a focus group participant: "We have one annual course…It's security awareness, privacy, incident response, rules of behavior, all these things" (S06). Because of the increased focus on privacy training within government organizations, a participant

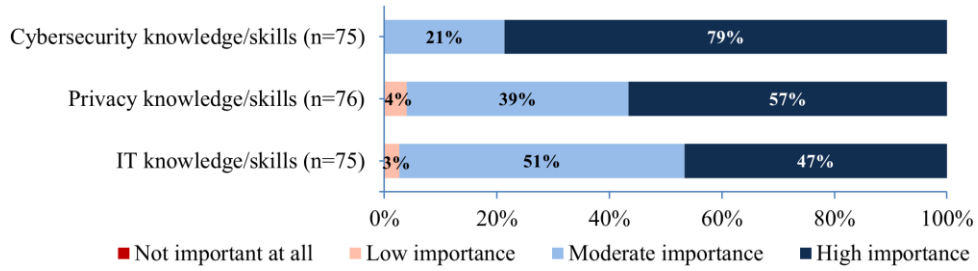

Figure 4: Technical Skills Importance Ratings

expressed concern that there are few resources for ensuring team members have the appropriate knowledge and skills:

> "Outside of the International Association for Privacy Professionals, I don't think there exists a good mechanism or assessment for the privacy workforce as of yet. So, for example, we have cybersecurity personnel who may be inheriting privacy responsibilities, but we don't have a tool yet that will help us gauge what their level of knowledge is with regards to privacy" (S11).

Information technology: IT knowledge and skills were also highly rated (98% moderate/high importance). One participant commented that it was valuable to have team members "who are familiar with different applications and how to use SharePoint and how to administer things in a way that are accessible to people" (D03). Another said, "Having a computer science background has helped me in my position…to automate things" (S11).

5.1.2 Professional Knowledge and Skills. Participants were asked to rate eight professional skills. Figure 5 shows the ratings.

Communication skills: Almost all (99%) rated written communication skills and 96% rated oral communication skills as moderately or highly important. Moderating and group facilitation skills were rated important by fewer (73%).

"Skills to translate technical speak into plain language" (Q40) for a diverse workforce was frequently mentioned as an important communication skill. A focus group participant saw the value of having a team member who is

> "capable of clearly communicating the security awareness…I currently have somebody on staff who is very excited, has fabulous ideas, and can be the most confusing person when trying to communicate" (D04).

Communication skills were also seen as necessary for engaging in discussions about security topics. For example, one participant praised a colleague who is a strong facilitator during security awareness events and had the "ability to really lead those information sessions for the users and answer all the questions" (S05).

Creativity and adaptability: Participants also viewed creativity and being open to adapting the program to workforce needs as important competencies (96% moderate/high

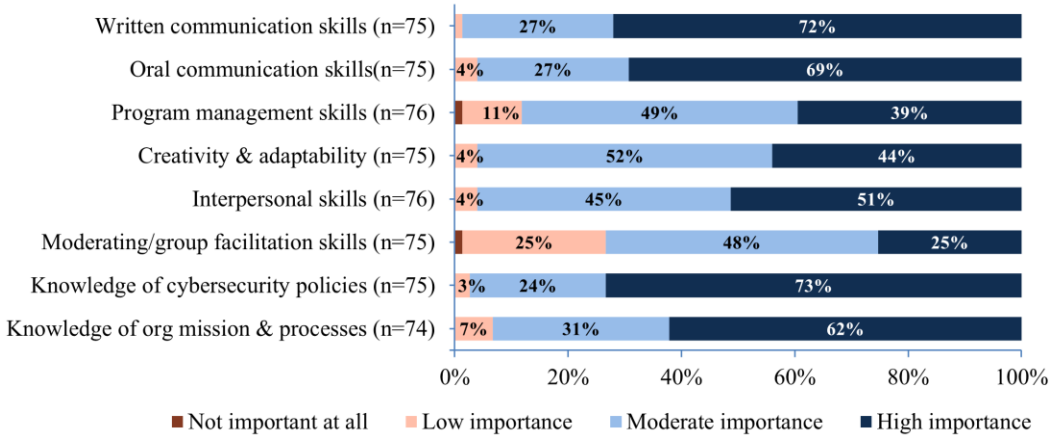

Figure 5: Professional Skills Importance Ratings

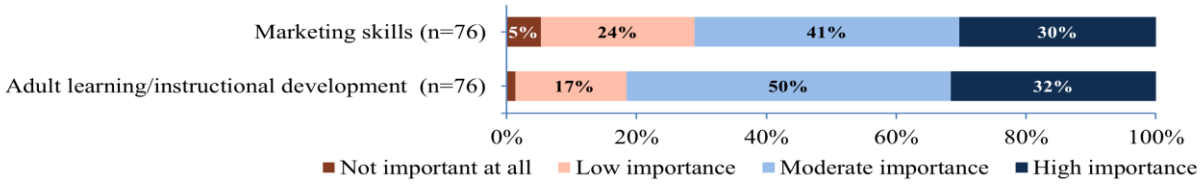

Figure 6: Specialized Skills Importance Ratings

importance). A participant emphasized the value of creativity since "A lot of what you put out is visual…so it needs to be engaging" (D01). Another recommended that security awareness professionals

> "be creative, open minded, and willing to fail and learn from those failures…Cybersecurity and related vulnerabilities are constantly changing, so your program needs to be flexible…Having a solid team that is creative overcomes the lack of funds" (Q35).

Interpersonal skills: Ninety-six percent rated interpersonal skills as moderately or highly important. Focus group participants expanded on these skills, citing empathy, building relationships, collaboration, customer service, patience, and listening skills. A Chief Information Security Officer stated, "You've got to be able to engage other people other than security nerds and professionals" (N07). Another participant emphasized the importance of "customer service skills, just dealing with some of the frustration from our workforce and having to complete these annual type trainings. Being able to be patient and work with them" (S02).

Program management: Eighty-eight percent of survey respondents viewed program management skills as important. When asked about desired skills, a focus group participant said, "project management skills because they need to coordinate with the people who actually do the work day in and day out. So, I don't expect for them to match to everything cybersecurity…if they'd be able to manage the project and manage the people" (N06).

Contextual knowledge: Almost all participants (97%) rated having knowledge of relevant cybersecurity policies as important. One participant remarked, "having knowledge of internal policies and procedures is certainly something that a candidate should have" (S11). Knowledge of organizational context (mission, processes, and dynamics) was rated important by 93%. A survey participant said that knowledge of "organizational politics" (Q70) was necessary. Another commented that it was essential to "understand the mission of the organization and how the security awareness program will strengthen or protect the mission" (Q84).

Other professional knowledge and skills: In an open-ended question, 25 participants offered additional thoughts on other professional knowledge and skills they believed to be of high importance, including analytic and critical thinking skills, psychology, and persuasion. For example, a survey participant noted the need for "critical thinking: the security awareness team needs to be able to understand new attack vectors quickly, process & prioritize them and then get them out to the work force in a targeted manner" (Q71).

5.132 Specialized Knowledge and Skills. We also asked participants to rate the importance of two specialized skillsets from other disciplines that could be applied to security awareness. Figure 6 shows the ratings.

Marketing skills: Almost three-quarters of survey participants rated marketing skills as moderately/highly important. A focus group participant commented on the value of having a person with a marketing background on their security awareness team:

> "We have people that have a kind of graphic design or marketing type background, which we think is important so that people can actually understand, or things are appealing in a way that people want to read them" (D03).

Adult learning or instructional development knowledge and skills: Having skills in learning or instructional development was rated as moderately/highly important by 82%. During the focus groups, several participants mentioned the value of these skills. One said, "I think having that foundation in education and understanding teaching techniques and skills and things like that would come before the cybersecurity knowledge" (N04). Another commented, "some type of learning management background is also useful…Oftentimes, it's not only about the information. It's how you present the information" (S11).

5.2 Mix of Knowledge and Skills Within Teams

To answer **RQ4**, participants rated their agreement for the statement "In my organization, the security awareness team has the right mix of necessary knowledge and skills" on a five-point scale ranging from "strongly disagree" to "strongly agree." Sixty-one percent agreed/strongly agreed that their team had the right mix of skills and knowledge, while 20% disagreed/strongly disagreed (see Figure 7).

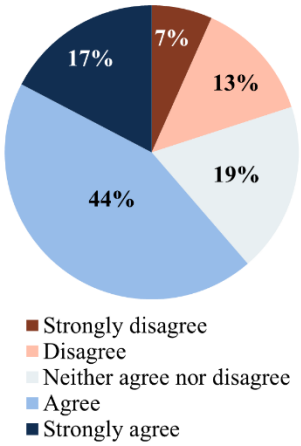

Figure 7: Agreement with Statement: "In my organization, the security awareness team has the right mix of necessary knowledge and skills."

Obtaining the knowledge and skills necessary for a security awareness role may not be trivial. In another survey question, 70% agreed or strongly agreed that they had been provided adequate professional development opportunities to help them in their security awareness role. However, a few focus group participants expressed frustrations. One observed:

> "Our agency recently obtained licenses within an online learning service…They have training that is associated with each of the NICE cybersecurity Work Roles. So, I was like, 'Okay, great, I'm going to go find my Work Role,' which is that learning coordinator one…That was the one role that they didn't have any courses associated with. And when I asked the question, I was like, 'Was this an oversight?' They [were] like, 'No.' It was just so mile-wide, inch-deep type of stuff that they really didn't have courses for this role" (S08).

Instead of having one individual with all requisite knowledge, several participants believed that organizations should build expertise by having multidisciplinary teams. One said, "If you're going to be producing any type of awareness content in any type of volume above the bare-bones minimum, you need a team" (D06). Another discussed their own multidisciplinary team:

> "I have industrial design specialists. I have people who can design, are very artful, creative people. I have people who can run a learning management system…good project managers. I have cybersecurity professionals." (D01)

However, not all organizations had the resources to build teams with the desired mix of skills. Therefore, they augmented the security awareness team by involving others in the organization. A focus group participant commented, "There was also someone else that came on the team part time…that had the HR experience. So, they were very helpful in helping me to navigate whatever issues that may come from the personnel requirements" (N09). Another participant discussed their organization's solution to expand the reach of the security awareness team into field offices within their large organization:

> "We also have a cyber guardians program…We have people across the country…that actually take a look at their facilities. If they see things that aren't right, they approach the employee and let them know that you shouldn't be plugging in a USB device or anything into the company computer. If they walk away from their computer, leave it unlocked, they address that" (N05).

6 DISCUSSION

6.1 Work Roles

Standardized work roles can be instrumental in helping individuals and organizations understand the necessary competencies for cybersecurity positions. However, we observed a lack of commonality of assigned NICE Framework Work Roles. Half of survey participants said they were not assigned to a NICE Framework Work Role or did not know if they were assigned. Assuming that government organizations have indeed met the OPM requirements to identify Work Roles [13], our findings may suggest that organizations have not adequately communicated these roles to their security awareness workforce. Furthermore, while acknowledging that participants may have Work Roles reflecting their non-awareness duties, we found there was no single Work Role assigned to a majority of non-managerial participants. This may suggest a lack of standardization in how organizations interpret the Work Roles in the context of security awareness.

These findings may have professional development implications not just for the government sector, but also for other organizations using the NICE Framework. Without a common Work Role reference, individuals may not know what knowledge and skills are necessary for their security awareness jobs. Organizations may not be able to properly gauge qualifications when hiring people to these positions or determine professional development activities for incumbents.

It may also be that no current Work Role adequately represents the duties and necessary knowledge and skills of security awareness professionals. To remedy this, a new NICE

Framework Work Role called a "Security Awareness and Communications Manager" has been proposed [19]. This role places less emphasis on technical knowledge and skills and more on professional skills such as communications, partnering, and project management. Spurred in part by this proposal and informed by preliminary results of our study, NICE is currently exploring the addition of a security awareness Work Role to the NICE Framework [9].

6.2 Skills Diversity Within Teams

As suggested in prior research that gleaned needed skills for security awareness, cybersecurity advocate, and change agent positions [5] [15] [17] [23], we found that government security awareness professionals believe their jobs require a diverse mix of both technical and professional knowledge and skills. These skills are sometimes attained through prior formal education or job experiences. This was evidenced by the educational diversity represented by participants, with over 80% of focus group participants and over half of survey participants holding formal degrees in non-computing disciplines. In addition, 60% of survey respondents had worked in a non-technical job. This diversity contrasted with a large, worldwide industry survey of security awareness professionals (conducted by SANS) in which fewer than 20% had a non-technical background [17]. Future research may be warranted to explore this contrast as it is currently unclear as to whether this is due to differences between government and industry sectors.

Based on their survey findings, SANS suggested that a purely technical background may be detrimental for the interdisciplinary security awareness role [17]. For example, highly technical people may have difficulty translating highly technical concepts into language understandable by a broad audience. In addition, it may be the case that security awareness duties may be a lesser priority for the majority who have other, non-awareness cybersecurity duties. However, neither the SANS survey nor our study attempted to gauge whether security awareness professionals with purely technical backgrounds were an actual detriment to organizational security outcomes.

Nevertheless, since our discoveries are rooted in the experiences of security awareness professionals, they may have implications for security awareness workforce hiring and development. Organizations may need to be more open to hiring candidates from less-technical backgrounds. They can also focus on building a team having all requisite skills, rather than trying to find all requirements in one or two individuals. While having a dedicated team of 2-3 individuals may be preferred [17], for resource-constrained organizations, awareness professionals can collaborate with other organizational groups to draw on specialized expertise.

Organizations can also support experiential and training opportunities for developing professional skills in addition to technology-focused skills. Security awareness professionals should be afforded the opportunity to share with other professionals via forums or conferences, e.g., the Federal Information Security Educators [11], EDUCAUSE [4], or SANS Security Awareness [18] communities.

7 CONCLUSION

Via focus groups and a follow-on survey, we explored the work roles, professional backgrounds, and desired knowledge and skills of U.S. government security awareness professionals. We found that organizations are inconsistent in assigning NICE Framework Work Roles to their security awareness professionals, which may indicate that current Work Roles are not standardized to the desired mix of technical and professional skills. Insights gained from these results are informing guidance and other initiatives to aid government organizations in building security awareness teams with the appropriate skillsets. While focused on the U.S. government, findings may also have implications for organizational security awareness professionals in other sectors and countries, especially since many non-government and foreign organizations use the NICE Framework.

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.

ACKNOWLEDGEMENTS

We would like to thank the anonymous reviewers and our colleagues Shanée Dawkins and Danielle Santos for their input that helped improved this paper.

REFERENCES

[1] Maria Bada, M. Angela Sasse, and Jason RC Nurse. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? https://arxiv.org/ftp/arxiv/papers/1901/1901.02672. pdf.

[2] Juliet Corbin and Anselm L. Strauss. 2015. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (4th ed.). Sage, Thousand Oaks, CA.

[3] Jennifer Cyr. 2017. The unique utility of focus groups for mixed-methods research. *Political Science & Politics* 50, 4 (2017), 1038.

[4] EDUCAUSE. 2022. Cybersecurity Program. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program.

[5] Julie M. Haney and Wayne G. Lutters. 2018. "It's Scary...It's Confusing...It's Dull": How cybersecurity advocates overcome negative perceptions of security. In *Proceedings of the Symposium on Usable Privacy and Security*. USENIX, Baltimore, MD, 411–425.

[6] Julie M. Haney and Wayne G. Lutters. 2019. Motivating cybersecurity advocates: Implications for recruitment and retention. In *Proceedings of the 2019 Computers and People Research Conference*. ACM, Nashville, TN, 109–117.

[7] Indeed. 2021. 15 Professional Skills (Plus Definition and Tips). https://www.indeed.com/career-advice/career-development/professional-skills.

[8] Richard A. Krueger and Mary Anne Casey. 2015. *Focus Groups: A Practical Guide for Applied Research*. Sage.

[9] National Initiative for Cybersecurity Education. 2021. Developing a Workforce for Security Awareness and Behavior Change: A NICE Framework Workshop. https://www.nist.gov/system/files/documents/2021/09/29/FinalSlides_AwarenessWorkshop_28sep2021%20%28508%20Compliant%29.pdf

[10] National Institute of Standards and Technology. 2020. NICE framework resource center. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework- resource-center.

[11] National Institute of Standards and Technology. 2022. FISSEA – Federal Information Security Educators. https://csrc.nist.gov/projects/fissea.

[12] Office of Management and Budget, 2020. Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2020. https://www.whitehouse.gov/wp-content/uploads/2021/05/FY-2020-FISMA-Report-to-Congress.pdf

[13] Office of Personnel Management. 2018. Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need. https://chcoc.gov/content/guidance-identifying-addressing-and-reporting-cybersecurity-work-roles-critical-need.

[14] Office of Personnel Management. 2022. GS-2210: Information Technology Management Series. https://www.opm.gov/policy-data-oversight/classification-qualifications/general-schedule-qualification-standards/0300/gs-2210-information-technology-management-series/

[15] Rodney Petersen, Danielle Santos, Matthew C. Smith, Karen A. Wetzel, and Greg Witte. 2020. NIST Special Publication 800-181 Revision 1: Workforce Framework for Cybersecurity (NICE Framework). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

[16] Everett M. Rogers. 2003. *Diffusion of Innovations*. Simon and Schuster.

[17] SANS. 2021. 2021 SANS Security Awareness Report: Managing Human Cyber Risk. https://www.sans.org/security-awareness-training/resources/reports/ sareport-2021/.

[18] SANS. 2022. SANS Security Awareness Resources. https://www.sans.org/ security-awareness-training/resources/.

[19] Lance Spitzner. 2019. NIST NICE Work Role Description for Security Awareness and Communications Manager. https://www.sans.org/blog/nist-nice-work-role-description-for-security-awareness-and-communications-manager/.

[20] Geordie Stewart and David Lacey. 2012. Death by a Thousand Facts: Criticising the Technocratic Approach to Information Security Awareness. *Information Management & Computer Security* 20, 1 (2012), 29–38.

[21] Richard Swedberg. 2020. Exploratory Research. In *The production of knowledge: Enhancing progress in social science*, Colin Elman, John Gerring, and James Mahoney (Eds.). Cambridge University Press, London.

[22] Mark Wilson and Joan Hash. 2003. NIST Special Publication 800-50 Building an Information Technology Security Awareness Program. https://nvlpubs.nist.gov/ nistpubs/Legacy/SP/nistspecialpublication800-50.pdf.

[23] Ben Woelk. 2015. The Successful Security Awareness Professional: Foundational Skills and Continuing Education Strategies. https://library.educause.edu/~/media/files/library/2016/8/erb1608.pdf.

A FOCUS GROUP QUESTIONS

Although the focus groups covered a wide range of security awareness topics, this paper only reports on a subset related to knowledge and skills.

1. When I say "security awareness and training," what does that mean to you? What comes to mind?
2. 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. 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. What's working well with your program?
5. What's not working as well and why? What are your challenges and concerns with respect to security awareness in your organization?
6. How do you determine the effectiveness of your program, if at all?
7. 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. What knowledge, skills, or competencies do you think are needed for those performing security awareness functions in your organization?
9. 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. 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. Is there anything else that we should have talked about, but didn't?

B SURVEY QUESTIONS

The following is the subset of survey questions relevant to this paper.

1. Has your organization assigned you to one or more NICE (National Initiative for Cybersecurity Education) Framework cybersecurity work roles?
    - Yes
    - No
    - I don't know
2. [If yes:] Which of the following NICE Framework cybersecurity work roles have you been assigned? Check all that apply.
    - ☐ Cyber Instructional Curriculum Developer
    - ☐ Cyber Instructor
    - ☐ Cyber Policy and Strategy Manager
    - ☐ Cyber Workforce Developer and Manager
    - ☐ Executive Cyber Leadership
    - ☐ Information Systems Security Manager
    - ☐ IT Investment/Portfolio Manager
    - ☐ IT Program Auditor
    - ☐ IT Project Manager
    - ☐ Privacy Officer/Privacy Compliance Manager
    - ☐ Program Manager
    - ☐ Other:

3. What is your role with respect to the security awareness program at your organization? Check all that apply.
   - □ I am the lead for the program responsible for implementation or management
   - □ I am a member of the security awareness team but not the lead
   - □ I oversee the contract for the program
   - □ I am a manager or executive who oversees and is responsible for the program administratively
   - □ Other:
4. How many years have you been involved with security awareness programs in your current organization and in other organizations (rounded to the nearest year)? Include time spent working on security awareness training and managing/overseeing security awareness programs.
   - ◦ Less than 1 year
   - ◦ 1 5 years
   - ◦ 6 10 years
   - ◦ 11 15 years
   - ◦ 16 20 years
   - ◦ More than 20 years
5. Approximately what percentage of your time at work do you spend on tasks related to the security awareness program?
   - ◦ Full-time
   - ◦ 75%
   - ◦ 50%
   - ◦ 25%
   - ◦ Less than 25%
   - ◦ Other:
6. If you have any degrees beyond a high school degree, in which disciplines/fields are your degrees?
7. In which of the following fields have you worked professionally? Check all that apply.
   - □ Cybersecurity
   - □ Information technology (not a cybersecurity focus)
   - □ Software development
   - □ Communications
   - □ Marketing
   - □ Graphic design
   - □ Human resources
   - □ Legal
   - □ Audit/compliance
   - □ Instructional design or education
   - □ Psychology or sociology
   - □ Physical security
   - □ Other:
8. Please rate the level of importance of having the following knowledge and skills in a security awareness team in an organization like yours? (not important at all – low importance – moderate importance – high importance)
   - Cybersecurity knowledge and skills
   - Privacy knowledge and skills
   - Information technology knowledge and skills
   - Written communication skills
   - Oral communication skills
   - Marketing skills
   - Adult learning/instructional development knowledge and skills
   - Program management skills
   - Creativity and adaptability
   - Interpersonal skills
   - Moderating/group facilitation skills
   - Knowledge of cybersecurity policies
   - Knowledge of organizational mission, processes, and dynamics
9. Other than the knowledge and skills listed above, please list any other knowledge and skills you think are of high importance for a security awareness team:
10. Please rate your agreement with the following statement: In my organization, the security awareness team has the right mix of necessary knowledge and skills. (strongly disagree – disagree – neither agree nor disagree – agree – strongly agree)
11. Please rate your agreement with the following statement: In my organization, I have been provided adequate professional development opportunities to help me in my security awareness role. (strongly disagree – disagree – neither agree nor disagree – agree – strongly agree)

C REPRESENTED ORGANIZATIONS

In both study phases, participants indicated the type and size of the organizations in which they worked as well as the number of people covered by the organization's security awareness program. This was an important distinction from organization size since government organizations may also be required to provide security awareness training to their contractors (non-government individuals) or have some government employees not be required to complete training. We collected data on the number of individuals having security awareness duties within the organizations. For simplicity, we refer to the individuals with security awareness program duties as a "team" while acknowledging that the concept of a security awareness team may not exist in all organizations. We also note that team size does not necessarily equate to full time equivalents.

Table 2 shows the diversity of organizations and programs represented in the study. Note that, although there were 29 focus group participants, two were from the same organization. Therefore, only 28 unique organizations were represented.

Table 2: Represented Organizations

		Focus Groups (n = 28)	Survey (n = 96)
Organization type	Independent agency	42.9%	35.4%
	Department	21.%	32.3%
	Sub-component	35.7%	31.3%
Organization size (# government employees)	Less than 100	0.0%	8.3%
	100 - 999	7.1%	9.4%
	1,000 – 4,999	32.1%	29.2%
	5,000 – 9,999	10.7%	10.4%
	10,000 – 29,000	17.9%	14.6%
	30,000 – 49,999	14.3%	3.1%
	50,000+	17.9%	21.9%
	Don't know	0.0%	3.1%
Security awareness program size (# government & contractor employees covered by the program)	Less than 100	0.0%	9.5%
	100 - 999	0.0%	12.6%
	1,000 – 4,999	25.0%	25.3%
	5,000 – 9,999	7.1%	7.4%
	10,000 – 29,000	21.4%	18.9%
	30,000 – 49,999	10.7%	2.1%
	50,000+	32.1%	22.1%
	Don't know	3.6%	0.0%
Security awareness team size (# government & contractor employees)	Very small (1-2)	25%	33.8%
	Small (3-4)	53.6%	29.7%
	Medium (6-10)	10.7%	14.9%
	Large (11+)	10.7%	21.6%