NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication (SP) 1288

FEDERAL CYBERSECURITY ROLE-BASED TRAINING APPROACHES, SUCCESSES, AND CHALLENGES

Julie Haney, Jody Jacobs, and Susanne Furman

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1288

NIST Special Publication (SP) 1288

FEDERAL CYBERSECURITY ROLE-BASED TRAINING APPROACHES, SUCCESSES, AND CHALLENGES

Julie Haney, Jody Jacobs, and Susanne Furman
Information Access Division
Information Technology Laboratory
National Institute of Standards and Technology

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1288

JANUARY 2023

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

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce
for Standards and Technology

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

NIST Technical Series Policies

Copyright, Fair Use, and Licensing Statements
Technical Series Publication Identiifier Syntax

Publication History

Approved by the NIST Editorial Review Board on:
2023-01-03

How to cite this NIST Technical Series Publication

Haney, JM, Jacobs, JL, Furman, SM (2023)
Federal Cybersecurity Role-Based Training Approaches, Successes, and Challenges
(National Institute of Standards and Technology
Gaithersburg, MD)
NIST Special Publication (SP) 1288.

https://doi.org/10.6028/NIST.SP.1288

NIST Author ORCID iDs

Julie Haney: 0000-0002-6017-9693
Jody Jacobs: 0000-0002-6433-884X
Susanne Furman: 0000-0002-7013-6603

Contact Information

usability@nist.gov

ABSTRACT

Most United States federal government organizations are required to conduct cybersecurity role-based training for federal government personnel and supporting contractors who are assigned roles having security and privacy responsibilities. Despite the training mandate, there has been little prior effort to look broadly across federal organizations to see how they are implementing these training activities and what issues they are experiencing. This lack of understanding may be hindering the development of improvements and resources for training activities. To address this gap, the Usable Cybersecurity team at the National Institute of Standards and Technology conducted a research study consisting of focus groups and a survey to gain insights into the approaches of and challenges faced by federal organizations when implementing role-based training activities. This paper reports the results of the study and suggests actions that organizations can take to improve federal role-based training activities.

Keywords: cybersecurity, role-based training

TABLE OF CONTENTS

NIST USABLE CYBERSECURITY

We are the Usable Cybersecurity team within the National Institute of Standards and Technology (NIST) Visualization and Usability Group. Our multi-disciplinary team conducts research at the intersection of cybersecurity, human factors, cognitive science, and psychology to ***"champion the human in cybersecurity."*** Through research and other human-centered projects, we seek to better understand and improve people's interactions with cybersecurity systems, products, and services. We provide data and guidance to policymakers, system engineers, and cybersecurity professionals so that they can make better decisions that consider the human element, thereby advancing cybersecurity adoption and empowering people to be active, informed participants in cybersecurity.

Why Usable Cybersecurity Is Important

> *Security must be usable by people ranging from non-technical users to experts and system administrators. Furthermore, systems must be usable while maintaining security. In the absence of usable security, there is ultimately no effective security.*
>
> *A Roadmap for Cybersecurity Research* [DHS2009]

Usable cybersecurity considers the relationships and interactions between people and cybersecurity, including people's perceptions, the challenges they encounter, and the design of usable systems, products, and services that also result in improved cybersecurity outcomes.

When organizations, policy makers, and cybersecurity professionals fail to consider the human element, there can be real consequences, for example: more calls to the help desk, people resorting to less-secure workarounds, user frustration, and the perception that cybersecurity is inconvenient and burdensome.

EXECUTIVE SUMMARY

Cybersecurity role-based training (RBT) includes specialized training on policies, procedures, and tools for individuals who are assigned roles having security and privacy responsibilities [SP800-53]. Most United States (U.S.) Federal Government organizations are required to conduct RBT for applicable federal government personnel and supporting contractors [CISA2022].

Despite the training mandate, there has been little prior effort to look broadly across federal organizations to see how they are implementing RBT activities and what issues they are experiencing. This lack of understanding may be hindering the development of improvements and resources for federal RBT activities. To address this gap, we - the Usable Cybersecurity team at the National Institute of Standards and Technology (NIST) - conducted a research study to gain insights into the approaches of and challenges faced by organizations when implementing RBT activities.

Our research initially focused on cybersecurity awareness programs targeted at organizations' general workforce. However, during focus groups of 29 federal employees with cybersecurity awareness duties, many participants discussed role-based training as being an especially challenging and related aspect of their jobs. Spurred by these discoveries, we conducted a follow-up online survey solely focused on role-based training that was completed by 82 federal employees.

We found:

- **RBT assignment:** There is no standard way that organizations determine which employees should be assigned RBT. Some use the *National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework)* as a guide, but others leave decisions up to the office of the Chief Information Officer (CIO) or even individual supervisors.

- **RBT content:** About two-thirds of surveyed participants said that their organizations create at least some RBT content on their own, which could be resource-intensive. Those who purchase training may find the cost to obtain content for many cybersecurity roles to be prohibitive. Indeed, over 40% of survey participants rated finding RBT materials and updating RBT as moderately or very challenging. On the upside, the majority (about 60%) said that their RBT content is tailored to their organizational mission and current security threats.

- **RBT approaches:** Almost all survey participants (95%) said their organizations offered at least some online training, while over half also allow live training options. Almost half utilize industry-recognized certifications to fulfill RBT requirements.

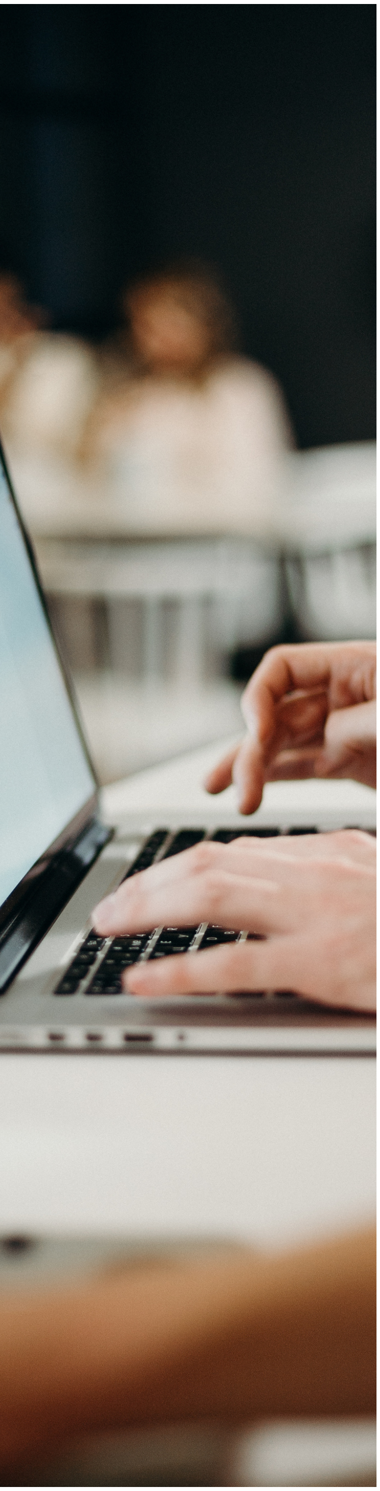
- **Compliance with mandatory RBT requirements:** Most organizations do not experience substantial challenges in tracking employee completion of RBT. Still, over a third are using a manual method (e.g., a spreadsheet) for tracking. Additionally, about 40% of organizations were moderately or very challenged in getting employees to complete training by the appointed deadline. This may be due to training overload, employee time constraints, or a lack of concrete consequences for not completing training.

- **Organizational support for RBT:** More than two-thirds of survey participants believed that organizational employees and leadership were supportive of RBT activities. Over 70% said they have adequate technology to support RBT activities. However, 42% disagreed that they have adequate funding and 52% disagreed that they have adequate staff for conducting RBT activities.

- **Measuring RBT effectiveness:** Just over half of survey participants rated their RBT activities as moderately or very successful. However, there is great variation in how organizations determine success, with most relying on compliance metrics, such as training completion rates, that do not necessarily measure impact on employee learning or behaviors. Close to 60% of survey participants rated measuring RBT success as challenging.

These results suggest the need to provide more guidance and baseline standards for federal RBT activities. An upcoming NIST update to *NIST SP 800-50 Building a Cybersecurity and Privacy Learning Program*, which our research has informed, may address many of the suggestions for supporting organizations through guidance. Additionally, federal organizations may benefit from standard, government-wide RBT content that could then be tailored to unique mission needs.

STUDY BACKGROUND AND PURPOSE



What is cybersecurity role-based training (RBT)?

Cybersecurity role-based training (RBT) includes specialized training on policies, procedures, tools, and methods for individuals who are assigned management, operational, and technical roles having security and privacy responsibilities [SP800-53]. RBT is tailored to specific roles within an organization and differs from the general cybersecurity awareness training targeted at all personnel within an organization.

U.S. Federal Government organizations are required to conduct RBT.

NIST Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, provides guidance for organizations in protecting their operations, assets, and personnel from security threats and risks [SP800-53]. Within the document, Awareness and Training Control (AT-3) “Role-based Training” addresses training for personnel with “responsibilities related to operations and supply chain risk management within the context of organizational security and privacy programs.” Furthermore, organizations are instructed to document, monitor, and retain records for their training activities. In addition to federal personnel, RBT applies to contractors providing services to federal organizations.

NIST SP 800-53 is a major basis for the Federal Information Security Modernization Act of 2014 (FISMA) [FISMA2014], which requires federal organizations to implement RBT [CISA2022].

There was no clear picture of how federal organizations conduct RBT and what challenges they experience when implementing these training activities.

We conducted a prior study that explored federal security awareness programs through focus groups and a survey [IR8420][IR8420A][IR8420B]. In the focus groups, we found that security awareness professionals were often also assigned responsibilities for role-based training activities, for which they identified significant challenges. However, at the time, no one had taken a broader look across federal organizations to see how RBT activities were implemented and what issues organizations were experiencing. This lack of understanding hindered the development of improvements and resources for federal RBT.

We conducted a research study to explore the approaches and challenges of federal RBT activities.

To address the lack of understanding about how RBT activities are implemented in the U.S. Federal Government, we conducted a study to answer the following questions:

Q1. How do federal organizations determine which employees need to take RBT?
Q2. How is RBT content obtained?
Q3. What approaches do federal organizations take in their RBT activities?
Q4. How do organizations determine the effectiveness of their RBT activities?
Q5. How do organizations approach compliance to government RBT mandates?
Q6. How well are RBT activities supported within organizations?
Q7. How do organizations determine the effectiveness of RBT?
Q8. What challenges do organizations face in implementing RBT activities?

Our study results can serve as a resource for RBT implementers, organizational decision makers, guidance developers, and policy makers.

This report documenting our study results can serve as a resource for federal professionals responsible for implementing, overseeing, or enacting policies related to RBT activities. In addition, our study is informing the update to *NIST SP 800-50 Building a Cybersecurity and Privacy Learning Program*, which will provide guidance to federal organizations. The report may also be valuable to organizations outside the U.S. Federal Government that implement similar training programs.

METHODOLOGY

To gain a better understanding of RBT approaches and challenges within the government, it was important to hear directly from government employees who were responsible for implementing RBT activities within their organization as well as managers who oversaw those activities. Therefore, we conducted a two-phased study consisting of focus groups and a survey that allowed these professionals to tell us about their experiences. This report synthesizes the results from both the focus groups and survey.

Focus groups provided important insights into role-based training challenges within organizations.

In the first phase of our research, we conducted eight focus groups of federal employees (29 participants total). Focus group participants were from three types of government organizations:

- Department-level Executive organizations (e.g., U.S. Department of Commerce)
- Sub-component agencies, which are semi-autonomous organizations under a department (e.g., NIST is a sub-component under Department of Commerce)
- Independent agencies, which are not in a department (e.g., Federal Trade Commission)

Although the focus groups were targeted at security awareness topics and challenges, participants were often also responsible for RBT. Therefore, they frequently discussed RBT as a related and significant challenge within their organizations. More details about the focus group methodology can be found in the Technical Appendix.

A follow-on survey provided an opportunity to hear from a larger number of participants about their RBT activities.

RBT discoveries from the focus groups prompted and informed a second phase consisting of an RBT-focused, online survey of federal employees (82 responses). Within the survey, we asked participants about how their organizations determine which employees are required to take RBT, their sources of RBT content and materials, the perceived level of support for RBT within their organizations, how they measure the effectiveness of RBT, and challenges they encounter with RBT activities. More details about the survey methodology can be found in the Technical Appendix.

Participants had diverse backgrounds and roles and represented different types and sizes of organizations.

We purposefully recruited our focus group and survey participants to represent a range of government organizations. We found participants through professional contacts, attendee lists of prior government security awareness forums, and security-focused, online government mailing lists. Our study participants came from a variety of professional backgrounds and held a number of job classifications and roles (Work Roles defined by NICE). They represented diverse government organizations of different types (departments, sub-components, and independent agencies) ranging in size from less than 100 federal employees to over 50,000 employees. More details about the participants, their organizations, and their RBT programs can be found in the Technical Appendix.

