NISTIR 8420B

The Federal Cybersecurity Awareness Workforce

Professional Backgrounds, Knowledge, Skills, and Development Activities

Julie Haney
Jody Jacobs
Susanne Furman
Fernando Barrientos

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8420B

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8420B

The Federal Cybersecurity Awareness Workforce

Professional Backgrounds, Knowledge, Skills, and Development Activities

Julie Haney
Jody Jacobs
Susanne Furman
Fernando Barrientos
Information Access Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8420B

March 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8420B
36 pages (March 2022)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8420B

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

Organizational cybersecurity awareness (hereafter shortened to "security awareness") programs may experience a number of challenges, including lack of funding and staff with the appropriate knowledge and skills to manage an effective program. While prior surveys and research have examined programs in the private sector, there is little understanding of whether these findings also apply within the U.S. government. To address this gap and better understand the needs, challenges, practices, and necessary competencies of federal security awareness teams and programs, NIST conducted a research study that leveraged both qualitative and quantitative methodologies. This companion document to NISTIR 8420 "Federal Cybersecurity Awareness Programs: A Mixed Methods Research Study" reports on a subset of study results focused on identifying the current job classifications, roles, and desired knowledge and skills for security awareness professionals within the federal government. Insights gained from these results are informing guidance and other initiatives to aid federal organizations in building security awareness teams with the appropriate competencies. While focused on the U.S. government, findings may also have implications for organizational security awareness professionals in other sectors.

Keywords

cybersecurity; cybersecurity awareness; focus groups; knowledge; mixed methods; professional development; security professionals; skills; survey; training; usable cybersecurity; work roles

Executive Summary

Security awareness programs aim to assist employees in recognizing and responding to security issues with a goal of achieving long-term behavior changes. Security awareness professionals are individuals who are tasked with managing and executing the security awareness programs within their organizations. Prior industry surveys and research studies have identified challenges security awareness professionals face. Many members of security awareness teams perform security awareness duties on a part-time basis without a job title that reflects their duties, and they may lack sufficient professional skills (e.g., communications, relationship-building) that were viewed as essential in security awareness roles. In addition, the lack of understanding that security awareness is a unique discipline may lead to ill-prepared awareness professionals. However, it is unclear if these challenges also apply to security awareness professionals in the United States (U.S.) government.

To better understand the needs, challenges, practices, and necessary competencies of federal security awareness teams and programs, we conducted a "mixed methods" research study that leveraged both qualitative and quantitative methodologies. We first conducted eight focus groups of federal employees who had security awareness duties or were managers or executives who oversaw the programs within their organizations. The focus groups then informed an online survey completed by 96 federal employees with security awareness responsibilities.

The research background and methodologies for these two phases are described in detail in NISTIR 8420 "Federal Cybersecurity Awareness Programs: A Mixed Methods Research Study." This companion document reports on a subset of results focused on identifying the current job classifications, security awareness roles, and desired knowledge and skills for security awareness professionals within the federal government. The following is a high-level overview of these results, with statistics from the survey unless otherwise indicated.

Security Awareness Duties and Work Roles

- 90% of survey participants performed security awareness duties on a part-time basis, with just over 55% spending 25% or less of their time. Focus group participants had similar allocations: 93% part-time and 39% spending 25% of less time.
- 50% of survey participants either did not know or were not sure of their National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework) Work Role. This was despite the Federal Cybersecurity Workforce Assessment Act which requires federal agencies to assign the NICE Framework coding structure to its cybersecurity and information technology (IT) positions. Those participants who knew their Work Role identified 11 unique Work Roles.

Professional Backgrounds

- Participants were diverse in their educational backgrounds, with 83% from focus group and 51% from the survey indicating that they have at least one non-STEM degree.
- 92% of survey participants had worked in cybersecurity positions and 76% had worked in IT jobs that did not have a cybersecurity focus. Less than 25% had worked in a variety of

other fields, including non-IT fields such as instructional design and education, communications, and human resources. We found that 40% of participants had only ever worked in a technical field (cybersecurity, IT, or software development).

Knowledge and Skills

- Survey participants rated the importance of having specific knowledge and skills represented on their teams. Not surprisingly, cybersecurity, IT, and privacy knowledge and skills were overwhelming rated as important (over 95% for each). However, many professional knowledge and skills – interpersonal skills, communication skills, creativity, and contextual knowledge of the organization and policies – were also rated highly by over 95% of survey participants. Focus group participants particularly emphasized the importance of oral and written communication skills, for example, being able to translate highly technical information into a language understandable by a diverse workforce.
- 61% of survey participants agreed that they have the right mix of skills and abilities within their security awareness teams. Participants mentioned it may be difficult to find a single individual who possesses all the necessary skills. Therefore, building a multi-disciplinary team or reaching out to other components in an organization, such as the human resources or public relations departments, can be beneficial.
- 70% of survey participants agreed that they were provided with adequate professional development opportunities. However, due to budgetary constraints or lack of specific role-based training, a few participants expressed difficulties obtaining security awareness-specific trainings.

This report can serve as a resource for federal security awareness professionals, organizational decision makers, policy makers, and guidance developers to: improve professional development activities for those with security awareness duties; inform hiring decisions for security awareness positions; and advocate for federal security awareness professionals. The results may also be valuable to security awareness professionals outside of the government who face similar challenges.

Table of Contents

List of Appendices

List of Figures

1 Introduction

Cybersecurity awareness (hereafter shortened to "security awareness") programs aim to help employees recognize and appropriately respond to security issues, with a goal of achieving long-term behavior change [WILSON]. Security awareness professionals are individuals who are tasked with managing and executing the security awareness programs within their organizations. Prior industry surveys and research studies have identified challenges security awareness professionals face. Many professionals perform security awareness duties on a part-time basis without a job title that reflects their duties, and they may lack sufficient professional skills (e.g., communications, relationship-building) that are viewed as essential in security awareness roles [SANS][WOELK]. In addition, the lack of understanding that security awareness is a unique discipline may lead to ill-prepared awareness professionals [BADA]. However, it is unclear if these challenges also apply to security awareness professionals in the United States (U.S.) government.

To better understand the needs, challenges, practices, and necessary competencies of federal security awareness teams and programs, we conducted a "mixed methods" research study that leveraged both qualitative and quantitative methodologies. The National Institute of Standards and Technology (NIST) Research Protections Office reviewed the protocol for this research project (ITL-2020-0238) and determined it meets the criteria for "exempt human subjects research" as defined in 15 CFR 27, the Common Rule for the Protection of Human Subjects.

We conducted the study in two sequential phases from December 2020 – July 2021. In the first phase, we collected qualitative data via eight focus groups with federal employees who had security awareness duties or were managers or executives who oversaw the programs within their organizations. Focus groups provided an understanding of current security awareness approaches within the government and the concepts and challenges viewed as most important by participants. These insights then informed a second phase consisting of a follow-on, online survey completed by 96 federal employees involved in their security awareness programs.

The research background and methodologies (study design, recruitment, data collection, and data analysis) employed for these two phases are described in detail in NISTIR 8420 "Federal Cybersecurity Awareness Programs: A Mixed Methods Research Study." This companion document, NISTIR 8420B, reports on a subset of results focused on identifying the current job classifications, security awareness roles, National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework) Work Roles, and desired knowledge and skills for security awareness professionals within the federal government. Specifically, these results answer the following research questions:

1. What job classifications and NICE Work Roles do federal security awareness professionals currently have?
2. What are the professional backgrounds of these professionals?
3. What are the desired knowledge and skills of federal security awareness professionals?
4. What professional development activities do these professionals engage in and do they feel those are adequate?

Study results will inform guidance to aid federal organizations in building security awareness teams with the appropriate competencies.

The report is organized as follows. Section 2 describes conventions used when reporting results. Section 3 reports participant demographics, including security awareness roles, job classifications and NICE Framework Work Roles, and professional backgrounds. Section 4 describes study results related to knowledge, skills, and professional development activities of federal security awareness professionals. Section 5 summarizes key takeaways from the study.

The target audience of this report consists of individuals involved with federal security awareness programs. The report can serve as a resource for federal security awareness professionals, managers, and organizational decision makers to: improve professional development activities for those with security awareness duties; inform hiring decisions for security awareness positions; and advocate for their organizations' security awareness professionals. Those who develop and manage federal security awareness guidance, policies, sharing forums, and initiatives may also benefit. In addition, the report may be valuable to security awareness professionals outside of the government.

2 Reporting Conventions

Because participants had the option of skipping survey questions, participants may not have answered all questions. Therefore, we include the number of responses (n) for each question with our summary statistics.

Inferential statistics were calculated for select questions to look for differences between the following groups:

- ***Organization type***
  - Department
  - Sub-component
  - Independent agency

- ***Program size*** - based on number of employees (federal employees and contractors) covered under the organization's security awareness program
  - Small – Less than 1,000 employees
  - Medium – 1,000 – 4,999 employees
  - Large – 5,000 – 29,999 employees
  - Very Large – 30,000+ employees

- ***Team size*** - the number of individuals directly tasked with security awareness duties
  - Very small – 1-2 people
  - Small – 3-5 people
  - Medium – 6 – 10 people
  - Large – More than 10 people

See NISTIR 8420 for details on statistical tests and level of significance.

The results of statistical analyses are highlighted in gray text boxes, with **statements of statistically significant results in bold**.

