NISTIR 8420A

Approaches and Challenges of Federal Cybersecurity Awareness Programs

Julie Haney
Jody Jacobs
Susanne Furman
Fernando Barrientos

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

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

NISTIR 8420A

Approaches and Challenges of Federal Cybersecurity Awareness Programs

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.8420A

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 8420A
73 pages (March 2022)

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

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 security awareness programs experience a number of challenges, including lack of resources, difficulty measuring the impact of the program, and perceptions among the workforce that training is a boring, "check-the-box" activity. 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 approaches and challenges of security awareness programs within the federal government. Insights gained from these results are informing guidance and other initiatives to aid federal organizations in building effective security awareness programs. While focused on the U.S. government, findings may also have implications for organizational security awareness programs in other sectors.

Keywords

cybersecurity; cybersecurity awareness; focus groups; measures of effectiveness; mixed methods; phishing; security professionals; survey; training; usable cybersecurity

Executive Summary

Security awareness programs aim to help employees recognize and appropriately respond to security issues, with a goal of achieving long-term behavior change. Industry and research surveys have revealed that organizational security awareness programs face a number of challenges, including lack of resources, difficulty measuring the impact of the program, and perceptions among the workforce that training is a boring, "check-the-box" activity. However, it is unclear if these challenges also apply to security awareness programs 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 the approaches and challenges of federal security awareness programs. The following is a high-level overview of these results, with cited statistics from the survey.

Required Annual Security Awareness Training

- Two-thirds of survey participants said they develop at least some required security awareness training content in-house, with 80% updating content at least once a year. Focus group participants expressed frustration that each organization had to acquire or create their own training. Instead, they desired standardized government training and guidance that allow customization for the unique needs of each organization.
- Automation was viewed as essential for efficient tracking of employees' completion of training. However, some organizations lacked this automation, especially when tracking contractors, who may not have access to organizations' learning management systems.
- When dealing with individuals who do not complete their training by the deadline, many organizations disabled accounts of non-compliant employees, resulting in higher compliance numbers. Still, almost half (47%) said that getting employees to complete the required training was challenging, largely because employees were busy or disinterested.

Security Awareness Approaches

- In addition to the required annual training, 79% of surveyed programs held a variety of security awareness activities throughout the year, such as speaker events, instructor-led sessions, webinars, and interactive activities like escape rooms. Smaller programs were less likely to offer additional activities.
- Programs often disseminated information that employees could use in both their work and personal lives, which was viewed as important for establishing consistent security habits. They have also recently introduced more topics relevant to teleworking.

- Programs utilized a wide range of other communication channels, such as email, newsletters, posters, and videos. However, 56% of surveyed programs had difficulty providing security awareness information in an engaging way, 47% experienced challenges customizing security awareness information to a diverse workforce, and 40% struggle with ensuring materials are Section 508 compliant, especially when utilizing interactive approaches.
- 85% of programs performed phishing simulations, which were often described as being one of the successful aspects of the security awareness program. While many focused on phishing click rates to gauge learning, others were more interested in reporting rates to demonstrate positive impacts on employee behavior.
- 44% of surveyed programs recognized employees for practicing good security behaviors via a variety of means, such as virtual awards, personal thank-yous, and formal recognitions. Several focus group participants described several successful incentive initiatives related to phishing simulations.

Informing the Security Awareness Program

- Participants frequently collaborated with other groups in the organization to augment and inform their programs, most commonly other cybersecurity and IT teams, but also with others such as human resources and communications.
- Programs used a variety of government and non-government resources to inform security awareness topics and approaches, e.g., workforce feedback, organizational security incident trends, news stories, and security mailing lists.
- While only 27% of survey participants expressed challenges collaborating or sharing information with other federal security awareness professionals, focus group participants frequently highlighted their desire for increased collaboration. For example, they suggested the creation of a central repository of awareness materials, ongoing working groups, or real-time online forums.

Program Success and Support

- Training completion rates were the most common way programs try to determine their effectiveness (84%). Behavior based measures (e.g., phishing click rates, reporting of phishing emails or other incidents) were utilized by over half.
- Over half (56%) of survey participants thought their leadership viewed compliance metrics as the most important indicator of program success, with slightly fewer (47%) having the same opinion themselves. However, in qualitative remarks, many focus group and survey participants disagreed with this compliance focus, instead emphasizing that the real purpose of security awareness is to affect employees' security behaviors; therefore, success should be measured in ways beyond training completion rates.
- 77% rated their security awareness programs as moderately or very successful. However, 44% of survey participants expressed challenges determining how to measure program effectiveness. Survey and focus group participants desired more guidance on appropriate metrics and government-specific data for benchmarking their own program.
- 48% of survey participants indicated that correlating security incident data with behaviors targeted by the security awareness program was challenging. Yet managers taking the survey listed security incident data as the measure of effectiveness most preferred for helping them

make decisions about the security awareness program, while training completion and phishing click rates were mentioned by much fewer.
- Large majorities (70% and greater) thought that security was a priority for the organization, that security was understood by leadership and employees as important, and that leadership and employees supported the security awareness program. However, only 35% of survey participants thought the program had been provided adequate funding and staff.

Study results can inform federal security awareness professionals, organizational decision makers, policy makers, and guidance developers in their efforts to improve and advocate for federal security awareness programs. The results may also be valuable to security awareness professionals outside of the government who face similar challenges. Additionally, although this study refers to security awareness programs, its focus is not only relevant to awareness but also to security training issues as well.

Table of Contents

List of Appendices

List of Figures

1 Introduction

Security awareness and training programs aim to help employees recognize and appropriately respond to security issues, with a goal of achieving long-term behavior change [WILSON]. Industry and research surveys have revealed that organizational security awareness programs may face a number of challenges, including lack of resources, difficulty measuring the impact of the program, and perceptions among the workforce that training is a boring, "check-the-box" activity [SANS][WOELK][BADA][STEWART][FERTIG]. However, it is unclear if these challenges also apply to security awareness programs 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 8420A, reports on a subset of results focused on the approaches and challenges of federal security awareness programs. Specifically, these results answer the following research questions:

1. What approaches and techniques do federal agencies employ in their security awareness programs?
2. What's working well with respect to security awareness training in federal agencies?
3. What's not working well? What are the challenges and concerns of federal security awareness programs?
4. How do organizations determine the effectiveness of the security awareness program?
5. What resources and guidance are used to inform the security awareness programs?
6. What do teams feel like they need to be more successful? What kinds of resources would be most beneficial?

Study results will inform guidance and other resources (e.g., sharing forums) to aid federal organizations in building effective security awareness programs.

The report is organized as follows. Section 2 describes conventions used when reporting results. Section 3 describes study results related to security awareness approaches, including required

security awareness training, communication channels, topics, and associated challenges. Section 4 provides results about sources of support for security awareness programs and resources that inform program topics and approaches. Section 5 summarizes how organizations determine program success and challenges in doing so. Section 6 describes results related to perceptions of program support. Section 7 summarizes key takeaways from the study related to program approaches and challenges.

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 and advocate for their organizations' security awareness programs. Those who develop and manage federal security awareness guidance, policies, sharing forums, and initiatives may also benefit. The report may be valuable to security awareness professionals outside of the government who face similar challenges. Additionally, although this study refers to security awareness programs, its focus is not only relevant to awareness but also to security training issues as well.

2 Reporting Conventions

This section describes the organization and reporting of study results. Results are focused on and organized according to the survey structure, with all statistics based on survey data. Because participants had the option of skipping survey questions, participants may not have answered all questions. Therefore, we include the number of survey responses for each question (n) 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 Security Awareness Approaches

In this section, we describe the ways in which federal security awareness programs disseminate security awareness information to their workforce, including the annual required training, other security awareness activities, and phishing simulations. We also provide results related to security awareness topics, approaches for recognizing employees for good security behaviors, how programs have adjusted their approaches due to the pandemic, and challenges they face in disseminating information.

3.1 Annual Required Training

U.S. Government organizations are mandated to implement annual, mandatory security awareness training for all employees (federal employees and contractors). This section details responses specific to the mandatory training component of security awareness programs.

3.1.1 Required Training Fulfillment

We asked participants in what ways their employees could fulfill annual security awareness requirements (Figure 1). Online, computer-based courses were the most popular method at 65%. The next most popular method (23% of participants) was via a live training event held by the organization.

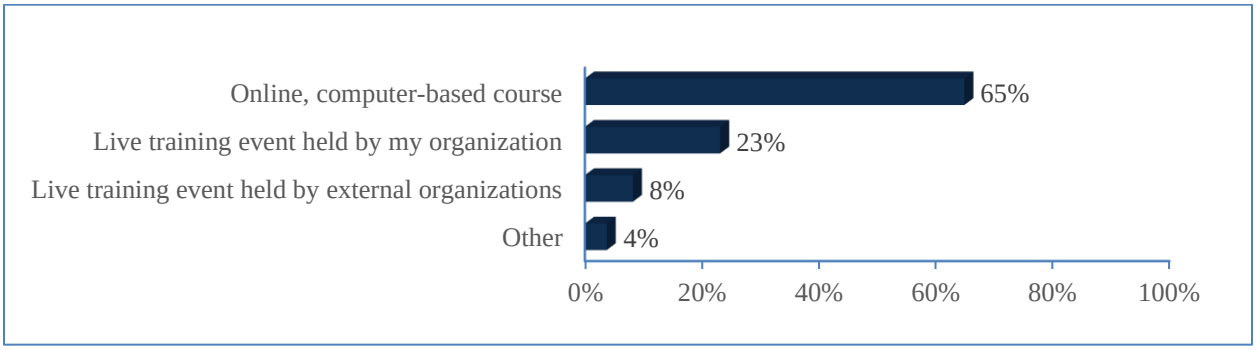

Figure 1: How training requirements can be fulfilled (n=89)

Sixty-four percent only selected one option, i.e., their organizations only provide one way for employees to complete required security awareness training.

For the number of ways in which employees could fulfill their training requirement, we found no statistically significant differences between groups (organization type, program size, team size) among those who only offer one way to complete training versus those that offer multiple ways.

As mirrored in the survey, focus group participants' organizations most often made use of computer-delivered security awareness training for the annual requirement:

> "Since we have a lot of our personnel in remote areas, we've been doing it through our learning management system primarily for the annual security awareness training." (D05)

> "For us, our general security awareness and training course is computer-based and it's online. We have a[n]…electronic learning management system. Everyone, all our employees and contractors have an account, and they log in and they complete it." (S08)

> "That's just delivered via e-mail, PowerPoint to the person." (N11)

Other organizations offer employees multiple options for completing their training:

> "For our main enterprise network, it's computer-based training that's taken annually…But for those who don't have access to the enterprise network often for certain other networks that we might maintain,…those are physical briefings done by the ISSOs [information system security officers] to those personnel. And then they sign an acknowledgment form." (D03)

> "We have a computer-based training for the annual cybersecurity awareness training requirement, which we load into our – [Department] has a learning center. So those that have access to that take the training there. In addition, we also offer instructor-led annual cybersecurity awareness training. This past year, obviously, it was remote. Generally, those are in person." (D04)

> "To accomplish their training, we do offer either online, or we typically – not this year because of the pandemic – but we typically host an annual IT Security Day event. And it's a one day, attend any one talk, and register. And then we process those registrations in our learning management system, actually, so that we have that artifact in our learning system that they attended that event." (S11)

3.1.2 Obtaining Training Content

We asked how the participant's organization obtained required security awareness training content (select all that apply) (see Figure 2). About two-thirds of the participants work in organizations that created training internally, with 31% purchasing training from outside their organization. Fewer obtain the content from other organizations.

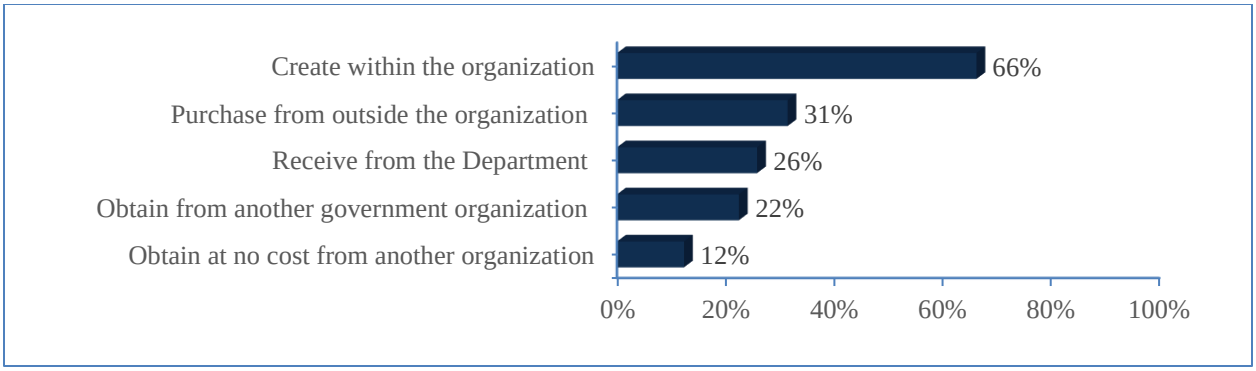

Figure 2: How required training is obtained (n=89)

The only statistically significant finding was among different types of organizations for the selection of "Purchase from outside the organization." For that option, there was a statistically significant difference between independent agencies (52% of 33 participants selecting this option) and sub-components (15% of 27 participants selecting this option). This result corresponds with data showing that many sub-components receive training directly from their Departments.

Focus group participants provided additional details on the sources of their required training. Many utilize training developed by other organizations:

> "We use [other government agency's] awareness training. We've kind of maintained a status quo throughout the years from that perspective." (D04)

> "For CSATs [cybersecurity awareness training], we use SANS as our provider, and we use those topics. So, whatever they offer as modules, we follow their guidance." (N03)

> "Our training is also web-based training. It's through the Department, through their learning management system, and they have a vendor designed training." (S02)

> "Check out free resources such as the IASE Cyber Awareness Challenge for material to include in your training" (Q57)

Others develop the content in-house:

> "For IT security and privacy awareness training, I just do this huge PowerPoint that covers all the topics that you need to cover and all our policies and procedures. Anything that's new from the year gets incorporated in the annual update. I send that PowerPoint over to the learning management folks and they do the online version with the voice-over and all that." (N11)

3.1.3 Update Frequency

Participants indicated how often their organization updates security awareness training content, with 80% answering that they update it at least once a year. No participants said they updated content more than every three years, and 4% did not know how often content was updated (see Figure 3).

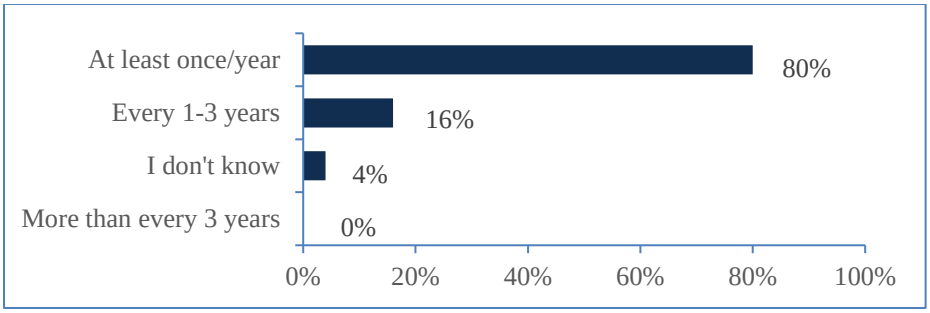

Figure 3: Required training content update frequency (n=89)

No statistically significant differences were found between groups.

Participant quotes from the focus groups and open-ended questions in the survey provide insights into the range of responses. Participants' comments reflect motivators for regularly updating annual training, such as addressing emerging threats and organizational feedback:

> "Cybersecurity and related vulnerabilities are constantly changing so your program needs to be flexible." (Q35)

> "We update annually based on what's been going on the previous year." (D02)

> "I try to make sure that any messaging or any type of awareness information I'm sharing is current, and it's not stale." (N10)

> "To make sure to respond appropriately to any inquires (positive and negative) and make improvements that are visible to your stakeholders." (Q40)

3.1.4 Non-Compliance Actions and Consequences

We asked participants what happens when employees do not complete their required training by the deadline designated by the organization (select all that apply question type). Figure 4 shows the non-compliance actions and consequences. The top three actions were: disabling accounts (74%), sending an email reminder (73%), and contacting the employee's supervisor (70%). Few participants (6%) said that failure to complete required training impacts employees' performance ratings. Three percent of respondents said their organization disables the employee's internet access.

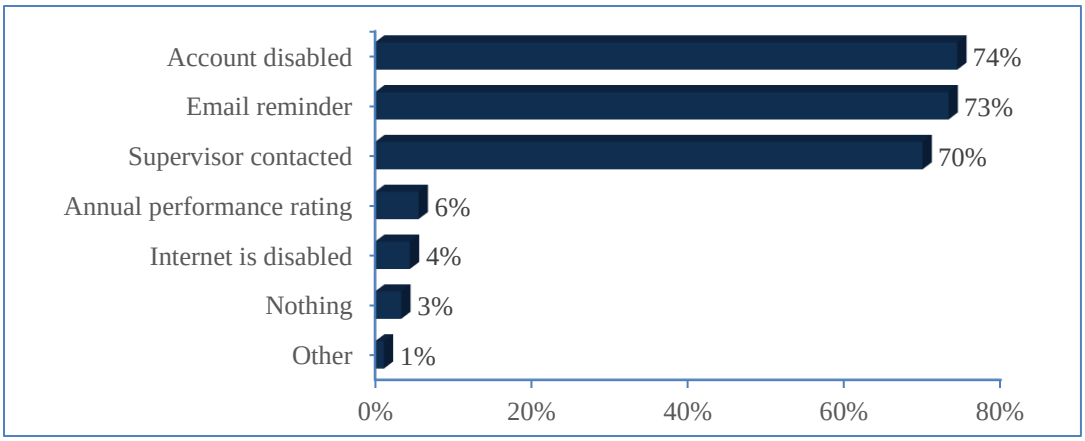

Figure 4: Required training non-compliance actions and consequences (n=90)

Consequences for non-compliance was a popular topic of discussion during the focus groups. A program lead talked about alerting supervisors to employee non-compliance:

> "I do send out messaging to…leadership regarding their employees that have not completed it prior to the deadline before their access is shut off so that they have an opportunity to get it done. But that seems to help us very well with ensuring that the training is completed timely." (N05)

However, sending email reminders was not always easy for everyone:

> "With our LMS [Learning Management System], we also are not allowed to send automated emails to remind people to take their training. So, I have to do that manually,…and I end up sending emails to about 2,000 users to remind them to take the training." (S10)

Disabling accounts was by far the most explicitly mentioned consequence by participants and was touted as being quite effective.