RESULTS

In this section, we present the results of our study. Unless specifically noted, summary statistics (counts and frequencies of responses) are from the survey. Because survey participants had the option of skipping survey questions, participants may not have answered all questions. Therefore, we include the number of responses (n) for each question with our summary statistics.

Where appropriate, we include direct quotes from the focus group participants and open-ended questions in the survey to further support or provide more insight into 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). Survey quotes are included exactly as participants typed them. 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.

We asked study participants to share their most important pieces of advice regarding role-based training. These responses are captured within **"Advice from the Field"** text boxes throughout the report.

TRAINING ASSIGNMENT

Organizations determine which employees are required to take role-based training in a variety of ways.

Over half **(56%)** of survey participants indicated that the office of the Chief Information Officer (CIO) or Chief Information Security Officer (CISO) determines which employees are required to take RBT (Figure 1). Less than half **(45%)** use the NICE Framework [SP800-181]. Almost a quarter **(24%)** leave it up to supervisors to make the decisions.

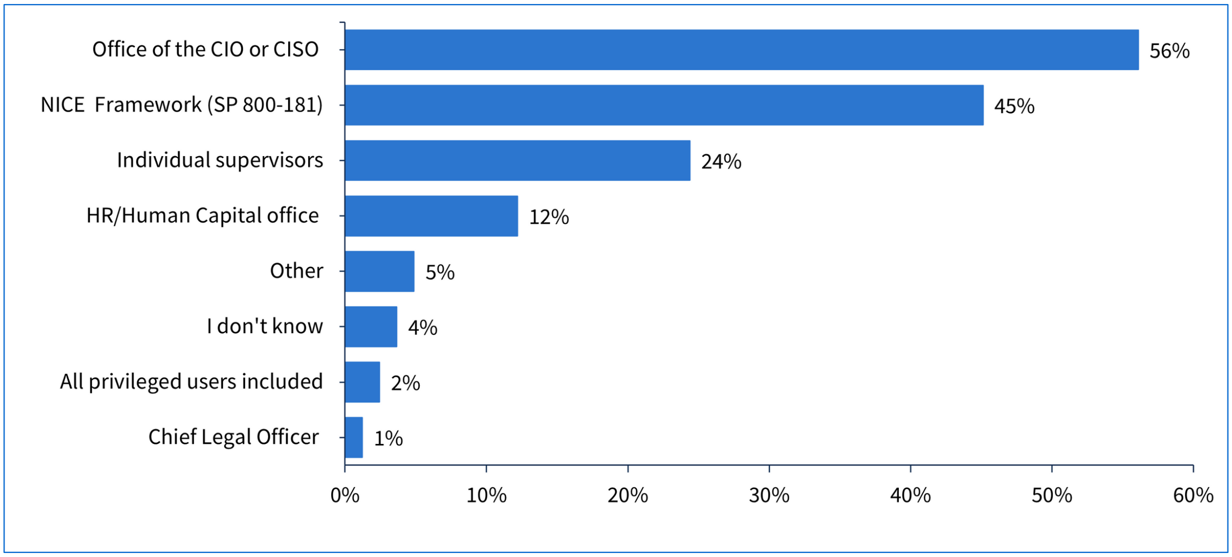


Figure 1. How organizations determine which employees take RBT (n = 82)

> *"We now have utilized the NICE cybersecurity workforce framework in order to have those specific work roles. We've aligned all of our federal employees and contractors to a specific work role." (S08)*
>
> *"[RBT assignment is] pretty much up to supervisors and the management groups who identify those personnel reporting to them that have significant information responsibilities." (D05)*

Some organizations experienced challenges when identifying which employees have to take role-based training.

Survey participants (n = 76) rated the level of challenge they experienced in identifying which employees have to take RBT.

26%	rated identifying employees as moderately/very challenging
72%	rated identifying employees as slightly/not challenging
1%	does not apply to their organization

"We need our human resources management system to be upgraded to more accurately track the job roles so that we can automatically align the job roles with the NIST [NICE] framework and automatically assign role-based trainings to the users." (D06)

Focus group and survey participants further expanded on challenges related to RBT assignment. Challenges included coordination issues between human resources (HR) and learning management systems (LMS) and inconsistent mapping between organizational positions and cybersecurity work roles.

ADVICE FROM THE FIELD: TRAINING ASSIGNMENT

"Identification of the work-force, federal staff and contractors, is crucial to establish and maintain. Staff, and contractors, come and go throughout the year so...on-going monitoring is necessary." (Q04)

"Define [RBT assignment] based on job roles, not [Office of Personnel Management] job series." (Q16)

"Inventory the roles and have a change management process for when a person changes roles. Identify performance metrics and coinciding cybersecurity workforce code for position description. Communicate the role, code, performance metrics, and training requirement with those users, annually." (Q22)

"Identify the roles providing critical cybersecurity support, so if necessary can be prioritized in a phased approach. Document the roles and the type of training needed and the frequency." (Q52)

RBT CONTENT AND APPROACHES

Organizations obtained RBT materials from a variety of sources, most often creating content in-house or purchasing from training vendors.

61% create RBT content within their organization (Figure 2). Over half **(55%)** of survey participants purchase RBT from another organization or vendor, and **just over a third** either receive RBT from their parent department organization (if a sub-component organization) or obtain RBT at no cost from another organization. Over half of survey participants **(54%)** selected more than one way that they obtain RBT content.

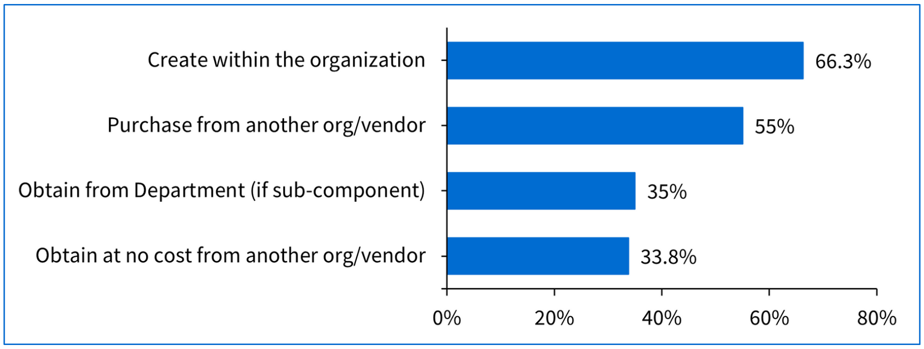


Figure 2. How organizations obtain RBT content (n = 80)

> *"We do have some courses that are...[from training] course providers, but we do a lot of our own content development usually using some subject matter experts or industry standards." (N05)*

Almost half of (44%) participants thought that finding RBT courses or materials was moderately or very challenging.

Survey participants (n = 76) rated the level of challenge they experienced in finding RBT courses or materials.

44% rated finding materials as moderately/very challenging

52% rated finding RBT materials as slightly/not challenging

3% challenges don't apply to their organization

Participants were most often challenged by the cost of buying or developing training materials or finding content applicable to their employees' roles. To address these challenges, participants in both the focus groups and survey recommended that standardized training be made available for use by all federal organizations.

> *"I would rather not spend like millions and millions and have an individual course for all 60 some Work Roles in the framework...There needs to be federal level trainings that are available...to get that 80% there. And then each department and agency can then take that and add their specific 20% that's the agency-related training information." (D02)*

ADVICE FROM THE FIELD: FINDING RBT MATERIALS

“Always use available ‘canned’ training when possible; tap information from subject matter experts and requirements for the course.” (Q09)

“Reuse content as applicable, and supplement with internal SOPs [standard operating procedures]…use commercial subscriptions where possible and feasible.” (Q22)

“Identify existing training resources from vendors and other government agencies – there are many free and paid training content available online, such as written documentation, blogs, vlogs, [online videos], and various types of online training materials.” (Q52)

Over half of participants update their RBT content at least annually, but updating content can be a challenge.

Over half of survey participants **(55%)** indicated that their organization updates RBT content every year (Figure 3). Almost **18%** noted that their organization updates their training less often than once a year.

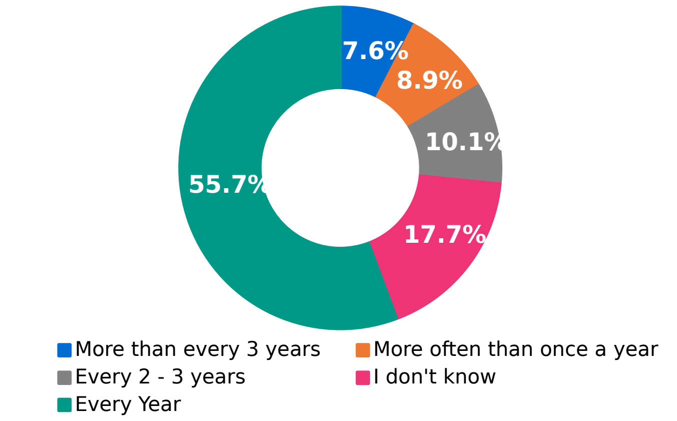


Figure 3. How often RBT is updated (n = 79)

Survey participants (n = 76) also rated the level of challenge they experience updating RBT content.

45% rated updating RBT as moderately/challenging
47% rated updating RBT as slightly/not challenging
8% challenge does not apply to their organization

“Stale training is often worse than no training. If your training covers the same basic content…year over year, you are not training effectively. Security evolves daily, and the training should reflect this." (Q23)

Almost all organizations provide online options for employees to complete RBT, while over half offer live training options.

95% of participants said their organizations offer online RBT (Figure 4). Almost two-thirds **(63%)** of participants' organizations allow employees to complete RBT via in-person or virtual training events held by their organizations, and over half allow employees to attend events outside the organization. Just under half of survey participants **(49%)** apply industry-recognized certifications towards fulfilling RBT requirements.

Over two-thirds **(68%)** of survey participants indicated that their organization allows more than one way to complete RBT. Several participants in both the focus groups and survey said that their organizations give employees the flexibility to choose what training to take as long as it applies to their specific job roles.

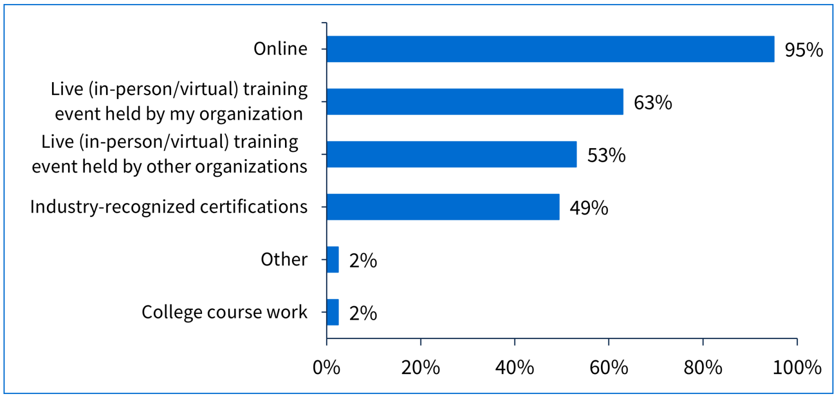


Figure 4. How employees complete RBT (n = 81)

"We don't have a lot of role-based training in our LMS , which is why we do our events and we let people go to whatever vendor training that they want to, as long as they can show that alignment with at least one of their job competencies." (D02)

ADVICE FROM THE FIELD: RBT OPTIONS

"Determine the best approach for your culture and operational environment." (Q06)

"Defer to professional certifications...for a subset of roles (e.g., control assessor, incident responder, security officers, etc.)." (Q22)

"Permit ability to assess-out for those having maturity in role." (Q22)

"I try to make sure that role-based training occurs throughout the entire year and not just a one-time affair, especially for those individuals that are dual-hatted and that's not their primary job...If they're not living and breathing it, they may not realize, 'Hey, I've got to make sure I look at this, and I'm looking for this type of content,' so to speak." (N10)

Just under 60% of participants agreed that their organization tailors RBT content to their organizational mission or current security risks.

Survey participants (n = 78) rated their level of agreement on whether their organization tailors RBT to the organizational mission and to current security risks to the organization (Figure 5). **54%** agreed or strongly agreed that their organization tailors RBT to their mission. More **(58%)** agreed or strongly agreed that their organization tailors RBT to current security risks.

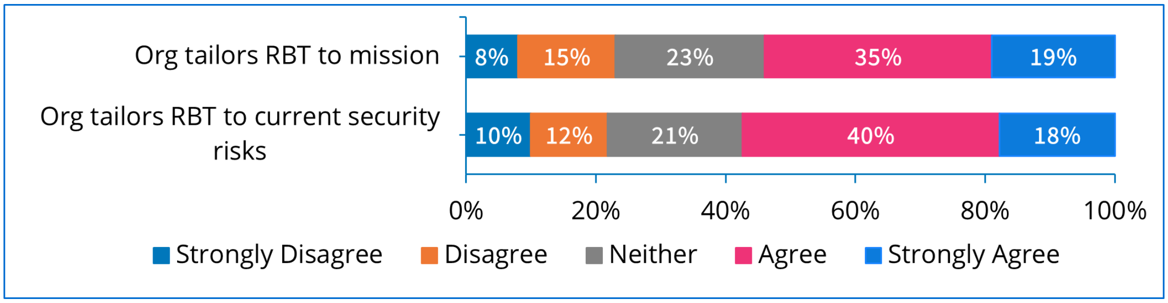


Figure 5. Organization tailors RBT to the mission and security risks - agreement (n = 78)

Participants discussed several ways in which they tailor RBT to their organizations, including: consulting with subject matter experts in the organization; obtaining feedback from employees on what topics are most relevant to their roles; addressing recent security issues within the organization; and focusing on current topics of interest for federal agencies. However, others discussed challenges, for example, not having the resources to develop training tailored to organizational roles or mission.

ADVICE FROM THE FIELD: TAILORING RBT

"Training for a 'new in role' and 'refresher training' needs are quite different. 'New in role' training needs to establish foundations for success not just a lecture on responsibilities. 'Refresher training' needs to focus on recent changes (e.g., in guidance, threat categories) and how to remain effective in the role. Nothing loses the audience faster than providing 'new in role' training to people that have been doing this for years." (Q23)

"Training needs to integrate within the organization's management structure. How does this role extend its practice to include security outcomes? How are risks communicated? How do budget requests for security topics handled? How do you work with other roles?" (Q23)

"Listen to the business units regarding what they need." (Q75)

"If you're responsible for Privileged User Training, get to know some privileged users – and their managers. Begin a dialogue. Solicit feedback." (Q19)

"Bring your ISSOs [Information Systems Security Officers] together to gather the most issues they see so that we could include those issues in the training." (Q30)

Over a third of survey participants said finding guidance on how to implement RBT activities is challenging.

Participants (n = 76) rated the level of challenge their organizations face in finding guidance on how to implement RBT activities.

34%	rated finding guidance as moderately/very challenging
61%	rated finding guidance as slightly/not challenging
5%	challenge does not apply to their organization

To address this challenge, survey participants indicated a desire for more government-provided guidance or platforms for sharing best practices and lessons learned.

“Role-based is hard, and it's hard because I don't believe that we're getting good direction... or it’s not targeted. It's like, ‘Hey, just do the best you can.’ So that's kind of frustrating.” (D01)

“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)

ADVICE FROM THE FIELD: IMPLEMENTING RBT

“Get your policies and procedures straight first. Make your processes repeatable and simple. Overburdening the process with nice-to-have but unnecessary elements is a recipe for failure.” (Q17)

"Create the documentation to establish a program and get it approved so there is continual program funding...Create a program plan that describes the mission, vision, and a phased implementation approach, including a continuous learning cycle.” (Q52)

TRAINING COMPLIANCE

While organizations most often use learning management systems to track RBT completion, over a third use a manual system for tracking.

Participants selected all methods that their organization utilizes to track RBT completion (Figure 6). Over half **(54%)** of survey participants use a Department-wide learning management system (LMS). Over a third **(37%)** utilize a spreadsheet or other type of manual method to track RBT completion. Only **7%** indicated that their organization does not track RBT completion. **29%** of survey participants use more than one method to track.

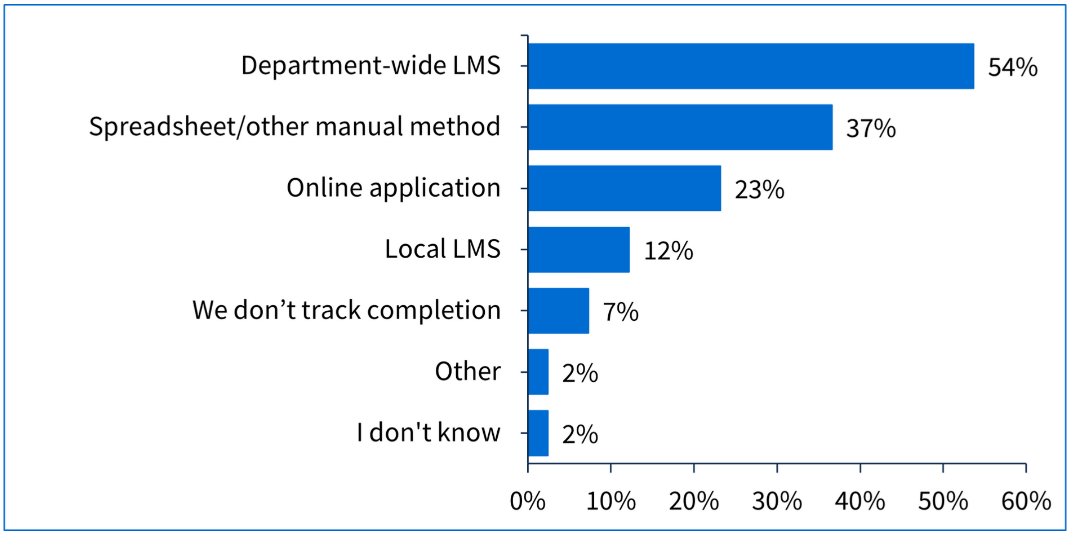


Figure 6. Tracking RBT completion (n = 82)

Most organizations do not experience challenges tracking RBT completion, but training tracking for contractors is more challenging than for federal employees.

Survey participants rated the level of challenge their organizations face when tracking federal and contractor employee completion of RBT (Figure 7). **19%** of participants indicated that it was very or moderately challenging to track federal employee completion of RBT. Over a quarter **(29%)** said it was very or moderately challenging to track contractor completion of RBT.

> *“We've explored self-paced training options, but ensuring compliance and tracking completion is challenging there.” (Q72)*

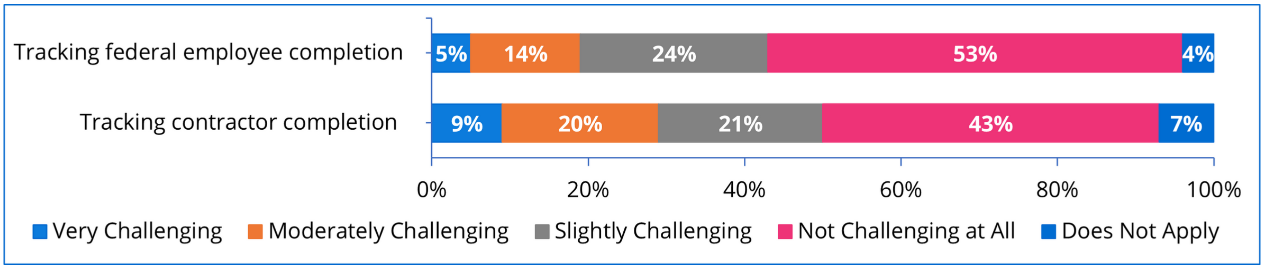


Figure 7. Tracking federal and contractor employee RBT completion (n = 76)

Organizations experienced challenges getting employees to complete RBT training by the appointed deadline.

Participants rated the level of challenge their organization experiences in getting employees to complete RBT (Figure 8). **40%** indicated that it is very or moderately challenging to get employees to complete required RBT. Slightly more **(42%)** indicated that it is very or moderately challenging to get employees to complete RBT that is not required.

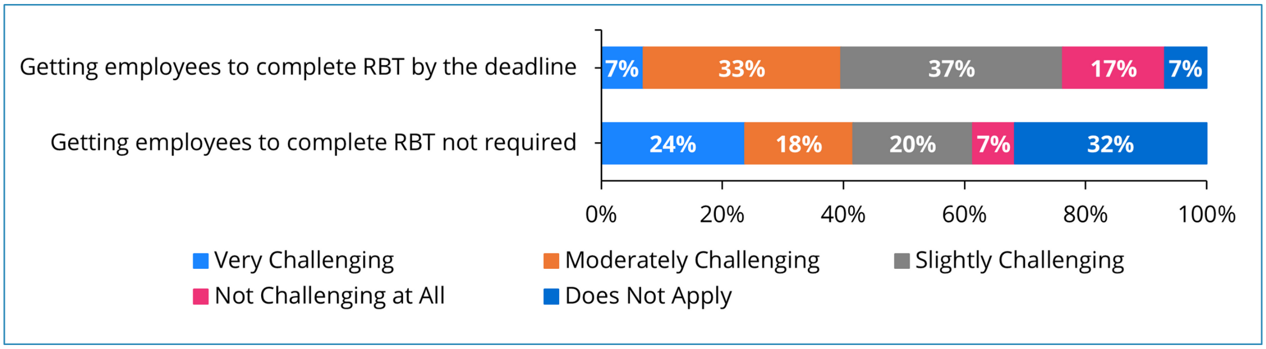


Figure 8. Level of challenge getting employees to complete RBT (n = 76)

While some organizations have been successful in achieving high compliance numbers, others experienced challenges in getting employees to complete training. Training overload (employees having to complete many mandatory training courses) and employee time constraints were often cited as hindrances to training completion. In some organizations, the lack of concrete consequences for failure to complete training was also an issue.

> *“Finding time during the workday to login and take required courses is extremely difficult...Since there are few if any repercussions, some people do not take the courses.” (Q60)*

When employees fail to complete training by the deadline, organizations often send email reminders, contact supervisors, or disable accounts.

We asked participants what they did when employees do not complete RBT by a specified deadline (Figure 9). **Over half** of participants stated that employees are sent a reminder email or their supervisor is contacted. **40%** said employee accounts are disabled, and **30%** disable or suspend network access.

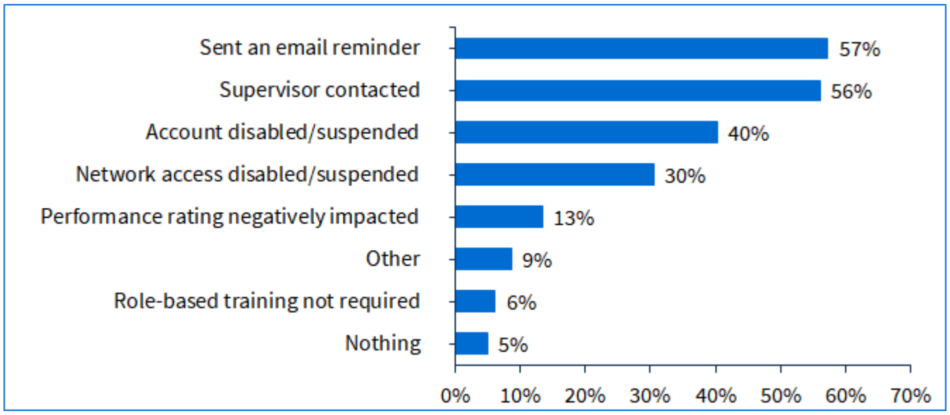


Figure 9. What happens when employees do not complete RBT (n = 82)

> *"This past fiscal year, actually, was the first time we've actually done so. We, historically, had low completion rates, and that's because no one feared that we actually would shut them off. So, they learned that we will.” (N06)*

ADVICE FROM THE FIELD: TRAINING COMPLIANCE

“Do not require all mandatory courses due at the same time.” (Q60)

"Report regularly to management on status, especially when you need to enforce compliance.” (Q11)

“Allow responses to fly in in waves because students often wait until the last minute, need a slight extension for completion, may not have understood directions or where to submit their course completion, and you should provide clear instructions.” (Q25)

“Automation for tracking” (Q38)

SUPPORT FOR ROLE-BASED TRAINING

The majority of participants agreed that employees understood the relevance of RBT and were supportive of RBT activities.

Almost two-thirds **(65%)** of survey participants agreed or strongly agreed that employees understand how/why RBT is relevant to them (Figure 10). **66%** agreed that employees were supportive of RBT activities.

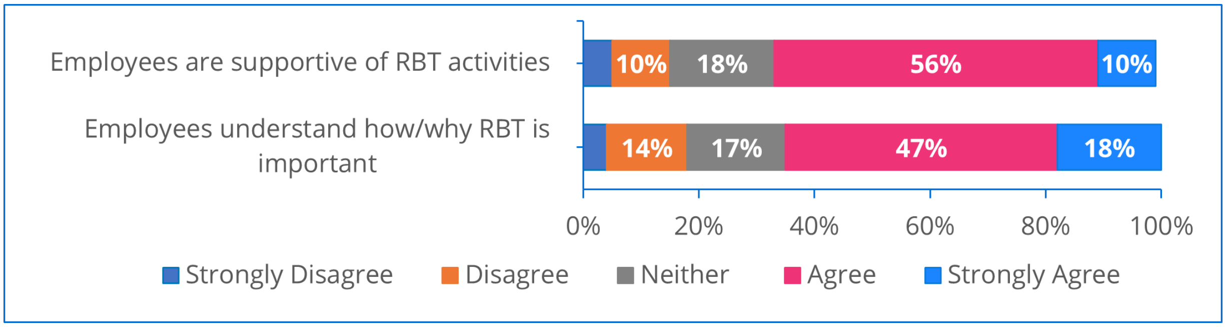


Figure 10. Employee understanding of and support for RBT activities – agreement (n = 78)

However, several organizations experienced challenges related to employees not understanding how RBT relates to their jobs and why they have been assigned training, especially if they do not have explicit cybersecurity roles. To mitigate this challenge, participants emphasized the importance of clearly communicating RBT relevance to employees' specific job roles.

> *"This year we held a briefing to communicate the role-based training requirement to stakeholders...The roll out of this program has been the easiest" (Q28)*
>
> *"We do get a lot of pushback where people are saying, 'What does this have to do with my position or what I'm working in at the time?' It's a little frustrating." (N02)*

ADVICE FROM THE FIELD: GAINING EMPLOYEE SUPPORT

"Focus on why role-based training supports the mission of your organization. Don't start with 'everyone needs to complete 1 course or 8 hours of training.' Frame as opportunity to build a better workforce to support mission, retain talent, etc." (Q28)

"Clearly communicate WHY an individual is assigned role-based training requirement." (Q33)

"Communicate to the stakeholders and to employees the training program." (Q52)

Most participants agreed that their leadership understood the relevance of RBT and were supportive of RBT activities.

70% of survey participants agreed or strongly agreed that leadership understands the relevance of RBT to them (Figure 11). In addition, almost three-quarters **(73%)** agreed or strongly agreed that leadership is supportive of RBT activities.

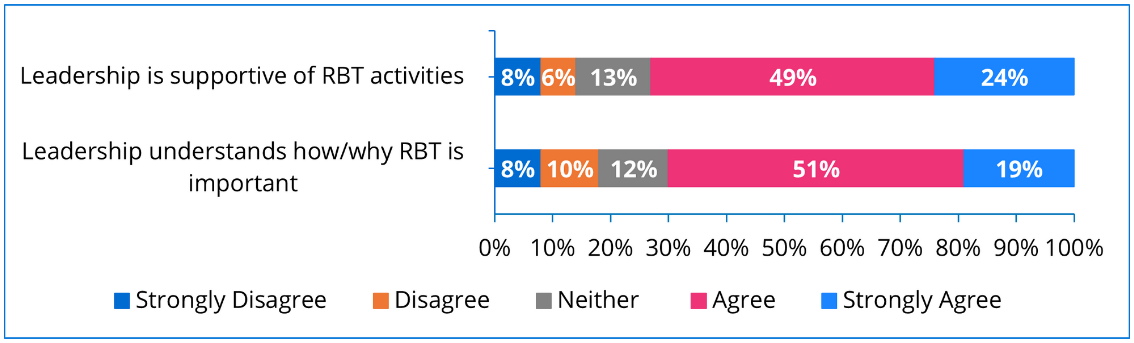


Figure 11. Leadership understanding of and support for RBT activities – agreement (n = 78)

While some participants touted the support they receive, a few survey participants expressed challenges gaining leadership support for RBT activities. Managers may view RBT simply as a compliance activity with little value. Lack of leadership support is often evidenced by inadequate funding for RBT activities.

> *"My sub-org's Directors and System Owners have understood the importance of RBT and supported having their staff complete their RBT courses." (Q54)*
>
> *"RBT is not taken seriously by…leadership at the CIO and above…It is a compliance exercise. I have submitted budget requests to improve the program and put comprehensive metrics in place, but they have been denied." (Q29)*

ADVICE FROM THE FIELD: GAINING LEADERSHIP SUPPORT

"Have management support; it'll be a culture change for the organization and it's much easier to get management buy-in early in the process and not while you're trying to get your CIO to do the training." (Q03)

"Obtain a sponsor for the program. Identify and communicate often to stakeholders. Get into as many meetings as you can to talk about your program. Stakeholders may have resources to support program." (Q28)

"Get leadership support prior to embarking on the efforts." (Q81)

Over half of participants disagreed that they had adequate funding and staff for RBT activities, but over 70% thought they had adequate technology.

42% strongly disagreed or disagreed that they have adequate funding for RBT activities (Figure 12). **52%** strongly disagreed or disagreed that they have adequate staff. Participants commented that resource challenges could hinder their ability to develop trainings tailored to multiple roles.

> *“We need to develop training that would help improve the security for every single role and we don't have the resources (time, money) to do it.” (Q03)*

Fewer participants **(28%)** strongly disagreed or disagreed that they have the necessary technology to support RBT activities. Several expressed the need for technology improvements, for example, a more robust learning management system or the ability to upload external training videos to existing platforms.

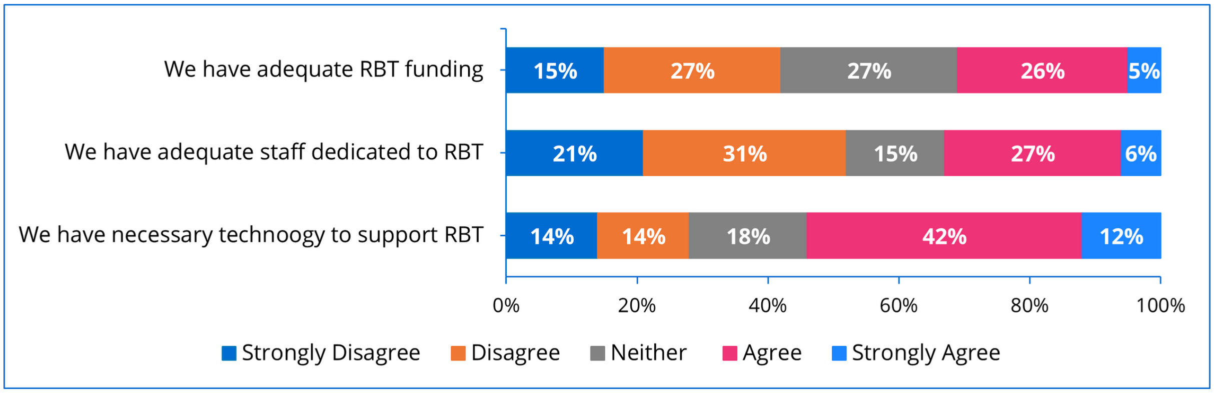


Figure 12. Organization has adequate funding, staff, technology for RBT activities – agreement (n = 78)

ADVICE FROM THE FIELD: RESOURCES

“Get management buy-in to allocate a specific, reasonable amount of annual funding for each person in each cybersecurity/privacy role to ensure they can get adequately trained (reasonable is thousands of dollars per person for specialized training, not under $100 per person).” (Q15)

“Prioritize the resources available to meet the critical training gaps.” (Q52)

DETERMINING TRAINING EFFECTIVENESS

Over half of participants rated their RBT activities as successful.

We asked participants to rate whether their RBT activities are successful on a scale ranging from very unsuccessful to very successful (Figure 13). Just over **28%** rated their RBT activities as slightly successful, and about **20%** rated their activities as very unsuccessful or unsuccessful.

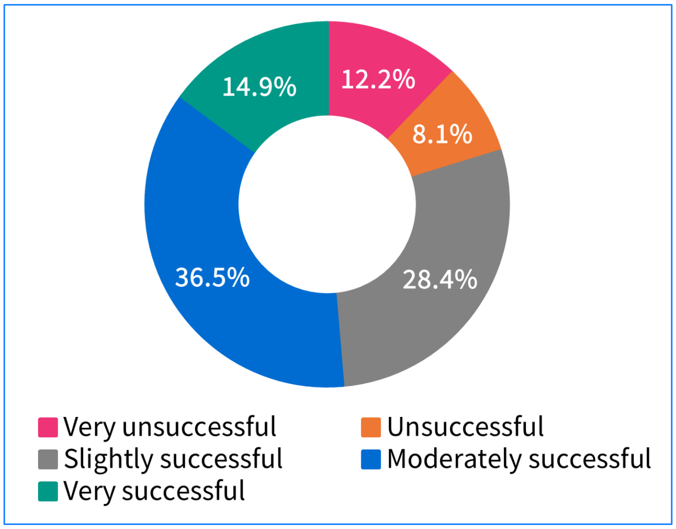


Figure 13. Success of RBT activities (n = 74)

Training completion rates were the most used method of determining the effectiveness of RBT, with much fewer considering evidence of employee learning.

Almost two-thirds **(65%)** of survey participants measure RBT effectiveness by using training completion rates, and just under half evaluate success via audit reports or evaluations (Figure 14). Less than half **(46%)** gauge effectiveness from informal employee feedback (e.g., in-person discussions, emails), and **34%** use employee surveys to determine training success. Just under a quarter **(24%)** examine behaviors (e.g., security incident trends and incident reporting) as evidence that employees are applying what they have learned through RBT. **9%** of participants do not attempt to measure the effectiveness of their RBT activities at all.

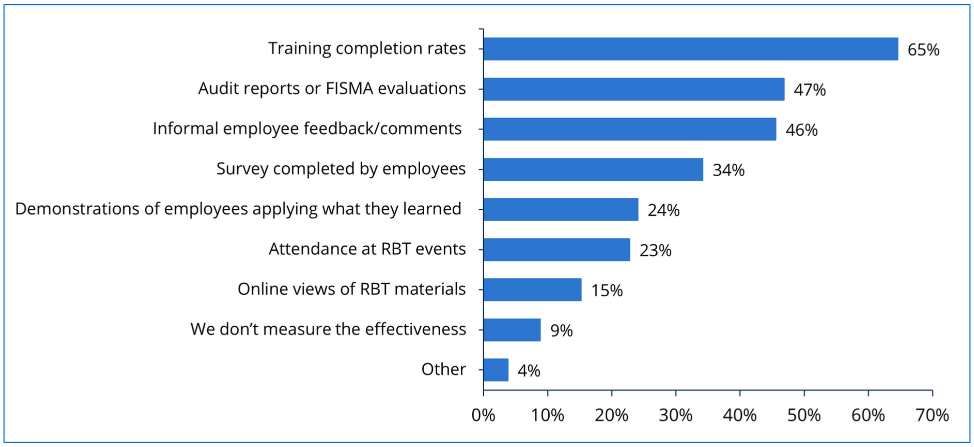


Figure 14. Measures of RBT effectiveness (n = 79)

> *"We have feedback that we get from employees...We make adjustments based on those critiques." (S09)*

Over half of participants said that determining RBT effectiveness was moderately or very challenging.

Survey participants (n = 76) rated the level of challenge they experienced in determining the effectiveness of their organization’s RBT activities.

58%	rated determining effectiveness as moderately/very challenging
38%	rated determining effectiveness as slightly/ not challenging
4%	challenge does not apply to our organization

“[What would help RBT efforts be more successful:] More emphasis on measuring the effectiveness of training and some way to prove out/use the skills that were learned from role-based training. People learn best when they have to do a task.” (Q24)

ADVICE FROM THE FIELD: DETERMINING EFFECTIVENESS

“Find good metrics to demonstrate participation and where possible, effectiveness.” (Q36)

“Create the metrics to showcase success.” (Q52)

LIMITATIONS

Because of our specific research goals towards aiding U.S. Government organizations, our investigation is limited to the U.S. Government, which may have different RBT policies and pressures as compared to other sectors. However, our findings may be transferable, at least in part, to other organizations.

Although we recruited participants from organizations of varying sizes and types, our participants may not represent the full range of government cybersecurity awareness programs. It is possible that more than one person from an organization may have completed the survey. Therefore, the 82 survey participants may not represent 82 unique organizations.

In this study, we relied on self-reported data from our participants. This kind of data may be subject to several biases, including:

- Social desirability bias - the tendency for people to answer questions in a way that is likely to be viewed favorably by others
- Self-selection bias - because participants choose whether to participate in a study, it may be that those with certain or strong opinions or ideas are more likely to participate
- Recall bias – people's memories of prior experiences may not be accurate
- Perception bias – the subjectivity of people's thoughts and interpretations may or may not reflect reality

We attempted to mitigate the impacts of these biases in several ways. First, we keep the identities of participants and their organizations confidential. The survey itself was anonymous in nature, which may encourage participants to be honest with their responses. Additionally, while some results are based on perceptions, it is important to understand people's subjective thoughts about RBT as these may reveal real-world issues.

DISCUSSION

In this section, we summarize the high-level takeaways from our study, including suggested actions for organizations based on the successes and challenges identified by our participants in the focus groups and survey. We also recommend actions that could be taken by supporting organizations, which are those government entities that produce RBT guidance documents, policies, and other resources for government organizations. An update to *NIST SP 800-50, Building a Cybersecurity and Privacy Learning Program*, may address some of the suggestions for supporting organizations.

RBT assignment is not standardized across the government.

There is no standard way that organizations determine which employees are assigned RBT. For many organizations, the office of the CIO is involved in the decision-making process. However, less than half of our survey participants use the NICE Framework, a defacto standard for identifying cybersecurity Work Roles and their associated Tasks, Knowledge and Skills. More concerning, some organizations leave role-based training assignment up to the (perhaps) subjective decisions of individual supervisors. Overall, about a quarter of participants rated determining RBT inclusion as moderately or very challenging, sometimes because of inconsistent cybersecurity Work Role mapping or lack of coordination between learning management and human resource systems.

SUGGESTED ACTIONS

FOR ORGANIZATIONS WITH RBT ACTIVITIES:

Consider using the NICE Framework to identify cybersecurity Work Roles within an organization. The NICE Framework can also be used to identify tasks, knowledge, and skills that can be incorporated into the training for those roles.

FOR SUPPORTING ORGANIZATIONS:

Develop guidance or policies on how organizations should assign RBT.

Obtaining and implementing relevant RBT can be challenging.

Some organizations struggle with finding RBT courses and materials and updating the training. Creating content in-house can be resource-intensive, while purchasing content, especially when in support of many Work Roles, can be cost-prohibitive. On a positive note, the majority of survey participants said that their RBT content is tailored to their organizational mission and current security threats, and over half update content on at least an annual basis to maintain relevance.

While almost all organizations utilize online training, others conduct live training, accept industry-recognized certifications, or allow employees flexibility in selecting what type of training to take. On one hand, these variabilities may be advantageous in tailoring training modalities to the needs of organizational employees. However, they may also reflect a lack of standardization and, sometimes, uncertainty about the type of training that satisfies RBT requirements. In fact, more than a third of our participants said that finding guidance on how to implement RBT activities can be challenging.

SUGGESTED ACTIONS

FOR ORGANIZATIONS WITH RBT ACTIVITIES:

- Do not “reinvent the wheel.” Use existing RBT content when possible.
- Talk to peers in other organizations about their RBT successes and lessons learned.
- Solicit feedback about RBT from managers and employees, including how the content and delivery could be improved or additional topics of interest to include in future offerings.
- Consider offering additional and engaging ways to complete RBT beyond the typical online course (e.g., attending security events or security certifications). Rather than limiting RBT to once a year, allow opportunities for employees to reinforce their learning throughout the year.
- Ensure course materials are updated with current topics most relevant to the organization.

FOR SUPPORTING ORGANIZATIONS:

- Provide guidance on how to implement an effective RBT program, including suggestions for approaches and where to find content.
- Explore the potential of developing or purchasing standard government RBT that would relieve the burden of content development while allowing for some customization to accommodate organizations’ unique missions.
- Provide venues for government information sharing about RBT, for example, lessons learned and examples of successful approaches. These venues could be online forums or events focused on security awareness and role-based training.

Organizations may experience challenges in their quest to meet mandatory RBT requirements.

While many survey participants said that their organizations leverage learning management systems to automate the tracking of RBT completion, over a third are using a manual method like a spreadsheet, which can result in extra burden placed on staff. While most participants said that they do not experience challenges tracking completion, tracking contractor training was more challenging than tracking federal employee training, sometimes because current LMS may not be accessible to contract staff.

Additionally, organizations were challenged in getting employees to complete training by the appointed deadline. This may be due to mandatory training overload, employee time constraints, or a lack of concrete consequences for not completing training (e.g., disabling accounts and network access).

SUGGESTED ACTIONS

FOR ORGANIZATIONS WITH RBT ACTIVITIES:

- Spread out mandatory training deadlines throughout the year to avoid employees becoming overwhelmed.
- Automate the training tracking process as much as possible, possibly through integration with learning management systems.
- Consider what actions to take for employees who fail to complete training. Instead of exclusively focusing on negative consequences, explore implementing positive incentives to encourage employees to complete training and practice good security habits.

FOR SUPPORTING ORGANIZATIONS:

- Develop and acquire systems (e.g., learning management systems) that allow organizations to handle both federal and contractor employees.
- Provide guidance on how organizations might manage training deadlines and incentivize RBT completion.

While many participants believe employees and leadership are supportive of RBT activities, support may not be reflected in funding and staff.

A majority of survey participants believe employees understand the relevance of RBT and are supportive of the program. Clear communications about why RBT is relevant to employee work roles is critical for garnering this support. Although most also thought that leadership was supportive of RBT activities, a perceived lack of funding and staff does not reflect this support.

SUGGESTED ACTIONS

FOR ORGANIZATIONS WITH RBT ACTIVITIES:

- To alleviate confusion about RBT assignment, clearly communicate to employees why RBT is relevant to their Work Roles and the organizational mission.
- Gain leadership support of RBT activities. Provide leadership with concrete metrics that show the success of RBT or highlight areas requiring additional attention and resources.

FOR SUPPORTING ORGANIZATIONS:

- Provide guidance and examples related to what kind of RBT data is most relevant to organizational decision makers and suggestions on how to effectively present that data to leadership.

Measuring the effectiveness of RBT can be challenging for organizations, with success often measured by completion rates rather than impact on behavior.

Over half of survey participants rated their RBT activities as moderately or very successful. However, there is great variation in how organizations determine that success, and determining RBT effectiveness was viewed as challenging by close to 60% of survey participants. Many rely on compliance metrics, such as training completion rates or FISMA evaluations, that do not necessarily reflect impact on employee learning or behaviors, which is the goal of RBT. The lack of meaningful metrics may also place RBT staff at a disadvantage in trying to gain leadership support for training activities.

SUGGESTED ACTIONS

FOR ORGANIZATIONS WITH RBT ACTIVITIES:

- Leverage and combine a variety of different types of metrics, both quantitative and qualitative. In addition to how many employees complete the training, programs could look at demonstrations of employee behaviors and learning (e.g., as demonstrated by staff-generated security incidents or security policy violations) and which Work Roles seem to have the most issues.
- Involve employees as active contributors by collecting feedback about the training and topics they would like covered, e.g., via anonymous surveys and focus groups.
- Incorporate measures of effectiveness into an iterative feedback loop to continually identify areas of concern, refocus, and improve RBT initiatives.
- Automate quantitative metrics as much as possible. For example, leverage existing technologies, such as learning management systems or security operations data queries.

FOR SUPPORTING ORGANIZATIONS:

- RBT guidance documents should provide suggestions on what measures to collect and how to gather meaningful measures of effectiveness.
- Guidance and policies should emphasize the importance of assessing behavioral impacts rather than simply relying on compliance metrics, which do not tell the whole story about the effectiveness of RBT.

TECHNICAL APPENDIX

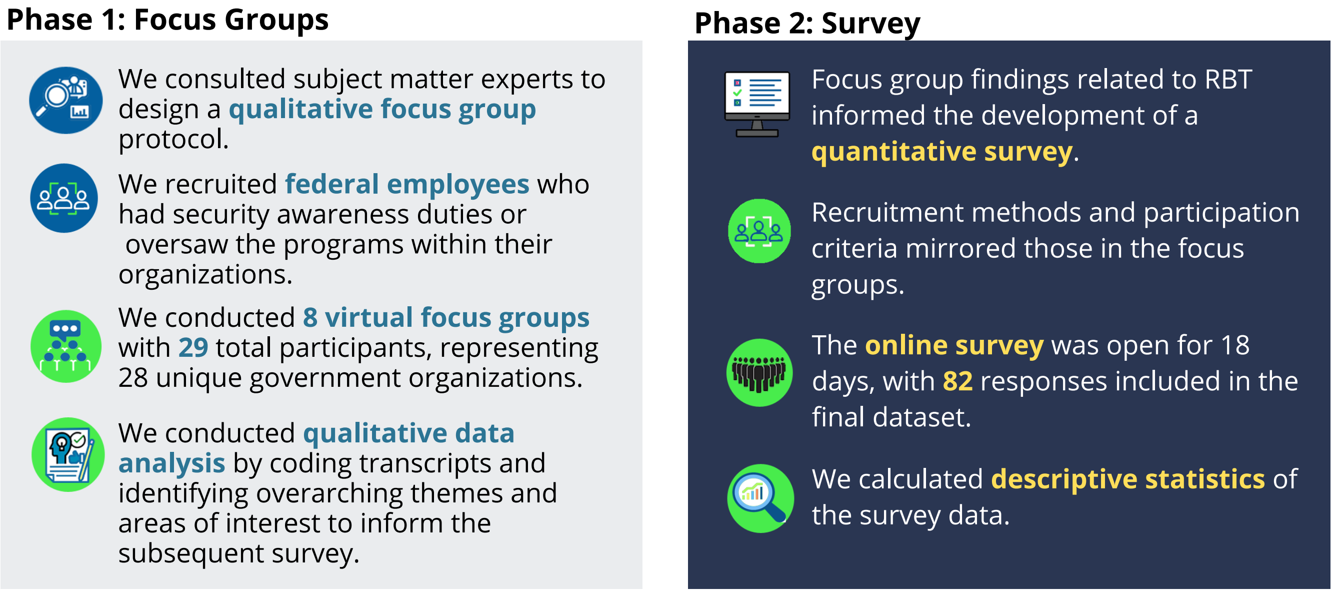
DETAILED STUDY METHODOLOGY

To explore federal security awareness programs, the study used a “mixed methods” research approach that leveraged both qualitative and quantitative methodologies [CLARK2019]. Qualitative research is used to capture why or how a phenomenon occurs as well as people’s experiences, beliefs, and motivations. Quantitative research methodologies involve “quantifiable” data (e.g., numerical or ordinal data) and are more focused on establishing generalizability or magnitude. Mixed methods studies take advantage of the strengths of both approaches.

We conducted the study in two sequential phases (Figure 15). In the first phase, we collected qualitative data via eight focus groups of federal employees involved in their organizations’ security awareness programs. The focus groups provided an understanding of how people think and talk about security awareness topics and what concepts and challenges participants viewed as most important. During the focus groups, because many security awareness professionals also had RBT duties, participants discussed RBT as being especially challenging.

Informed by insights gained in the focus groups, we subsequently conducted two follow-up surveys: one focused on security awareness and another focused on RBT. The RBT survey was completed by 82 federal employees involved in their organizations’ RBT activities. This report integrates the RBT-specific results from the focus groups and the RBT survey. Results from the prior security awareness study can be found in three related publications:

- *NISTIR 8420 Federal Cybersecurity Awareness Programs: A Mixed Methods Research Study* [IR8420]
- *NISTIR 8420A Approaches and Challenges of Federal Cybersecurity Awareness Programs* [IR8420A]
- *NISTIR 8420B The Federal Cybersecurity Awareness Workforce: Professional Backgrounds, Knowledge, Skills, and Development Activities* [IR8420B].



Phase 1: Focus Groups

We consulted subject matter experts to design a **qualitative focus group** protocol.

We recruited **federal employees** who had security awareness duties or oversaw the programs within their organizations.

We conducted **8 virtual focus groups** with **29** total participants, representing 28 unique government organizations.

We conducted **qualitative data analysis** by coding transcripts and identifying overarching themes and areas of interest to inform the subsequent survey.

Phase 2: Survey

Focus group findings related to RBT informed the development of a **quantitative survey**.

Recruitment methods and participation criteria mirrored those in the focus groups.

The **online survey** was open for 18 days, with **82** responses included in the final dataset.

We calculated **descriptive statistics** of the survey data.

Figure 15. Methodology at a glance

FOCUS GROUP METHODOLOGY

Focus Group Design

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

We selected a multiple-category design for the focus groups, which involved focus groups with several types of participants to allow for comparisons across or within categories [KRUEGER2015]. Based on SME discussions, we decided on three categories:

1) Department-level Executive organizations (e.g., U.S. Department of Commerce),
2) Sub-component agencies, which are semi-autonomous organizations under a department (e.g., NIST is a sub-component under Department of Commerce), and
3) Independent agencies, which are not in a department (e.g., Federal Trade Commission)

The focus group protocol consisted of 11 questions covering topics such as cybersecurity awareness approaches, successes, challenges, measures of effectiveness, wish lists, and necessary knowledge and skills for security awareness teams. See the Study Instruments section of this appendix for the full focus group instrument.

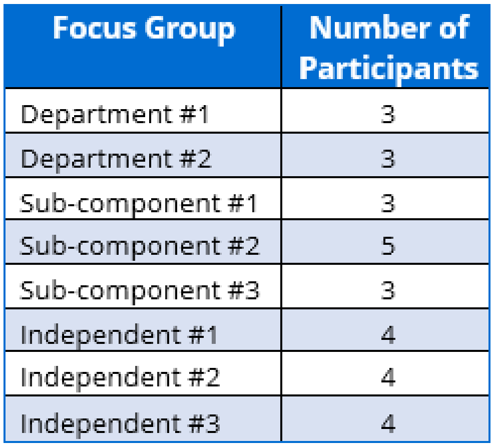
Focus Group Recruitment

We selected potential focus group participants to represent the diversity of federal agencies. We identified participants via several avenues: recommendations from the SMEs; researchers' professional contacts; an online cybersecurity-focused mailing list for the Small and Micro Agencies Chief Information Security Officer (CISO) Council [SMAC2022]; speakers and security awareness material contest participants from the last three years of the Federal Information Security Educators (FISSEA) conference [FISSEA2022]; and LinkedIn and Google searches. Participants had to be federal employees and have knowledge of the cybersecurity awareness programs in their organizations either because they had security awareness duties or oversaw the programs.

Focus Group Data Collection

Between December 2020 and January 2021, we conducted eight virtual focus groups with 29 total participants. Focus group sessions lasted 60-75 minutes, with each having 3-5 participants. Multiple focus groups were conducted for each category of organization. Table 1 shows the number of participants in each focus group. The sub-component #2 focus group included two participants from the same organization. In all, 12 independent agencies and 9 of the 15 unique Departments (considering both the department-level and sub-component participants) were represented in the focus groups.

Table 1. Number of participants in each focus group



Focus Group	Number of Participants
Department #1	3
Department #2	3
Sub-component #1	3
Sub-component #2	5
Sub-component #3	3
Independent #1	4
Independent #2	4
Independent #3	4

All focus groups were audio recorded and transcribed. Participants also completed a short, online survey to gather demographic and organizational information (see Focus Group Instruments later in this appendix). To ensure anonymity and to be able to confidentially link data between the focus groups and demographic survey, we assigned each participant a reference code. Individuals from Independent agencies are identified as N01 – N12, department-level organizations as D01 – D06, and Sub-components as S01 – S11.

Focus Group Data Analysis

Data analysis started with coding, which involves categorization of focus group data. We labeled units of text within the focus group transcripts based on the topic or represented concept, with these labels being called “codes.” Units may consist of a phrase, sentence, or multiple sentences. For example, the unit of text “I partner with our internal communication group on a lot of activities to lean on their communication expertise” was assigned the code “Collaboration - Internal.”

Initially, each member of the research team individually coded a subset of three transcripts (one from each category of focus group) using a preliminary code list based on the focus group questions and then added new codes as needed. We met several times to discuss codes for this subset and develop a codebook (a list of codes to be used in analysis). As part of the final codebook, all codes were “operationalized,” which involved formally defining each code to ensure understanding among all coders. Coding continued until all transcripts were coded by two researchers, who met regularly to discuss code application and resolve differences. The entire research team convened to discuss overarching themes identified in the data and areas of interest to include in the subsequent survey.

SURVEY METHODOLOGY

Survey Design

We developed the RBT survey questions and answer options based on areas of interest identified in the focus groups. The survey was reviewed by three SMEs: a security training manager in a sub-component agency, a manager of a government-led cybersecurity workforce program, and a privacy expert involved in developing RBT guidance.

The final survey (see Survey Instruments) addressed the following topics:

- Participants' level of involvement with respect to RBT and their job classifications
- Organizational information (type, number of federal employees)
- RBT program information (number of employees taking RBT, number of staff charged with implemented RBT)
- RBT assignment to employees
- RBT content and approaches
- RBT compliance with training requirements
- Organizational support for RBT activities
- Determining RBT effectiveness and success

The survey included several question types:

- Multiple choice questions, which prompt participants to either select one option or check all options that apply
- Likert scale questions, which provide a range of options (e.g., Strongly Disagree – Disagree – Neither agree nor disagree – Agree – Strongly Agree) and are used to gauge participants' opinions and perceptions
- Open-ended questions, which require participants to type their answers into a comment box and are used to obtain qualitative responses that may not be otherwise anticipated

Survey Recruitment

To participate in the survey, participants had to be federal employees directly involved in or overseeing their organization's RBT activities. Survey recruitment was conducted in several ways. We sent emails to our focus group participants and other professional contacts involved in security training inviting them to either complete the survey themselves if they had RBT duties or forward the survey to appropriate staff in their organization. Emails were also sent to three security-related government mailing lists: Small and Micro Agency CISO Council [SMAC2022], FISSEA [FISSEA2022], and Federal Cybersecurity and Privacy Professionals Forum [FCPPF2022].

Survey Data Collection

We implemented the survey on an online survey platform. The survey was open for two weeks in March 2022. The first page of the survey included an information sheet detailing the purpose of the study, participation criteria, study procedures, and how survey data would be protected. Prospective participants were then asked if they were federal employees and if they were involved in implementing or overseeing RBT within their organizations. Those that answered yes to both questions were permitted to continue the survey. All survey responses were anonymous.

Survey Data Analysis

Once the survey was closed, we compiled a final data set. We removed partial responses in which participants did not complete most responses or those for which responses appeared to have been randomly completed (e.g., all options for all questions were selected). Eighty-two survey responses were included in the final dataset.

For responses generating quantitative data, we calculated descriptive statistics (e.g., frequencies and percentages of participants selecting particular responses) to provide a summary of responses. We coded open-ended survey responses in a manner similar to the focus group data. The initial survey codebook was based on the codebook from the focus groups, with new codes added as needed. Two research team members individually coded all responses for each open-ended question, then met to resolve any differences in code application.

ETHICS

The 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.

Prior to data collection, participants in both the focus groups and survey were informed of the study purpose and how their data would be protected. Data were recorded without personal identifiers and not linked back to individuals or organizations. Throughout this report, any mentions of participant organizations or other potentially identifying information has been redacted.

SURVEY PARTICIPANT DEMOGRAPHICS

RBT Roles

Figure 15 shows the distribution of survey participants' RBT roles within their organizations. Over half **(51%)** lead RBT activities, including those who also are managers. **10%** of participants also oversee the contract for the activities (not shown in the chart).

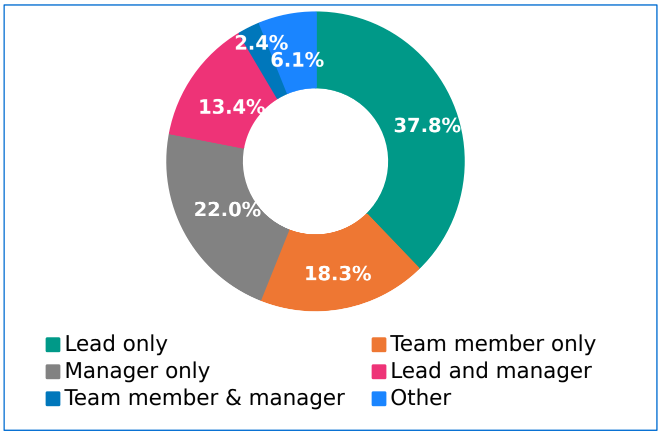


Figure 16. RBT role (n = 82)

Years Involved in RBT Activities

Most participants had substantial experience working on RBT, with a little over **60%** of participants indicating that they had at least five years of experience (Figure 16).

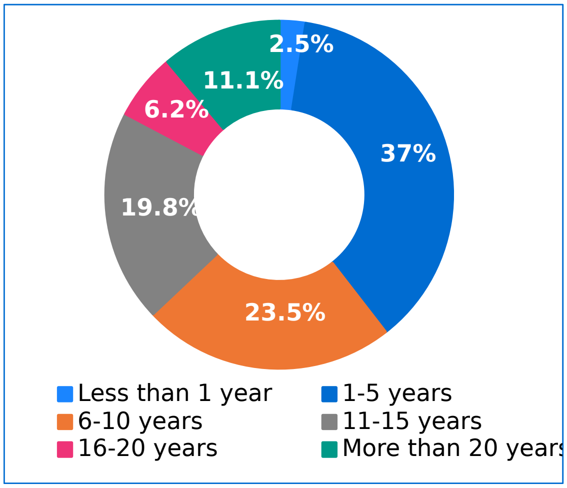


Figure 17. Number of years of RBT experience (n = 81)

Percentage of Time Working on RBT Activities.

Approximately **75%** of participants indicated that they spend **25%** or less of their time on RBT activities (Figure 17). Less than **8%** of participants indicated that they work full-time on RBT activities.

89% of survey participants indicated that, in addition to their RBT duties, they are involved in implementing or overseeing other security or privacy training or awareness program activities in their organization.

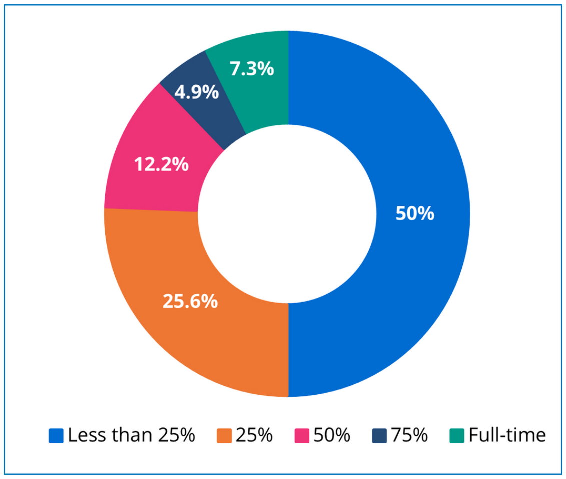
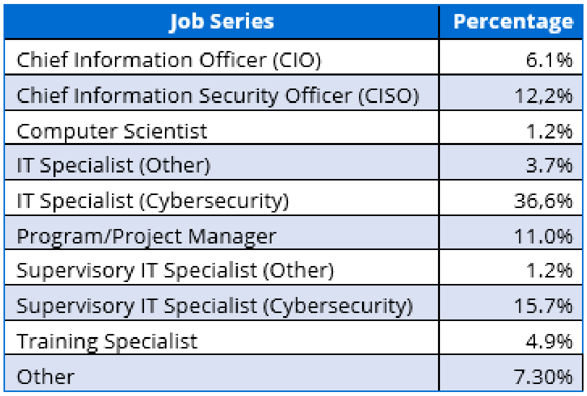


Figure 18. Percentage of time spent on RBT activities (n = 82)

Job Series Classifications

A little over **40%** of participants said their job series classification is an IT Specialist in either cybersecurity or another specialty (Table 2). Approximately **17%** were in supervisory roles, and **11%** were program managers.

Table 2. Job series classifications (n=82)



Job Series	Percentage
Chief Information Officer (CIO)	6.1%
Chief Information Security Officer (CISO)	12.2%
Computer Scientist	1.2%
IT Specialist (Other)	3.7%
IT Specialist (Cybersecurity)	36.6%
Program/Project Manager	11.0%
Supervisory IT Specialist (Other)	1.2%
Supervisory IT Specialist (Cybersecurity)	15.7%
Training Specialist	4.9%
Other	7.30%

NICE Framework Work Roles

Less than half of survey participants **(46%)** said they were assigned to a NICE Framework Work Role (Figure 18). Almost a fourth **(22%)** did not know if they were assigned a Work Role.

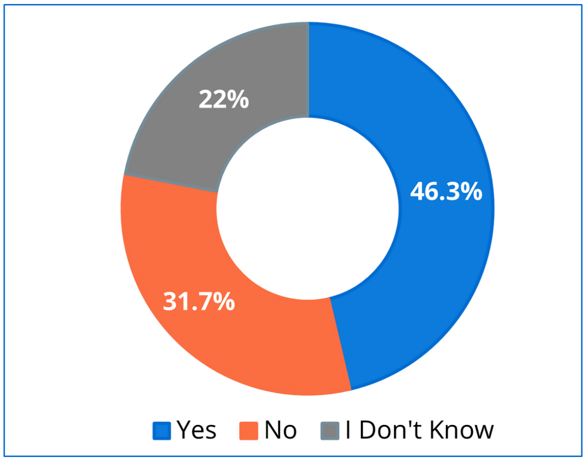


Figure 19. Assigned to a NICE Framework Work Role (n = 82)

Those participants assigned to a NICE Framework Work Role indicated which Role(s) they have (Figure 19). The most common work role selected was Cyber Policy and Strategy Planner **(32%)**. **26%** of participants said that they were assigned to the Cyber Workforce Developer and Manager Work Role.

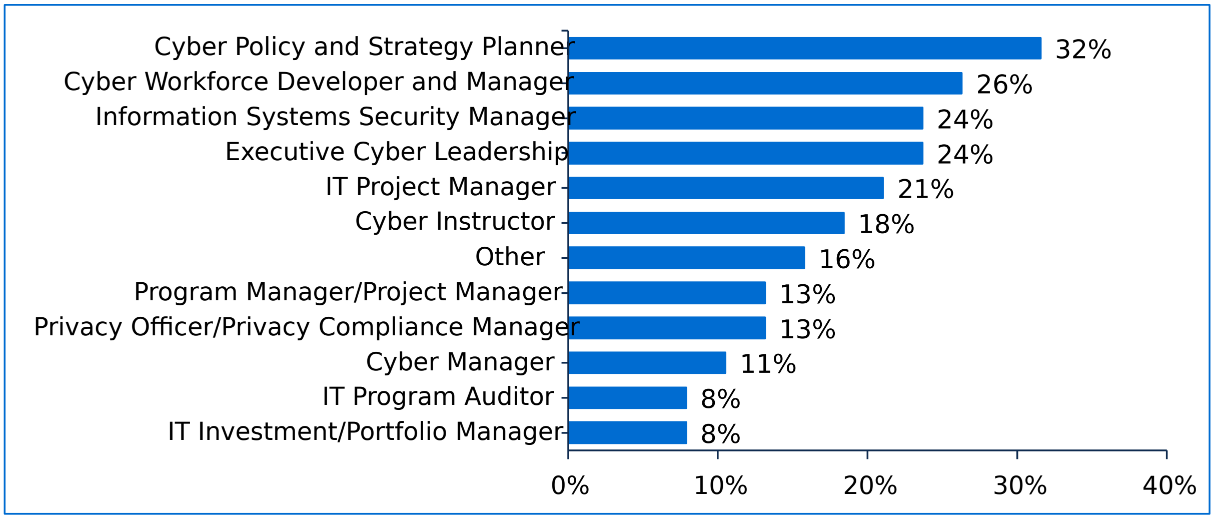


Figure 20. NICE Framework Work Roles (n = 38)

SURVEY ORGANIZATIONS

Organization Type

About **44%** of survey participants worked for a sub-component agency, about a third for an independent agency, and about a fourth for a department-level organization (Figure 20).

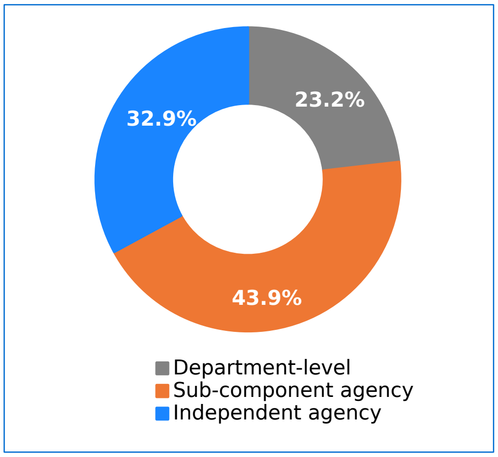


Figure 21. Type of organization (n = 82)

Organization Size

Participants worked in organizations of diverse sizes (Figure 21). Approximately **70%** of participants were from an organization with less than 10,000 employees.

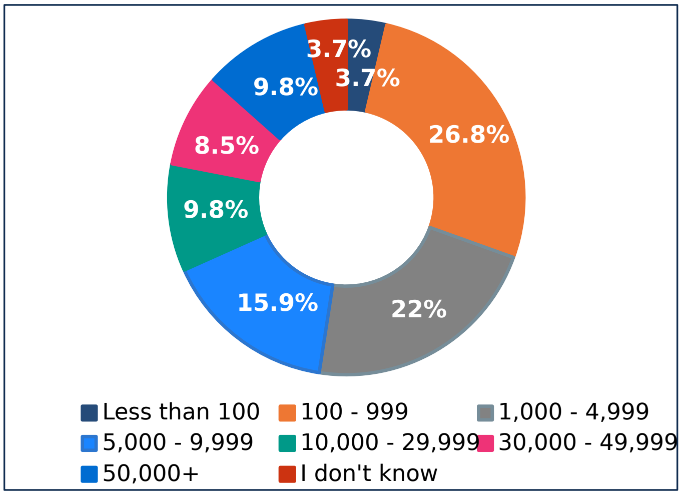


Figure 22. Organization size (n = 82)

ROLE-BASED TRAINING PROGRAMS

Number of Individuals Working on RBT Activities

About **50%** of participant organizations have just one to two team members responsible for RBT activities (Figure 22). Just over **28%** have more than six RBT team members. Note that team size does not necessarily equate to full-time equivalents (FTEs). An FTE is a unit of measurement indicating the workload of an employee, with 1.0 FTE being a full-time employee.

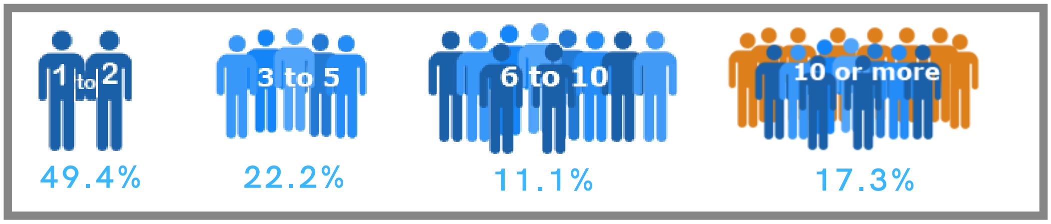


Figure 23. Number of RBT team members (n = 81)

Number of Employees Required to Take RBT

About half **(49.4%)** of survey participants estimated that less than 1,000 employees (both federal and contract) are required to take RBT within their organizations (Figure 23). About **6%** said that none of their employees were required to take RBT.

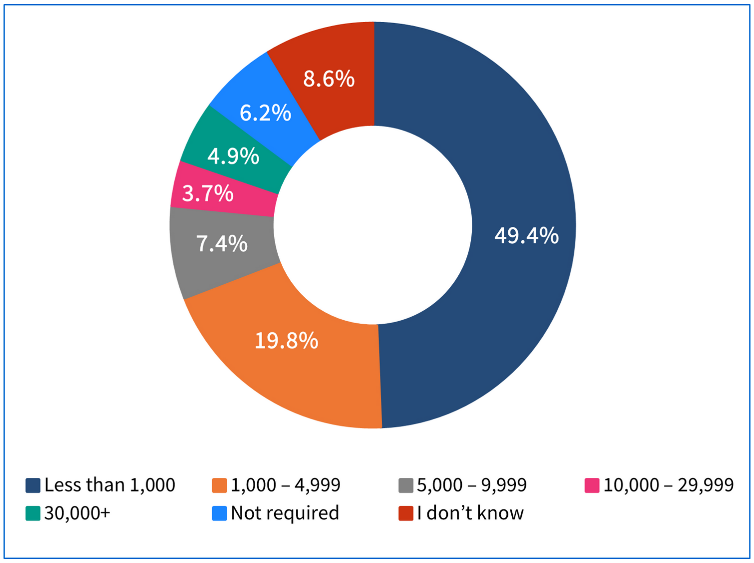


Figure 24. Number of employees required to take RBT (n = 81)

REFERENCES

[CISA2022] Cybersecurity & Infrastructure Security Agency (2022) Security and Awareness Training. Available at https://www.cisa.gov/security-and-awareness-training

[CLARK2019] Clark, VLP (2019) Meaningful integration within mixed methods studies: Identifying why, what, when, and how. Contemporary Educational Psychology 57(2019):106-111. Available at https://www.sciencedirect.com/science/article/pii/S0361476X19300128

[DHS2009] Department of Homeland Security (2009) A Roadmap for Cybersecurity Research. Available at https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap_0.pdf

[FISMA2014]Federal Information Security Modernization Act (P.L. 113-283), December 2014. Available at https://www.govinfo.gov/app/details/PLAW-113publ283

[FISSEA2022] National Institute of Standards and Technology (2022) FISSEA – Federal Information Security Educators. Available at https://csrc.nist.gov/projects/fissea

[FCPPF2022] National Institute of Standards and Technology (2022) Federal Cybersecurity and Privacy Professionals Forum. Available at https://csrc.nist.gov/projects/forum

[IR8420] Haney J, Jacobs J, Furman S, Barrientos F (2022) Federal Cybersecurity Awareness Programs: A Mixed Methods Research Study. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency/Internal Report (IR) 8420. Available at https://doi.org/10.6028/NIST.IR.8420

[IR8420A] Haney J, Jacobs J, Furman S, Barrientos F (2022) Approaches and Challenges of Federal Cybersecurity Awareness Programs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency/Internal Report (IR) 8420A. Available at https://doi.org/10.6028/NIST.IR.8420a

[IR8420B] Haney J, Jacobs J, Furman S, Barrientos F (2022) The Federal Cybersecurity Awareness Workforce: Professional Backgrounds, Knowledge, Skills, and Development Activities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency/ Internal Report (IR) 8420B. Available at https://doi.org/10.6028/NIST.IR.8420b

[KRUEGER2015] Krueger, RA, Casey, MA (2015). Focus Groups: A Practical Guide for Applied Research (Sage Publications), 5th Ed.

[SMAC2022] CIO.gov (2021) About the SACC and SMAC Councils. Available at https://www.cio.gov/about/members-and-leadership/SMACC/

[SP800-53] National Institute of Standards and Technology (2020). Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53 Revision 5. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[SP800-181] Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020). Workforce Framework for Cybersecurity (NICE Framework) (Rev. 1). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181 Revision 1. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

STUDY INSTRUMENTS

Focus Group Demographic Questionnaire

Note: All questions (except the first question) were optional and could be skipped by the participant. Participants had signed the informed consent before taking the survey.

1. What is your participant code? This was provided by the NIST research team in an email. _______

This first set of questions is about you and your professional background.

2. What is your job title? ___________________________

3. What is your role with respect to the security awareness program at your organization? Please check all that apply.
   - ☐ I am the government lead for the program
   - ☐ I am a member of the security awareness team, but not the lead
   - ☐ I oversee the contract for the program
   - ☐ I am a manager or executive who oversees the program administratively
   - ☐ Other: ____________________________

4. Aside from security awareness responsibilities, what other job functions/roles do you have within the organization?

   ____

5. How many years have you been involved with security awareness programs in your current organization or in other organizations? Include time spent working on security awareness training and managing/overseeing security awareness programs.

   o Less than 1 year
   o 1 - 5 years
   o 6 - 10 years
   o 11 - 15 years
   o 16 - 20 years
   o More than 20 years

6. Approximately what percentage of your time at work do you spend on tasks related to the security awareness program?

   o Full-time
   o 75%
   o 50%
   o 25%
   o 10%
   o Less than 10%
   o Other: ____________

7. How many years have you been a federal employee?

   o Less than 1 year
   o 1 – 5 years
   o 6 – 10 years
   o 11 – 15 years
   o 16 – 20 years
   o More than 20 years

8. How many years did you spend as a contractor supporting the federal government?
o None
o Less than 1 year
o 1 – 5 years
o 6 – 10 years
o 11 – 15 years
o 16 – 20 years
o More than 20 years

9. How many years have you worked at your current organization (including years as a contractor)?
o Less than 1 year
o 1 – 5 years
o 6 – 10 years
o 11 – 15 years
o 16 – 20 years
o More than 20 years

10. How many years have you worked in some kind of cybersecurity role?
o Less than 1 year
o 1 – 5 years
o 6 – 10 years
o 11 – 15 years
o 16 – 20 years
o More than 20 years

11. Please list any security certifications you have earned: ____________

12. What is your age range?
o 18 – 29
o 30 – 39
o 40 – 49
o 50 – 59
o 60+

13. What is your highest level of education?
o Less than high school degree
o High school degree or equivalent
o Some college
o Associate degree
o Bachelor’s degree
o Master’s degree
o Doctoral or Juris Doctoral degree
o Other: _____________

14. If you have any degrees beyond a high school degree, in which disciplines/fields are your degrees?
____

15. What is your gender?
o Female
o Male
o Other
o Prefer not to answer

This next set of questions is about your organization and security awareness program.

16. Approximately how many federal employees work in your organization? ______________________________

17. Approximately how many people within the organization are covered by your security awareness program? Include federal employees and contractors as applicable.

    ____

18. Which of the following describes your security awareness program?
    o Handled all in-house by federal employees
    o Mix of federal employees and contractors working on-site
    o All contractors working on-site
    o Outsourced completely to an external company working off-site
    o Other: _________________

19. Where is the placement of the security awareness program within the organization (for example, in the CIO's office)?

    ____

20. How many federal employees within your organization have at least some day-to-day security awareness responsibilities? Do not include managers who only oversee the program administratively. ____________

21. How many contractors within your organization have at least some day-to-day security awareness responsibilities?

    ____

22. Approximately how many total full-time equivalents are allocated to security awareness responsibilities? Include federal employees and contractors. ______________

23. What is the approximate budget allocated towards security awareness in your organization?

    ____

24. Please enter any additional information you feel is necessary to clarify any of your responses.

    ____

Focus Group Instrument

1. Please tell us your name, organization, and your role with respect to security awareness. [This question was not audio-recorded. Participants could decide what they wanted to share.]

2. When I say "security awareness and training," what does that mean to you? What comes to mind?

3. Tell me about your organization's approach to security awareness and training.

4. How do you decide what topics and approaches to use for your security awareness program?
   a. [Probe for sub-components:] What kind of guidance/direction, if any, does your department provide? How much leeway do you have to tailor the training to your own organization?
   b. [Probe for department-level agencies:] What kind of guidance/direction, if any, do you push down to sub-components within your department?

5. What's working well with your program?

6. What's not working as well? What are your challenges and concerns with respect to security awareness in your organization?

7. How do you determine the effectiveness of your program, if at all?

8. If you could have anything or do anything for your security awareness program, what would that be?
   a. [Probe:] What would you do to solve the challenges you currently experience?
   b. [Probe:] What kinds and formats of resources and information sharing would be most beneficial?

9. What knowledge, skills, or competencies do you think are needed for those performing security awareness functions in your organization?

10. If you had one or two pieces of advice for someone just starting a security awareness program in an agency like yours, what would that advice be?

11. Is there anything else that we should have talked about, but didn't?

Survey Instrument

Screener

1. To be eligible to complete this survey you must be a federal employee. Please indicate if you are a federal employee.
   o Yes, I am a federal employee
   o No, I am not a federal employee

2. Do you have responsibilities for implementing cybersecurity role-based training activities in your organization or are you a manager or executive who oversees the role-based \ training activities in your organization?
   o Yes
   o No
   [if no to 1. – provide a "thank you, but you're not eligible to participate" screen]
   [if no to 2. – provide a "thank you, but you're not eligible to participate" screen]

For the purposes of the survey:
The term *organization* refers to your federal agency.

The term *employees* refers to both federal employees working for your organization and contractors (non-federal individuals) supporting your organization unless explicitly categorized as one or the other (i.e., "federal employees" or "contractor employees").

The term *security* will be used as a shorthand for "cybersecurity" or "information security." Reference to physical security or personnel security is different and will be labeled as such.

Role-based training activities provide security and privacy information to organizational employees who have significant security responsibilities. This type of training is not to be confused with security or privacy awareness activities that involve security/privacy information targeted at the general workforce within the organization.

Examples of role-based training include, but are not limited to:

- Training on specific tools required for employees to perform security-related job duties
- Training for employees who have privileged access to applications or systems
- Training for oversight roles such as information systems security officer (ISSO), information systems security manager (ISSM), or auditors
- Training for employees who manage access and authorizations to applications and systems
- Training on organizational policies and procedures related to security and privacy configurations, settings, controls, etc.
- Cybersecurity for employees in leadership positions, such as "Cybersecurity for Executives," Cybersecurity for System Owners," or "Becoming A Chief Information System Officer"

Examples of types of training that are NOT role-based include, but are not limited to:

- General-user annual security or privacy awareness training
- Leadership or management training not related to security
- Coding/software development classes
- Organizational orientation and onboarding briefings
- Training on tools not having a security purpose

As a reminder, in order to maintain anonymity, when responding to open-ended questions, please do not include any information that might identify you or your organization. However, should you accidentally include such information, the researchers will redact it from the research record.

Information about You
In this first section, we'll ask you about your job and professional background.

3. Which of the following best matches your official position title?
   o Chief Information Officer (CIO)
   o Chief Information Security Officer (CISO)
   o Computer Scientist
   o IT Specialist (Cybersecurity/INFOSEC)
   o IT Specialist – Other
   o Program/Project Manager
   o Supervisory Computer Scientist
   o Supervisory IT Specialist (Cybersecurity/INFOSEC)
   o Supervisory IT Specialist – Other
   o Training Specialist
   o Other: ____________________

4. Has your organization assigned you to one or more NICE (National Initiative for Cybersecurity Education) Framework cybersecurity work roles?
   o Yes
   o No
   o I don't know

   4A. <if yes> Which of the following NICE Framework cybersecurity work roles have you been assigned? Check all that apply.
   ☐ Cyber Instructional Curriculum Developer
   ☐ Cyber Instructor
   ☐ Cyber Policy and Strategy Planner
   ☐ Cyber Workforce Developer and Manager
   ☐ Executive Cyber Leadership
   ☐ Information Systems Security Manager
   ☐ IT Investment/Portfolio Manager
   ☐ IT Program Auditor
   ☐ IT Project Manager
   ☐ Privacy Officer/Privacy Compliance Manager
   ☐ Program Manager
   ☐ Other: ________________________________

5.What is your role with respect to role-based training activities? Check all that apply.
   ☐ I am the government lead for the activities
   ☐ I am a member of the role-based training team but not the lead
   ☐ I oversee the contract for the activities
   ☐ I am a manager or executive who oversees the activities administratively
   ☐ Other: _________________________

6. How long have you been involved with role-based training activities in your current organization and in other organizations (rounded to the nearest year)? Include time spent working on role-based training and managing/overseeing role-based training activities.
   o Less than 1 year
   o 1 – 5 years
   o 6 – 10 years
   o 11 – 15 years
   o 16 – 20 years
   o More than 20 years

Information about Your Organization

7. In which type of organization do you work?
   - o Department-level - for example, Department of Commerce or Department of Transportation
   - o Sub-component agency or bureau that is under a Department. For example, NIST is a sub-component under Department of Commerce and FAA is a sub-component under Department of Transportation
   - o Independent agency
   - o I don't know

8. Approximately how many federal employees work in your organization? If working at the department level, please do not include employees working in any sub-component agencies under the department.
   - o Less than 100
   - o 100 – 999
   - o 1,000 – 4999
   - o 5,000 – 9,999
   - o 10,000 – 29,999
   - o 30,000 – 49,999
   - o 50,000+
   - o I don't know

Information about Your Role-based Training Activities

9. How many individuals (federal employees and contractor employees) have responsibilities for implementing role-based training activities in your organization? Do not include managers who only oversee the activities administratively or employees who just take the training.
   - o 1-2
   - o 3-5
   - o 6-10
   - o More than 10

10. Approximately how many employees within your organization (federal employees and contractor employees) are required to take role-based training? If working at the department level, only include employees in sub-component agencies if the sub-components do not have role-based training activities of their own.
    - o No employees are required to take role-based training
    - o Less than 1,000
    - o 1,000 – 4,999
    - o 5,000 – 9,999
    - o 10,000 – 29,999
    - o 30,000+
    - o I don't know

11. How does your organization identify which employees take role-based training? Check all that apply.
    - ☐ We use the cybersecurity work roles described in NIST Special Publication 800-181 "Workforce Framework for Cybersecurity (NICE Framework)"
    - ☐ The Human Resources/Human Capital office makes the decision on which work roles must take the training
    - ☐ The office of the Chief Information Officer or Chief Information Security Officer makes the decision on which work roles must take the training
    - ☐ The office of the Chief Legal Officer makes the decision on which work roles must take the training
    - ☐ Individual supervisors decide if their employees must take the training
    - ☐ I don't know
    - ☐ Other: ________________________

12.How does your organization track role-based training completion? Check all that apply.

☐ Customized online application that links employees to training
☐ Department-wide Learning Management System (LMS)
☐ Local or sub-component Learning Management System (LMS)
☐ Spreadsheet or other manual method
☐ We don't track role-based training completion
☐ Other: ________________________
☐ I don't know

13. In what ways can employees complete their role-based training? Check all that apply.

☐ Online course
☐ Live (in-person or virtual) training event held by my organization
☐ Live (in-person or virtual) training event held by other organizations
☐ Industry-recognized certifications
☐ Other: __________________

14. What happens to employees who do not complete role-based training required to perform their duties by t the deadline provided? Check all that apply.

☐ We do not require role-based training.
☐ They receive an email reminder.
☐ Their supervisor is contacted.
☐ Their account is disabled/suspended.
☐ Their network access is disabled/suspended.
☐ Their annual performance rating is negatively impacted.
☐ Nothing
☐ Other: _____________

15. How does your organization obtain role-based training materials or content? Check all that apply.

☐ Create within the organization
☐ Purchase from another organization/vendor
☐ Obtain from the Department (if you are a sub-component)
☐ Obtain at no cost from another organization/vendor
☐ Other: ______________________________

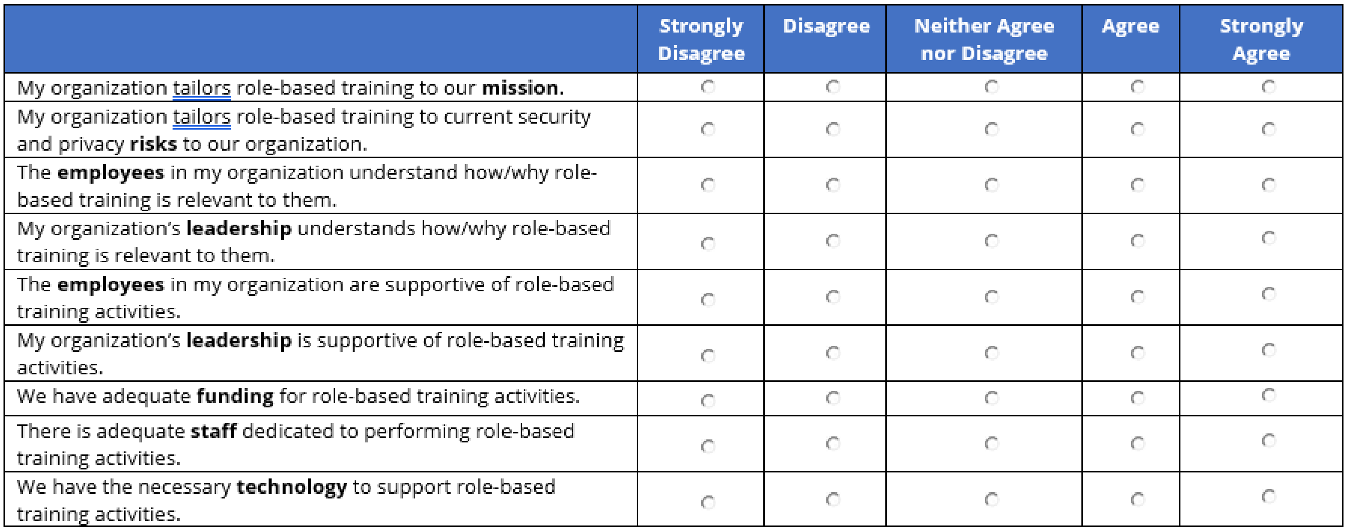
16. How often is role-based training content updated?

o More often than once a year
o Every year
o Every 2 – 3 years
o More than every 3 years
o I don't know

17. How does your organization determine or measure the effectiveness of your role-based training activities? Check all that apply.

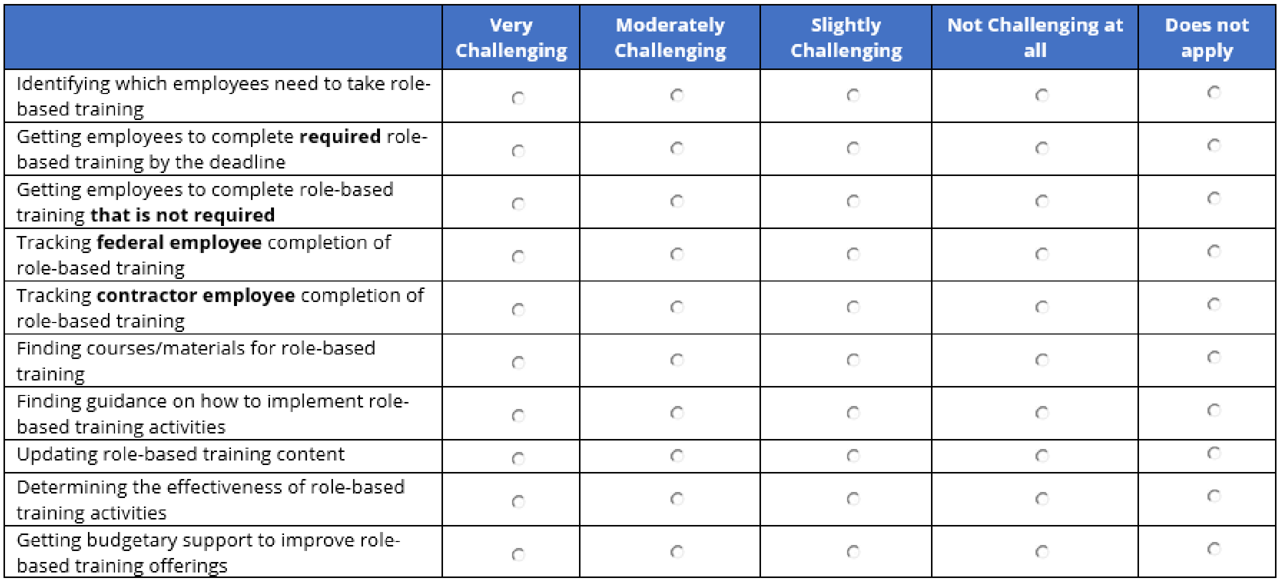
☐ Training completion rates
☐ Audit reports or FISMA (Federal Information Security Modernization Act of 2014) evaluations
☐ Surveys completed by employees
☐ Informal employee feedback/comments (for example, in-person, emails)
☐ Attendance at role-based training events
☐ Online views of training materials
☐ Demonstrations of employees applying what they learned (e.g., security incident trends, incident reporting)
☐ We don't measure the effectiveness
☐ Other: ________________________

18. Please indicate your level of agreement with each of the following statements



	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
My organization tailors role-based training to our **mission.**	○	○	○	○	○
My organization tailors role-based training to current security and privacy **risks** to our organization.	○	○	○	○	○
The **employees** in my organization understand how/why role-based training is relevant to them.	○	○	○	○	○
My organization's **leadership** understands how/why role-based training is relevant to them.	○	○	○	○	○
The **employees** in my organization are supportive of role-based training activities.	○	○	○	○	○
My organization's **leadership** is supportive of role-based training activities.	○	○	○	○	○
We have adequate **funding** for role-based training activities.	○	○	○	○	○
There is adequate **staff** dedicated to performing role-based training activities.	○	○	○	○	○
We have the necessary **technology** to support role-based training activities.	○	○	○	○	○

19. Please rank the level of challenge your role-based training program encounters with the following:



	Very Challenging	Moderately Challenging	Slightly Challenging	Not Challenging at all	Does not apply
Identifying which employees need to take role-based training	○	○	○	○	○
Getting employees to complete **required** role-based training by the deadline	○	○	○	○	○
Getting employees to complete role-based training **that is not required**	○	○	○	○	○
Tracking **federal employee** completion of role-based training	○	○	○	○	○
Tracking **contractor employee** completion of role-based training	○	○	○	○	○
Finding courses/materials for role-based training	○	○	○	○	○
Finding guidance on how to implement role-based training activities	○	○	○	○	○
Updating role-based training content	○	○	○	○	○
Determining the effectiveness of role-based training activities	○	○	○	○	○
Getting budgetary support to improve role-based training offerings	○	○	○	○	○

20. Please describe any other challenges your organization faces with respect to role-based training: <open-ended text box>

21.In your opinion, how successful are your role-based training activities overall?

- o Very unsuccessful
- o Unsuccessful
- o Slightly successful
- o Moderately successful
- o Very successful

22. What are the most successful aspects of your role-based training activities? <open-ended text box>

23. What could help your organization's role-based training efforts be more successful? <open-ended text box>

24.. What are the most important pieces of advice or lessons learned you might pass on to someone just starting a role-based training effort in an organization like yours? <open-ended text box>

25. Please provide any additional information related to your organization's experiences with role-based training that you would like to share with us. <open-ended text box>

CONTACT US:

https://csrc.nist.gov/projects/usable-cybersecurity

usability@nist.gov