Direct quotes from the focus groups and open-ended questions in the survey are included where appropriate to further support or provide more insight into quantitative survey results. Quotes from the survey are attributed to individual survey participants by denoting an anonymous identifier consisting of "Q" followed by the participant number (e.g., Q48). In attributing quotes to focus group participants, individuals from Independent agencies are identified as N01 – N12, Department-level organizations as D01 – D06, and Sub-components as S01 – S11.

3 Professional Demographics

Focus group participants were asked to complete a short online survey to collect demographic information, including their current job roles and professional backgrounds. Survey participants provided similar information within the survey itself. In a few instances, demographic questions not included in the focus groups were added in the survey and vice-versa. For example, in the survey, we added questions to better understand which NICE Framework Work Roles are commonly assigned to those involved in federal security awareness programs. In this section, we differentiate between data collected in the focus groups and the survey.

The demographics in this report focus on a set of data relevant to discovering the current roles and professional backgrounds of those working in security awareness within the U.S. government. Other data related to the organizations and teams represented in the study (e.g., types of organizations, organization and program size, security awareness team size) are reported in NISTIR 8420.

3.1 Security Awareness Duties

3.1.1 Security Awareness Roles and Percentage of Time

Security awareness roles and percentage of time spent on security awareness duties are described in NISTIR 8420. Because these demographics are useful for contextualizing the results in this report, for ease of reference, Figure 1 summarizes the represented roles and Figure 2 summarizes percentages of time (one focus group participant did not answer this question).

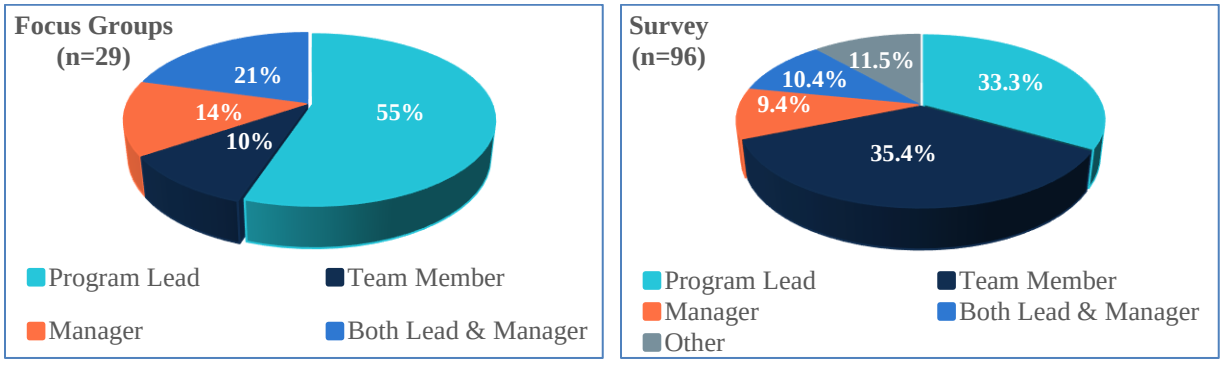

Figure 1: Security awareness roles - Focus groups (left), Survey (right)

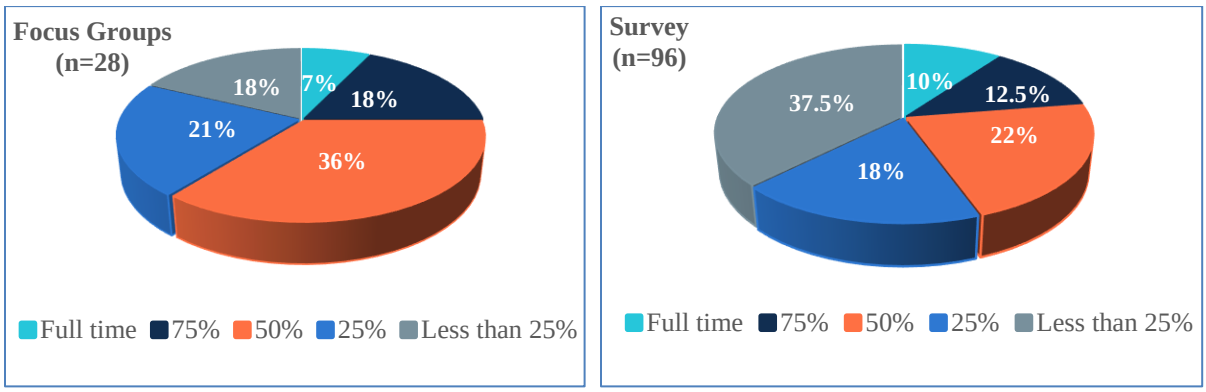

Figure 2: Time spent on security awareness duties - Focus groups (left), Survey (right)

3.1.2 Years of Security Awareness Experience

Focus Groups

When asked how long they had been involved in security awareness programs, all focus group participants indicated that they had at least one year of experience, with 69% having at least 6 years of experience. Figure 3 shows the distribution of years of experience.

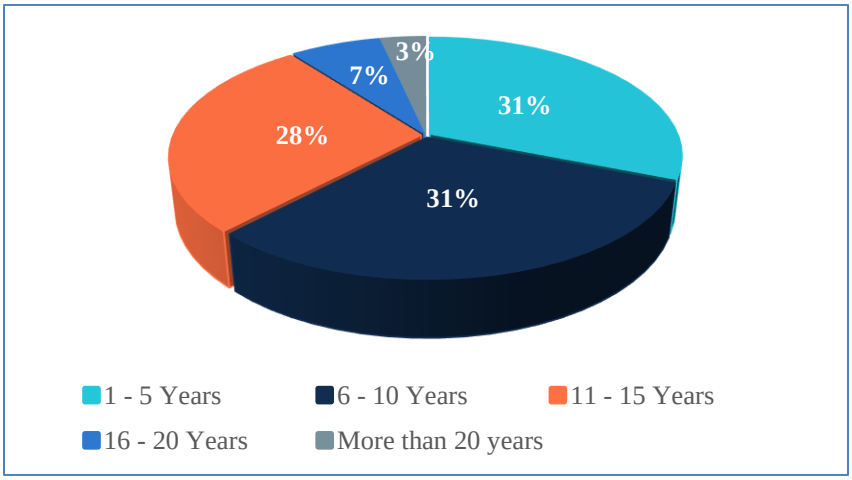

Figure 3: Focus Groups - Years involved with security awareness programs (n=29)

Survey

Participants tended to be quite experienced working with security awareness programs, with 74% indicating six or more years of experience. Figure 4 shows the distribution of years of experience. Only one participant had less than one year of experience.

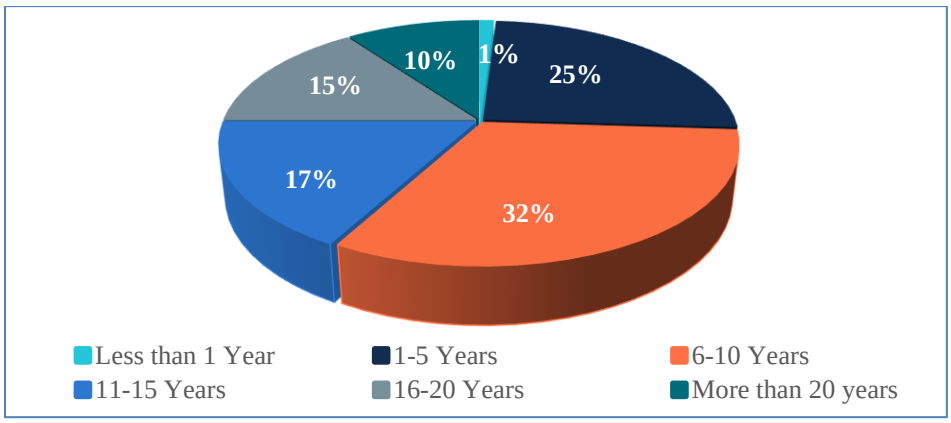

Figure 4: Survey - Years involved with security awareness programs (n=96)

3.2 Work Roles

This section describes the job classifications and NICE Framework Work Roles held by participants at the time of the study.

3.2.1 Job Classifications

Focus Groups

Focus group participants indicated their job title in a fill-in-the-blank style question. Because of the open-endedness of the responses, job titles were of varying granularity. Some were job classifications (e.g., "IT Specialist") while others named their functional role (e.g., "Manager, Awareness and Training"). We categorized the job titles of the 29 participants into the following breakdown (job category followed by number of participants):

- Training Lead/Manager (n=9)
- IT Specialist (n=8)
- Other Security (n=4)
- Supervisory IT Specialist (n=2)
- Chief Information Security Officer (CISO) (n=3)
- Other Manager (n=3)

In an open-ended question, we also asked what other job functions or roles the participants had in addition to their security awareness responsibilities. All but two participants had other substantial cybersecurity duties beyond awareness training, for example, incident response, supply chain risk management, audits and compliance, policy, information systems security management, privacy awareness and training, cybersecurity role-based training, and project management.

Survey

The survey deviated from the focus group in that it asked about official job classification and roles in "select all that apply" (rather than open-ended) questions. As shown in Figure 5, when selecting their job classification, half selected IT Specialist (Cybersecurity). Supervisory IT Specialist (Cybersecurity) was the second most common response at 20%. Figure 5 shows all

job classification responses. Three job classifications listed in the survey were not selected by any participants: IT Specialist (Other), Computer Scientist, and Supervisory IT Specialist (Other).