> "[Training completion] went from darn-near 72-percent completion rate to 98 percent in like three days once we started disabling accounts…Disabling accounts and actually doing what you say you will do works well for the program." (N06)

> "We've been manually disabling people for years, and that's the reason why our numbers have been in the high 90s, between 98 and 99 point something." (N09)

> "I have only had to disable maybe 5 or 10 people in the past years. And last year, I think I had none because I'm very aggressive and letting them know, 'Hey, you need to complete the training. If you don't require the training anymore, then you need to let me know'." (S09)

> "In order to enforce this training, it's imperative to have that backend information and the means to cut people off or withhold their access until they meet the requirements." (S11)

"Non-compliance shutoff maintains 100% compliance." (Q43)

3.1.5 Challenges: Required Training

Participants rated their challenges with required training on a four-point scale ranging from "very challenging" to "not at all challenging," with a "does not apply" (N/A) option (see Figure 5).

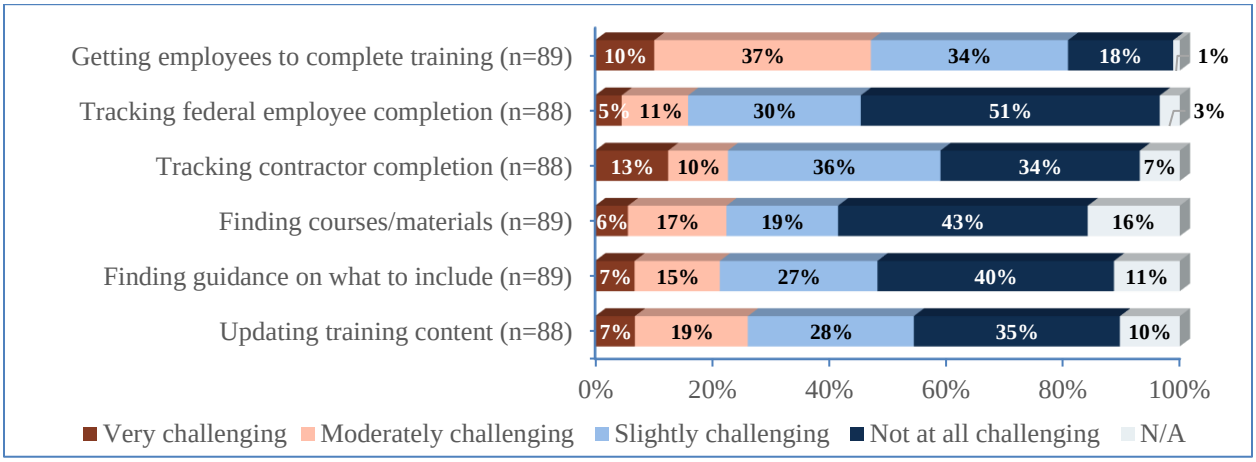

Figure 5: Challenges – Required training

The following provides more detail on survey results for each challenge while incorporating example supporting quotes from focus group and open-ended survey questions to provide additional, qualitative insights.

Getting employees to complete required training by the appointed deadline: Almost half (47%) of survey participants thought getting employees to complete required security awareness training by the organizational deadline was very or moderately challenging.

No statistically significant differences were found between groups.

Within the focus groups, participants voiced concerns that employees view required training as a generic, "check-the-box" exercise and may feel overwhelmed by having to complete numerous other mandatory organizational training courses:

> "I could see how someone taking the training could say, 'This is not applicable to me,' and kind of just get through it to just get the training, get off the list, and be done with it." (N10)

> "You've got IT security, physical security, personnel security, etc. And they have their own training requirements…It's inefficient." (S11)

> "People are busy. They have all kinds of tasks to be doing. They have other trainings that are required, and we are still trying to figure out how to most seamlessly help our users want to do this training." (S05)

As a result, employees may put off taking the training until the last minute:

> "They put it off, put it off even though it takes roughly an hour. They put it off throughout the year. Even though we're giving them messages throughout the year, they'll wait. And then when we had to come up with this big, long list of people we're disabling accounts, then it becomes a political nightmare." (N08)

> "Our biggest problem is with our executives. They are the ones who are more than likely not to have taken the training in a timely manner, and we can't exactly lock them out." (S03)

> "It really shouldn't take them six, eight months to complete the course. But you got to know your user population to know that some people just wait until the last minute and then to know the technical constraints of your learning management system. Our system, even though we have 60,000 licenses, can really only handle 4,000 concurrent users at one time. So if everyone waits until August 15th, it overloads the system, it's just a total disaster." (S08)

To address this challenge, several organizations implemented rolling deadlines:

> "Successfully implementing a rolling deadline made tracking completions much, much, much easier. Now completion rate by individual deadlines are higher than completion date for one annual deadline date was." (Q45)

> "We pick a certain line of business, a silo within our agency to focus on heavy with management reminders, individual reminders like every month. So that we're not waiting until August 1st, between August 1st and August 15th, sending out 40,000 reminders. We break that down as to not overload the system." (S08)

Tracking which federal employees have completed their required training: Only 16% of survey participants thought that tracking federal employee completion of required training was very/moderately challenging.

No statistically significant differences were found between groups.

Some participants mentioned successes they had tracking who had completed training:

> "We eliminated a paper-based training option which streamlined our processes and made tracking completion and labor involved in providing the training much easier!" (Q45)

> "Automating the process, it's really got people to notice things, their due dates and when they need to have the training completed." (N09)

> "It's all about automation. And I used to track our five to eight thousand users on spreadsheets. And I was the single help desk. But we've since matured beyond

> that and now have automated tools…Our onboarding site is a self-registration site so that our new staff can go and self-register, take their training, and then that ties into our primary learning center once they're on board and approved. We reconcile those transcripts. So, we do have now the automated means where we do tie it into our backend account management system so that, truly, people aren't getting access to things before they've taken that training and signed the rules of behavior. So, automation is key because the level of effort for, particularly, smaller agencies, where they may not have access to tools or there's a single person, is really impactful and inefficient." (S11)

In contrast, several focus group participants discussed issues they encountered with tracking, primarily due to non-automated or non-standard tracking methods:

> "Some of our processes are still manual as far as still working off Excel spreadsheets for tracking users' completion of activities." (S02)

> "Certain individuals are considered VIP [very important people] and screened and handled differently, adding overhead to the management/tracking." (Q88)

One program lead commented on the impacts of human resource records not being updated in a timely manner to reflect employees leaving the organization:

> "I don't know why it takes so long for people to get out of the system, but it skews our [security awareness training compliance] numbers. And our FISMA number is never going to be correct if the system's not right." (S09)

Tracking which contractors have completed their required training: Twenty-three percent of survey participants felt that tracking contractor completion of training was moderately or very challenging.

No statistically significant differences were found between groups.

Although less than a quarter of survey participants viewed contractor tracking as particularly challenging, this topic was repeatedly mentioned in the focus groups as a substantial problem. The difficulty was often due to contractors not having the same level of access to organizational networks or learning management systems or a lack of integration between systems; therefore, tracking could often not be automated:

> "We have about 10,000 contractors that don't have network accounts that have to take training and being able to identify those and track is a nightmare." (D01)

> "Only feds have access [to the Learning Management System], so contractors we have to handle separately is a lot of manual work, and that leads way to human error." (D04)

> "Tracking contractor compliance is an issue, specifically because they don't all have…licenses for our learning management system…[We need] some type of federal learning management system that each agency could have a piece of and load their contractors in and the content and track their compliance with some kind of exportable report to help us track compliance. And maybe even that report comes out in a common format that can be loaded into any internal systems because, again, tracking contractor compliance is a logistical nightmare across the board" (D06)

Finding courses/materials for required training: Twenty-three percent of survey participants experienced substantial challenge finding required training course materials, while 43% experienced no challenge at all in this area.

No statistically significant differences were found between groups.

Open-ended responses in the survey and focus groups revealed more detail about the challenge of having to create/obtain relevant materials:

> "We have a limited budget, so we tend to create our own training presentations, which are not very engaging or exciting. In the past, we've used [another government organization's training], which received some positive feedback. Unfortunately, some of the information in that training is not relevant to our small agency." (Q57)

> "I don't think that there's enough material that's commonly available such that we can grab it and then customize. (S11)

Participants expressed frustration that each organization had to acquire or create their own training, with several recommending standardized government training that could be shared and customized to individual organizations:

> "There are some topics, probably 80% of the topics, everybody needs to know about. So, why are we buying that over and over again at each agency as opposed to give us the 80% solution and let us pay for the other 20%? That would be more efficient…There needs to be more coordination at the federal level to make sure we're more efficient in how we spend money on this…Stop solving this problem agency by agency." (D01)

> "[We need] standardized documents across federal agencies to satisfy mandatory federal requirements to then allow agencies the flexibility to tailor more engaging content to their agency on their determined frequency." (N01)

> "We need quality training materials that can be shared." (Q63)

Finding guidance on what to include in required security awareness training: Less than a quarter (22%) of survey participants indicated challenges finding guidance on what to include in required training.

We found a statistically significant difference among groups for the "Finding guidance on what to include in training" challenge for: independent agencies and Departments (z = 2.959); and independents and sub-components (z = 3.374). Among participants from independents (n=33), 13 (39%) indicated that they were very or moderately challenged to find guidance, while only 10% (3/29) of Department participants and 11% (3/27) of sub-component participants experienced this level of challenge. There were no significant findings for organizations of different program or team sizes.

Several focus group participants commented on their desire to have more standard guidance on training:

> "There are no best practices or organizational change management around this program. Agencies are left to their own means to do the best they can to implement this requirement." (N04)

> "How long does the course have to be? Does it have to be specific?...We've asked for that guidance on a consistent basis, but all we have is the general guidance to pass down." (S04)

Updating required security awareness training content: Updates to required training were viewed as very/moderately challenging by 26% of survey participants.

No statistically significant differences were found between groups.

Participants commented on their challenges:

> "More frequent updates to online CBT [computer-based training]. Some courses are dated and 'corny' – this doesn't represent the organization well as some CBT seems a little gimmicky bordering on childish." (Q38)

> "Every year there are certain things that you have to keep telling people over and over. So, to a certain extent, for me, the training is going to be somewhat the same year after year because I have to cover these areas…There's a lot to cover in that one hour and to make it relevant is always a challenge every year." (N11)

In the focus groups, challenges with training updates were often linked to a lack of resources, especially for smaller security awareness teams:

> "We don't really have the resources to develop our own [sub-component] or Department-specific content every year, keep it up to date." (D04)

3.2 Other Security Awareness Activities

In addition to the required security awareness training, programs may distribute information to their workforce throughout the year via a variety of means and communication channels. We sought to discover which approaches organizations take and what topics are covered.

3.2.1 Number of Additional Activities

We asked participants how many other security awareness activities or events their organizations offered per year in addition to required annual training (see Figure 6). Twenty-one percent had no additional activities, 43% had only one or two additional security awareness activities, and 24% had four or more activities.

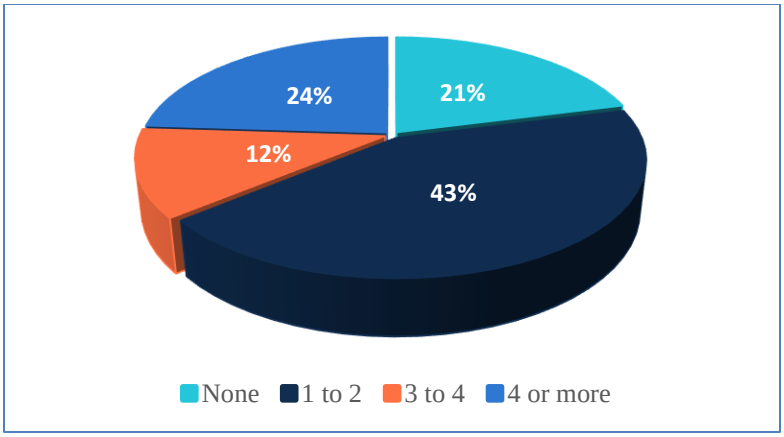

Figure 6: Number of additional security awareness activities or events (n=86)

There was a statistically significant difference in the number of additional security awareness activities offered by programs of the following sizes: small and large (z = -2.039); small and very large (z = -3.266); and medium and very large (z = -2.482). In organizations with small program coverage (n = 18), 44% had no additional activities beyond the required annual security awareness training and 39% had 1-2 additional activities. Among those with medium program sizes (n = 22), 27% had no additional activities and 45% had 1-2 activities. This was in contrast to very large programs (n = 22) in which only one had no additional activities and 59% had three or more activities.

In addition, **there were significant differences among the following security awareness team sizes: very small and medium (z = -2.787); and very small and large (z = -2.463).** Almost 42% of very small teams (n = 24) had no additional activities, and the same percentage only held 1-2 additional activities per year. In contrast, all medium-sized teams (n = 11) had at least one additional activity, with 55% having three or more activities per year. In large teams (n = 13), only one organization had no additional activities, and 54% had at least three.

There were no significant findings for different types of organizations.

Focus group participants commented on the importance of distributing information multiple ways throughout the year, not just during the annual required training:

> "That's generally our approach in terms of general awareness, just trying to keep the message out there all the time in front of the employees." (D01)

> "Don't just rely on that one or that core set of the security awareness trainings or material, have some other awareness campaigns that go on throughout the year just to try and keep it at the forefront of everybody's mind." (S01)

> "A standard or more guidance on the frequency of communication throughout the year would be really good. Sometimes, executive leadership really wants to limit the awareness training to that one hour at a lot of agencies, and it really needs to be more than that throughout the year…It could be different types of awareness activities throughout the year just to keep the concept fresh in your user's mind throughout the year and not just once a year." (D06)

3.2.2 Communication Channels

Participants indicated how their organizations communicate and disseminate security awareness information. Figure 7 shows the frequencies of communication methods. Online, computer-based methods (89%) and email (84%) were the most popular methods. Over half used newsletters (55%) or websites (51%) to disseminate information. Less than a third made use of videos, pamphlets/handouts, activity fairs, or escape rooms.

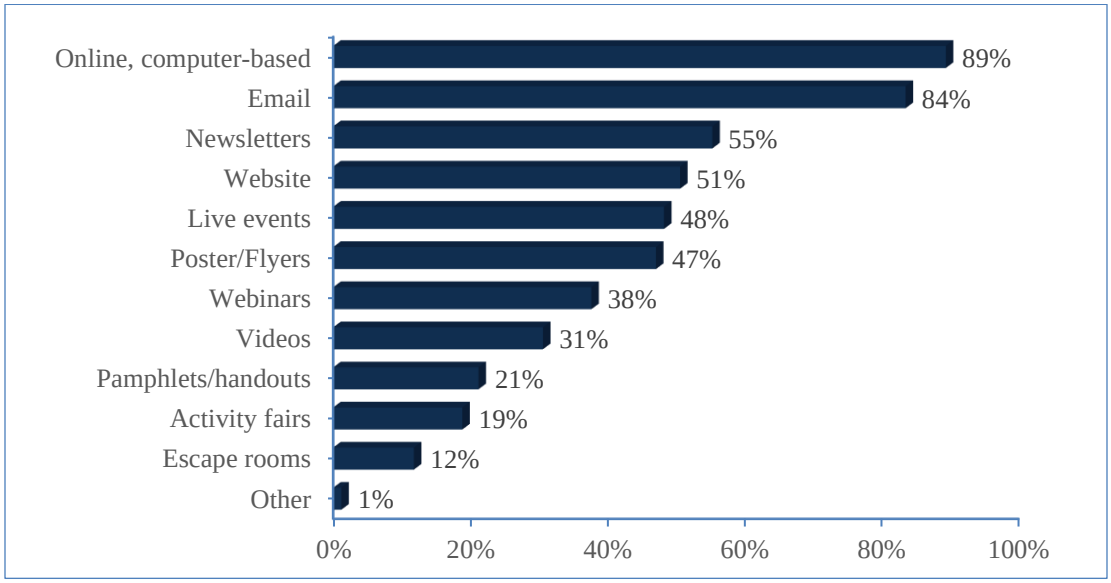

Figure 7: Security awareness communication channels (n=85)

Participants provided more detail on the types of activities their organizations held, ranging from live events for the whole workforce to activities targeted at specific groups within the organization:

> "We now do monthly cybersecurity brown bags where we talk on a cybersecurity topic." (N06)

> "Before the pandemic, we were organizing more events in person, some expos and things that were more fun for users that could count toward things like specialized training but would not replace the general training. And after COVID, we've already had one expo that was virtual which went over really well and was fun, I think, for anyone that wanted to participate in our organization…It includes speakers, it includes forums or maybe panelists." (S05)

> "Smaller events or a large kind of instructor-led event to really heighten users' awareness of various topics relative to security and now in privacy as well." (S11)

> "Our monthly webinars where…users could come in and have an in-person discussion about the awareness topic. Or they could join virtually…and participate and ask questions on the particular cybersecurity awareness topic." (D06)

> "We hold an annual cybersecurity awareness symposium. Usually, it's been a two-day event where we've had breakout sessions that are individualized focused areas within cybersecurity as well as generalized cybersecurity awareness. And sometimes we'll offer vendors to come in and speak, and then other times it's federal employees." (D04).

> "We do a regional office training. We try to hit all of the regional offices at least every two years. And during that time, we will tour the workspaces, meet with IT specialists, conduct manager forums to conduct privacy and security programs' requirements." (N12)

Participants were particularly enthusiastic about interactive approaches to imparting security awareness information:

> "Each quarter we have a security awareness activity, whether it's a virtual scavenger hunt, or last month we had a speed dial where they had to send in an email once they found a certain item, it's in what policy, and tell us what page it was on." (N05)

> "We have done the escape rooms. So, they did some in person before the pandemic, but we've done the virtual escape rooms, which I thought were fun and one of the most fun educational approaches that I've noticed so far using our modern technology to deliver more of a game experience." (S05)

Other organizations put out quick tips using various communication avenues:

> "What we have done is try to inform our community of how important it is for them to understand cybersecurity and to take the training by using splash screens when they first log on." (S03)

> "Short, quick-hitting, videos and audio work the best. Nothing exceeds 15 minutes and most are 5 minutes or less. On demand streaming!" (Q58)

> "We also prepare biweekly tips. That's every other week. And these are tips that are sent to [agency groups] and they can display it on their electronic bulletins …And these tips are very short. They're only like one or two sentences just to kind of catch the eye and remind people that they need to be diligent and watch out for certain things." (N09)

Organizations often held events or sent out additional communications during the month of October, which has been designated as Cybersecurity Awareness Month (previously called National Cybersecurity Awareness Month) [CISA].

> "We have our annual Cybersecurity Awareness Month program every October. This year, we were able to do that online, but we usually have a live program." (N09)

> "This past year, we created a little trivia game that we incorporated in our weekly tips that we send out to the enterprise. What we do is use the theme that's pushed out by, I think it's DHS [for Cybersecurity Awareness Month], for the whole month. Each week we center the broadcast on the theme and then we included the trivia game link where they get questions, and the more questions they get right, they get a little message at the end that they basically were cyber gurus or cyber ninjas or whatever the term we would do for that week to show that they were successful in answering the questions correctly." (S02)

We also calculated the **total number of communication channels** used by participants' programs. Figure 8 shows the percentages. Only 7% disseminated security awareness information in just one way, with the largest percentage (41%) utilizing 2 - 4 methods and 22% using eight or more methods.

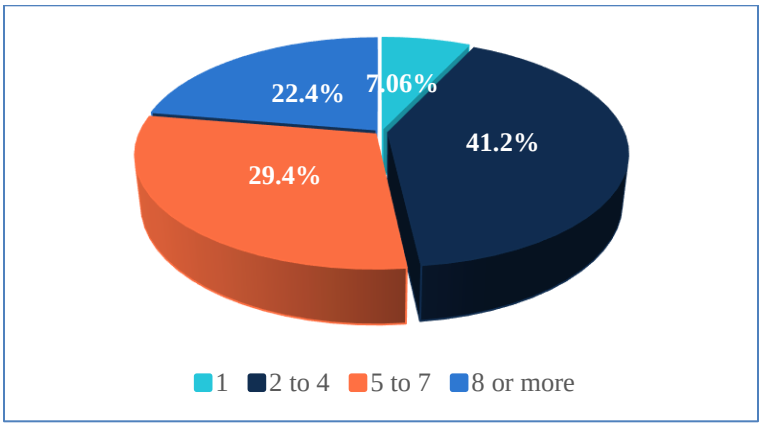

Figure 8: Number of security awareness communication channels (n=85)

We found statistically significant differences for the number of dissemination methods between small and very large programs (z = -2.792), with 72% of small programs (n = 18) and only 27% of very large programs (n = 22) disseminating information in four or fewer ways.

While using multiple communication channels was encouraged, participants acknowledged that distributing too much information could be counterproductive:

> "In the role of CISO, I'm very hesitant to bombard people with a lot of information because I don't want them to ignore me when I need them to pay attention. So, I try to be very selective about what information I'm providing and how often that information gets provided." (N10)

> "Balancing communications to keep people aware without kind of coming off as spam by producing too much material, which can get to a point where nobody's even reading it anymore." (D03)

> "Our big fear is that people will throw our – and we've seen it – that if we send too many notifications and stuff, they send it to either a junk box or they send it to a mailbox they never look at." (N07)

3.3 Topics

Participants indicated topics that their security awareness programs addressed via training courses, events, or other communications in the past 1 - 2 years. Figure 9 shows the security awareness topics and percentages of programs addressing those topics. All participants' programs covered the topic of social engineering, and over 90% addressed passwords and authentication, malware, and privacy topics. Security considerations when installing or updating software was the least covered topic but still addressed by 64% of programs.

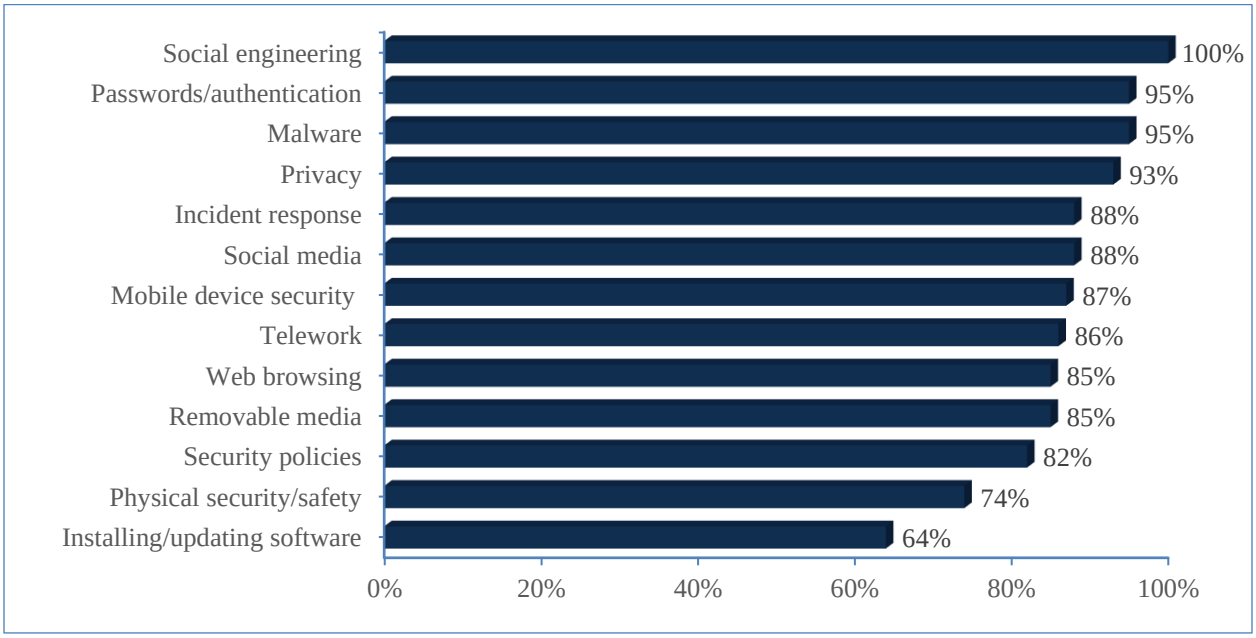

Figure 9: Security awareness topics (n=85)

We also wanted to know how often the participant's security awareness program provided information applicable to their employees' personal or home lives. Figure 10 shows the response results. Seventeen percent never or rarely provide topics that are applicable to employees' personal or home lives. Forty-one percent provide it a moderate amount or a great deal.

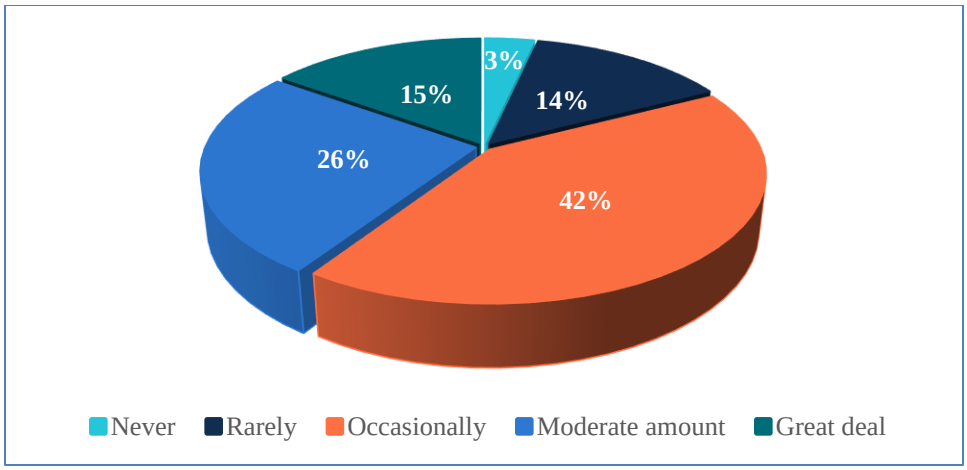

Figure 10: Frequency with which security awareness programs provide information applicable to employees' personal lives (n=86)

As observed in participants' open-ended responses, making a work-home connection was viewed as essential for habituating good security choices no matter where people are or what they're doing. When asked what advice they have for making programs successful, several survey participants mentioned the work-home connection:

> "Use examples that the employees are likely to encounter in their daily work and personal experiences." (Q42)

> "Get out of generic advice filled with platitudes and focus on specific activities that help employees in their daily lives (home and work)." (Q29)

> "The most successful aspect of our security awareness program is the positive feedback that we receive from staff stating that the information provided also helps them in their personal lives. This makes us feel as though we are serving a dual purpose with the security awareness information that we are providing to those within our agency." (Q32)

> "Start by focusing on helping people secure what they care about (such as their kids online) so they start developing awareness that they bring back to the office." (Q50)

Focus group participants also discussed their efforts to integrate security information that could help employees in both their work and personal lives:

> "We educate our end-users from a holistic perspective. It doesn't just touch your work life, it touches your personal lives as well. So, making sure that you have secured all of your devices, whether it's work or personal or your at-home computer. We also did some education around internet safety with kids and teenagers during our National Cybersecurity Awareness Month." (N04)

> "Especially with the times that we're in now, a lot of people are working from home constantly. So, we try to educate our users on how to help their families and stuff using the internet from home and your work computers from home." (N02)

> "In my mind, security awareness, it's not just about being educated. It is about actually creating a lifestyle, changing their mindset in your practices and your behaviors. And the only way, in my opinion, that that can happen is if I make it relevant, if I make what I'm telling you relevant to your everyday life, in meeting you where you're at. So, if I can't meet you where you're at, then I don't feel as if I'm doing an effective job." (N10)

3.4 Phishing Simulations

We asked participants if their organizations perform phishing simulations (sometimes called phishing exercises) in which employees receive fake phishing emails to teach them to recognize characteristics of actual phishing attacks. As Figure 11 shows, the majority of participant organizations (just over 85%) perform some type of phishing simulation.

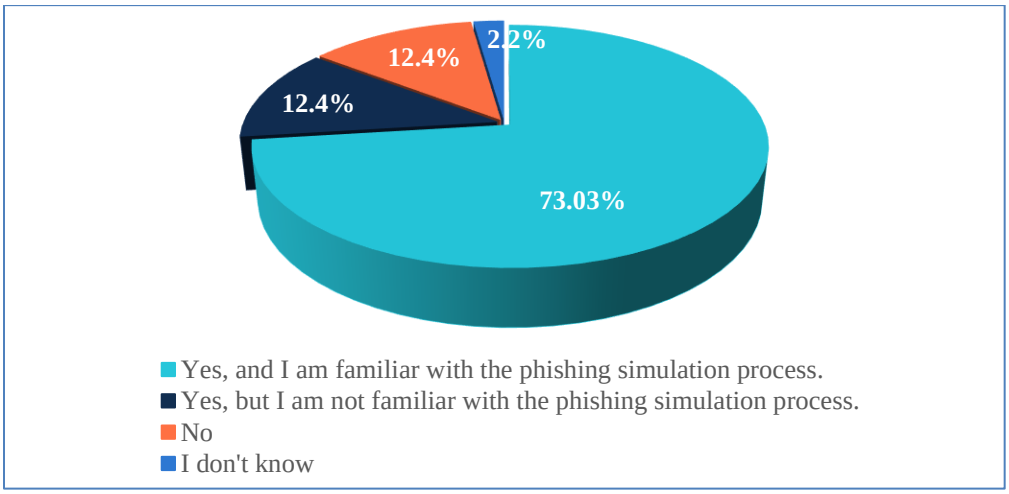

Figure 11: Organizations performing phishing simulations (n=89)

Participants provided more detail on their phishing simulations:

> "We are also doing phishing exercises. They are targeted phishing exercises, and we do report them on by clicks, and they are even broken down reported by organization and what area within the agency." (N02)

> "We also carry out the simulated spear phishing exercises to kind of gather data on how the Department is taking the phishing training and whether they're carrying that out." (D03)

> "Since it has been on the annual FISMA report for the last several years now, we do phishing exercises, and it's really been a fairly recent activity." (D05)

Participant quotes also provide insight about the intent of phishing simulations within organizations, including identification of a phishing email and subsequent reporting:

> "Detection of phishing emails needs to become ordinary not extraordinary." (Q61)

> "What we also tried to get our employees aware of, that not only should you not click on the link, but you should also report it so that if it is a real phishing exercise, those that are responsible for looking into it and investigating are aware of it. So, we've gotten more tickets open based off of our phishing exercises, which is more participation and awareness that we've been able to determine from those exercises that we are putting out." (S02)

> "We'll see an uptick in who reports what they don't know to be the phishing exercise to our security operations center. But it also depends on the topic and how clever the email is, too. So, the more clever, more relevantly tied to what resources they may currently be using at the Department, we may see more people get caught. But we do see where people do begin to recognize a little bit more and actually report it, which is what we also want to train." (D04)

Some organizations provide a reporting button within the email application to make it easy for employees to report suspected phishing emails:

> "Part of the phishing program is the ability to report, and this year we were able to add a report phishing button so users could actually report the phishing exercises with just a click as opposed to having to send an email, and we saw phishing reporting rise. It was just overwhelming adding that technology. That has worked very well in terms of engaging employees. I would say that that's probably the area where we've seen the biggest increase." (D01)

> "We've added a reporter button. So when they see that email, they just click it, and it goes straight to the service desk. And that has definitely helped our numbers go up with the reporting aspect of the phishing emails." (N02)

> "Make it easy to check/mark spam and report questionable issues." (Q33)

Overall, phishing simulations were often viewed as one of the most successful aspects of security awareness programs:

> "I would say that the ethical phishing program is going really well. It took some time to get the buy-in of leadership to launch some of the tougher scenarios, but the users are getting it. The users are reporting the emails and recognizing them, and the susceptibility rate is going down really low." (D06)

> "And one thing that's come out in this talk is how important each of our phishing programs are to our awareness training program. So, if we had this conversation maybe three years ago, we wouldn't be talking about the phishing programs as much. But because that's such an area where people are most susceptible and most able to have our agencies compromised, that's become very important." (D01)

> "Over the past 2 years, we've seen a drop in our phishing click-thru rates likely because of our increase in phishing simulations." (Q37)

> "One thing that's worked pretty well is the phishing exercise program that we introduced a few years ago. We actually used an open-source and borrowed the customizations from another agency and deployed it, basically, at very minimal cost." (D05)

Participants who indicated that their organization had a phishing program with which they were familiar were then asked a series of follow-up questions about the program, with responses described next.

3.4.1 Frequency of phishing simulations

Participants indicated how often their organizations conducted phishing simulations. As seen in Figure 12, 75% conduct phishing simulations either monthly or quarterly, while just under 5% of organizations conduct simulations more frequently than once per month.

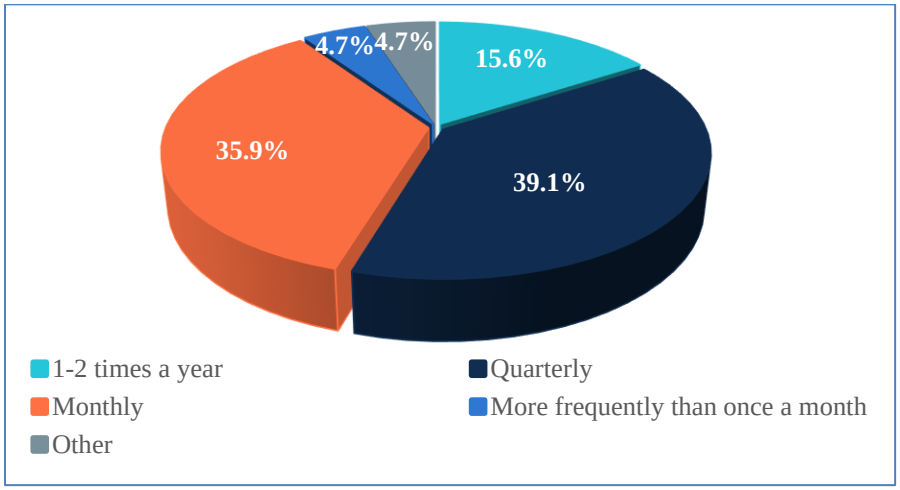

Figure 12: Phishing simulation frequency (n=64)

We found significant differences in the frequency of phishing simulations based on program size, specifically between small and very large organizations (z = -2.208) and medium and very large organization (z = -2.726). Among very large programs, 50% conducted phishing simulations at least monthly, as compared to small programs with 33% and medium with 20%. There were no significant findings for organizations of different types or team sizes.

Focus group participants commented on the frequency of their phishing exercises, most often monthly or quarterly:

> "We do quarterly phishing tests as well. And we just select an audience, maybe rotate around the foundation or a group of people and put together phishing emails together and we send them." (N11)

> "We do that [phishing exercises] on a regular monthly basis to a subset of our employee population." (D05)

> "Phishing entire workforce with email access…monthly" (Q61)

3.4.2 Handling Repeat Clickers

We also asked participants what happens to repeat clickers in their organization (those who repeatedly fall victim to phishing). Participants selected all options that applied. Figure 13 shows the percentages for each response option. In 41% of organizations, repeat clickers had to complete additional training, and 26% notified clickers' supervisors. However, in 8% of organizations, nothing is done at all for repeat clickers.

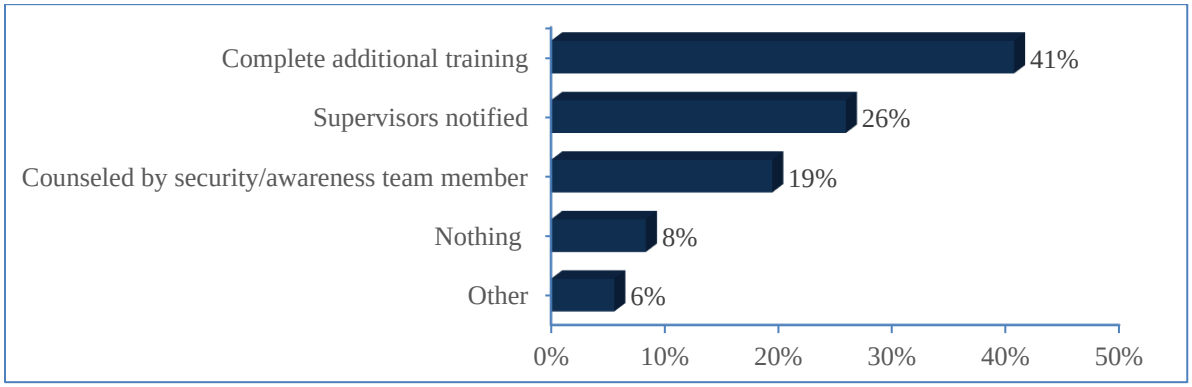

Figure 13: Repeat clicker consequences (n=64)

In many organizations, repeat clickers are assigned additional training:

> "Part of those phishing exercises we also have a policy for behavioral escalation based on whether or not employees pass or fail those exercises. When employees exhibit unacceptable behavior, they have to take more training." (D01)

> "If there is a repeat offender when it comes to phishing exercises, we do assign them refresher training." (N04)

Some organizations follow up with clickers in other ways:

> "The most benefits I think we are going to see is the monthly debrief after phish emails are sent out. We have about 70% return rate, meaning folks report on the phishing about 70%. And so, at this point, we don't know what's going on with the rest, the 30% that don't report. And so we're sending out debriefs now on a monthly basis. We show why an email should have rung a bell with folks. So, we're hoping that that is going to change user's behavior because now they can see how they could have figured out that this was a red flag." (N03)

> "If it looks like there's a lot of repeat offenders, then I think there's another conversation that takes place with the division or the staff that are doing the clicking." (N11)

Others recognize the need to address repeat clickers, but have yet to implement any specific procedures:

> "We are currently working on some enforcement training for those who are clicking on these exercises. Right now, we are just giving them information once they have clicked on them, what to do, and that. But we are looking into incorporating training to those who are continuously clicking on these links." (N02)

> "What we do is look at how to advise them on additional training. We haven't decided on what that means outside of those tools that are available to us through either other cybersecurity awareness training videos or opportunities, but we haven't created anything internally ourselves." (S02)

3.5 Recognizing Positive Security Behaviors

We asked participants if their programs rewarded or recognized employees for practicing positive security behaviors (see Figure 14). Over half of the programs did not recognize employees, whereas less than a third provided a certificate or badge or personal thank you. Other organizational recognitions were only awarded by 14%.

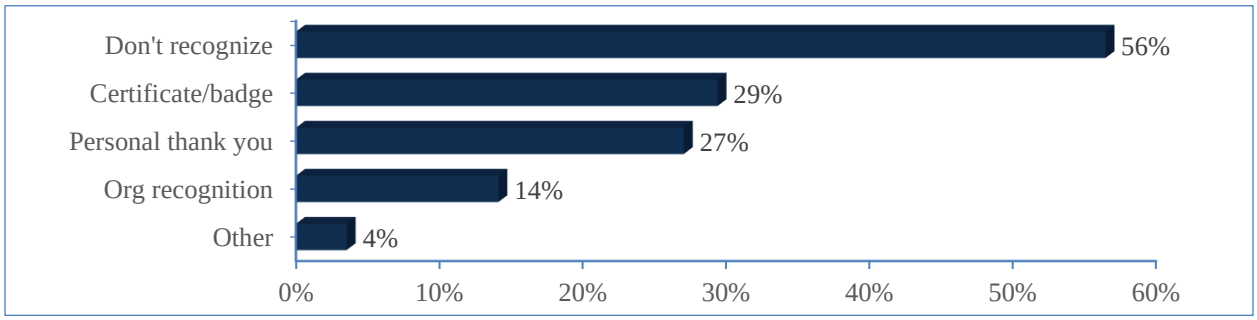

Figure 14: Ways in which good security behaviors are recognized (n=85)

Incentive programs and rewards were discussed by survey and focus group participants. Survey participants reflected on the value of acknowledging good security behaviors:

> "[Security] is sometimes an overwhelming challenge, and atta-girl, atta-lady, and atta-boy pats on the back have to be issued BUT NOT superficially." (Q73) (emphasis theirs)

> "Focus less on bad behaviors and highlight good behaviors -- help employees learn from model employees, not through negative examples." (Q29)

> "Finding a way to recognize folks for doing the right thing or being more strategic in our employees ability to recognize and build a stronger security awareness program and bond with the employees. I am not sure how to do this, but I believe it may be a great alternative way to get employees more engaged." (Q93)

One focus group participant explained why her organization does not broadly recognize employees for their positive security behaviors:

> "Our leadership has been a little hesitant to display any names. I guess that there might be a union issue as well. So, I send specific info only to the directors of the respective divisions, that's about as far as we go concerning names for anything." (N03)

Other focus group participants elaborated on incentive programs linked to their organizations' phishing simulation efforts:

> "We've implemented something that we call [NAME]. [NAME] Program is based off of our phishing exercise results…The [NAME] program gives you level one through five. So, as you move up in your levels, you become more robust with your education and knowledge when you receive a phishing email. So just from reporting, which is your level one, that's the number of times that you actually report a phishing email, versus getting up to a level five where you're actually helping out your fellow co-workers to identify phishing, or how to identify maybe not a phishing exercise email, but maybe an email from the wild… That program has been pretty successful. The [organization is] very competitive internally. So, they like to get those [rewards] at their desk when we can provide it to them physically, or they get those in an email. Then we actually have an overall division board for the best rating for the phishing exercise for that quarter. So, the divisions get recognition as well." (N04)

> "We're analyzing those phishing results, so we do agency-wide phishing exercises as well as specialized spear phishes against targeted groups. And we'll post a leaderboard that is available to all of our components as well as, we've worded it, a '[NAME] award'…So, they get emails of recognition, certificate recognition as a shark award for successfully following our reporting process. And we introduced a phish hunter program, which is actually a phish hunter badge, and it's an icon that employees can display on their signature icon in Outlook, as well as on our agency organizational chart." (N01)

3.6 Changes Due to Pandemic

We asked participants about changes to their security awareness program approaches due to the pandemic and if they anticipated continuing those changes after the pandemic. Sixty participants answered this open-ended question. Focus group participants also commented on these program changes.

Unsurprisingly, because most organizations moved to telework during the height of the pandemic, in-person events had been put on hold, with virtual events taking their place. Many participants touted the success of their virtual programs and planned to continue having a virtual component after employees return to in-person work:

> "We have gotten great feedback from the virtual environment. We will potentially keep the virtual environment because it is convenient for users." (Q47)

> "We were able to reach people outside of the [headquarters] area and increase our attendance from 100 to over 500 participants." (Q40)

> "I would say engagement is increasing. I don't know this year if it was because of the virtualness and they're looking for something to do or not, but we had record attendance at our National Cyber Security Awareness Month events in 2020." (D06)

However, several participants, although in the minority, indicated that virtual events had not been as well-received:

> "We virtualized everything. It wasn't as popular. We will resume…in-person options upon return." (Q56)

> "Attendance is lowered due to everything being a virtual meeting." (Q44)

Several participants indicated that their organizations had increased or improved other types of secure awareness communications, such as email or the organization's cybersecurity website. Others stated that their security awareness programs had added new topics relevant to a remote workforce, such as: connecting personal devices to work laptops; virtual private networks (VPNs) and encryption of communications; wireless security; secure use of online collaboration tools; operational/physical security when teleworking; proper handling of controlled unclassified information; and security information that could be used in employees' personal lives.

3.7 Challenges: Security Awareness Approaches

We asked participants to rate their level of challenge with respect to various facets of security awareness approaches on a five-point scale ranging from "very challenging" to "not at all challenging," with a "does not apply" (N/A) option. Figure 15 shows the challenge ratings.

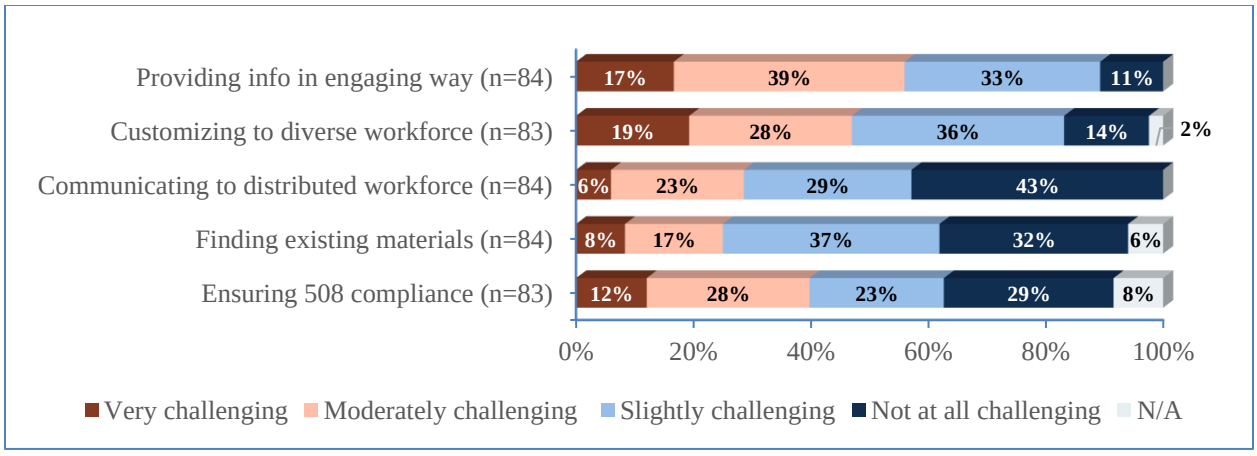

Figure 15: Challenges – Security awareness approaches

For all challenges, no statistically significant differences were found between groups.

The remainder of this section provides more detail on survey results for each challenge while incorporating example supporting quotes from focus group and survey participants to provide additional, qualitative insights.

Providing security awareness information in an engaging way: Over half (56%) of survey participants indicated that being able to provide security awareness information in an engaging way was very or moderately challenging. Only 11% rated it as not challenging at all.

Focus group participants elaborated on challenges they have engaging their workforce:

> "If a user clicks on a phish – an authorized phishing exercise – an education page comes up, and we see that users don't linger. They click away within seconds. They cannot possibly have read all of that information. Also, for the October Cybersecurity Month, we sent out weekly messages. We had a poster board. So, we've tried a variety of things. And we received one single response saying this was nice or interesting. So, I think we just have a bit of an issue with users not lingering on the material." (N03)

> "A couple of concerns for us is keeping the awareness training engaging. So, our users, definitely, they're tired of death by PowerPoint. They don't want to see it delivered that way. But that puts us in a difficult spot sometimes because of resource constraints and the frequency that we have to deliver the training. So, we can't typically create something that is new in that turnaround that's required of us." (N01)

> "In the commercial area in the same kind of field, it seems like they're a lot more technologically forward. They have a lot more tools and a lot more bells and whistles in what they can present to their people that can present information to them related to security than I'm finding, at least with my agency. Some of our training previously were PowerPoint slides that were totally boring, that people really don't want to sit and read through or listen to, and doesn't have the whole splash that you can get for some of the external or commercial environments. So, I wish we had a lot more of that resources available to us here in the government." (S02)

Several survey participants expressed advice for overcoming current challenges in delivering engaging material:

> "Actually prepare people for what they need to know, not try to make people sit through multiple hours of online courses where they retain little and there is so much superfluous information that the key points get lost." (Q63)

> "Interactive programs have proven much more effective then *[sic]* slideshow-based programs." (Q25)

> "Engaging people IRL [in real life] more instead of over the computer screen." (Q37)

Customizing security awareness information to people with varying needs and levels of IT and security knowledge (diverse workforce): Security awareness information is meant for the general workforce, but that workforce is made up of individuals with varying backgrounds and job roles.

Customizing information to be understandable and relevant to a diverse workforce was seen as challenging by 47% of survey participants. Several participants commented on the need to tailor security awareness content to different roles and groups of individuals within the organization:

> "Separate the 'new employee needs to know' from the refresher training. One size courses do not fit all." (Q29)

> "One of our biggest challenges is the diversity of our workforce. We have people that are out [working in the field]. We have people at an office such as…a supervisor, then we have people at a district office that strictly do administrative duties, and then we have headquarters and leadership folks that have a more sensitive role…With our phishing campaigns, one of the attributes we track is what their job is. And we are finding that people that are the busiest and the most pressed for time are the ones that click on our phishing emails the most. So, we have narrowed it down to about three work groups that are the repeat clickers and cause us the most pain. So, our challenge is to find ways to make an impression on those people that they need to slow down and really look at the email before they click." (N05)

> "Many personnel in the organization are cyber experts, difficult to balance the program." (Q25)

> "I have been doing research on different learning styles amongst people in different generations and trying to offer training in accordance with that." (N09)

> "I would have a program that adapts the content based on the knowledge level of the individual. Like learning programs that will continue to challenge your understanding of a particular topic until you master it. For example, some individuals have difficulty understanding how to identify a phishing email. The ideal training program would continue to demonstrate/test the individual until they could easily identify a phishing email without fail regardless of how complex it may be." (N10)

Communicating security awareness information to a distributed work force: Some of the organizations represented in our study had a workforce stationed in multiple areas of the country or world. A pandemic-induced transition to a remote workforce also introduced challenges similar to those experienced with distributed workforces. Twenty-nine percent of survey respondents said that they were very or moderately challenged when trying to communicate security awareness information to their distributed workforces. Several focus group participants also encountered this challenge:

> "One of our challenges is that we have employees all over the world, which is challenging – not from a language barrier perspective, but from the perspective that some people have trouble with internet access in certain parts of the world. Also, there is a large portion of our population who don't work in a normal office setting – they're out in the field, so they aren't on their computer on a regular basis." (S10)

> "In the past, everything is just PDFs and documents that don't really work in the remote environment, especially when people are now accessing things through their phones." (D03)

Finding existing security awareness materials to use: A quarter of survey participants rated finding existing security awareness materials to be very or moderately challenging, as echoed by several focus group participants:

> "If there was a central repository within the federal government even, of various trainings and awareness pamphlets, flyers, presentations, stuff like that, that the various agencies could actually share and leverage back and forth, I think that would definitely better help us make use of what limited resources we do have." (S01)

> "We've been holding off on assigning additional training to repeat phish offenders because we are fearful of the months that lie ahead. What will we do with the same staff members 4 clicks from now? We don't have that much material which we could suck into our Learning Management System in order to assign to users." (N03)

> "I don't think that there's enough material that's commonly available such that we can grab it and then customize. So, it would be nice if there were more government-wide topics where those agencies that are identifying the regulations would produce some training relative to cybersecurity or privacy…If there were more government-wide or more small vignettes of training that we could tap into to create some greater training material, that would be very useful." (S11)

Ensuring security awareness materials are 508 compliant: When ensuring that security awareness communications and materials are compliant with Section 508 of the Rehabilitation Act, 40% of survey respondents encountered challenges. Survey and focus group participants offered additional insights on this challenge:

> "Supporting offices like 508 must be properly staffed to adequately fulfill request for review and editing to make content 508 compliant." (Q96)

> "We did cybersecurity escape rooms, and that was a huge win for us. Users loved the idea of that. But, unfortunately, some of those things cannot be delivered to the masses or are not 508 compliant." (N01)

> "With the videos or with all communications, 508 compliance is generally a challenge. And I think there needs to be, on a whole, a larger compromise to allow the production of content that is not 508 compliant for users that don't require the use of assistive technologies and to allow a complement communication that is Section 508 compliant. For instance, I wanted to introduce some virtual reality type scenario training. Well, there's no way that you're going to make a 3D environment Section 508 compliant. So, there's a large part of the population that could benefit from that interactivity because that's their learning nature. It's more engaging. It's different, and you can make it a little bit more

specific. And you can take that same concept and you can put it into a format for those users that do require the use of assistive technology." (D06)

4 Aiding and Informing the Security Awareness Program

This section reports on results related to which internal and external resources (e.g., information, forums, and other groups) influence and inform federal security awareness programs or aid in the delivery of security awareness information.

4.1 Department Influence

For participants whose organization was a sub-component (i.e., agency under a Department), we wanted to know what best described their security awareness program's relationship with their departmental security awareness program. Figure 16 shows that over half (56%) of sub-components were required to use the security awareness training from the Department. For 31%, the Department provided the training, but use is optional. In 6% of cases, the Department either provided topics but no training or did not provide sub-components with any materials or guidance.

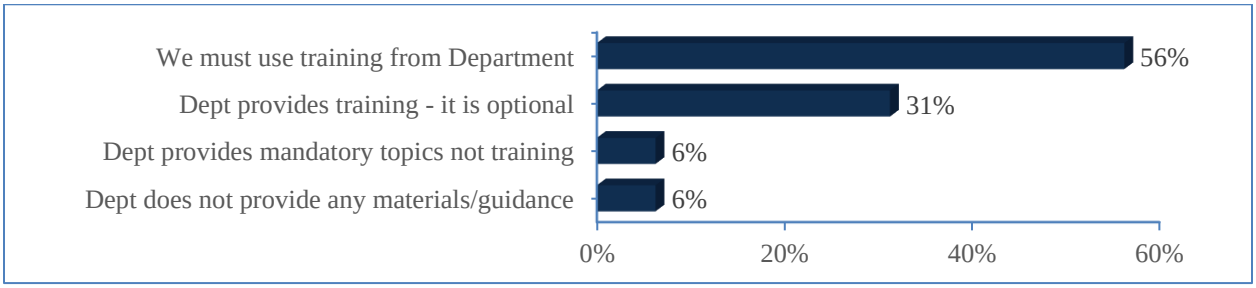

Figure 16: Subcomponents' security awareness relationships with their Departments (n = 32)

Focus group participants from sub-component organizations had very different experiences related to what security awareness material was passed down from or mandated by their Departments, ranging from complete to no autonomy.

"We really don't get a whole lot of guidance on our training from [the Department]." (S04)

"We basically are able to tailor our training on our own. We do get input from Department, but we are not dictated by Department on our security awareness program." (S03)

"Our Department, they create their own security awareness course and we sort of have the flexibility to use it or create our own and seems like they give us complete flexibility regarding creating our own." (S06)

"They [the Department team] start with the same approach every year where they are developing the annual training at the Department level and the agencies are providing input for improvement and development before it's released to users, so we can provide ideas for topics directly for the training." (S05)

> "[The Department] handles the program. We don't really have room to… contribute any…response to the content…We're kind of limited. I wish we had more leeway, whether it's money, having the capability to get either a contract with a vendor, independent of the Department, to design our own training tools. We don't have that right now. I wish we did." (S02)

For those participants who worked at the Department level, we asked if their organizations provided security awareness training or materials to sub-component agencies (see Figure 17). Over half of the Departments (53%) provided security awareness training that their sub-component agencies must use, and 17% provided optional training. Seven percent did not provide any materials or guidance, and 3% provided topics but no training.

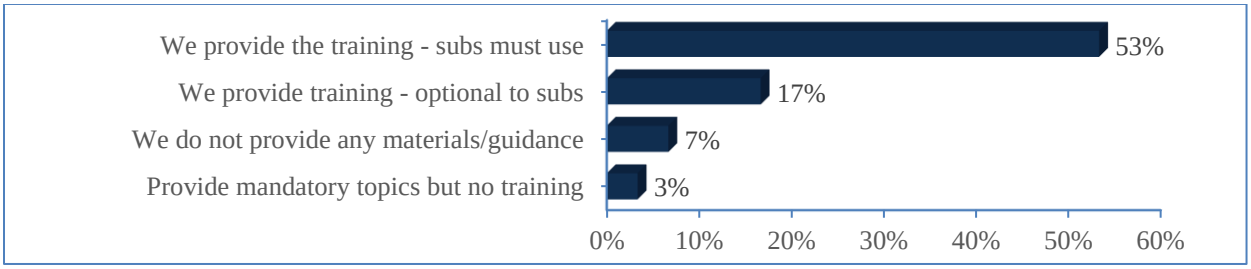

Figure 17: Departments' security awareness relationships with their sub-components (n = 30)

Department-level participants from the focus groups commented on this relationship:

> "All of the content that we produce is available for all of the subagencies. About [half of the] subagencies use our content, and another [half] or so are large enough where they'll use a portion or they'll create their own that's a little bit more targeted and branded to their mission." (D06)

> "Departmental sets out minimum requirements for all security controls, including training. And if the agencies within the Department go above and beyond that's great, and that's encouraged." (D05)

> "In regard to broader like our [security awareness] symposium, we've started taking the approach of wrapping in our [sub-components] to try to see what their needs are to get more of a collaborative effort to get something consolidated at the departmental level." (D04)

4.2 Internal Sources

4.2.1 Collaborations with Internal Groups

Participants were asked what other teams/groups within their organization they collaborate with or consult in their security awareness mission (Figure 18). Over 70% collaborated with the incident response team (77%), the privacy team (73%), and the IT team (71%). Much fewer work with the General Counsel (39%) and Human Resources (HR) (38%).

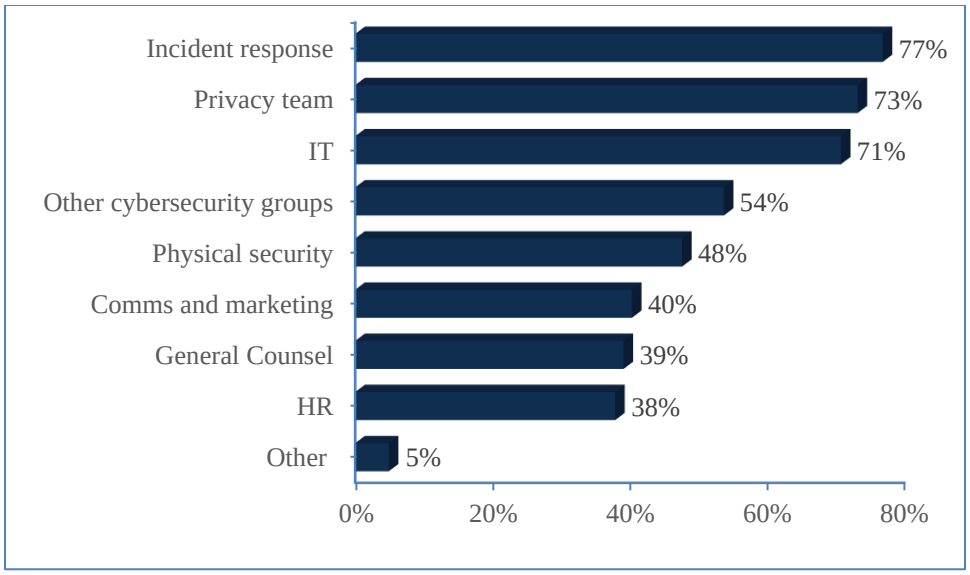

Figure 18: Internal groups collaborating with security awareness programs (n=81)

Internal collaboration was discussed extensively within the focus groups. Not surprisingly, security awareness teams often consulted with other security or IT groups:

> "I do consult with members of the SOC [Security Operations Center] to see if there's anything glaring that I need to include in my training each year." (N09)

> "Also working with the help desk, just what type of problems our users encounter that are related to security issues." (S05)

> "Being tied directly to the cybersecurity policy team has made it easier because the awareness team always has whatever the latest guidance is and can push that out very quickly." (D03)

> "We've worked closely with the information security officials" (N08)

> "I'm located in the chief information security office, and there are…divisions in that office that provide a wide range of cybersecurity services to the Department. And those managers have responsibilities for things such as identity management, internet response, data loss prevention. So, within any year, I reach out to those stakeholders to ask, 'What's important for the user to understand about cybersecurity awareness? What do you want to talk to the customer about? What kind of behaviors are you seeing that you want us to help encourage them to do or not to do?." (D01)

> "Build relationships with offices within your organization- Incident Response, Help Desk,…FISMA Compliance." (Q24)

Beyond other technology-focused teams, participants also commented on the value of working with other groups in the organization:

"The learning management folks help me out on some of the communication aspects." (N11)

"Partner with many, varied internal organizations to minimize the burden on staff and create a routine process across the varied internal organizations. For example, processes should be the same for security, as for privacy, physical security, ethics, etc." (S11)

"I gave the example of just my legal counterparts and human resource counterparts, for a variety of different reasons, making sure that course material doesn't promote or say something that would contradict a legal requirement, not to mention human resources – their training requirement is from a federal human resource perspective, so they're just – certainly might have also good resources to collaborate with and leverage in terms of ideas and platforms." (D04)

"Build bridges with your communication teams and the communication workflow and develop a smooth, repeatable process so that once your communications are produced, that the production and the distribution is standardized." (D06)

4.2.2 Sources for Topics and Approaches

We asked participants what sources within their own organization inform security awareness topics and approaches (Figure 19).

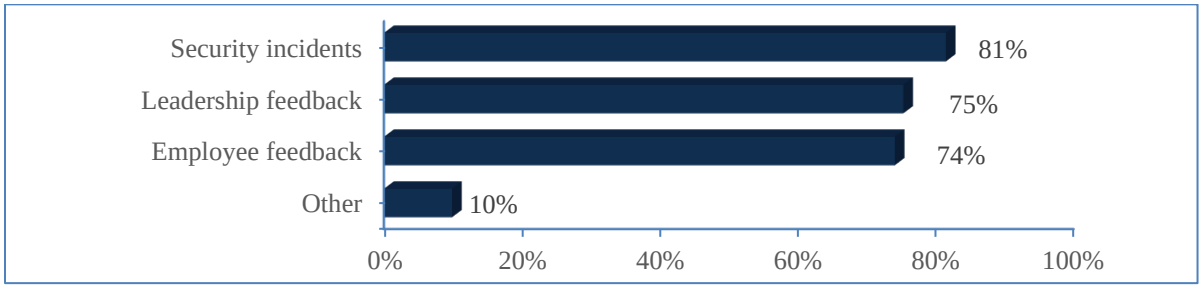

Figure 19: Internal sources informing security awareness topics and approaches (n=81)

Security incidents: Security incidents experienced by the organization were a common source driving security awareness content (81% of survey participants). Participants provided additional details:

"Security incident reports that are used to influence the topics in the training. This way, you may be able to see a difference in behavior." (Q53)

"Pick general security awareness topics based on the incidents that the Department experienced over the previous year." (D06)

"If we see our monitoring tool might be catching a lot of emails going out that maybe unencrypted or people not following specific policies that we have, then we'll put out a reminder or something related to that." (N12)

Leadership feedback: Leadership direction and feedback was selected by 75% of participants. This input often drives the priorities of the security awareness program:

> "Sometimes it would be based on priorities for the Department that the Secretary or even the CIO will have." (D02)

> "If there's a certain type of breach or attack somewhere, we'll get a request from the Secretary or somebody to say, 'Hey, we want you to stop everything you're doing and create an article or create a e-blast on this topic'." (D06)

Employee feedback: Almost ¾ of survey participants indicated that employee feedback informs their program. Several organizations discussed how they adjusted their security awareness content based on direct feedback from the workforce:

> "We ask our employees for topics that they may be interested in." (S09)

> "Feedback from the customers, too, or the people that take the training. If they have any feedback about something that needs to be improved or something that I overlooked, then I will incorporate that into the training as appropriate." (N11)

> "With our different groups, they are very vocal throughout our agencies just asking for help. The various groups that we have will come up with their own themes about what they want more guidance on, actually. And that often does dictate the types of presentations or other ideas for information that we need to get out to them and then maybe the whole agency." (S05)

> "There is a more formal effort with the voice of the customers that my management office uses on an annual basis." (N09)

4.3 External Sources

We asked participants to indicate the external sources that help inform their organizations' security awareness program. Figure 20 shows the response frequencies for this select-all-that-apply question.

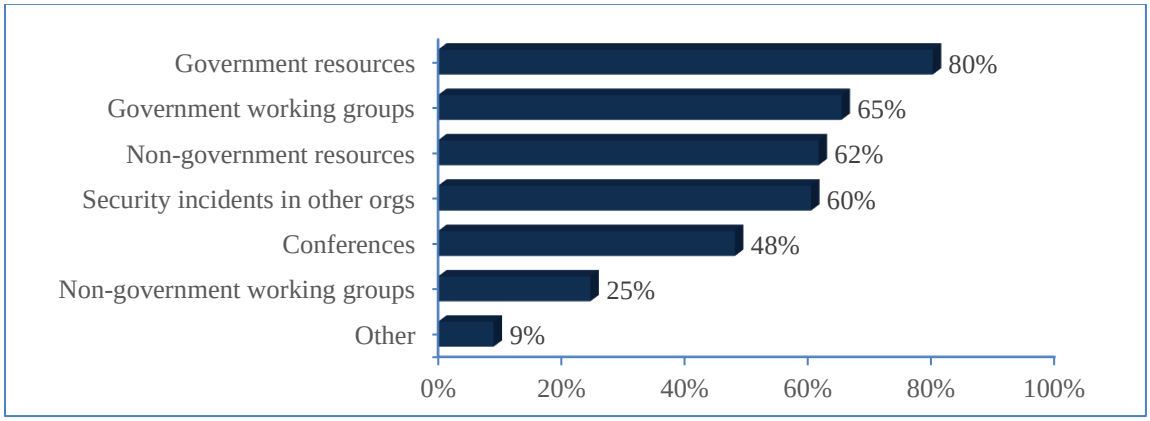

Figure 20: External sources informing security awareness content and approaches (n=81)

Government resources and working groups: A large majority of organizations (80%) were informed by government resources, with 60% informed by government working groups. Participants mentioned specific resources:

> "I think historically in terms of topics or for the October Cybersecurity Awareness Month, we definitely leverage what's being done at the federal level and push that out." (D04)

> "For me, usually my first go-to is what is CISA [Cybersecurity and Infrastructure Security Agency] about, right, because they kind of got the scope on the entire .gov space. At the same time, they work with industry as well. So, anything that they are bringing to light, I try to emulate that and try to kind of go, 'Hey, this is something that CISA's saying is important as a threat. You, as an individual, need to know that this is a threat. This way you are aware of what's going on the other way'." (N10)

> "The NIST SP [Special Publication] 800 publications are useful" (Q78)

Participants also talked about direct interactions they have with other government organizations:

> "We also created a Department level Security Awareness Training Working Group which has benefited the security awareness programs throughout the Department." (Q23)

> "We bring in speakers from outside. We've had speakers from [other government agencies]. We've partnered with [a Department] to join their annual event in October as well." (N08)

> "Building friendships with our counterparts at other agencies, we then do some information sharing so that we can kind of help each other with, 'Okay. What were the challenges that you had this past year? What were the things that worked well? And what would you need to change?'…If we kind of ask ourselves this throughout the year and share the results, we can help each other build more efficient programs for our respective agencies." (D02)

Non-government resources: Non-government security resources were used by 62% of survey participants' organizations. Sources most often included news stories and online security resources:

> "The other things that I would get topics from which is just general news stories. Something that kicks off in the news, like when Equifax had the breach, that was one. It was like, 'Hey, here's what happened with Equifax. Here's how it could potentially impact you. And here's how we can avoid it'." (N10)

> "We do a lot of Googling, just to find out what's going on out there. Cybersecurity online magazines, things like that, we pull from those resources as well." (N04)

Security incidents in other organizations: Sixty percent of survey respondents utilize information on security incidents in other organizations, as reflected in the focus groups:

> "We annually meet with [an external organization's] computer security incident response center, and I get them to produce a list of user-induced or incidents that could have been prevented by users, kind of by category. And I take a compilation of those, the most recent Verizon data breach report, and the IBM threat report and kind of take a mix of the top threats from those three sources and kind of whittle them down into about eight or so topics for the cybersecurity awareness training." (D06)

Security awareness topics frequently were attuned to seasonal security incidents/attacks, for example attempted impersonations of the Internal Revenue Service during tax season or online shopping incidents during holidays:

> "We use seasonal messages and also relevant topics of observed activity within the cyber security realm. For instance, when we see an uptick in ransomware activity nationally/internationally we may develop an awareness article about that." (N05)

> "We do seasonal things or get our information mostly by the Weekly Wire, I'd say, during the tax season and the holiday season. And certainly, when COVID started, we had a brief campaign, in the beginning, asking people to watch out for certain types of phishing emails." (N11)

Conferences and non-government groups: Fewer survey respondents selected conferences (48%) or non-government working groups or forums. A participant mentioned an industry forum for security awareness professionals:

> "SANS Secure the Human. It's an online forum…and they have people from all over the world, and they share ideas, share solutions, share lessons learned." (S10)

4.4 NIST Security Awareness Resources

In the survey, we asked participants if they used security awareness and training resources sponsored by NIST. The Federal Information Security Educators (FISSEA) [FISSEA] is a government organization assisting federal agencies in strengthening cybersecurity awareness and training programs. The group holds an annual conference or seminar series. To gauge familiarity with FISSEA, we asked participants if they had heard of FISSEA and attended any FISSEA events. While 62% had heard of FISSEA, only a third had attended a FISSEA event. Figure 20 shows the responses for FISSEA attendance.

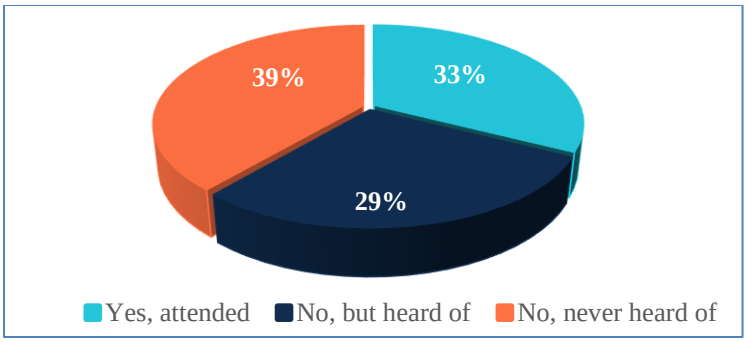

Figure 21: FISSEA awareness and attendance (n=80)

Several participants mentioned FISSEA specifically:

> "I have for many years been involved with FISSEA and get approaches that way." (D05)

> "I would say get involved with the NIST FISSEA group to attend that conference, yearly conference. I've gotten a lot of great ideas attending that conference and also looking on the FISSEA website. They have a contest and looking at all the submissions people turn in for those contests will give you a lot of great ideas for security awareness." (S06)

We also asked participants if they had ever used the NIST Special Publication 800-50 "Building an Information Technology Security Awareness and Training Program" to inform their security awareness program. While the large majority (84%) had heard of the publication, less than half (48%) had used it. Figure 22 shows the response frequencies.

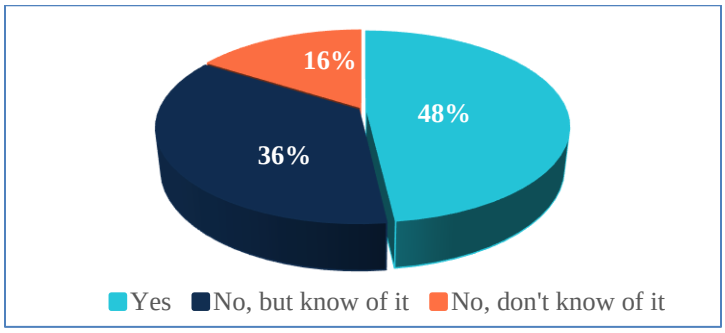

Figure 22: NIST Special Publication 800-50 awareness and use (n=81)

4.5 Challenges: Informing the Security Awareness Program

Participants were asked to rate the level of challenge experienced when trying to collaborate and use security awareness resources on a five-point scale ranging from "very challenging" to "not at all changing," with a "does not apply" (N/A) option (see Figure 23).

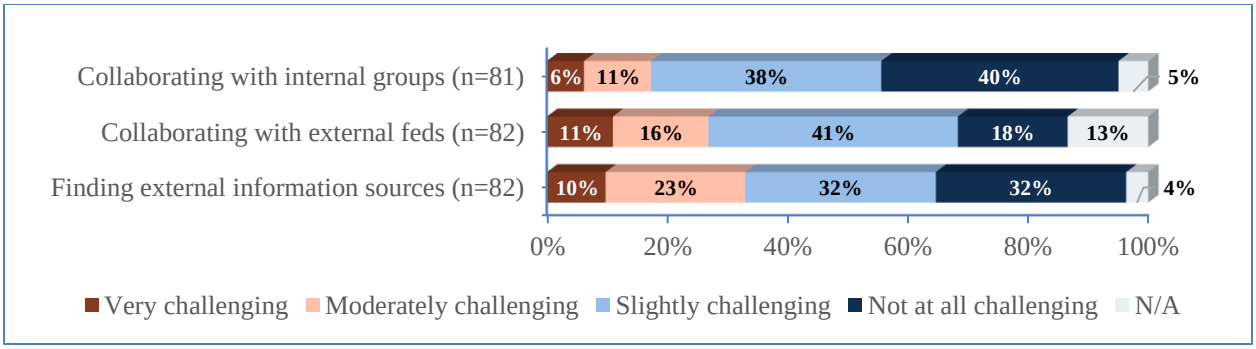

Figure 23: Challenges - Informing the security awareness program

For all challenges, no statistically significant differences were found between groups.

The following provides detail on survey results for each challenge while incorporating example supporting quotes from focus group and survey participants.

Collaborating/sharing information with other groups in my organization: Only 17% of survey participants indicated that collaborating with internal groups was very or moderately challenging. A few focus group participants discussed this challenge as it related to division of training responsibility within the organization:

> "Our biggest challenge is that we have a disparate training program in place. It doesn't all fall under a single umbrella. Consequently, it makes it difficult to coordinate and collaborate with each of the different leads." (S03)

> "Bifurcation's a problem because we're depending on another group to put that tool [a phishing tool] in place. And when it's not in place, we can't actually carry out the exercise in a way that won't overwhelm our incident response team that handles phishing reporting." (D03)

Collaborating/sharing information with other federal security awareness professionals: Twenty-seven percent of survey respondents thought collaborating or sharing with other government security awareness professionals was very/moderately challenging.

While participants saw value in collaborating with other federal employees in similar roles, this collaboration was not always achieved. After benefiting from hearing the experiences and lessons learned of their counterparts during the focus groups, many participants expressed a desire for more collaboration and information sharing across government organizations:

> "There's a lot of things that we're doing across Departments that's the same. If we could coordinate more of that so that we could spend more money on the things that are more targeted to help improve our organizations, that would be a definitely nice to have." (D01)

> "I would like working groups or content posted on a website." (N04)

> "I really would like to see or hear what other people are doing as far as the content. Are they doing things on site? Are they doing things internally in the…learning management system. Are they doing stuff in the cloud? How does that work for your organization?" (N07)

> "I think resources available to the entire government to help either create the material or promote the material or some sort of resource pool like that as well as talking amongst ourselves. And I've picked up several good tidbits from everybody else in the phone call today that I can go back and probably implement almost immediately. So, having this type of forum, maybe on an ongoing basis would be a big help as well." (N08)

> "Right now we kind of see what other agencies are doing at FISSEA once a year. But if there are general ongoing open channels, that would be very helpful." (S06)

> "Too bad there is not a working group that meets periodically so we can share our best practices" (S09)

> "Having a federal forum for federal program managers would be useful to exchange best practices but must omit contractors as to avoid the push to use their products/services." (S11)

Finding external sources of information relevant to my security awareness program: A third of survey participants experienced challenge finding information sources relevant to the unique needs of their own program. Focus group participants echoed this challenge:

> "There's a lot of resources out there to leverage. It's just the challenge is to be able to integrate it into your organization and not make it look like it's so out of place." (D05)

> "While there are multiple trainings that are available out there, many are outdated and in need to be refreshed for the current threat landscape." (S01)

5 Determining Program Success

This section describes results about how organizations gauge the success of their security awareness programs.

5.1 Measures of Effectiveness

We asked participants in what ways their organizations try to measure or determine the effectiveness of their security awareness program (Figure 24). Security awareness training completion rates (84%) and phishing simulation click rates (72%) were the most popular measures of effectiveness, followed by program audits/evaluations with 67% of participants. Less than 30% selected attendance at security awareness events, employee surveys, and online views of security awareness materials. Four percent said that they do not attempt to measure program effectiveness.

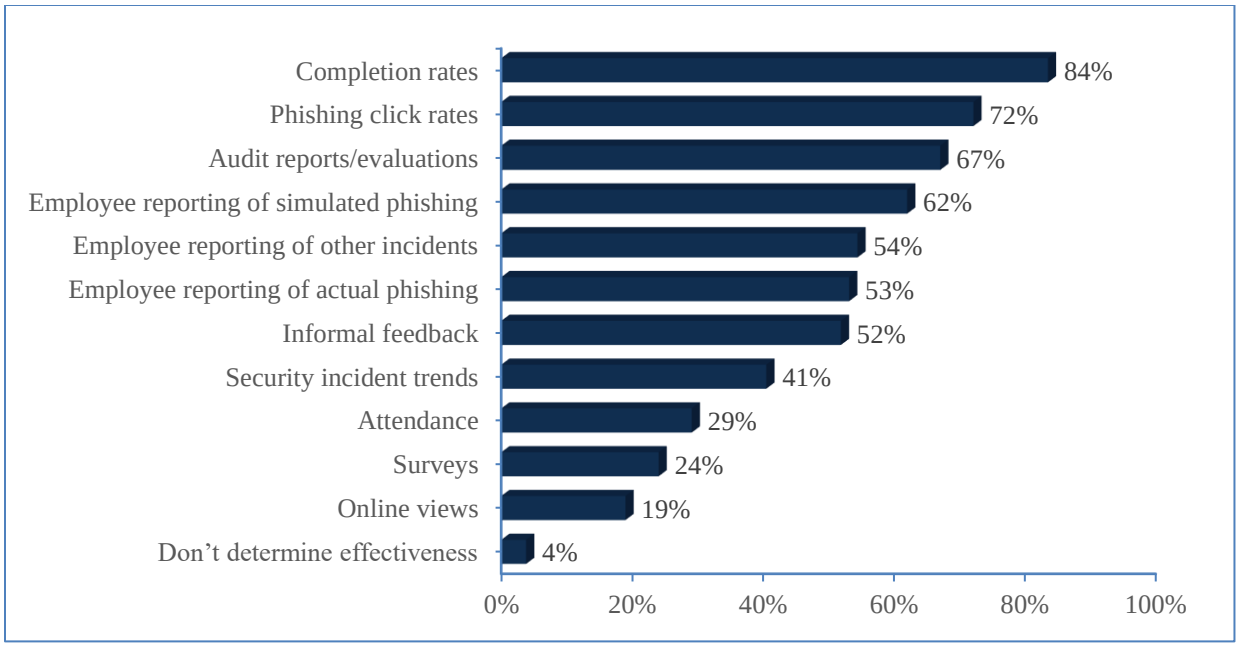

Figure 24: Measures of effectiveness (n=79)

We also examined the number of effectiveness measures that participants selected (Figure 25). The majority (64%) use at least five different measures, and only 4% selected just one measure of effectiveness.

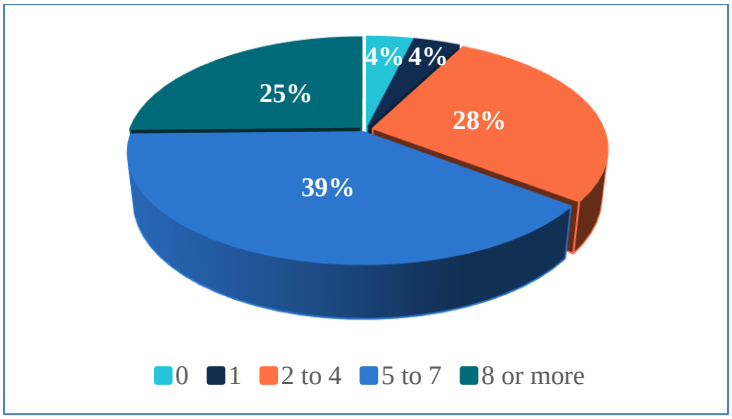

Figure 25: Number of measures of effectiveness (n = 79)

For the number of ways organizations measure effectiveness, no statistically significant differences were found between groups.

In the focus groups and survey, participants provided more details on the variety of methods they employ to determine the effectiveness of their security awareness programs. Training completion rates and independent inspector general (IG) audits were used to demonstrate compliance with security awareness training mandates (usually, FISMA):

> "We have to collect statistics on it because I think you have to report it in your CIO FISMA metrics quarterly." (N11)

> "We do have to track completion metrics, and we determine our agency success as 98% of our users complete it within the agency's time frame." (N01)

> "First is FISMA evaluation from IG. Normally, they'll tell us that they think we did a good job with training awareness or not." (N06)

Several participants indicated that they review user-generated security incidents and security operations trends to help determine whether certain security topics are being effectively taught and translated into action by the workforce.

> "Current internal program is in the first year of monthly education flyers, however so far reportable incidents have declined significantly. Next step is for the team to figure out how to develop the analytics reports to support the effectiveness of the program and identify topics that need more training." (Q65)

> "Really it goes to how many violations and incidents we're actually seeing within our environment. So, I mean, as we see more and more of those go down, both for the real-world ones and any of our test red teaming type ones, error thing, that for us is probably the best indicator that it's actually having an effect in a positive manner." (S01)

> "I would look more to our incidents and questions that we get from our help desk in terms of IT security to identify whether or not our audiences really understand that general awareness content." (S11)

Participants often used phishing simulation click rates as well as reporting of simulated and real-world phishing to determine the effectiveness of phishing-related training:

> "The Phishing campaign we have in place with a 3rd party vendor…is measurable through their tracking of employees opening, clicking on and/or reporting test messages." (Q78)

> "We analyze the metrics that come back from our phishing exercises, the reporting of those. We look at the uptick across the type of phish that we're doing, across the incentives that we're offering, if there's an uptick in users interacting appropriately." (N01)

> "We'll see an uptick in who reports what they don't know to be the phishing exercise to our security operations center." (D04)

Several organizations make use of informal or formal employee feedback to determine if their security awareness efforts are perceived as valuable:

> "For all of our virtual events and at the end of our training, we have surveys for all of the participants. And it gives them a rating scale and asks them, was the

> training effective? Was the content effective? Was the delivery or the presenter's delivery effective? And we use that feedback to measure our training." (D06)

> "We do get, actually, feedback from users who did click or were concerned about the [phishing] exercise, and they'll give us their opinion about certain things that they think would be more beneficial, so we started including some of that information." (S02)

> "I personally try to visit a lot of people or at least talk to them virtually throughout the year. I try to talk to as many people in my organization as possible just to get a feel for what they find out. And one of the things I usually kind of bring up at some point is security awareness. And I'll ask them, 'Do you look at the emails from our information security email? Do you read our articles?'." (N07)

> "Listen to employee feedback on what they like and dislike about the program, and actually adapt to that feedback." (Q29)

Participants elaborated on other measures of effectiveness used in their organizations, such as event attendance and views of online materials:

> "We keep tally of whenever we have a speaker, we make sure that we determine all the people that are there and sort of use those as some rough stats as to success with the campaign." (S04)

> "The attendance is trending upward indicating interest in topics, presenters, and discussions." (Q35)

> "We started actually posting all of our various awareness newsletters and flyers and whatnot within our SharePoint environment. And we're using Microsoft Office 365 Dynamics to actually track everything in the interaction of our users with those to determine how many people are even going out and reading them, how long they're actually spending on them." (S01)

> "For the news articles on the internet, we have questions of the week, and we use the results of the questions of the week that are posted after the article is posted with the hope that the user has read the article and then is able to successfully answer the question." (D06)

5.2 Compliance as Indicator of Success

To determine if compliance with government mandatory training requirements (e.g., as measured by training completion rates) was regarded as the most important indicator of program success, in the survey we asked participants to rate their agreement with two statements on a five-point scale ranging from strongly disagree to strongly agree (see Figure 26).

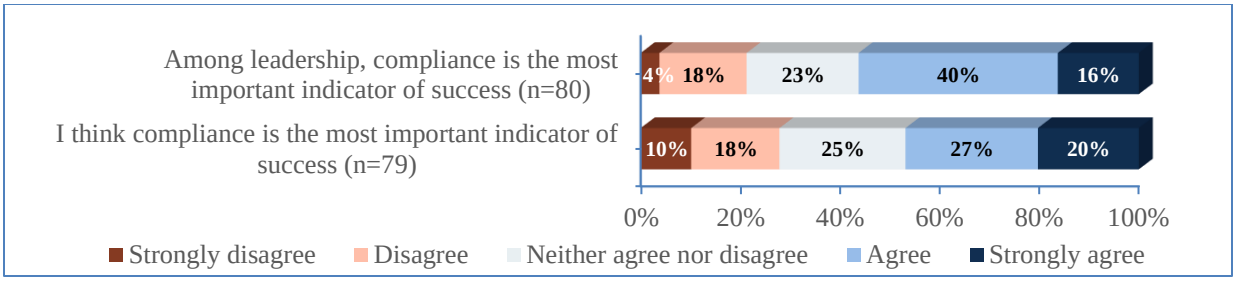

Figure 26: Agreement that compliance is the most important indicator of success

Among leadership, compliance is the most important indicator of success: In the first statement, participants were asked to indicate whether they believed their organization's leadership thinks compliance is the most important indicator of security awareness program success. Over half of responding participants (56%) agreed or strongly agreed with this statement, and 22% either disagreed or strongly disagreed.

In the focus groups, several participants commented on how compliance metrics garner leadership attention:

> "We have found that, yes, management pays attention to things with compliance, but that, in my mind, doesn't really identify effectiveness…We've also really found audits to be effective in helping push the cause. Now, that doesn't identify effectiveness either, but it does help increase management awareness and attention to supporting these programs." (S11)

> "When FISMA scores are involved, I think management looks at FISMA being green as effectiveness." (S10)

I think compliance is the most important indicator of success: In the second statement, participants were asked to rate their agreement related to their own opinion on compliance being the most important indicator of program success. As compared to the leadership perspective, fewer (47%) agreed or strongly agreed with this statement and more (28%) disagreed or strongly disagreed.

No statistically significant differences for the two compliance statements were found between groups.

Despite almost half of survey participants believing compliance is the most important indicator of success, many participants in both the focus groups and survey voiced a concern that compliance metrics in the form of training completion rates, although required, do not demonstrate long-term attitude or behavior change, which should be the real goals of security awareness training.

> "Completion of training is one statistic, but that doesn't really tell you whether anything's sunk in. It tells you that they got through the course, and they took it in record time, maybe, and they're done." (N11)

> "We do not want to offer training just to check the box just for compliance. We know that there is a compliance piece, but I have been working very hard to try to offer training that kind of coincides with different people's learning styles because I want the training to be effective. I want to change user behavior. I want us to be safe." (N09)

> "[Security awareness is] ensuring that they [employees] are receiving appropriate training, obviously, to meet federal requirements, but also to kind of go above and beyond that to actually ensure that that training is effective." (D03)

> "I believe that training is a mechanism to inform and change behavior rather than being just a compliance measure." (Q53)

> "Audits are not tying training to outcomes, so leadership is focused on what the auditors are measuring and making recommendations to improve (e.g. did everyone take training?). Auditors rarely comment on the quality or likely effectiveness of training content, or use their own testing (e.g. phishing, knowledge testing of sample of users) to find out what is really going on (actual effectiveness/outcomes, versus presence of checklist items that might or might not be achieving the desired outcomes)." (Q43)

> "Given that 95% of major Federal incidents were caused by negligent or indifferent staff,…we need to move beyond awareness and compliance and get to a full Organizational Change Management Approach (perhaps ADKAR [Awareness, Desire, Knowledge, Ability and Reinforcement]) that is based on measuring changing mindsets and behavior. Annual training is not enough to move the needle." (Q56)

5.3 Using Effectiveness Data

We asked participants how their security awareness program uses the program effectiveness data (Figure 27). Most commonly, programs use the data to demonstrate training compliance (78%). or to improve or inform the program (70%). Over half use the data to demonstrate the value of their program to leadership (58%). Less than a quarter provide the data to employees (24%) or pass on the data to help other groups in the organization (22%).

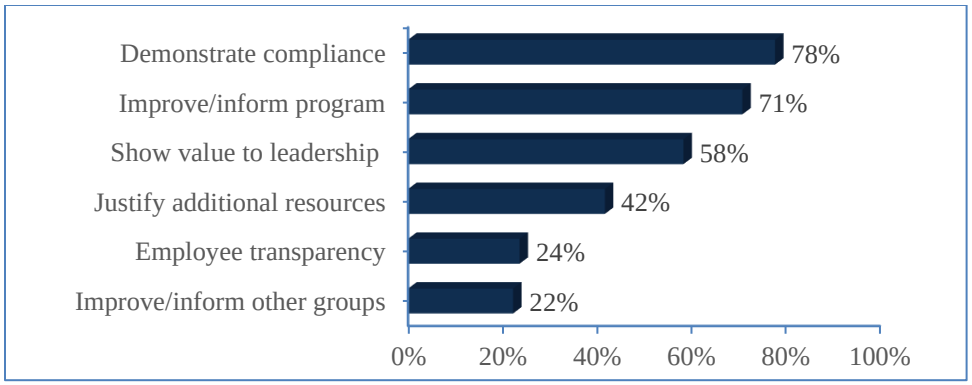

Figure 27: How effectiveness data is used (n=72)

No statistically significant differences were found between groups.

Participants provided examples of how they use effectiveness data:

> "We do have compliance metrics that we report. Management does pay attention to that, and it does heighten awareness with staff that." (S11)

> "I pretty much monitor the type of incidents that come in. And there's two threat vectors that generally indicate how well the user base is aware of what's going on, particularly around improper usage and with email-based threat vectors. So, [if] those numbers are low and it makes sense, fantastic." (N06)

> "Capture metrics to show where you started (e.g. phishing susceptibility, training rates, incident data), inform your program's strategy and tactics, and show progress." (Q43)

5.4 Manager Preferences for Demonstrating Effectiveness

For those participants who were managers or executives involved in making decisions about the security awareness program, we asked an open-ended question about what data would help demonstrate the value and effectiveness of the program to them. Twenty-nine participants answered this question. Table 1 shows the types of data mentioned by participants, example responses, and the number of participants indicating that this type of data would be helpful to them.

Security incidents were the most frequently mentioned type of valuable data (59% of those responding to this question). In addition, the mapping of relationships between different data types (e.g., completion rates, security incidents, phishing click rates) was mentioned by four participants (14%) as being valuable in identifying trends and areas needing additional attention. However, in the previous question on measures of effectiveness, only 41% said that their security awareness program uses security incident data, possibly demonstrating a gap in current measures. Compliance metric data in the form of phishing metrics (31%) and training completion rates (24%) were other commonly mentioned data types. This differs from the 56% of survey

participants who believed that their management thinks compliance is the most important indicator of success.

Table 1: Manager perspective - Data demonstrating security awareness program value (n = 29)

Type of Data	Example Responses	Number Participants
Security incidents	"We also need incidents more granularly analyzed and categorized as to the types of human actions/inactions that contributed, and who, so we can adjust both general training and targeted follow-up training with individuals (i.e. organizational and individual needs assessment)." (Q43)	17
Phishing data	"Effectiveness is generally measured by phishing reporting to the security team or phishing clicks during a phishing exercise." (Q74)	9
Completion rates	"Metrics for timely completion of training" (Q38)	7
Employee/user feedback	"We also review feedback of the training." (Q39) "Surveys" (Q88)	6
Other employee demonstrations of behavior	"Ability to recognize areas of concern" (Q93) "Adhering to the rules of behavior" (Q39)	6
Data relationships	"The data that would be most beneficial to demonstrate the value and effectiveness of the security awareness program would be the annual CSAT [cybersecurity awareness training], IT Professional/Role Based Training, and Phishing Click data graphed with the Network Monitoring data and Helpdesk reporting data on attempted non-approved access, Phishing and Spam email blocks, and other similar type data to show and compare between user knowledge and actions." (Q17)	4
Training topics	"Categories of questions pertaining to each area of operations (e.g., HR, Legal, Program & Project operations, Scientific & Engineering groups, IT specialties, Business Intelligence & Decision management, etc). Topical areas help to identify the practical application of cybersecurity across the organization and in each phase of lifecycle management/operations." (Q38)	4
Employee reporting	"The number of staff who actually recognized an incident, report them, and follow recommended practices. If staff don't do these basic things then they have not learned and the program is not successful." (Q30)	3
Participation, attendance	"Event attendance" (Q24)	3
External data	"Other federal data on compliance with training mandates" (Q41) "peer agency metrics" (Q83)	3
Knowledge testing	"Exam scores, number of times a course is repeated, most likely failed questions, most often passed questions" (Q38)	3

5.5 Overall Program Success

We asked participants to rate the success of their security awareness program on a four-point scale ranging from "very unsuccessful" to "very successful." As shown in

Figure 28, 77% rated their programs as moderately or very successful. Only 4% rated their programs as very unsuccessful.

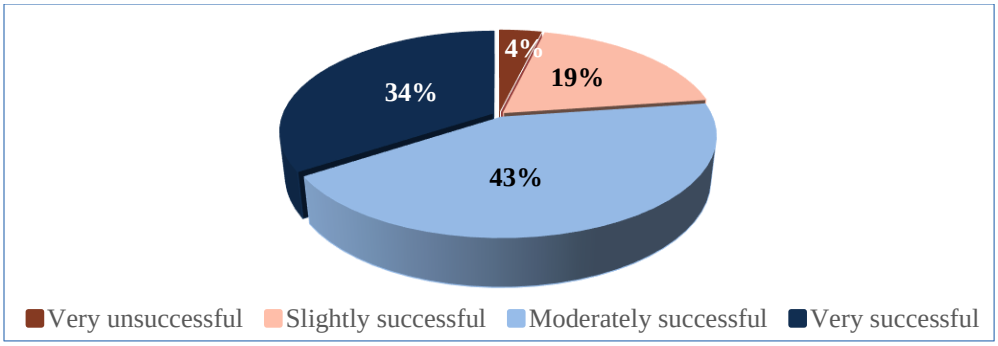

Figure 28: Program success ratings (n=80)

No statistically significant differences were found between groups.

During the focus groups, participants differed on the ultimate indicator of success for their security awareness program. Many emphasized compliance:

> "Our ability to get 99% of our workforce compliant with their annual security awareness training." (Q23)

> "Our most successful aspect is our 99.9% completion rate with over 40K employees." (Q39)

> "100% training compliance before the deadline." (S06)

However, others saw overall success as being grounded in a tangible reduction in incidents:

> "It is the reduction, the elimination or reduction, mitigation of all those threats and vulnerabilities, those incidents that have to be reported and even those that don't have to be reported just you want to make sure that we have smooth sailing as far as our daily operations, that there's no impact to the way– the service that we're supposed to provide for the federal government." (S08)

> "That is really the number of incidents that we end up having and tracked throughout the year and ultimately, not to be on the five o'clock news for some type of compromise or breach." (S01)

5.6 Challenges: Determining Program Success

We asked participants to rate challenges experienced by their programs related to determining

program success on a five-point scale ranging from "very challenging" to "not at all challenging" with a "does not apply" (N/A) option (Figure 29). The remainder of this section provides detail on survey results for each challenge and includes example supporting quotes from focus group and survey participants.

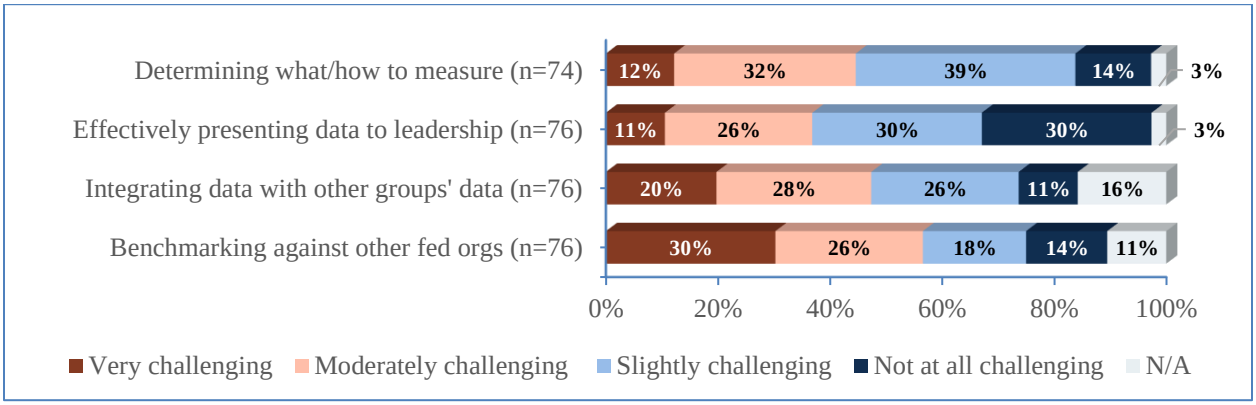

Figure 29: Challenges – Determining program success

For all challenges, no statistically significant differences were found between groups.

Determining what and how to measure: Forty-four percent of survey participants thought that determining what to measure and how to measure program effectiveness was very or moderately challenging. Only 14% found it not at all challenging.

Although most programs make at least some attempt to determine success, almost half of focus group participants expressed uncertainty about how to gauge effectiveness:

> "How do we determine whether or not it is effective? We have not come up with that solution yet, but that's one of the things that we're taking a look at as we roll out these trainings. To see how are we making an impact? How are we making a difference when we educate our workforce?" (N04)

> "How effective? That's a very, very difficult thing to determine. With some training, you might include an assessment of how well the participant listened, based upon a test or something like that, but when you train someone in an activity, unless you circle back to see how well they are employing what they've learned, I just don't know how you are going to really bonify the effectiveness of your program." (S03)

> "From my agency that's been kind of one of my gripes personally, is that we really don't do kind of an effective type of measurements, we don't really have the baseline. We kind of figure out what the requirement is and what we know people have to do. But we really don't do a whole bunch of the other side of the feedback loop." (S08)

> "We run security awareness campaigns and…we really have no idea how much of it is absorbed" (S04).

Participants expressed a desire for more government guidelines on how to measure effectiveness:

> "I feel a lot of people are really challenged by this is metrics, everything as far as metrics for effectiveness of the programs, coming up with something standard that all the departments and agencies could actually end up measuring or have measured for them to try and really determine whether or not the programs that are out there are effective or what parts need to actually be focused on." (S01)

> "Government standards on…measuring effectiveness." (Q75)

> "Analysis procedures on phishing data would be useful. Outside of individual campaigns, it is difficult to analyze and understand issue areas that phishing campaigns could assist in identifying." (S11)

> "I think some federal guidance on how we can all track the effectiveness of our programs would be good." (D03)

Despite challenges in finding good measures of effectiveness, one survey participant had this advice:

> "Don't let incomplete or imperfect data stand in the way of moving forward with changing behavior for the positive." (Q27)

Effectively presenting data to leadership: Presenting program data to leadership in an effective way was deemed very or moderately challenging by 37% of survey participants. Thirty percent found it to be not challenging at all.

One focus group participant expressed frustration with not being able to convince her leadership to help solve challenges faced by the security awareness team:

> "I have no idea how to solve the issues and challenges as even though I have expressed challenges to the Department it appears they all fall on deaf ears." (S09)

Other participants recommended the type of information that should be provided to leadership:

> "Write up some type of training and awareness program plan so that you can document what it is that you want the program to do and how you want it to work and all of the players that would be involved so that you can brief senior leadership on that, because if you don't have their buy-in, then your program is probably not going to go anywhere." (D02)

> "If you can, get leadership's attention early. Have them sign-off on the list of

> topics you plan to cover. My CISO is very hands on, so I gave him a spreadsheet that stated the topic, the media type used to cover that topic, if there was a knowledge check/test question on it." (Q37)

> "Focus awareness program and communications with leadership on reducing actual risk to systems and data, not on compliance with minimal requirements (which are not enough to adequately reduce risk)." (Q43)

Integrating/correlating security awareness data with data collected by other groups in my organization: Being able to bring together data from multiple groups to inform the security awareness program was viewed as very or moderately challenging by 48% of survey participants. Only 11% said they were not at all challenged with this.

A few focus group participants commented on how their organizations are not currently correlating security awareness data with security incident data:

> "Ideally, you'd be able to track the incidents and see based on your security awareness and training and if your incidents are going down. We are not doing that probably due to lack of resources." (S06)

> "I hear a bunch of people saying that you guys use the number of incidents as a metric…I'm sort of struggling with that because I came from the technical side and didn't start off as a trainer or in the training field, and there's just so many attack vectors. I don't understand how you can associate incidents with the training." (S04)

Benchmarking my organization against other federal organizations: Over half (56%) of survey participants felt challenged to benchmark (compare) their organization's security awareness program against programs in other government organizations. Several participants expressed a desire to have more federal information as a comparison point:

> "What we've been looking for is click rates in the government, right? There's industry click rates and surveys and stuff like that for phishing examples. But even talking with DHS, they don't have any click-rate studies or surveys." (N08)

> "With our phishing exercise results, I would love to have a different measurement. I would love to have a different baseline or, I agree, a standard way of looking at our agency or across agencies or across departments. We could judge apples to apples to know where we are, how we stand up to someone else, and where we could focus our training so that where we are making improvement where it is needed, not just wherever it's required." (S08)

> "Other federal data on compliance with training mandates" (Q41)

6 Program Support

Participants rated their level of agreement (from strongly disagree to strongly agree) for several statements related to organizational views on security and support for the security awareness

program. The following subsections describe the results.

6.1 Organizational Support for Security

Survey participants indicated their agreement with three statements related to organizational support for and recognition of the relevancy of security. Agreement was indicated on a five-point scale ranging from "strongly disagree" to "strongly agree." Figure 30 shows the results for each statement.

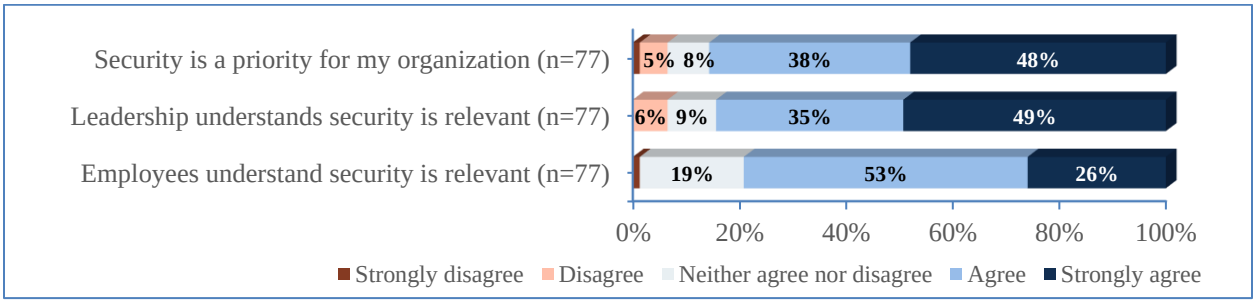

Figure 30: Agreement for statements about organizational support for security

No statistically significant differences were found between groups.

Security is a priority for my organization: A large majority of survey respondents (86%) agreed or strongly agreed that security is a priority for their organizations. Only 6% disagreed or strongly disagreed.

As reflected in the survey, most focus group participants believed security was a priority for their organization. For example, a security awareness program lead commented:

> "We've built a security culture over the past– what, since 2003, when GISRA [Government Information Security Reform Act] and FISMA first came out and security awareness training was a requirement. I've seen changes." (N11)

However, one participant felt that security was not valued in his Department:

> "In our organization, our mission does not incorporate security in the same way a lot of other agencies do. So, it's not a priority." (D05)

My organization's leadership understands how/why security is relevant to them: When asked to indicate whether their leadership understands how security is relevant to them, 84% answered affirmatively. Only 6% disagreed, with no participants strongly disagreeing.

A few participants remarked that their management valued security:

> "We have great support for our security and privacy program as well, and that matters…If you hear management talking about security and privacy in various conversations, then you know that the word is kind of out and that people are on

> board with it. So, that's kind of what I listen for." (N11)
>
> "Strong leadership by example" (Q51)

The employees in my organization understand how/why security is relevant to them: As compared to leadership's understanding of the importance of security, slightly fewer (79%) participants thought the employees in their organizations understand the relevancy, while more (19% vs 9%) were neutral. Only 1% strongly disagreed.

Participants stressed the importance of ensuring the information is viewed as personally relevant to employees and their specific roles within the organization:

> "Making sure that when we do pick content or that we're doing some training, that we bring it home for people so they can relate to it. So, we give a lot of examples of things that actually do happen. Some of these things are kind of crazy, but they do happen in the real world." (N04)
>
> "My advice would be to try to make it fun and try to make it relatable to the agency's mission, as well as to the person. So, we like to tie in examples of, 'Hey, you lock your home door. Lock your computer. You're protecting agencies' employee data. If there's a breach, that's your mom's data. That's your data.' Really trying to personalize it to make them feel the connection, and how them following proper guidance is really making our agency safe." (N01)
>
> "I want to be able to where, hey, an individual, regardless of where they're at, when they see something, the first thing they think of, 'Ooh, how's this going to impact my privacy? How's this going to impact my security? How's this going to impact my network?'…It's like, 'Is it relevant to my general users?' Obviously, for my more technical or more in-depth people, yes, I do need to give you more details from a technical standpoint. But for my everyday Joe Schmo sitting in front of the computer, just getting the job done, what is relevant to them and having them have more of a cybersecurity mindset?" (N10)
>
> "Help people see the connection between the requirements and their daily work. Provide real life examples of how this helps the organization better execute its mission and operational needs. With 'buy-in' from people at all levels, then you don't have to carry the total burden – people develop pride in their own areas of expertise and self-govern the necessity of incorporating cybersecurity (and other areas of security) into their routines, processes, and workforce." (Q38)

Others expressed concern that not all employees took responsibility for security or saw the relevance of security in their day-to-day work:

> "One of the hurdles that I have to try and get past is where people might think that the [the organization] network is more secure, and therefore, a person can do other things on the network that they might not try elsewhere or at home or in the public. So that's just one sort of myth." (N11)

> "One of the biggest challenges that I see is no one's really understanding the risk, understanding what the risk is and being able to convey that to the business units and the business operations side. So, from an education standpoint, again, we're back to people are taking the required annual training, but they're not seeing how it impacts their work on a daily basis and how they need to apply what they're learning to what they're doing every day." (N10)

> "Organization-specific security awareness training is hard if you don't have a team that can provide the level of specialization is needed. Or else it's the generic training that isn't necessarily useful your role at work." (Q84)

6.2 Organizational Support for the Security Awareness Program

Participants rated their level of agreement for two statements about perceived support for the security awareness program. Figure 31 shows the agreement percentages.

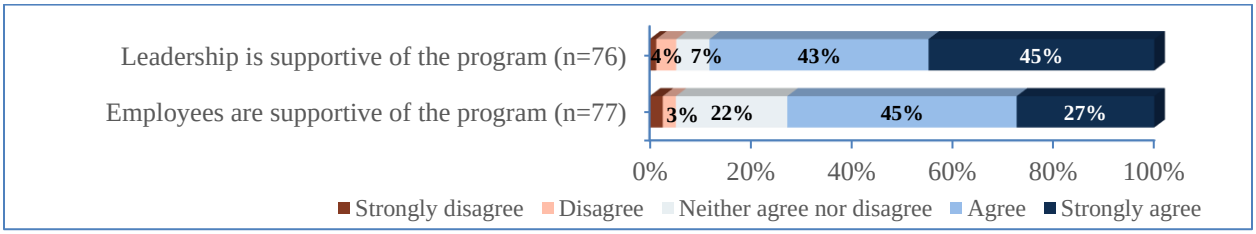

Figure 31: Agreement for statements about organizational support for the security awareness program

No statistically significant differences were found between groups.

My organization's leadership is supportive of the security awareness program: A large majority (88%) thought their leadership was supportive of their program. Only 5% disagreed or strongly disagreed.

When asked what advice they would provide to their colleagues, gaining leadership support was the one of the most frequently mentioned topics:

> "Make sure you have management support so that you can ensure that you have the visibility within the agency so people understand that this is not something that you just ignore. This is something that's required, and this is something that is important to the work and to the protection of our agency." (N12)

> "My first advice would be to establish and maintain a good working relationship with senior management because their support can make or break your program." (N09)

> "If you aren't getting support from your direct supervisor, speak to others within your organization who might be able to go to bat for you. I was able to get a full-time contractor support this way." (Q23)

> "Upper management support is a must and the key to success!" (Q58)

Several participants cited the strong leadership support they had as one of the most successful aspects of their programs:

> "I would say we have good support from our management and executives. They seem to give us a lot of flexibility. If we want everyone to have a phishing exercise, they give us a little leeway to do so. If we draft a newsletter or a poster or something, they'll send it out to the user population agency-wide." (S07)

> "Now with management support, with the tying into people's performance evaluation plans, so that there is visibility and consequences if folks don't complete their set security awareness training or role-based training. So, the management support and the upper level of support in the tie into HR [human resources] performance plans has really helped us to achieve a higher, I think, a completion rate within our agency, for at least for federal employees." (S08)

However, some were vocal about the perceived lack of leadership support for the program:

> "I don't think management would do it unless it was mandated by law…At least every few years, I have to quote the legal basis for delivering this required training." (D05)

> "Security awareness training is definitely not a priority. They've got a lot of other things going on in the organization, and training just is not a priority." (S10)

> "Anything that was done in the past was personal initiative. I've done newsletters, websites, tried to get Hollywood movies regarding security shown with discussion afterwards, tried to get a "security game" (I was told that was insulting). Management just didn't care." (Q34)

A few survey participants expressed the need for more leadership support for their program to be successful:

> "More support from senior leadership outside of the IT/CIO office." (Q88)

> "Full support from upper management at the Department level. If the Department were to emphasize the importance of security awareness programs, it would trickle down to the Components." (Q23)

The employees in my organization are supportive of the security awareness program: Seventy-two percent of survey participants thought that employees were supportive of their program. Just 6% disagreed/strongly disagreed.

When asked about successful aspects of their program, some participants commented on employee engagement and interest in the program:

> "Popular with the people encouraging engagement and behavior change." (Q56)

> "Participation and enthusiasm of employees." (Q58)
>
> "Feedback from staff; the care they pay the training materials." (Q83)
>
> "I did see an increase in that to where people were stopping before they took the action versus saying, 'Oops, I did something wrong'…It's like, is it really sinking in…If something kicked off in the news, I'd have individuals come back and say, 'Hey, I heard this on the radio' or, 'I saw this in the news. Does this impact us?' or…'How can I can protect against it?" So, people are definitely more aware of what was going on and then asking the right questions." (N10)

However, others remarked that some employees lack the time or motivation to engage with security awareness information or activities:

> "We get so many emails of just users that they just don't have the time." (D06)
>
> "The expectation is that we know all this information, but we don't have the time to really learn it." (D01)
>
> "A lot of times we'll find that sometimes our users aren't engaging with the message, or they may delete it, or they don't report it the way that we want them to." (N01)

6.3 Resources for the Security Awareness Program

Survey participants indicated their level of agreement about three statements about whether the security awareness program has adequate resources in the form of funding, staff, and technology. Figure 32 shows the results.

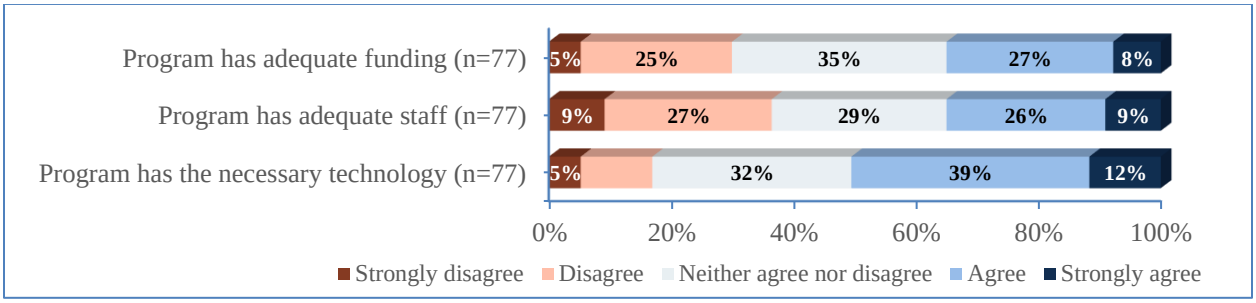

Figure 32: Agreement for statements about adequacy of resources for the security awareness program

We have adequate funding for the security awareness program: Only a little over one third of participants (35%) agreed/strongly agreed that their security awareness program has adequate funding, with 30% disagreeing or strongly disagreeing.

For "Program has adequate funding," there were statistically significant differences between: very small and large teams (*z* = -2.445); and small and large teams (*z* = -2.925). For very small teams (n = 22), 32% disagreed/strongly disagreed with the statement and 23% agreed/strongly agreed (the remainder were neutral). For small teams (n = 19), 47% disagreed/strongly disagreed and only 16% agreed/strongly agreed. In contrast, large teams (n = 12) were more likely to agree/strongly agree that they had adequate funding (67%).

There were no significant findings for organizations of different types or program sizes.

When asked what could help their programs be more successful, more funding was a common response:

> "Resource is always one of the biggest challenge in recent years. With limited resource, the focus is to accomplish other priority missions instead of this program." (Q69)

> "Funding and spending flexibility. There is no lack of high production quality, impactful, continuously updated content from commercial sources available at reasonable prices due to economies of scale. Finding content is not the problem– getting funding/approval to purchase it is the problem." (Q43)

> "We have a very small budget for our cybersecurity awareness program. I've seen some products in the private sector that are very slick and customizable, but they're also expensive. I also might ask for a travel budget, so we could provide some in-person training. We have facilities throughout the country and to hit each one would be quite expensive." (S06)

We have adequate staff dedicated to the security awareness program: When asked about program staffing, 35% agreed/strongly agreed that they had adequate staff, while 36% disagreed/strongly disagreed.

For "Program has adequate staff," there were differences between: very small and large teams (*z* = -2.198); and small and large teams (*z* = -2.758). While a large number of participants with very small and small teams did not think they had adequate staff (45% and 58%, respectively), only 8% (one) participant in a large organization disagreed with the statement.

There were no significant findings for organizations of different types or program sizes.

Staff resources were closely related to perceived lack of funding. Participants often discussed needing more staff to improve their programs:

> "I think we have all the pieces that we need to build on…It's just having the staff to support it. At my Department, there's one federal employee who is responsible for the program for the entire Department. There [are] contractors that supplement that work but definitely could use more resources, more so on the federal side." (D01)

> "We have a robust program. We are need *[sic]* more staff to execute efficiently and effectively." (Q44)

> "Additional staff/SMEs to help create content other than only myself." (Q74)

> "Actually having the ability to have dedicated training staff to write and update the training, make them more interactive here, and help determine better and more efficient knowledge checks in there." (S01)

> "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. But since we have so much problem just maintaining courses, I can't imagine trying to stand up an engaging website at this point either." (D05)

The fact that most security awareness team members were part-time and had other duties also contributed to the staffing shortage:

> "The team…who perform the security-related operations for our network, they're the same team that helps create and manage the training. So, if we have an issue or a series of issues, sometimes we may have to either delay training or make a lighter version of training." (N07)

> "I have one person who it's not a full-time position for them because we were doing performance metrics as well, both for training as well as other metrics related to security. So, I'd like to be able to put more staff power to it. And that also goes for resources into maintaining our websites, the SharePoint sites, investigating and finding new information, new newsfeeds or what have you to be able to put out there on a timely, updated, routine basis." (N08)

Lack of staff was not the only issue; staff turnover was also viewed as a disruption for programs:

> "Frequent staff turnover, including CISO and CIO positions decrease the long-term success of a program because ideas, funding and priorities change and ultimately limit program strength and growth opportunities. Meaning you can't build a great house, if you keep ripping up the foundation every year or two." (Q24)

> "We have a high turnover in this industry in security and security awareness. And for instance, we just lost about, I'd say, a third of our workforce in our CISO organization due to financial cutbacks. A lot of our contract staff has been eliminated." (N05)

> "I think the biggest issue that I run into is we've had a lot of turnover in our contract staff. So, I haven't had anyone supporting me consistently for a while now." (S04)

We have the necessary technology to support the security awareness program: Over half of survey participants (51%) agreed/strongly agreed that they have adequate technology for their security awareness program. Just 17% disagreed/strongly disagreed.

For "Program has the necessary technology," there were significant differences between: very small and small teams (z = 2.871); small and medium teams (z = -2.586); and small and large teams (z = -2.534). Whereas only 21% of small teams agreed/strongly agreed that they had adequate technology, significantly more agreed for very small, medium (n = 10), and large teams (55%, 60%, and 75%, respectively).

There were no significant findings for organizations of different types or program sizes.

A few participants mentioned various technologies as being positive contributors to the success of their programs:

> "Having an automated tool to be able to pull which employees have completed the security awareness program." (Q71)

> "There's been innovation to improve how those things are viewed through different means, putting things on SharePoint and making them so that they can be navigated." (D03)

However, others noted various technologies or tools that they needed but currently lacked:

> "More robust interactive system, allow real world like simulations." (Q25)

> "Automated measurement tools with defined metrics." (Q64)

> "Personnel management system that syncs with the Learning Management System." (Q24)

> "The Department hasn't had a spear phishing exercise for, I think, nearly two years because of a lack of a tool." (D03)

7 Key Takeaways

In this section, we summarize key findings from study results related to security awareness approaches and challenges.

7.1 Required Training

Two-thirds of represented organizations develop at least some required training content in-house, with 80% saying they update content at least once a year. Sub-components often receive training

from their Departments, with most being mandated to use what is provided without modification.

Less than a quarter of organizations were challenged to find required training course materials or struggled with lack of guidance on what to include in required training. This was particularly problematic for independent agencies who do not receive training materials from a parent organization. To address this challenge, multiple participants expressed the need for standardized government training and guidance that allows customization for the unique needs of the organization.

Automation was viewed as essential for efficient tracking of employees' completion of training. But some organizations lack this automation, especially when tracking contractors, who may not have access to organizations' learning management systems.

When dealing with individuals who do not complete their training by the deadline, many organizations disable accounts of non-compliant employees, resulting in higher compliance numbers. Still, almost half said that getting employees to complete the required training was challenging. Employees are busy, have to complete other mandatory training, and may find the training boring or irrelevant to their work roles.

7.2 General Approaches

The majority of programs address well-known security topics (e.g., phishing, passwords, malware) in addition to privacy topics, with many organizations incorporating information that employees can also use in their personal lives. Recently, organizations have introduced additional topics relevant to teleworking.

Phishing simulations were used by most represented programs and were often described as being one of the successful aspects of the security awareness program. While many focus on phishing click rates to gauge learning, others also view reporting rates as indicators that employees' behaviors are being positively impacted.

Most programs hold a variety of security awareness activities throughout the year in addition to the mandated annual training, including speaker events, instructor-led sessions, webinars, and interactive activities such as escape rooms. However, smaller programs are less likely to offer additional activities.

Programs utilize a wide range of other communication channels, such as email, newsletters, posters, and videos. However, they may be challenged in several ways. Especially for interactive approaches, programs struggle with ensuring materials are Section 508 compliant. They also have difficulty providing security awareness information in an engaging way and customizing security awareness information to a diverse workforce with different needs and levels of security knowledge.

Finally, about half do not take advantage of the benefits of positive reinforcement as they do not recognize employees for practicing good security behaviors.

7.3 Collaboration

Programs frequently collaborate with other groups in the organization, most commonly other cybersecurity and IT teams. However, less than half partner with their communications team,

despite the importance of communication knowledge and skills as highlighted in NISTIR 8420B "The Federal Cybersecurity Awareness Workforce."

While just over a quarter of survey participants expressed challenges collaborating or sharing information with other federal security awareness professionals, focus group participants frequently highlighted their wish lists for greater government collaboration. For example, they expressed a desire for a central repository of materials or ongoing working groups or forums. While there are government working groups focused on training (e.g., the Interagency Information Security Training Working Group or FISSEA), it may be that many participants are not aware of existing groups or prefer another type of group (e.g., real-time, online forum).

7.4 Sources of topics and approaches

Programs use a variety of internal resources to inform security awareness topics and approaches. Most are taking into account employee and leadership feedback to inform their program as well as looking at security incidents within the organization to drive topics or areas of emphasis.

Programs also utilize external government and non-government sources, although government resources were more popular. Teams often pull from hot topics in the news and industry security incident reports.

7.5 Measuring Success

Over three quarters of survey participants rated their security awareness programs as moderately or very successful. Training completion rates were the most common measure of effectiveness. Behavior based measures (phishing click rates, reporting of phishing emails or other incidents) were utilized by over half.

Less than a half try to correlate organizational security incident trends with behaviors learned or reinforced through security awareness information. Not surprisingly, this data integration was seen as very or moderately challenging by just under half of participants. In contrast, managers listed security incident data as the measure of effectiveness most preferred for helping them make decisions about the security awareness program, while training completion and phishing click rates were mentioned by much fewer.

Just under half of represented programs thought that determining what and how to measure was moderately or very challenging. Participants desired more guidance on measures of effectiveness, including more government-specific data for benchmarking their own program.

Over half of survey participants think their leadership views compliance as the most important indicator of program success, with slightly fewer having the same opinion themselves. However, in qualitative remarks, many focus group and survey participants disagreed with this compliance focus, instead emphasizing that the real purpose of security awareness is to affect employees' security behaviors; therefore, success should be measured in ways beyond training completion rates.

7.6 Program Support

Large majorities (at least 70%) thought that security is a priority for the organization, that security is understood by leadership and employees as important, and that leadership and employees supported the security awareness program. However, despite the claimed

organizational support, only about a third thought the program had been provided adequate funding and staff.

8 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:

- Explore the potential of developing or purchasing standard government training that relieves the burden of content development but allows for some customization to accommodate organizations' unique missions.
- Provide updated guidelines to help organizations in the various aspects of their security awareness programs, for example: how to implement and enforce required training; topics to address; development of engaging communication materials and methods; measures of effectiveness; use of positive reinforcements; collaboration with internal and external groups; and how to gain support and resources for the security awareness program. A planned update to NIST SP 800-50 and SP 800-16 will likely address many, if not all, of these issues.
- Develop guidance to improve the interpretation of phishing simulation click rates. For example, the NIST Phish Scale seeks to help organizations rate phishing detection difficulty by incorporating contextual elements in addition to traditional phishing cues [STEVES].
- Provide tools to help programs produce more engaging materials in a variety of formats. Allow alternative formats to appeal to different learning preferences without the requirement for Section 508, as long as similar compliant material is available in another format.
- Expand marketing of the FISSEA conference/seminar series. Consider the creation of a real-time, online forum to encourage ongoing collaboration among federal security awareness professionals.

For organizations with security awareness programs:

- Automate the training tracking process and develop systems that can handle both federal and contractor employees. Integrate other systems (e.g., HR) as necessary.
- Explore implementing positive incentives to encourage employees to complete training and practice good security habits.
- Consider offering additional ways to complete training beyond the typical online course. Ensure course materials are updated with the topics most relevant to the organization.
- Reinforce security awareness information and learning throughout the year, not just via once-a-year training. Utilize a variety of communication methods, including events and interactive activities, to appeal to different learning preferences. Incorporate information that employees can use both at work and at home.
- Emphasize impact on employees' attitudes and behaviors more than compliance when determining program success.

- Ensure leadership support of the security awareness program, including providing adequate resources and allowing program staff to enforce training completion (e.g., by disabling accounts if training is not completed in time).

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

[CISA] Cybersecurity and Infrastructure Security Agency (2021) *National Cybersecurity Awareness Month (NCSAM)*. Available at https://www.cisa.gov/national-cyber-security-awareness-month

[FERTIG] Fertig, T, Schütz, AE, Weber, K (2020) Current Issues of Metrics For Information Security Awareness. European Conference on Information Systems (Online). Available at https://aisel.aisnet.org/ecis2020_rp/184

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

[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/

[STEVES] Steves, M, Greene, K, Theofanos, M (2020) Categorizing Human Phishing Difficulty: A Phish Scale. *Journal of Cybersecurity* 6(1):tyaa009. Available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927333

[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
IT	Information Technology
LMS	Learning Management System
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology