NIST Cybersecurity Role-Based Training Study

Jody Jacobs, Julie Haney, and Susanne Furman
National Institute of Standards and Technology
May 2022

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

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Study Overview

Purpose: To better understand the needs, challenges, and approaches of federal cybersecurity role-based training (RBT) activities

Focus Groups

8 focus groups of feds **(n=29)** working in departments, sub-component agencies in departments, and independent agencies

Online, Anonymous Survey

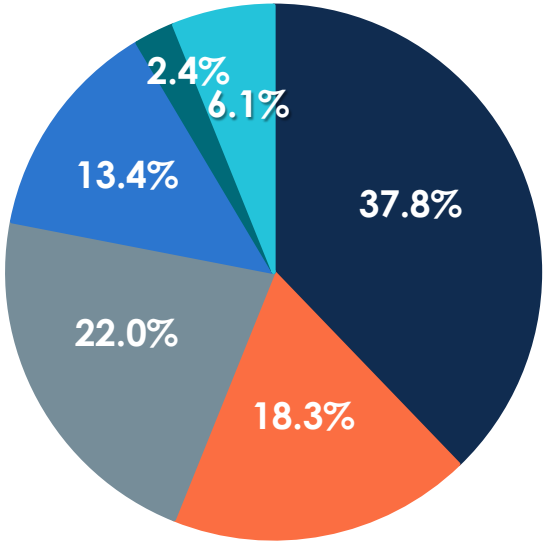
Survey of a broader population **(n=82)** of feds who are responsible for implementing or overseeing RBT activities

Study results are informing the revision of NIST SP 800-50 and 800-16 and can serve as a resource for those implementing or overseeing RBT activities.

Who took the survey

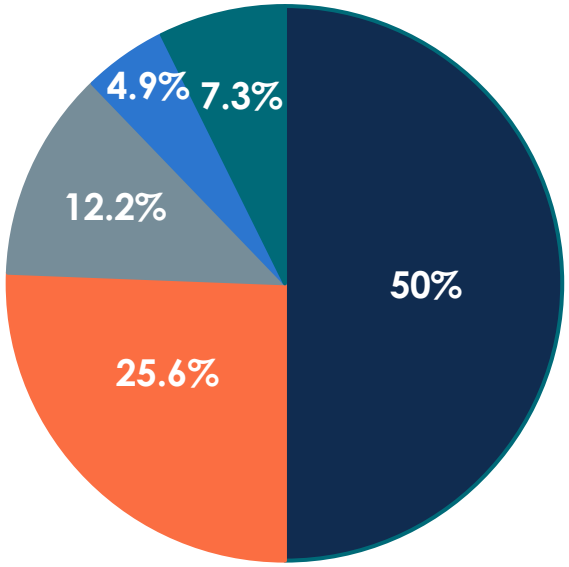
RBT Involvement

RBT Roles



- Lead only
- Team member only
- Manager only
- Lead and manager
- Team member and manager
- Other

% of Time Spent on RBT

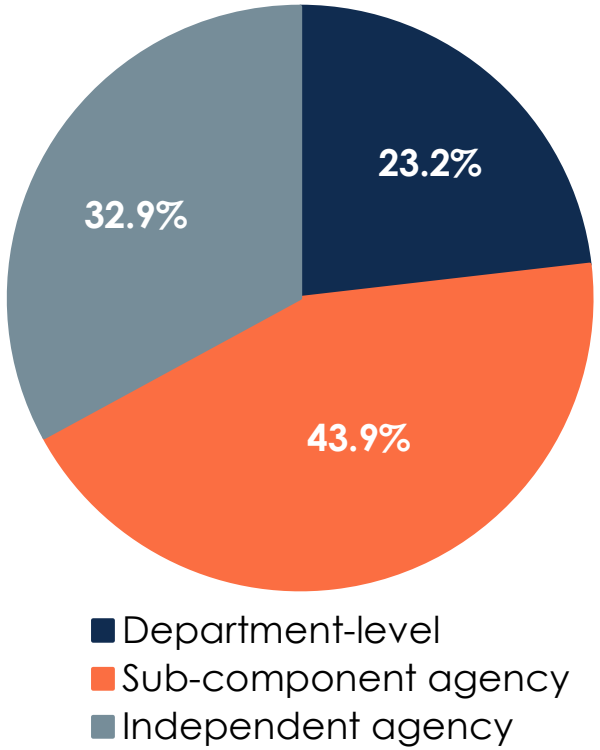


- Less than 25%
- 25%
- 50%
- 75%
- Full-time

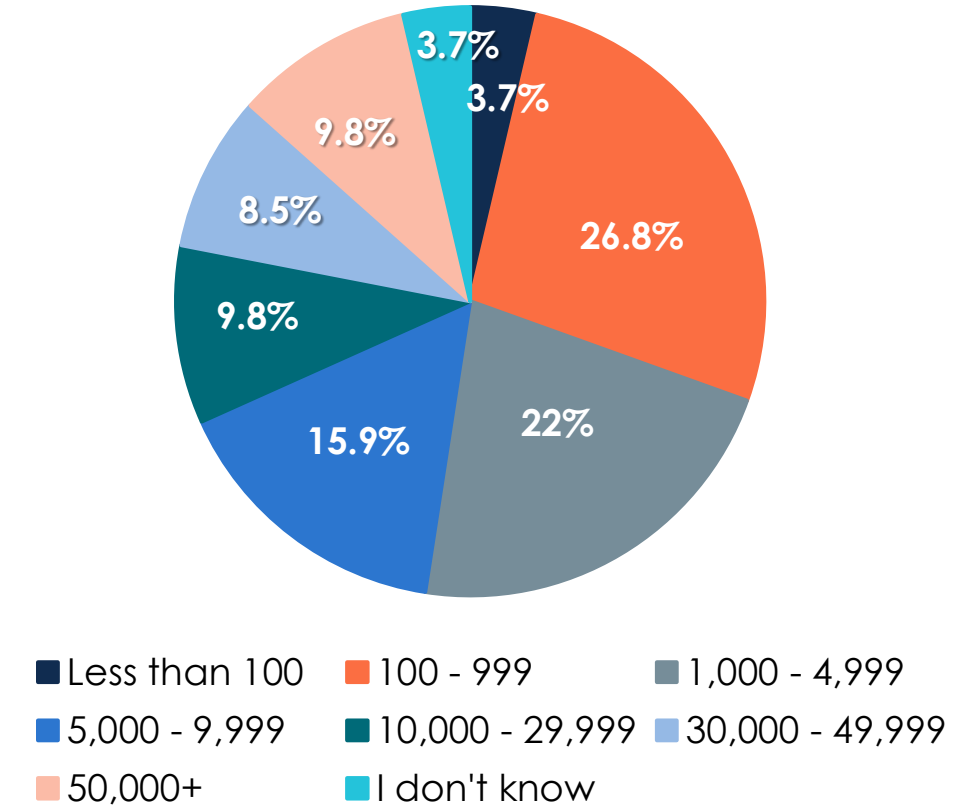
60% had more than 5 years of experience with RBT

Represented Organizations

Organization Type

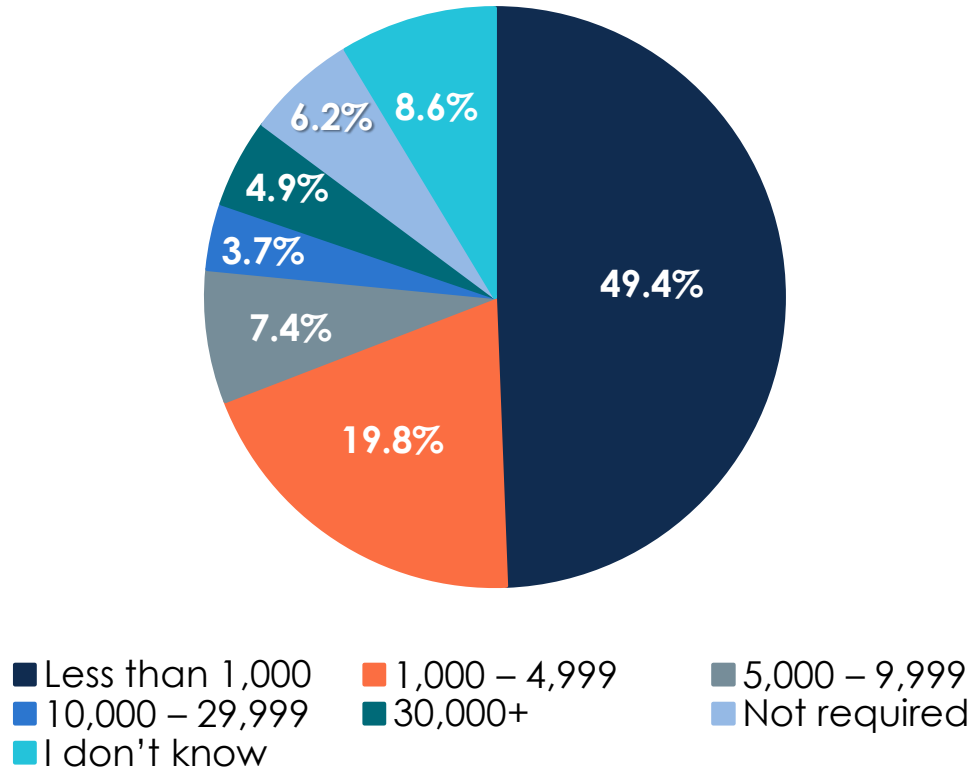


Organization Size (# federal employees)

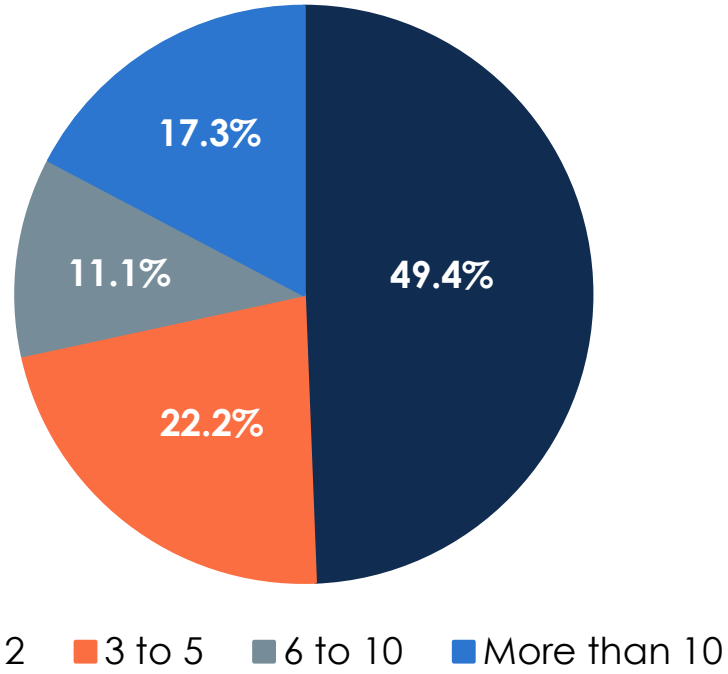


Represented RBT Activities

Employees Required to Take RBT

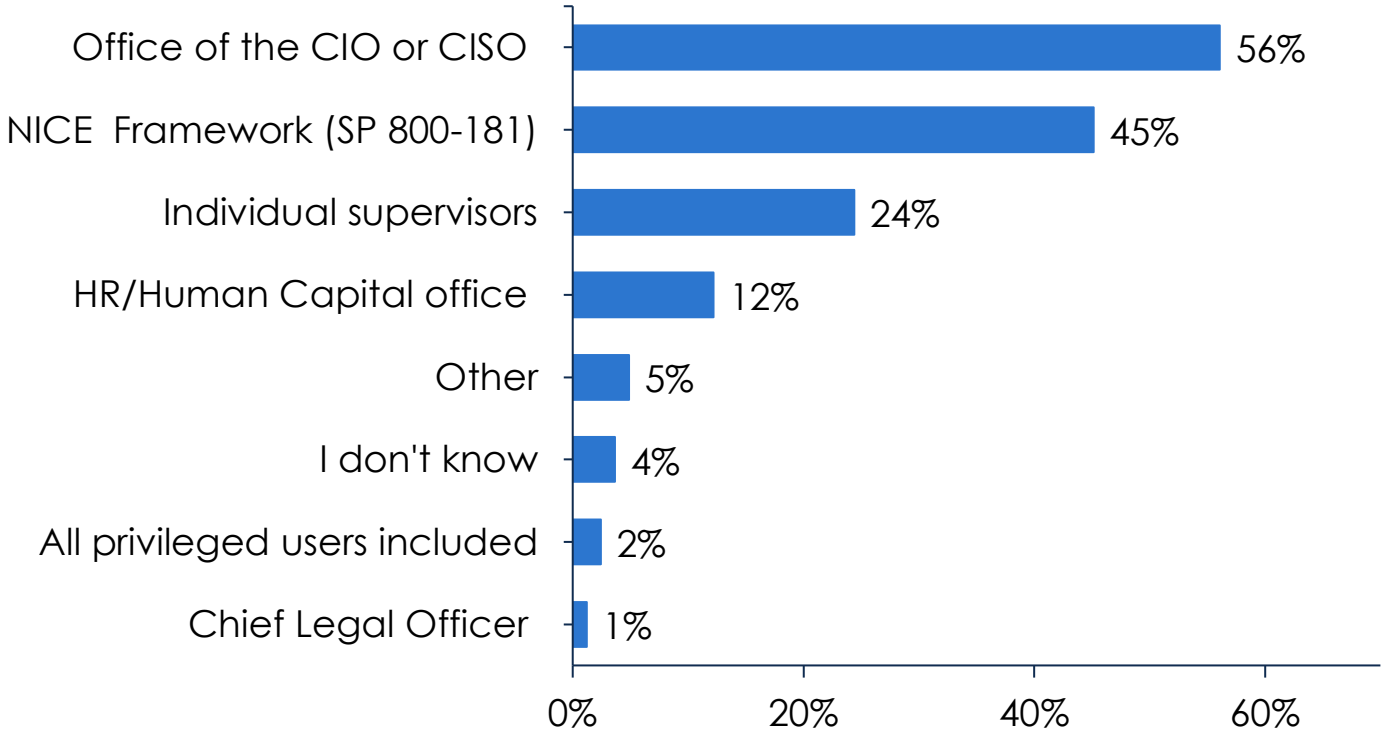


RBT Team Size



What we found

RBT Assignment Responsibility

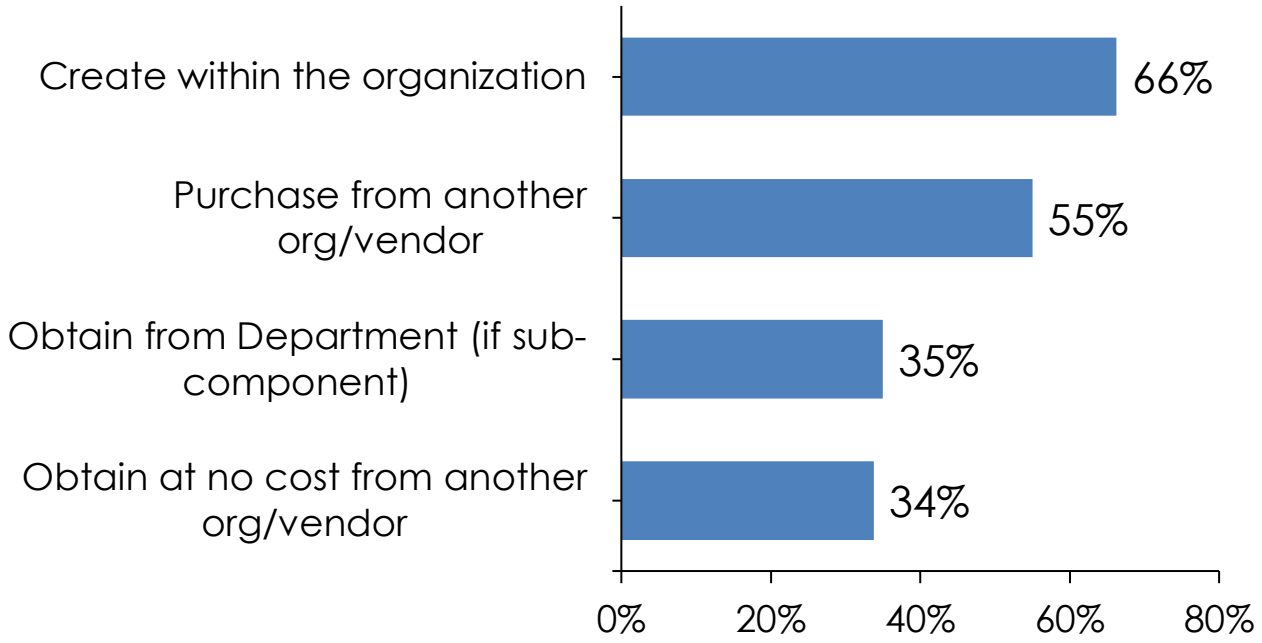


How organizations determine which employees take RBT (select all that apply)

26%: Identifying which employees need to take RBT is moderately/very challenging

"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 framework and automatically assign role-based trainings to the users." (Q53)

RBT Content, Materials, and Guidance



How organizations obtain RBT content (select all that apply)

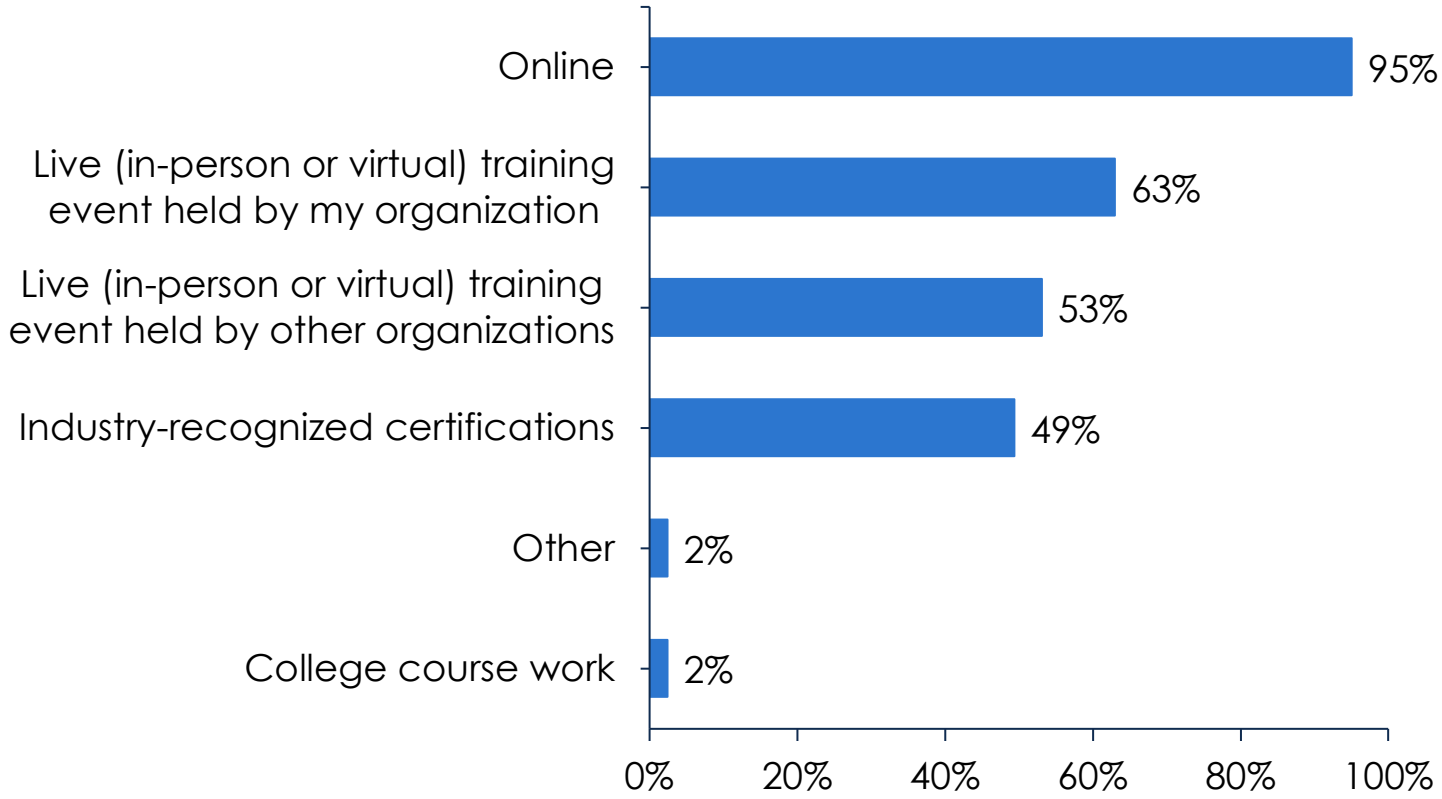
44%: Finding RBT **content** is moderately/very challenging

34%: Finding RBT **guidance** is moderately/very challenging

Strong desire to have **standard training** available to all feds

"Why does each agency need to develop their own role-based training? Much efficiency could be achieved through centralizing aspects of this." (Q53)

RBT Methods and Formats



How employees can complete RBT (select all that apply)

68% indicated that their organization allows more than one way to complete RBT.

Some organizations allow for employee choice.

"We allow things like any type of event that's at least one hour in length that is cyber related and also applicable to their specific job duties." (S05)

Tailoring RBT Content

54%: Agreed/strongly agreed that their organization tailors RBT to the **mission**.

58%: Agreed/strongly agreed that their organization tailors RBT to current **security risks**.

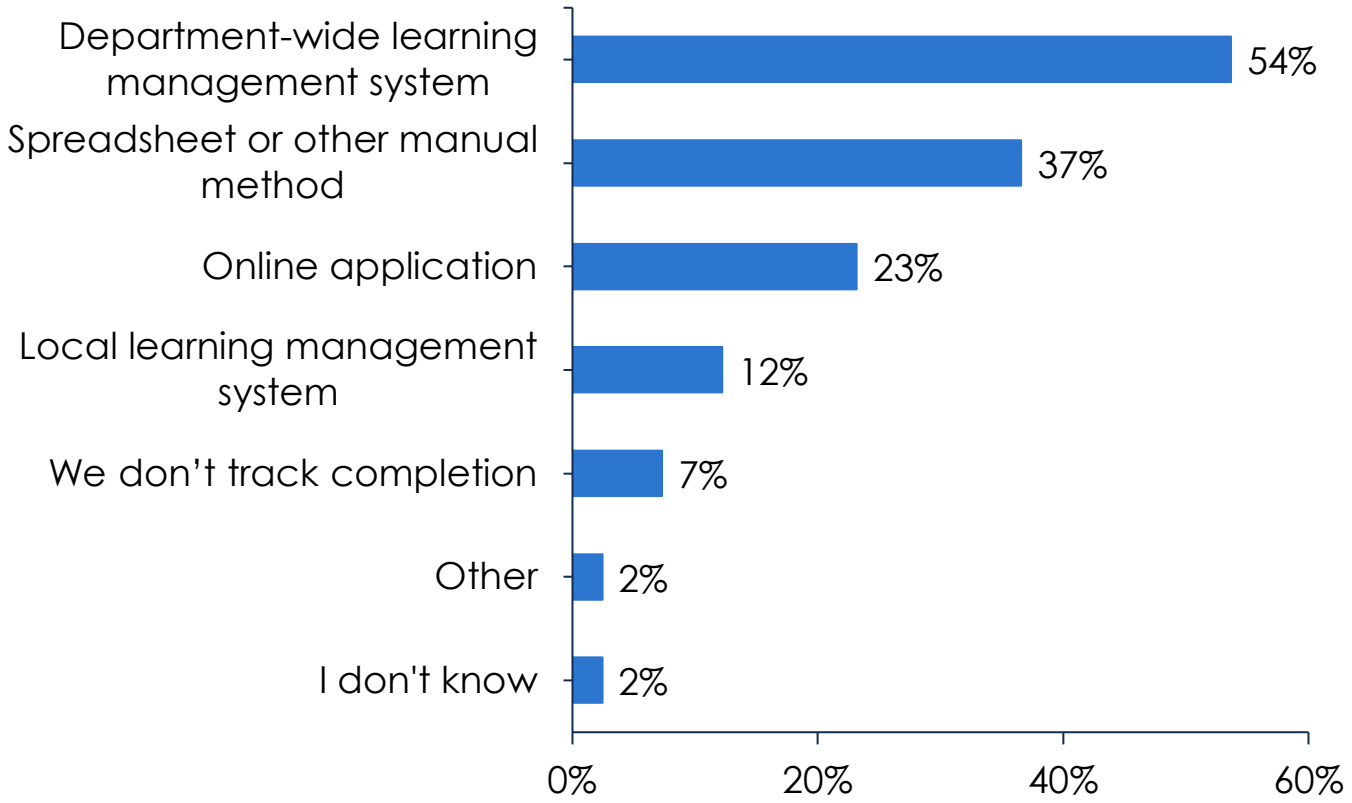
Successes:

"[We bring] ISSOs together to gather the most issues they see so that we could include those issues in the training." (Q30)

Challenges:

"Approach to role-based training is overly tactical, focusing on IT-specific elements (e.g., patching) rather than developing and managing processes that reliably improve cybersecurity outcomes." (Q23)

RBT Completion Tracking



How orgs track RBT completion (select all that apply)

19%: Tracking federal employee RBT completion is moderately/ very challenging

29%: Tracking contractor RBT completion is moderately/very challenging

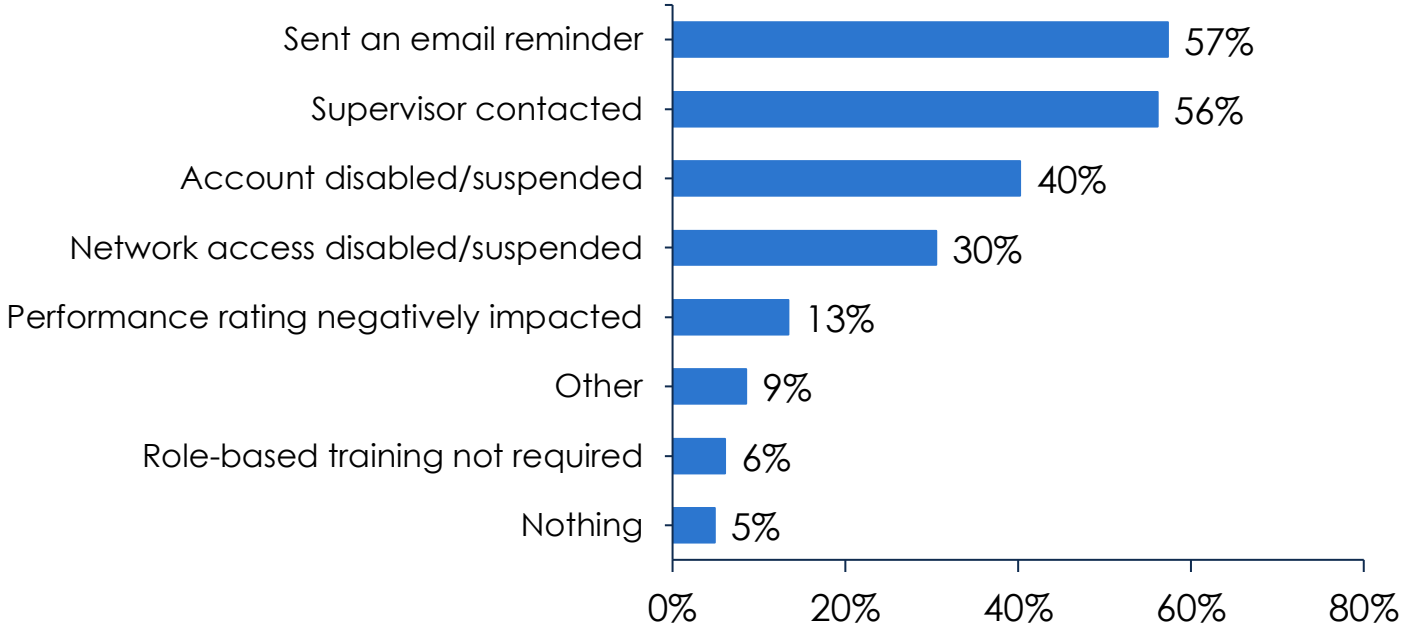
"We've explored self-paced training options, but ensuring compliance and tracking completion is challenging there." (Q72)

Employees Training Compliance

40%: Getting employees to complete **required** RBT is moderately/very challenging

42%: Getting employees to complete RBT that is **not required** is moderately/very challenging

"There is no time. There are too many duties for the few cyber employees. Training and hands-on always fall to the wayside." (Q59)



What happens if employees fail to complete required RBT (select all that apply)

Workforce Support

65% said *employees* and 70% said *leadership* understand how/why RBT is **relevant** to them.

66% said *employees* and 73% said *leadership* are **supportive** of RBT activities.

Several expressed challenges:

"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)

"RBT is not taken seriously by the IT department and leadership at the CIO and above…I have submitted budget requests to improve the program and put comprehensive metrics in place, but they have been denied." (Q29)

RBT Resources

42%: Disagreed/strongly disagreed that they have adequate **funding**

52%: Disagreed/strongly disagreed that they have adequate dedicated **staff**

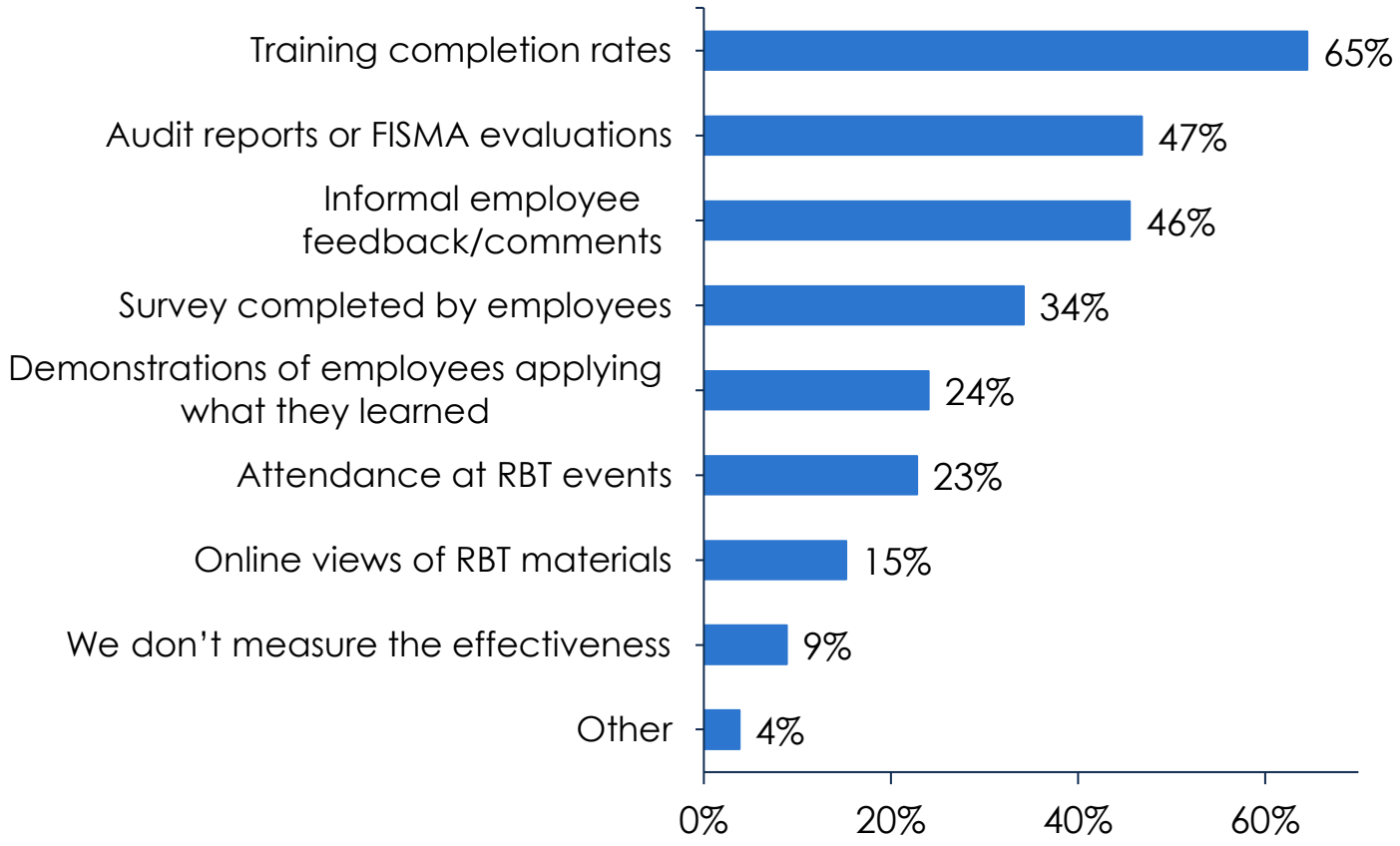
28%: Disagreed/strongly disagreed that they have adequate **technology**

48%: **Getting budgetary support** to improve RBT offerings is moderately/very challenging

"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)

"Our Agency has 0 dedicated funding and 0 dedicated administrative or human capital resources for role-based training." (Q49)

Measuring Effectiveness of RBT Activities



Measures of RBT effectiveness (select all that apply)

58%: Determining the effectiveness of RBT activities is moderately/very challenging

"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 and if there was modular project that could be used to show the benefits of learning." (Q24)

Perceived Success of RBT Activities

52%: RBT activities are successful/very successful

- 77% in security awareness survey

28%: RBT activities are slightly successful

- 19% in security awareness survey

20%: RBT activities are unsuccessful/very unsuccessful

- 4% in security awareness survey

"[Employees] like the core training we provide and are always asking for follow-up training and refresher courses." (Q75)

"Irrelevant training, and users does not feel motivated in any ways." (Q02)

Advice from the field

The Big Picture

Plan a robust program from the onset	"Get your policies and procedures straight first. Make your processes repeatable and simple." (Q17) "Create a program plan that describes the mission, vision, and a phased implementation approach, including a continuous learning cycle." (Q52)
Obtain support and prioritize resources	"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) "Create the metrics to showcase success." (Q52) "Prioritize the resources available to meet the critical training gaps." (Q52)
Assign RBT appropriately	"Define based on job roles, not job series." (Q16) "Clearly communicate WHY an individual is assigned role-based training requirement." (Q33)

Content and Approaches

Seek out existing and updated training	"Identify existing training resources…There are many free and paid training content available online." (Q52) "Stale training is often worse than no training…Security evolves daily, and the training should reflect this." (Q23)
Tailor RBT to the organization and workforce	"Make the curriculum pertinent to the types of issues your support staff and others have actually had to deal with and solve." (Q70) "Listen to the business units regarding what they need." (Q75)
Be flexible	"Permit ability to assess-out for those having maturity in role." (Q22) "Do not require all mandatory courses due at the same time." (Q60)

Thank you!

Jody Jacobs: jody.jacobs@nist.gov
Julie Haney: julie.haney@nist.gov
Susanne Furman: susanne.furman@nist.gov
Group Mailbox: usability@nist.gov

NIST Usable Cybersecurity Program:
https://csrc.nist.gov/usable-cybersecurity

NIST Cybersecurity Awareness Study reports:
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8420.pdf
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8420A.pdf
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8420B.pdf