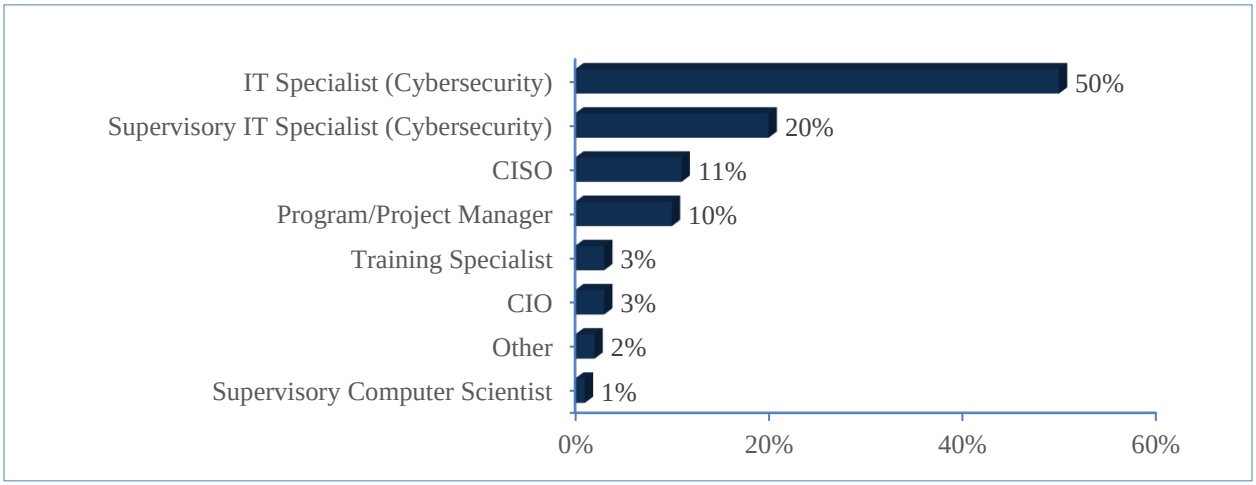

Figure 5: Survey - Job classification (n=94)

Figure 6, Figure 7, Figure 8, and Figure 9 show the job classification breakdowns by security awareness role. More than half of participants identifying as Program Lead or Team Member had the job classification of IT Specialist (Cybersecurity). Unsurprisingly, all but one of the nine managers selected supervisory or executive job classifications. Job classifications for those acting as both a Lead and Manager were distributed across six different classifications.

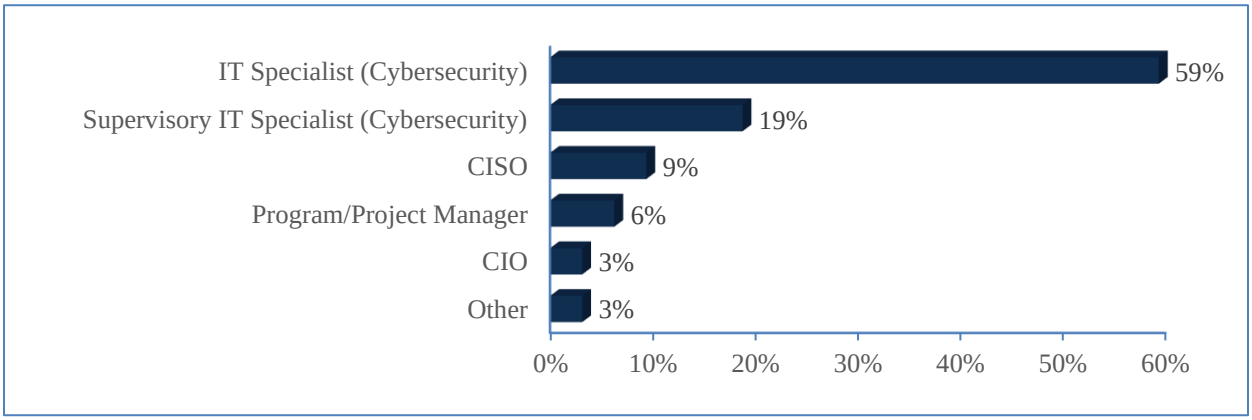

Figure 6: Survey - Job classifications of Program Leads (n=32)

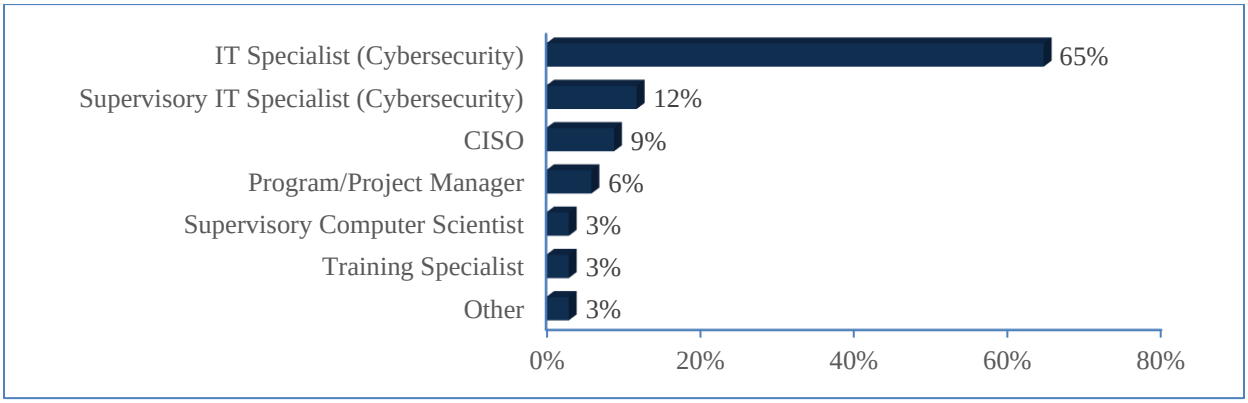

Figure 7: Survey - Job classifications of Team Members (n=34)

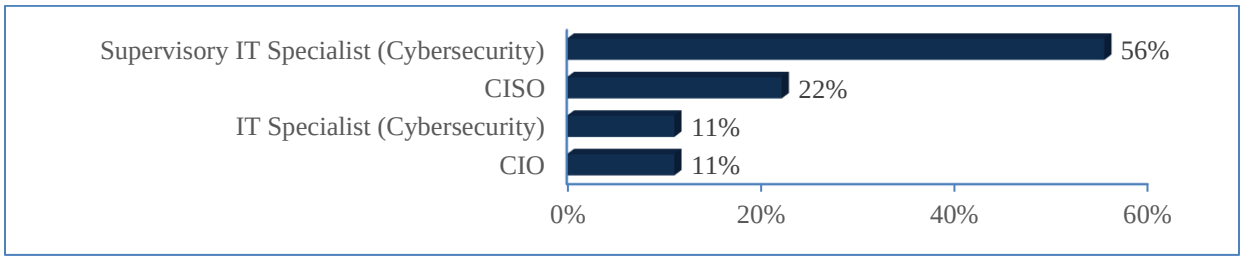

Figure 8: Survey - Job classifications of Managers/Executives (n=9)

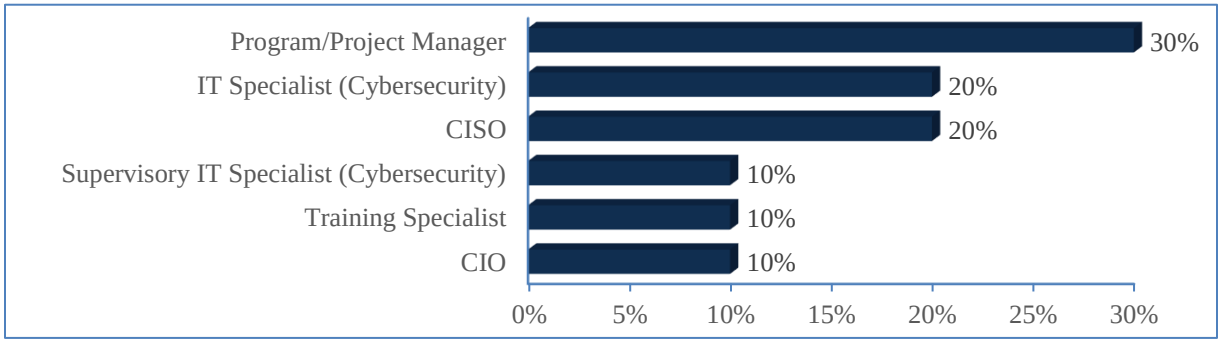

Figure 9: Survey - Job classifications of participants who are both Program Leads and Managers/Executives (n=10)

3.2.2 NICE Framework Work Roles

In the survey only, we asked participants if they were assigned a NICE Framework Work Role. Of the 96 participants who responded, 50% said "Yes," 29% said "No," and 21% responded "I don't know" (Figure 10).

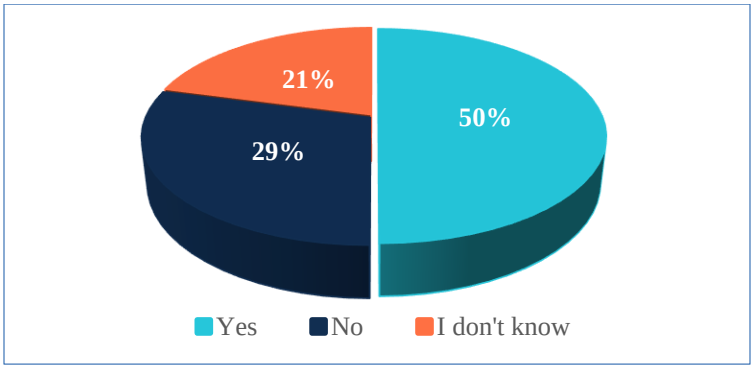

Figure 10: Survey - Assigned to a NICE Framework Work Role (n=96)

Those who answered affirmatively were then asked which Work Role(s) they were assigned, with 45 participants responding. Twenty participants (44%) selected two or more Work Roles. Figure 11 shows the distribution of Work Roles. Information Systems Security Manager was the most common role at 40%, followed by Cyber Policy and Strategy Manager (29%) and Cyber Workforce Developer and Manager (22%). Nine other Work Roles were selected.

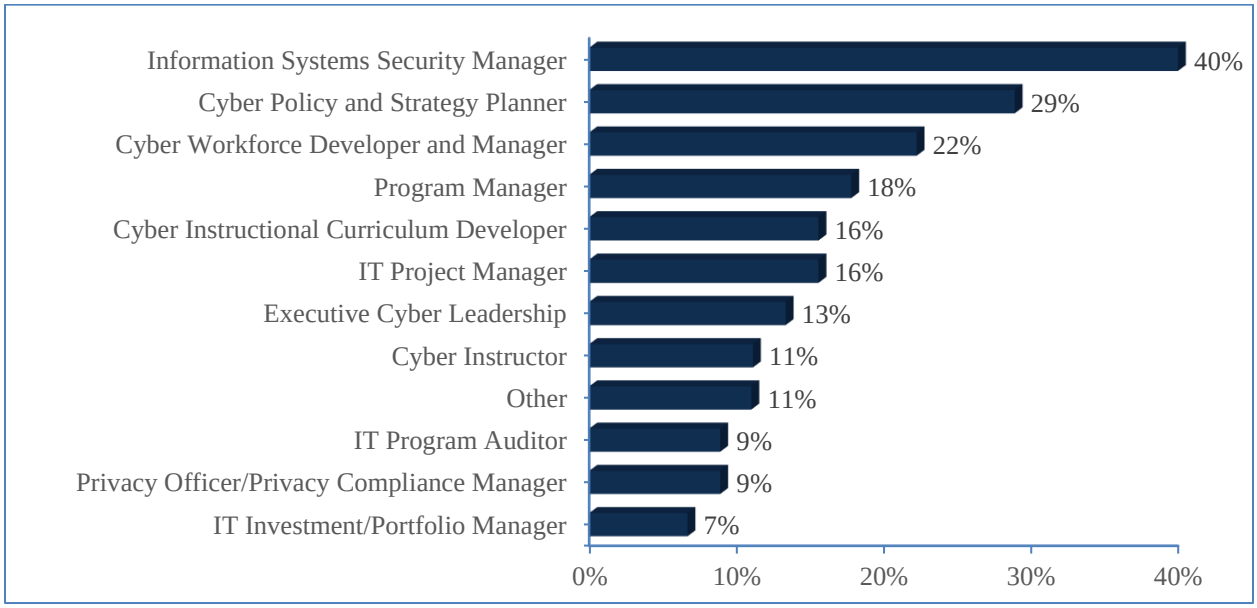

Figure 11: Survey - NICE Framework Work Roles (n=45)

We also looked more granularly at which Work Roles were assigned to the various security awareness roles (Table 1). Of particular interest, 40% of those responding who had program lead responsibilities reported as having the Information Systems Security Manager (ISSM) role, one third had the Cyber Workforce Developer and Manager role, and 27% held the Cyber Policy and Strategy Planner role. ISSM was the predominant Work Role among security awareness team members (61%), followed by Cyber Policy and Strategy Planner (33%). Note that, given most participants only work part-time on security awareness, some of these Work Roles may not be directly associated with participants' security awareness duties, but rather their other cybersecurity duties.

Table 1: Survey – Number of NICE Framework Work Roles for each security awareness role (n=45)

	Program Lead	Team Member	Manager or Executive	Program Lead & Manager	Other Role
Cyber Instructional Curriculum Developer	3	3	1	0	0
Cyber Instructor	2	1	1	0	1
Cyber Policy and Strategy Planner	3	6	1	1	2
Cyber Workforce Developer and Manager	5	3	1	0	1
Executive Cyber Leadership	1	0	2	3	0
Information Systems Security Manager	3	11	0	3	1
IT Investment/Portfolio Manager	1	1	0	1	0
IT Program Auditor	1	1	0	0	2
IT Project Manager	1	2	2	1	1
Privacy Officer or Privacy Compliance Manager	2	1	0	0	1
Program Manager	1	4	0	2	1
Other	0	1	1	0	3
	(n=10)	**(n=18)**	**(n=5)**	**(n=5)**	**(n=7)**

3.3 Professional Backgrounds

Participants answered questions about their professional backgrounds, including their formal education, job experience, experience working in security awareness, and industry-recognized certifications.

3.3.1 Education

Focus Groups

The focus group demographic survey asked about participants' educational background. All but three of the focus group participants had a bachelor's degree or higher (Figure 12).

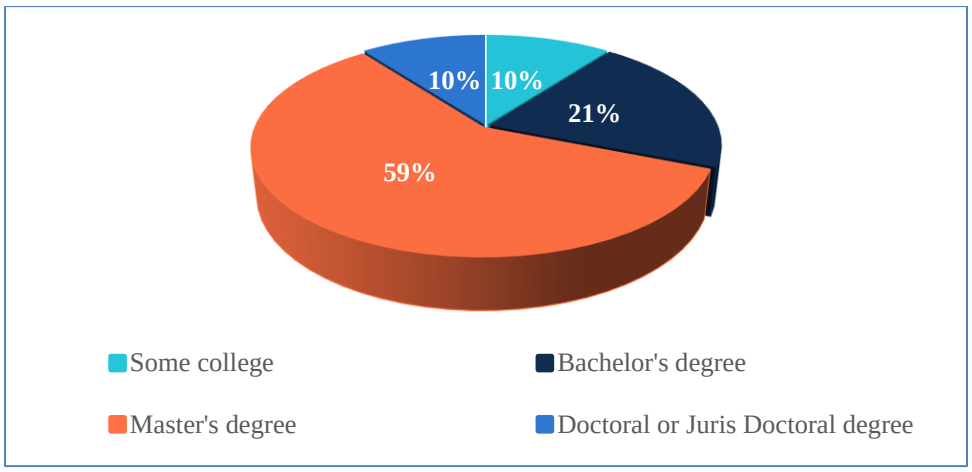

Figure 12: Focus Groups - Level of education (n=29)

Participants were also asked in which disciplines or fields they held post-secondary school degrees. We organized responses to this open-ended question into three categories:

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

Of the 23 valid responses, 83% of participants had at least one non-STEM degree, and just under half (48%) held a degree in a computing-related field (Figure 13). Note that, because this was an open-ended question, participants may not have entered in all their degrees if they had received multiple degrees. For example, in some instances, participants only entered an advanced degree (e.g., "MBA") without specifying their bachelor's degree field. Responses that only indicated a type of degree (e.g., "BS") without a discipline were excluded from the count.

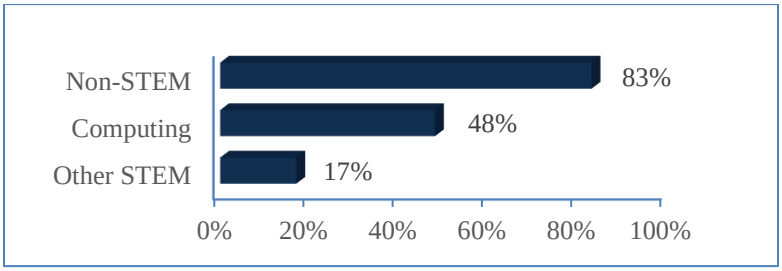

Figure 13: Focus Groups - Degree disciplines (n=23)

Survey

In the survey, we were more interested in degree disciplines versus the type of degree. Figure 14 shows represented degree disciplines among survey participants as indicated in an open-ended question. Of the 80 participants responding, 56% had at least one computing degree, and 51% had a degree in a non-STEM field. Twenty-two participants (28%) earned at least one degree in

both a computing/STEM discipline and a non-STEM discipline.

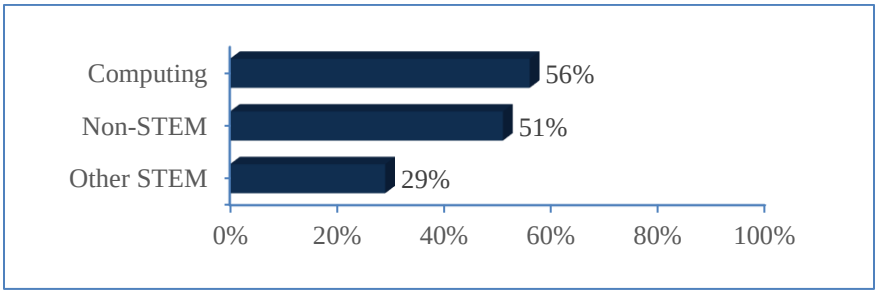

Figure 14: Survey - Degree disciplines (n=80)

3.3.2 Job Experience

Focus Groups

In the focus group demographic survey, we asked participants how many years they had worked as government employees, in their current organization, and in a cybersecurity role. Eighty-three percent (n=24) of focus group participants had worked as federal employees for more than five years (21% for more than 20 years). Seventy-two percent (n=21) had worked in their current organization for more than five years (14% for more than 20 years). All but three participants had worked in some kind of cybersecurity role for at least 6 years, with 28% with more than 20 years of cybersecurity experience.

Survey

In the survey, we opted to focus more on capturing the diversity of participants' professional backgrounds rather than number of years having worked in the government or an organization. Participants selected fields they had worked in professionally over the course of their career (Figure 15). Almost all participants (92%) have worked in cybersecurity and 76% have worked in IT jobs that did not have a cybersecurity focus. Participants also selected a variety of other fields, including non-IT fields such as instructional design/education, communications, and human resources. We found that 40% of participants (n = 38) had only worked in a technical field (cybersecurity, IT, or software development).

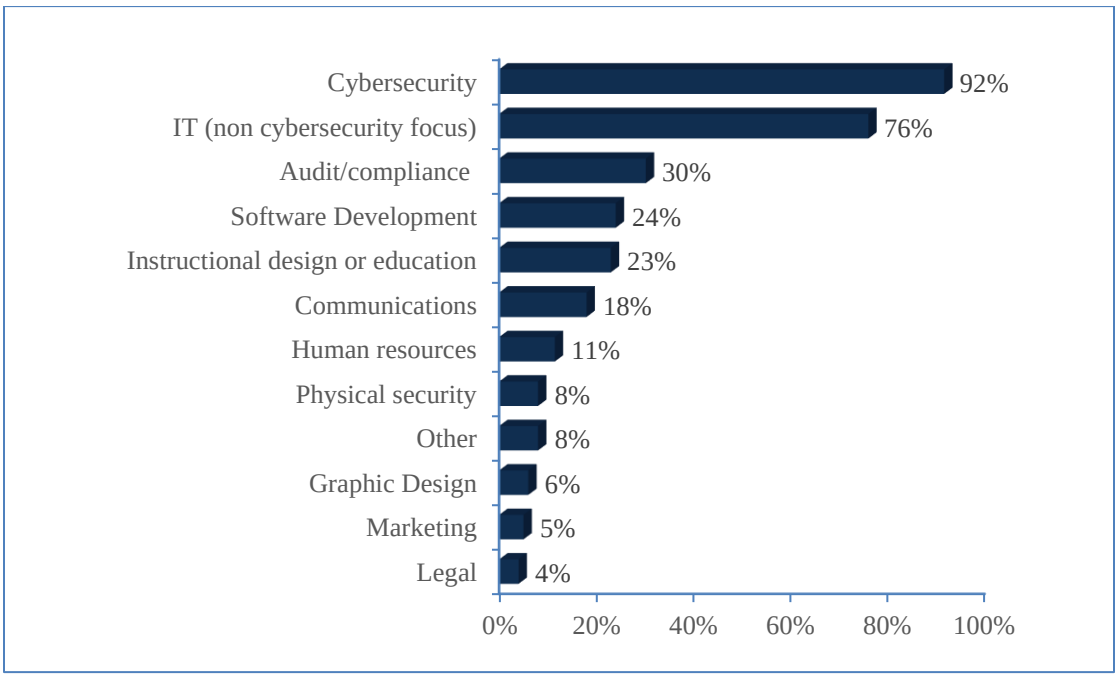

Figure 15: Survey - Fields worked in professionally (n=96)

3.3.3 Industry-recognized Certifications

Focus Groups

In an open-ended question, participants were asked what, if any, industry-recognized certifications they held (Figure 16). The Certified Information Systems Security Professional (CISSP) certification was the most common certification at 65%. Certified Information Security Manager (CISM) was the second most commonly held certification at 29%. The "Other" category includes certifications only mentioned by one or two individuals.

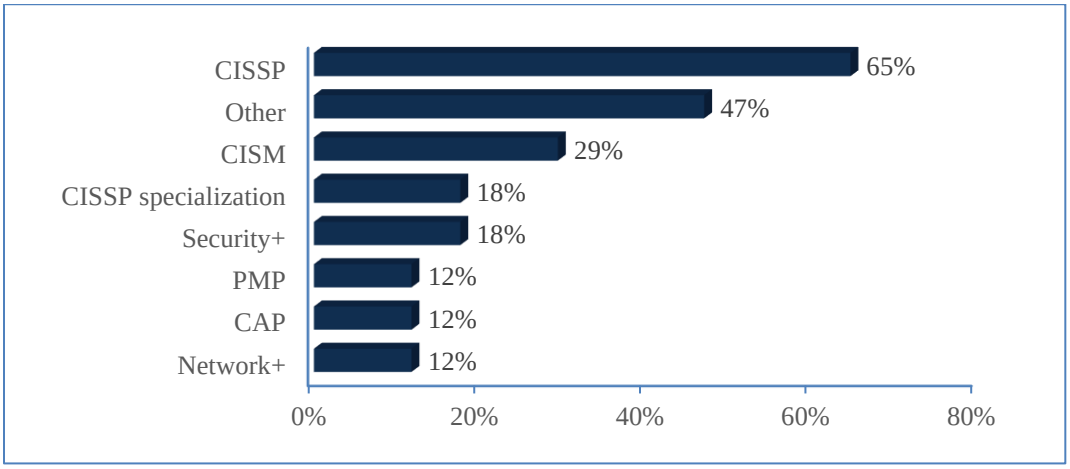

Figure 16: Focus Groups - Industry-recognized certifications (n=17)

Survey

Survey participants were able to select certifications from a list as well as being able to enter other certifications in an "Other" field. As depicted in Figure 17, the Certified Information Systems Security Professional (CISSP) was the most commonly held certification at 46%, followed by Security+ at 29%. Twenty percent did not have an industry-recognized certification.

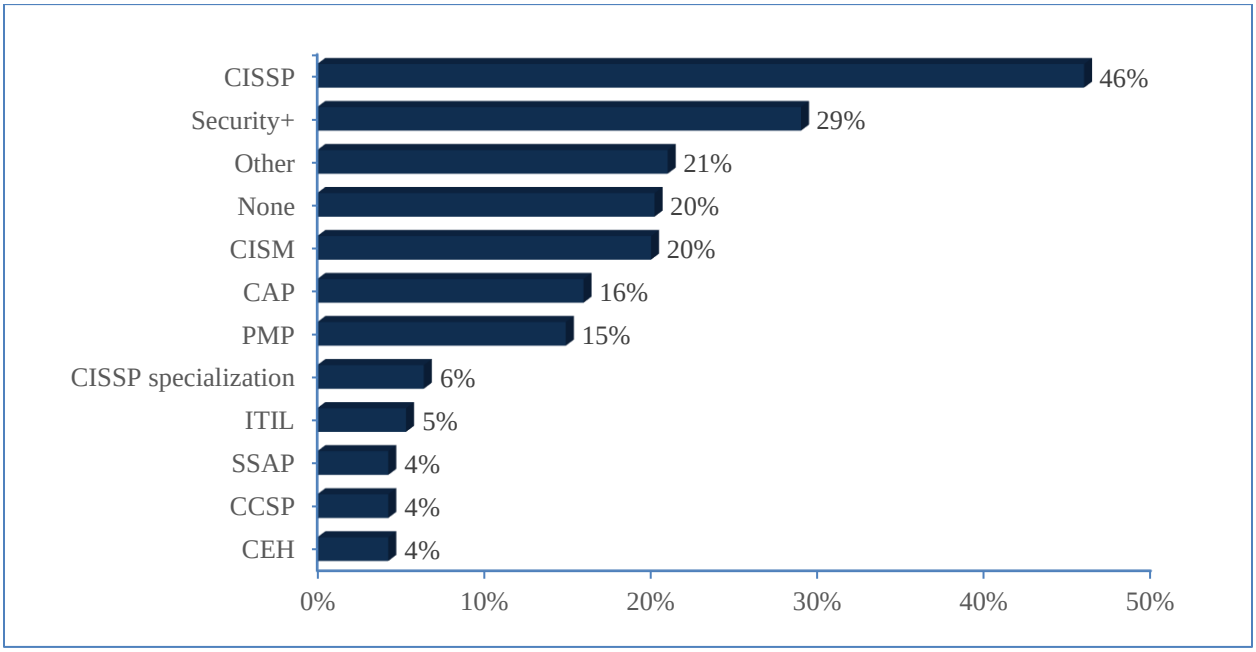

Figure 17: Survey - Industry-recognized certifications (n=94)

4 Knowledge, Skills, and Professional Development

This section describes study results related to the knowledge, skills, and professional development opportunities of security awareness professionals. The results are organized according to the survey structure, with all statistics based on survey data.

4.1 Knowledge and Skills Importance Ratings

We asked participants to rate the importance of having certain knowledge and skills held by individuals in their security awareness teams on a four-point scale ranging from "not important at all" to "high importance." These knowledge and skills were originally identified in the focus groups. In a follow-on, open-ended question, participants also had the opportunity to add other knowledge or skills they believed to be of high importance. Twenty-five participants offered additional thoughts, although some input just provided additional detail on knowledge/skills categories already included in the rating question. In this section, we organize the knowledge and skills into three categories – technical, professional, and contextual – and provide participant quotes for additional detail. When reporting those skills deemed "important," we are referring to those marked as having high or moderate importance by participants.

4.1.1 Technical Knowledge and Skills

Figure 18 shows how survey participants rated the importance of several categories of technical

knowledge and skills: cybersecurity, privacy, and IT.

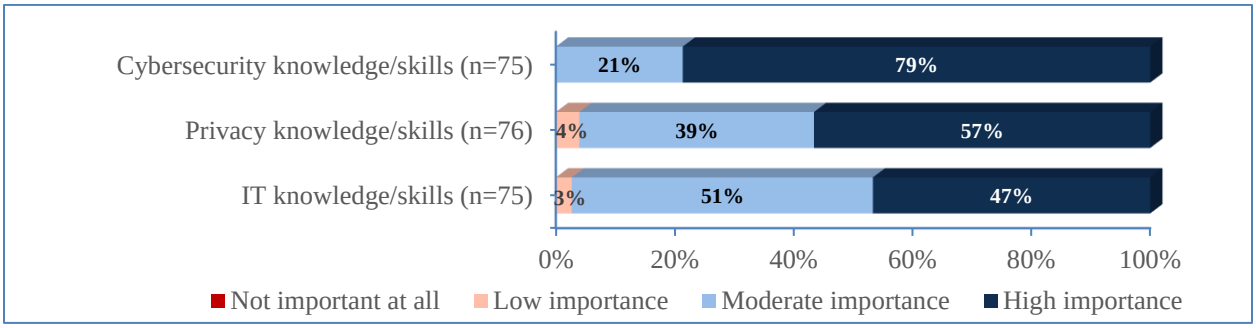

Figure 18: Technical knowledge/skills importance ratings

Cybersecurity: Not surprisingly given the focus of the role, cybersecurity knowledge was overall rated the most important (100% moderate/high importance) and had the largest percentage of participants rating it as having high importance (79%).

When asked what knowledge or skills was needed for security awareness professionals, focus group participants often mentioned expertise in cybersecurity:

> "[It's important to have] a fundamental cybersecurity knowledge component because I've had both feds 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… And it has taken some time to bring non-cybersecurity knowledge individuals up to speed to where I can say, 'Here, write me something on this subject,' and it'll come back in a fairly decent format." (D06)

> "I think you need someone who is able to converse with network engineers, incident response teams, and when those people start talking about like FIPS [Federal Information Processing Standards] encryption or cloud infrastructure or something like that." (S06)

> "I would say that having a background in cybersecurity does help when you are developing content because I believe that people should have an understanding of the content they're developing." (S10)

However, not all participants felt that deep cybersecurity knowledge was required for the security awareness role:

> "We can rely on [training vendors], and all the other companies for that [cybersecurity-specific] material." (N03)

> "I'm not a SME [subject matter expert] in any of these areas per se. I am more so the coordinator of the training so I can connect these needs with those that need

> the information. But I am not a Unix administrator. I am not a network engineer. So, I can take my best guess. I have a CISSP. I know what you're talking about. I'm just not a SME in that area. I cannot deliver the training myself." (S08)

Information Technology: IT knowledge and skills were also highly rated (98% moderate/high importance). Participants often valued team members with knowledge of IT (e.g., software, network technologies) and associated data analysis, which they could apply to the program:

> "[We need] people who are familiar with different applications and how to use SharePoint and how to administer things in a way that are accessible to people. My example now is trying to update our materials so that they can be viewed on mobile devices. We're lucky to have somebody on our team who's technical and can actually implement that." (D03)

> "Having a computer science background has helped me in my position. And it's helped me from collaborating with others and pushing my own agenda to automate things, to collaborating with others on content, and so forth." (S11)

> "Cybersecurity is not as important as maybe a basic understanding of data and how to manipulate it so that we can report on this and see how effective the things are." (N03)

Privacy: Privacy knowledge and skills were likewise rated as important (96% moderate/high importance). Privacy training often falls under the duties of security awareness teams:

> "We have one annual course, and we've bundled a lot of training requirements in this one course. It's security awareness, privacy, incident response, rules of behavior, all these things in one course." (S06)

> "We have a privacy awareness day during the year." (S03)

> "In the ISA [information security awareness] training, we included PII [personally identifiable information] and privacy training. However, recently, I guess, this year, we created a PII course that will be mandated by everyone in our agency." (S09)

Because of the increased focus on privacy training within government organizations, one focus group participant expressed concern that there are few resources for ensuring team members have the appropriate privacy-related knowledge and skills:

> "For this relatively newer area, which has to do with the competency of privacy workforce, currently, 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)

4.1.2 Professional Knowledge and Skills

Professional knowledge and skills (sometimes called "soft" or "non-technical" skills) are those used by individuals to relate to their environment and the people around them [INDEED]. In the survey, participants were asked to rate the following professional skills: written and oral communication skills; program management; creativity and adaptability; interpersonal skills; moderating and group facilitation; and contextual knowledge of cybersecurity policies and the organization's mission, processes, and dynamics. Figure 19 shows ratings for each item.

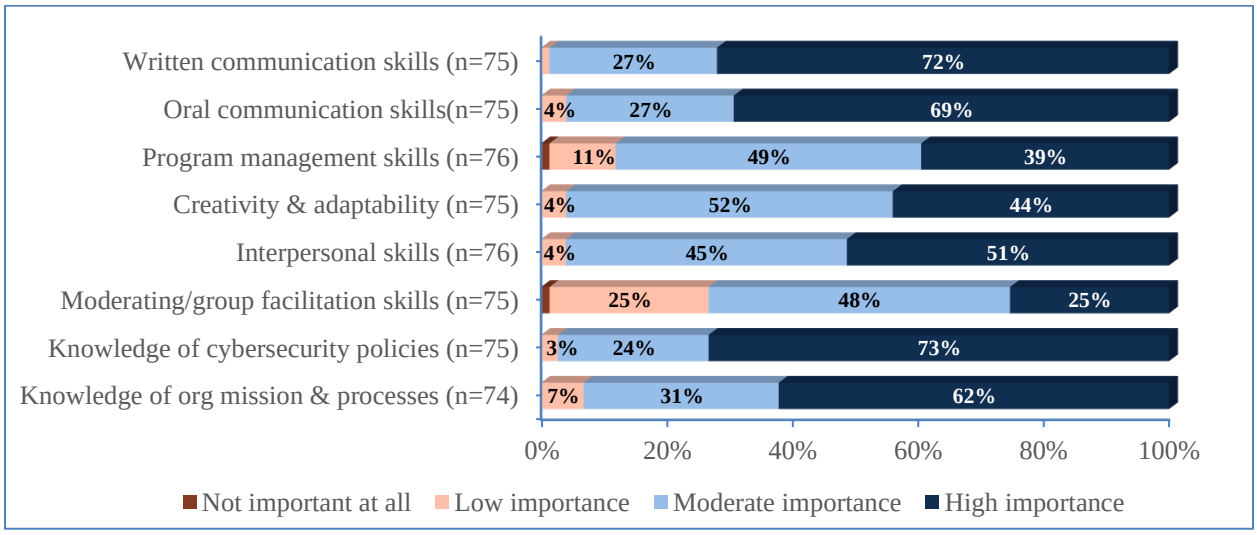

Figure 19: Professional knowledge/skills importance ratings

Communication skills: Communication skills were rated highly by survey participants: 99% rating written communication skills as moderately/highly important and 96% for oral communication skills. Moderating and group facilitation skills were viewed as important by fewer participants (73% moderate/high importance).

The importance of communication skills, particularly being able to translate highly technical information into a language understandable by a diverse workforce, was frequently mentioned by survey and focus group participants:

> "You also need employees who understand cybersecurity and are able to communicate it in a way that your average employee can understand. So that's really an important skill." (D01)

> "Skills to translate technical speak into plain language" (Q40).

> "Some of my team members have English backgrounds or writing backgrounds, which helps them to write things in a way that, A) people can understand but, B) aren't necessarily open for interpretation." (D03)

> "For me, not only having a background in IT security but having somebody who is capable of clearly communicating the security awareness. Like I currently have somebody on staff who is very excited, has fabulous ideas, and can be the most

> confusing person when trying to communicate the actual piece of the security awareness. So, you certainly don't want to have just that wall of text…You get eyes glazed over." (D04)

> "I think communication skills, not just for putting the right words in the material and into the training deck itself, but if you do get helpdesk calls about, 'Why is this? What is that?' you need to be able to feel that and communicate on a professional level as well." (N08)

> "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 the needs of the workforce as important competencies (96% moderate/high importance). Several participants commented on these:

> "Creativity. A lot of what you put out is visual. It might be online training or posters or…websites, posters on websites. So it needs to be engaging." (D01)

> "I would like to just have more creative staff available to work with to maybe stand up a specialized website for security training with the resources." (D05)

> "I would say also being open to different perspectives of something that maybe you are already sure is working perfectly, but someone might come along with a different perspective altogether that might make something easier or work better." (S05)

> "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: Interpersonal skills were rated as moderately or highly important by 96% of survey participants. Participants expanded on these skills, citing empathy, building relationships, networking/collaboration, customer service, patience, and listening skills.

> "I know I have to hunt users down every single year for CSAT and be nice about it too…Just every single day for an entire month, I try to communicate with user, 'Hey, you haven't taken your CSAT yet. How about it?' Or I'm educating a user tomorrow who her director flagged her as having failed a few phishing exercises, and she does not want to be trained. So how do I address that? How do I stay friendly with her, and not make her angry with me while complying with her director's requests or requirements?" (N03)

> "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)

> "Empathy for employees." (Q29)
>
> "They have to have patience. You've got to be able to engage other people other than security nerds and professionals." (N07)
>
> "Collaboration - that's key - building those relationships, and collaborating with others, particularly, in my instance, where there's various business units. And getting those folks engaged and working with them to build a better experience is really imperative." (S11)
>
> "Be consistent, have patience, learn all you can about the program and have customer service skills." (S09)

Program Management: Eighty-eight percent of survey respondents viewed program management skills as important. Several focus group participants commented on the importance of this skill:

> "I think they would have to be a strong project manager or COR [contract officer's representative] because those are the things that in order to run a program, you might not be able to contract. You don't want the contractor pushing your project. You want your fed person doing that." (D01)
>
> "I'm thinking a little bit of project management skills because they need to coordinate with the people who actually do the workday in and day out. So, I don't expect for them to match to everything cybersecurity, that is if they'd be able to manage the project and manage the people. I think that's probably the biggest skill that's needed." (N06)
>
> "Logistics and event planning are key KSA [knowledge, skills, and abilities] areas." (Q56)

Contextual Knowledge: Having knowledge of relevant cybersecurity policies was viewed as important by 97% of survey participants. Knowledge of organizational context – including mission, processes, and dynamics – was rated important by 93%. Several participants commented on this organizational knowledge:

> "A part of a requirement for my job as well, that I need to be able to interpret policy in a nutshell to help the users." (S05)
>
> "Having knowledge of internal policies and procedures is certainly something that a candidate should have." (S11)
>
> "Understanding what the culture is. So like if the culture is more of a, 'Well, we've always done things the same way,' then you need to understand that going in when you're creating the program." (N10)
>
> "Understand the federal mandates and the organizational culture towards training.

> These to *[sic]* aspects are crucial to how you develop or mature your program" (Q44)
>
> "Organizational politics" (Q70)
>
> "Understand the mission of the organization and how the security awareness program will strengthen or protect the mission." (Q84)
>
> "Learn about your community of learners. You need to know who they are and how best to reach them." (S03)

Other Knowledge and Skills: Participants also mentioned other professional knowledge and skills not included in the survey, including analytic and critical thinking skills and psychology/persuasion:

> "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)
>
> "Ability to identify, measure, and analyze metrics - for both improving the program and communicating with leadership." (Q75)
>
> "Analytical skills to see worldwide trends or risks and apply them to our organization's posture." (Q60)
>
> "Psychology" (Q33)
>
> "Ability to persuasively 'manage up'." (Q66)

4.1.3 Specialized Knowledge and Skills

We also asked participants to rate the importance of two specialized knowledge/skills developed in other fields that can be applied to security awareness: marketing and adult learning/instructional development. Figure 20 shows the ratings.

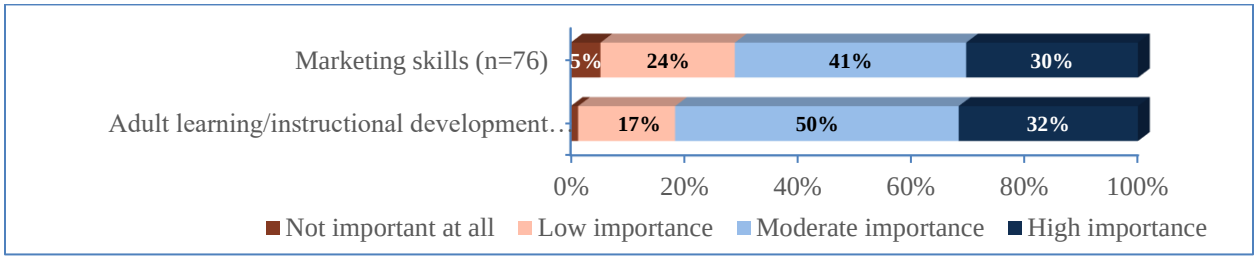

Figure 20: Specialized knowledge/skills importance ratings

Marketing skills: Marketing skills were viewed as being of moderate or high importance by 71% of survey participants. These skills were rated as the least important overall, with 24% rating them as having low importance, and 5% as not important at all. A focus group participant commented on the value of having a person with marketing skills contributing

to his organization's security awareness program:

> "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. Historically, years ago, we would send out things that were kind of wall of text, and we just know no one is actually going to read those things." (D03)

Adult learning or instructional development knowledge/skills: Having knowledge of and skills in adult learning or instructional development was seen as moderately or highly important in security awareness teams by 82%. During the focus groups, several participants mentioned the value of having someone with skills in adult learning and education on the security awareness team:

> "From an awareness training perspective, personally, I think having that foundation in education and understanding teaching techniques and skills and things like that would come before the cybersecurity knowledge." (N04)

> "Because this is training, you need someone who's an industrial design specialist, a training specialist, someone who knows adult learning." (D01)

> "Someone that maybe has 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)

4.2 Mix of Knowledge and Skills Within Teams

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 or strongly agreed that their team had the right mix of skills and knowledge, while 20% disagreed or strongly disagreed (Figure 21).

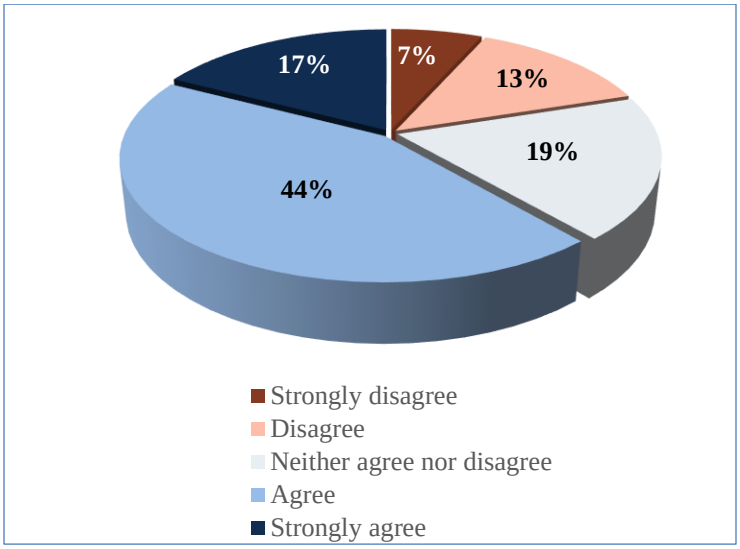

Figure 21: Agreement for team having the right mix of knowledge and skills (n=75)

We found a statistically significant difference in responses between participants in departments and sub-components (*z* = 2.396) and departments and independent agencies (*z* = 2.506). Participants who agreed/strongly agreed that they had the right mix of skills totaled 86% of 22 participants in departments as compared to sub-components with 52% of 23 participants and independents with 50% of 30 participants.

Several participants believed that organizations should have multidisciplinary teams if possible:

> "I would say that 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 because in the current environment, there's all kinds of ad hoc items that come about…There's no way one person can do it without a lot of backup." (D06)

> "That's the purpose of having a contractor. You can bring on all those pieces that you need to have a program…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, technical. I have good project managers. I have cybersecurity professionals." (D01)

> "Have a diverse team relating to experience." (Q25)

However, not all organizations have the resources to build teams with the desired mix of skills. Therefore, they often augmented the security awareness team by involving others in the organization:

> "I partner with our internal communication group on a lot of activities to lean on their communication expertise." (D05)

> "We depend on pulling in other resources to help with [the security awareness program], and that, again, goes back to being tied to the threat team and to the policy team." (D03)

> "We also have a cyber guardians program, which is an ambassador program, so to speak, where 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. And sometimes we use little cards to remind them, like a tent card that we might set on their desk." (N05)

> "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 and so forth." (N09)

4.3 Professional Development

4.3.1 Professional Development Activities

Participants selected the professional development activities that have helped them gain the knowledge and skills needed for their security awareness roles. Figure 22 shows the frequencies of each activity. Self-study was the most popular activity (85%), followed by computer-based courses (79%), and conferences (76%). Fewer participants selected college courses (43%). Only 7% said that they had not engaged in any professional development activities.

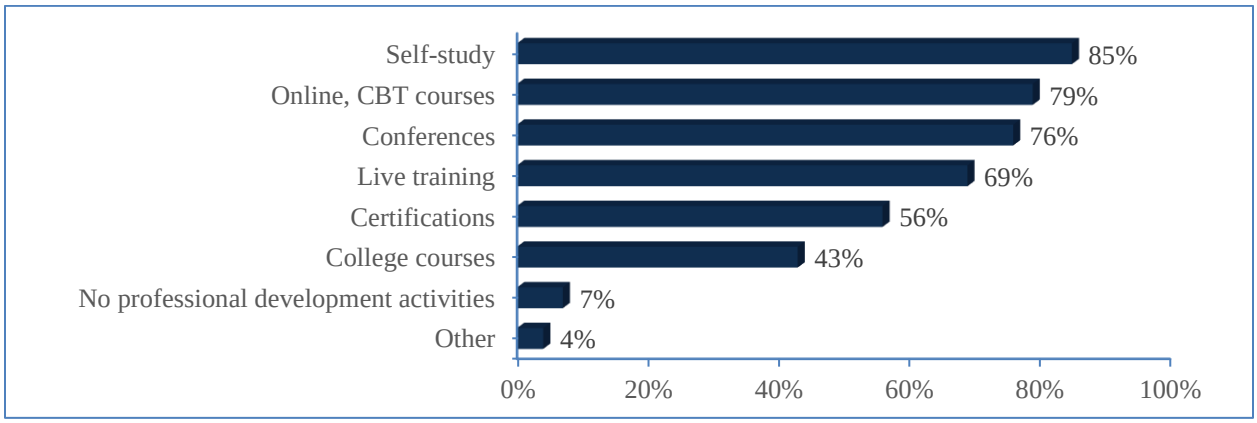

Figure 22: Professional development activities (n=75)

We note that while 56% indicated they engaged in certification activities to help them in their security awareness roles, this percentage differs from the 93% who said they had at least one industry-recognized certification (as reported in section 3.3.3). This may be because not all certifications are directly applicable to the security awareness role.

Several participants offered advice on the need for professional development:

> "Continue to seek outside security awareness training and professional development activities." (Q91)

> "It can be overwhelming at first but remember you are a sponge and try to soak up the various information that is available to you to fully understand your role and responsibility to educate others." (Q32)

> "Learn from peers who have already done it (networking, conferences, training)." (Q43)

4.3.2 Adequacy of Professional Development Opportunities

We asked participants to rate their agreement with the following statement: "In my organization, I have been provided adequate professional development opportunities to help me in my security awareness role" on a five-point scale ranging from "strongly disagree" to "strongly agree." Seventy percent agreed or strongly agreed that they were provided with adequate opportunities, and only 17% disagreed/strongly disagreed (Figure 23).

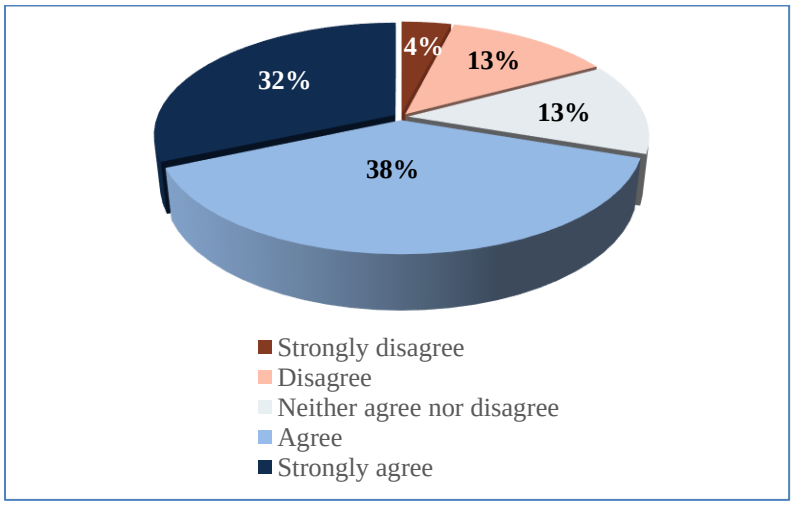

Figure 23: Agreement for having adequate professional development opportunities (n=76)

No statistically significant differences were found between groups (organization type, program size, team size).

A few participants expressed frustrations about trying to obtain training specific to their security awareness role:

> "They don't let me do training so much anymore. They won't spend any money on me…So, I'm constantly looking for free education and expanding my base that I already have." (S05)

> "Our agency recently obtained licenses within an online learning service…They have training that is associated with each of the NICE cybersecurity work rules. Right. So, I was like, 'Okay, great, I'm going to go find my work role,' which is that learning coordinator one, and I was like, 'Let me see what training they have.' 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)

5 Key Takeaways

In this section, we summarize key findings from the study results related to security awareness professionals' backgrounds, knowledge, and skills.

5.1 Security Awareness Professional Work Roles

Excluding executive classifications (CISO, Chief Information Officer - CIO), most survey participants were IT Specialists (Cybersecurity) or supervisors in that same job series, suggesting a commonality across the federal security awareness professionals represented in the study.

However, commonalities in assigned NICE Framework Work Roles were not as apparent. Half of survey participants indicated that they either were not assigned to a NICE Framework Work Role or that they did not know if they were assigned. A 2018 OPM memo mandated that federal agencies "are required to identify and code Federal positions performing information technology, cybersecurity or other cyber-related functions…The position coding is based on the work roles described in the NICE Framework" [OPM]. Assuming that organizations have indeed met the requirements in the OPM memorandum, our findings may suggest that organizations have not adequately communicated Work Roles to their security awareness workforce. This may have professional development implications in that, without a Work Role reference, individuals and organizations may not know what knowledge and skills are necessary for security awareness jobs or how to gauge qualifications when hiring people to these positions.

Those participants who knew their NICE Framework Work Roles indicated 11 different Work Roles (individuals may be assigned to more than one Work Role), not including those who selected the "other" option. We acknowledge that not all identified Work Roles may have directly applied to security awareness duties since most participants have other job duties. However, we found that there was no single Work Role assigned to a majority of participants, with information system security manager (ISSM) coming the closest (40% of participants having that Work Role). This finding may suggest a lack of standardization in how federal organizations interpret the NICE Framework Work Roles in the context of security awareness.

5.2 Diversity of Disciplines, Knowledge, and Skills

A substantial number of participants in both the focus groups and survey held formal degrees in non-computing disciplines, demonstrating the educational diversity represented in the federal security awareness community. The vast majority of participants had worked in the cybersecurity and IT fields, with smaller percentages having worked in other fields that may be of benefit as a security awareness professional, such as communications, human resources, or graphic design.

Forty percent had *only* worked in a technical field. Industry experts have suggested that enlisting only technical people to work in security awareness may be problematic since highly technical people often have a difficult time presenting security information in a way that is understandable to non-technical people [SANS]. However, our study does not attempt to gauge the level of communication skill among participants, so it is unknown as to whether the technical backgrounds may be a detriment within the surveyed organizations.

While technical knowledge and skills in cybersecurity and IT were unsurprisingly rated highly by almost all participants, professional skills – especially communication, creativity and adaptability, interpersonal, and knowledge of policies and organizational context – were also seen as of high or moderate importance for security awareness teams. Privacy knowledge and skills were also highly rated, which reflects the growing trend of many security awareness teams now taking on privacy training responsibilities.

5.3 Building a Team with the Right Skills

Since it may be difficult to find one individual who has all the desired knowledge and skills, having a discipline-diverse security awareness team was viewed as beneficial. Over half of survey participants agreed that their security awareness teams had the right mix of knowledge and skills, although participants in departments were more likely to agree than their counterparts from sub-component and independent agencies. This may be because departments have more staff resources to contribute to the program.

Building a team, as alluded to within the focus groups, was often achieved by hiring contract staff with specialized skills. However, many organizations may not have the resources to hire an entire team, as evidenced by the third of represented organizations having only one or two individuals assigned to security awareness duties, as described in NISTIR 8420. Therefore, participants emphasized the importance of establishing relationships with other organizational groups to draw on specialized expertise to aid the security awareness program.

5.4 Professional Development

Survey participants indicated a variety of professional activities they engage in to help them in their security awareness roles, most commonly self-study, online courses, and conferences. While the majority agreed that their organizations provide them with adequate professional development opportunities, 30% were either neutral or did not agree. It is unknown if this is an organizational issue (e.g., leadership does not encourage/allow security awareness professionals to take training, lack of training budget) or if the problem lies in there not being sufficient training specific to the security awareness role.

6 Moving Forward

Based on our findings, we offer the following suggestions and potential opportunities to address the most significant issues identified in our study.

For those developing government-wide guidelines, policies, and sharing platforms:

- Identify dedicated, standard Work Role(s) for security awareness professionals. NICE is currently exploring the addition of an awareness Work Role to the NICE Framework.
- Develop training specifically geared towards helping security awareness professionals in their roles. Such training should go beyond technical, security topics and address professional skills necessary to be effective.

For organizations with security awareness programs:

- Be open to hiring candidates from less-technical backgrounds.
- Communicate NICE Framework Work Roles to the security awareness workforce.
- If possible, build a team having all requisite skills, rather than trying to find all requirements in one or two individuals. While having a dedicated team may be preferred, for resource-constrained organizations, awareness professionals can be encouraged to collaborate with other organizational groups to draw on specialized expertise.
- Support experiential and training opportunities for developing professional skills in addition to those that are technology focused. Afford security awareness professionals opportunities to share with other professionals via forums or conferences, (e.g., FISSEA).

Acknowledgements

The authors of this document would like to acknowledge those who have made this work possible. We would like to thank the federal employees who took time out of their busy schedules to participate in the focus groups and survey and provide their valuable perspectives. We would also like to thank the following individuals who provided valuable input and feedback on the study: Rodney Petersen, Marian Merritt, Danielle Santos, Karen Wetzel, Alen Kirkorian, Dan Jacobs, Sarah Moffat, Clarence Williams, and Daniel Eliot.

References

[BADA] Bada, M, Sasse, AM, Nurse, JRC (2019) Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour? *arXiv preprint*. https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf

[FISSEA] National Institute of Standards and Technology (2021) *FISSEA – Federal Information Security Educators*. Available at https://csrc.nist.gov/projects/fissea

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

[OPM] U.S. Office of Personnel Management (2018) Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need. (U.S. Office of Personnel Management, Washington, DC). Available at https://chcoc.gov/content/guidance-identifying-addressing-and-reporting-cybersecurity-work-roles-critical-need

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

[STEWART] Stewart, G, Lacey, D (2012) Death by a Thousand Facts: Criticising the Technocratic Approach to Information Security Awareness. *Information Management & Computer Security* 20(1):29-38.

[WILSON] Wilson M, Hash J (2003) Building an Information Technology Security Awareness and Training Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-50. https://doi.org/10.6028/NIST.SP.800-50

[WOELK] Woelk, B (2015) The Successful Security Awareness Professional: Foundational Skills and Continuing Education Strategies. *EDUCAUSE Center for Analysis and Research*. Available at https://library.educause.edu/~/media/files/library/2016/8/ erb1608.pdf

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CIO	Chief Information Officer
CISO	Chief Information Security Officer
FISSEA	Federal Information Security Educators
FTE	Full Time Equivalent
ISSM	Information Systems Security Manager
IT	Information Technology
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology