NIST Security Awareness Study

Julie Haney, Jody Jacobs, and Susanne Furman
National Institute of Standards and Technology
September 2021

NIST 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.

Problem

Organizational security awareness programs face numerous challenges.

- May lack tools, resources, and appropriate competencies to effectively manage and execute programs
- May be compliance (vs. impact) focused

Unclear if these challenges apply to U.S. Government programs

Study Overview

Purpose: To better understand the needs, challenges, practices, and competencies of federal security awareness professionals and programs

Focus Groups

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

Online, Anonymous Survey

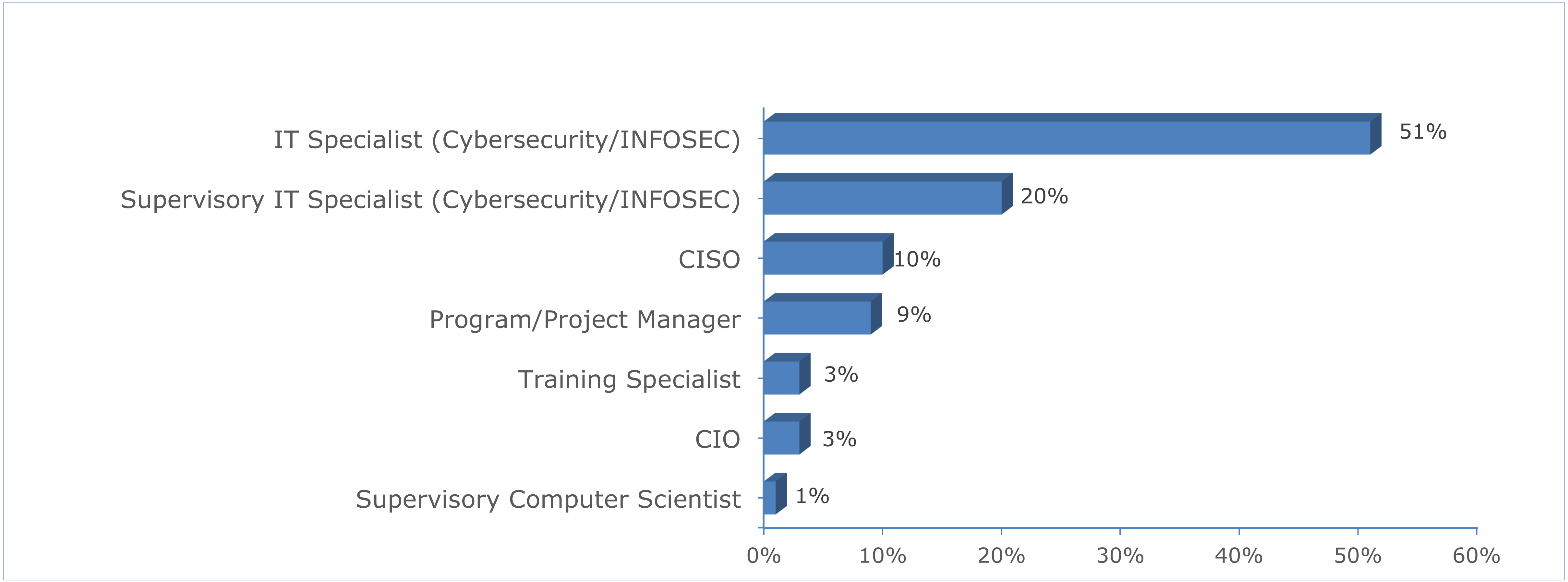
Survey of a broader population **(n=96)** of federal security awareness professionals

Study Participants and Organizations

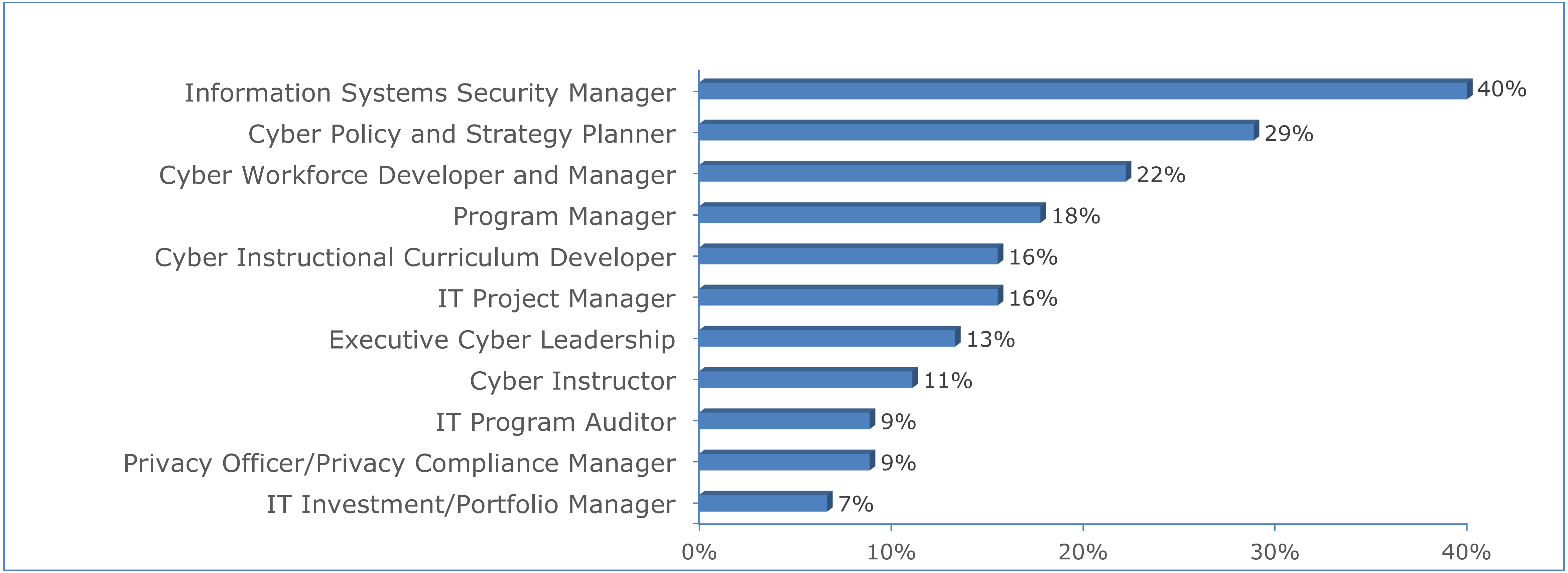
Security Awareness Involvement

	Focus Groups	Survey
Security awareness role	◘ **76%** program leads 10% program team members 14% managers/CISOs	◘ **45%** program leads 36% program team members 21% managers/execs (~52% leads)
% of time on security awareness	◘ **93%** are part-time 38% <= ¼ of their time	◘ **90%** are part-time 56% <= ¼ of their time
Security awareness experience	◘ **69%** with > 5 years **all** with > 1 year	◘ 74% with > 5 years **99%** > 1 year

Job Classifications (survey)



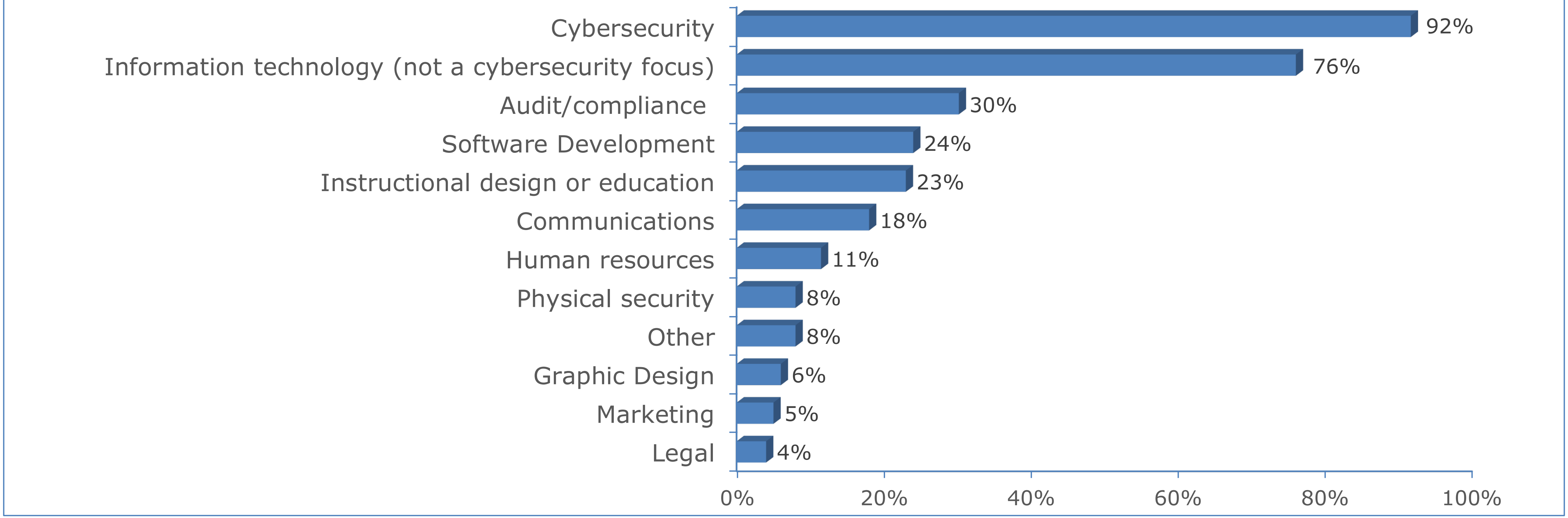
NICE Framework Work Roles (survey)



Discipline Diversity

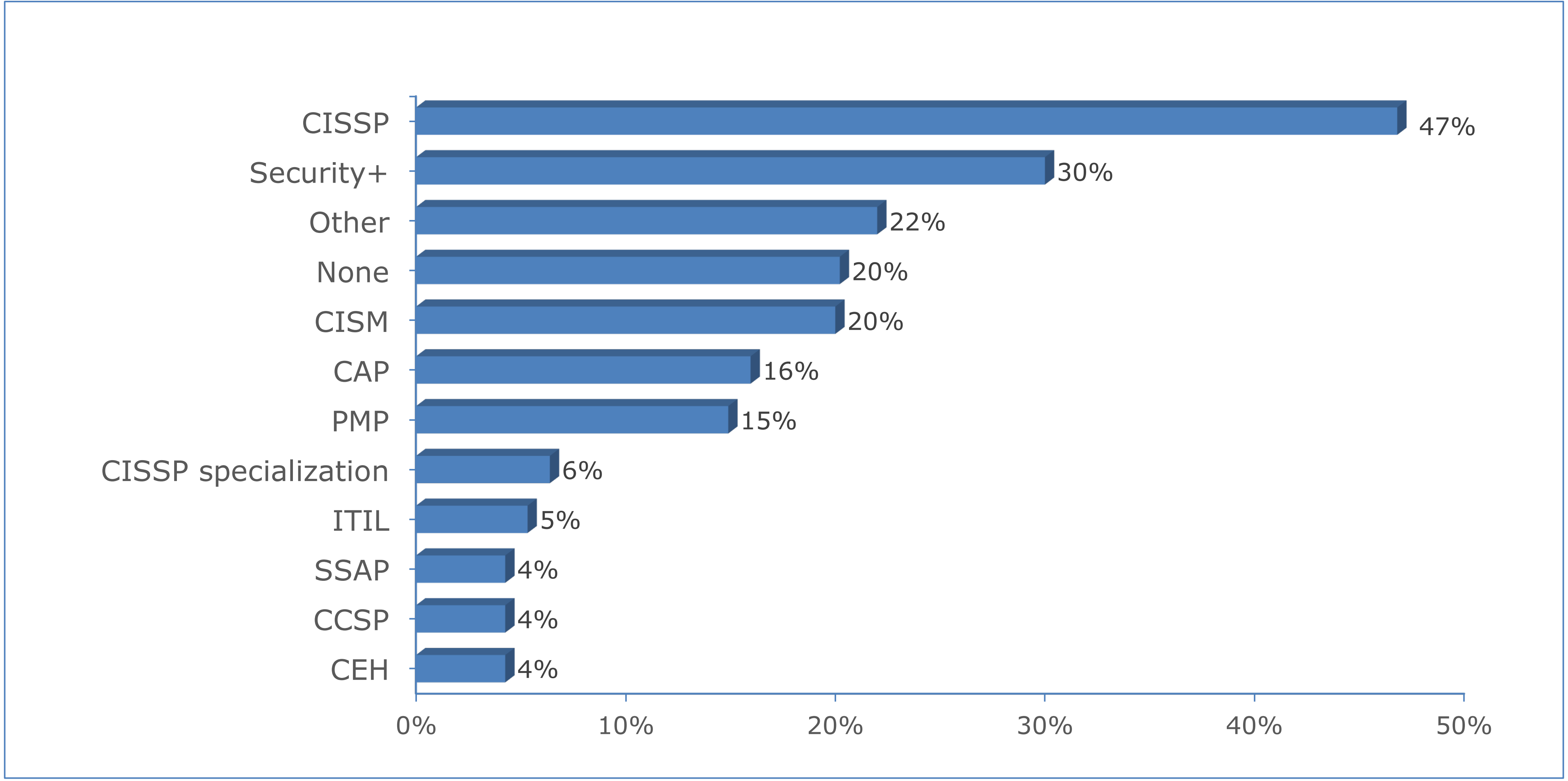
83% of ***focus group*** and **68%** of ***survey*** participants had at least one non-computing degree

Fields Worked in Professionally (survey)



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

Industry-recognized Certifications (survey)

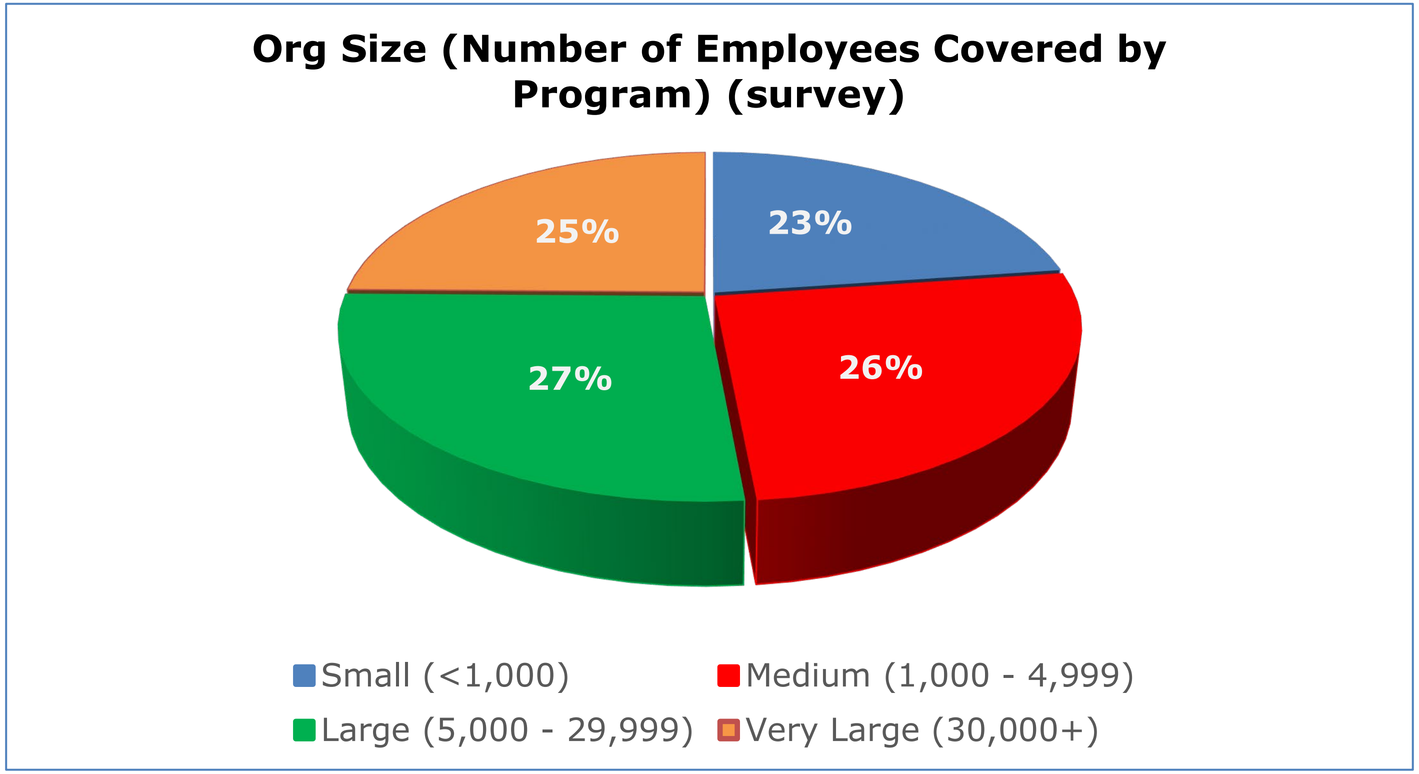


National Institute of Standards and Technology
U.S. Department of Commerce

Represented Organizations

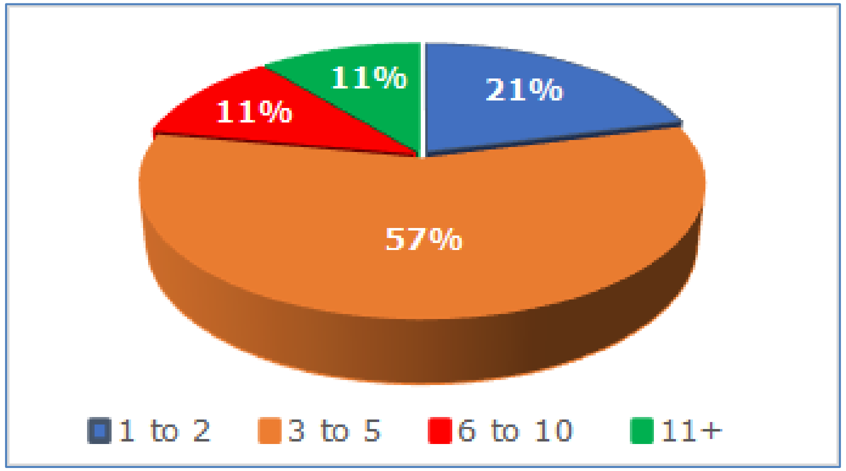
Focus Groups: ~21% from departments
38% sub-components
41% independents

Survey: ~32% departments
31% sub-components
35% independents

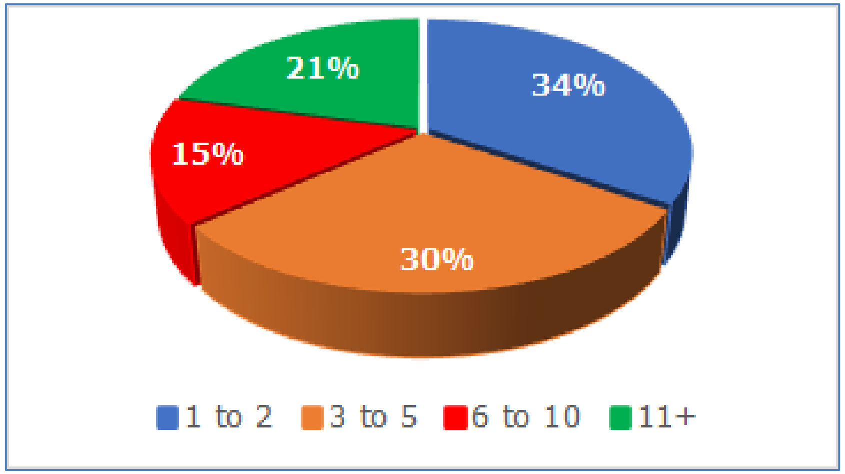


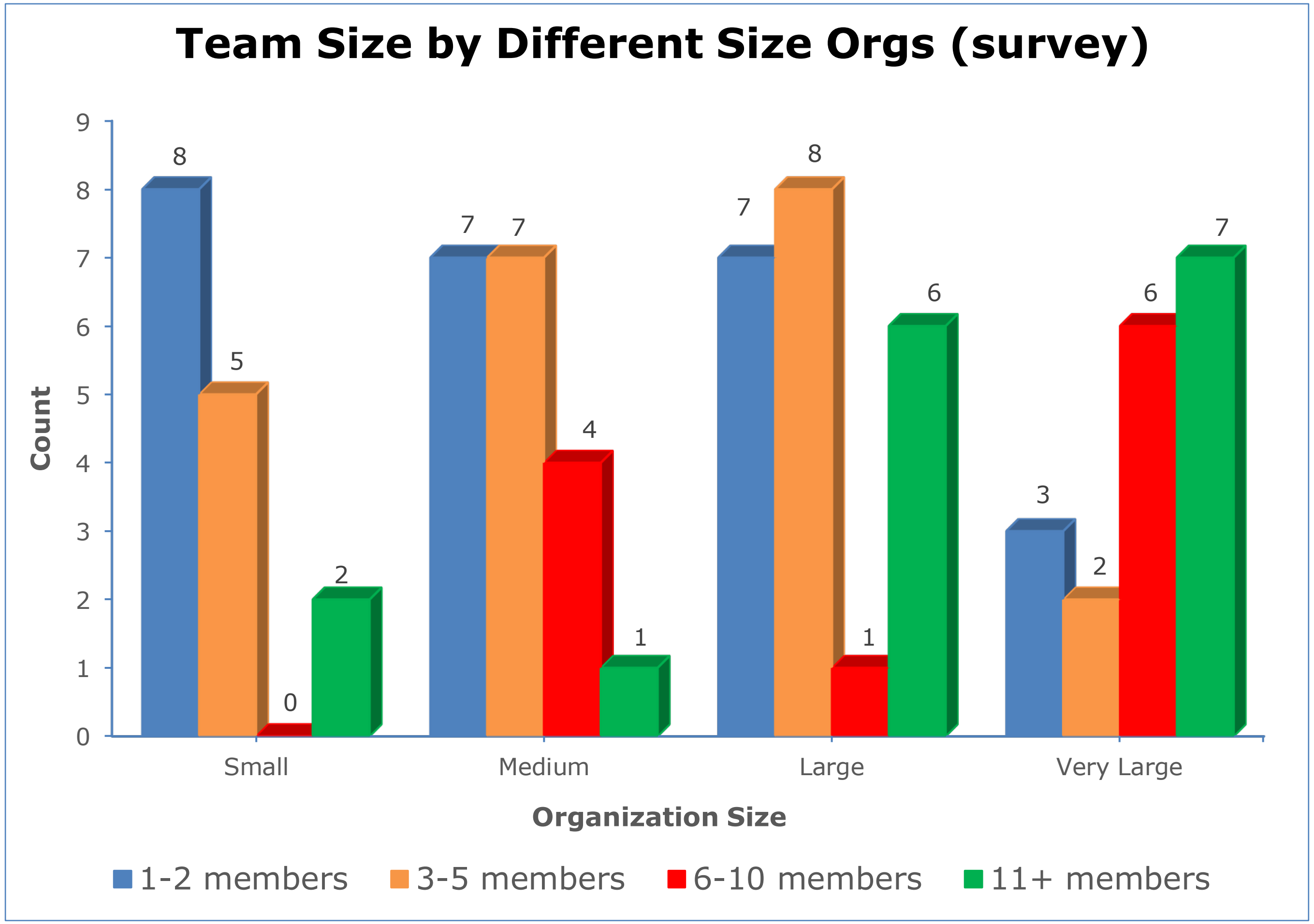
Security Awareness Team Size

Focus Groups



Survey

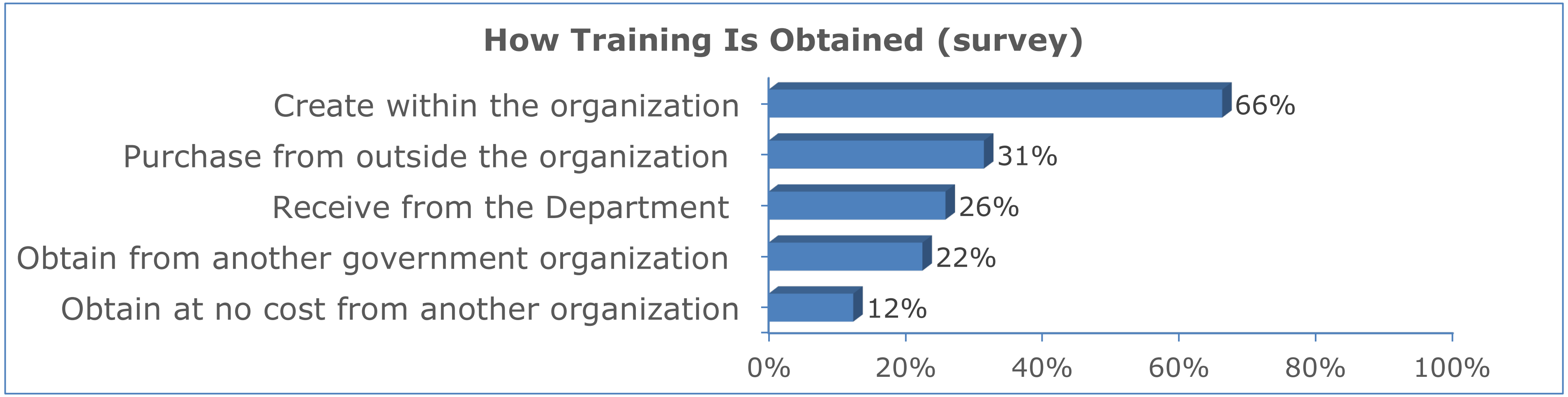




Team Size by Different Size Orgs (survey)

Results

Required Annual Cybersecurity Training



- Training delivered online, computer-based or live events
- Training is obtained from variety of sources
- **80%** update training at least once per year
- The handling of non-compliance varied from email reminders to **~75%** disabling account or network access

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

Required Annual Training Challenges

47% Getting employees to complete training

23% Finding course materials

22% Finding guidance on what to include

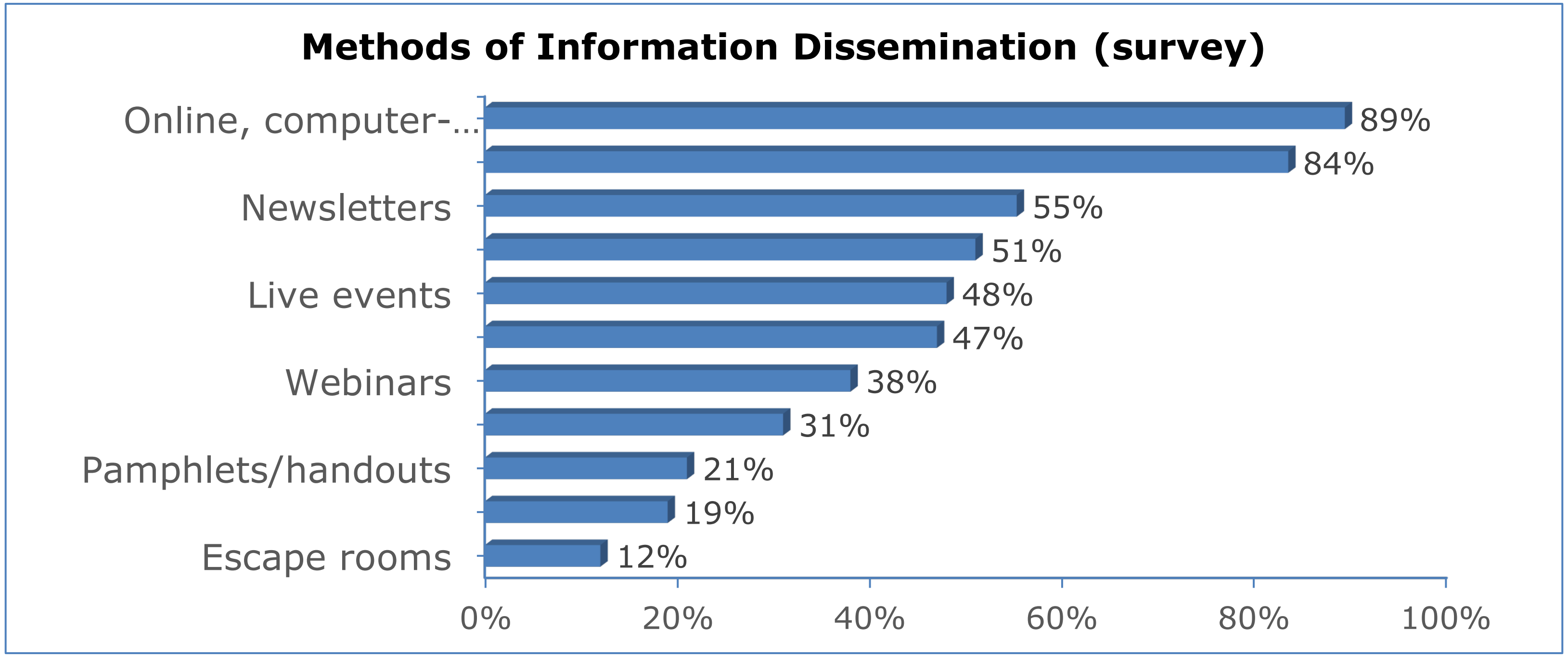
Focus Groups: Lack of course content standardization across agencies

"There are some topics, probably 80% of the topics, everybody needs to know about. So why are we buying that over and over again at each agency?" (D01)

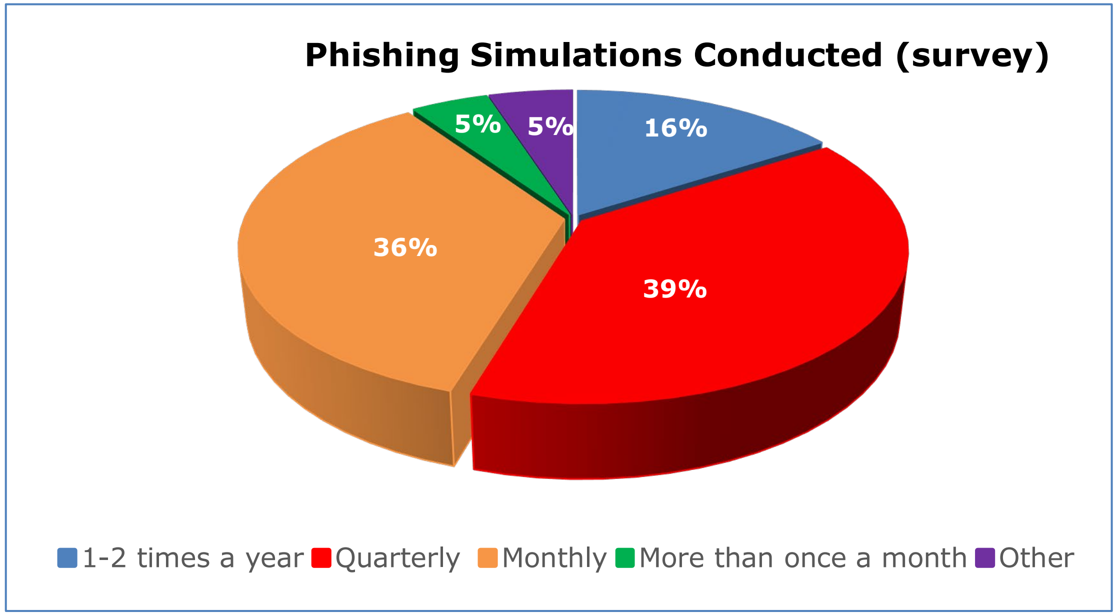
National Institute of Standards and Technology
U.S. Department of Commerce

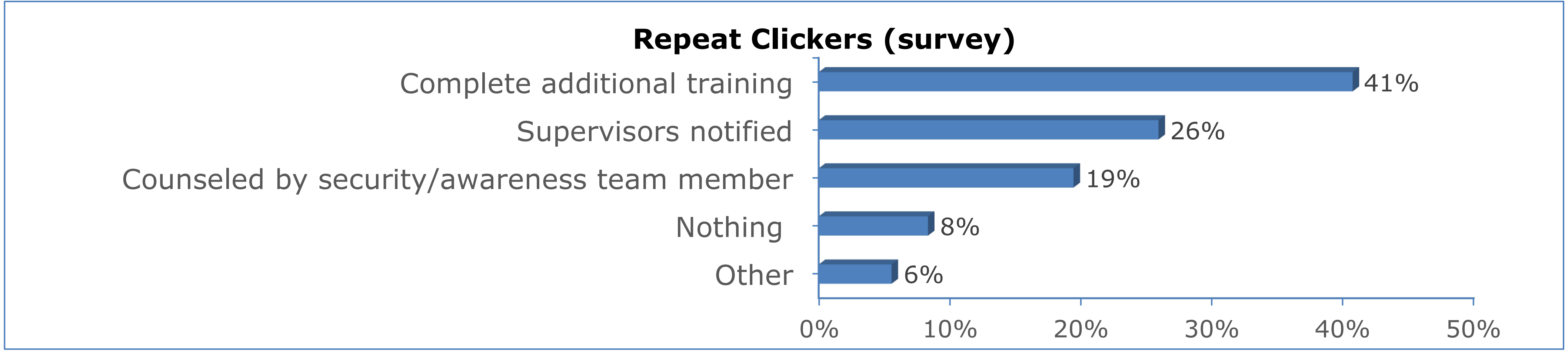
Approaches

- **21%** have no security awareness events or interactive activities beyond required training or phishing simulations
- **56%** don't recognize or reward employees for good security behavior
- Disseminate information using various methods: **7%** only use 1 method, **41%** 2-4 , **30%** 5-7, **22%** 8+



Phishing Simulations





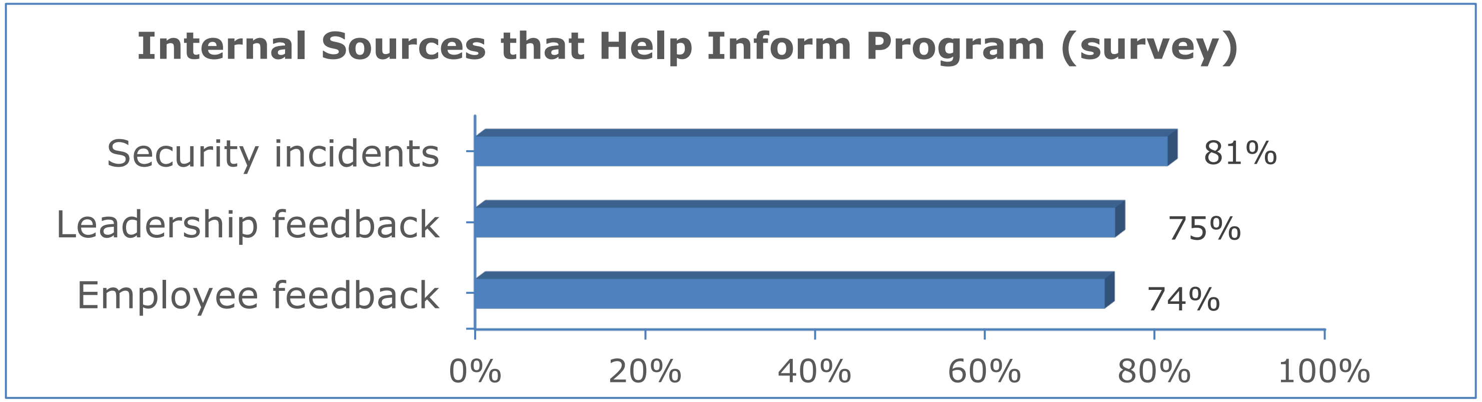
Approaches Challenges

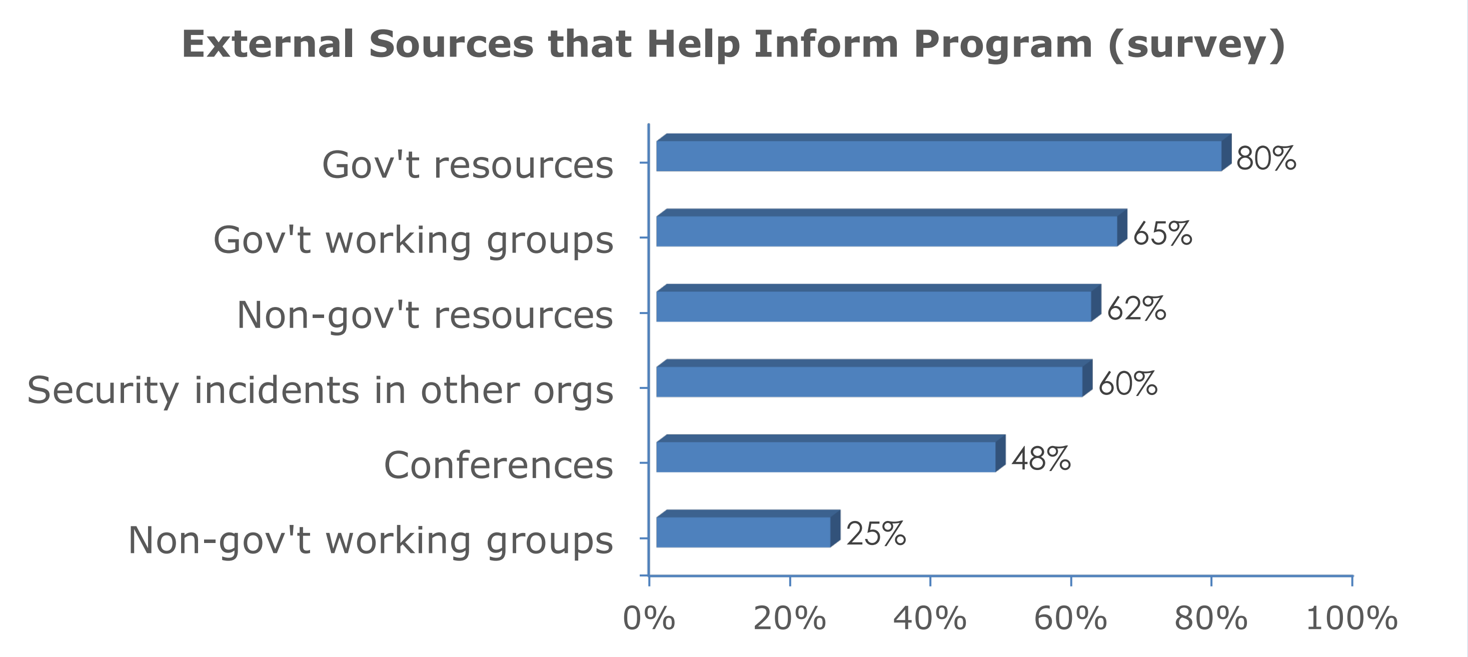
56%	Providing information in an engaging way
47%	Customizing for diverse workforce
29%	Communicating to distributed workforce
40%	Ensuring 508 compliance

"We're trying to reinforce the information, but we still want to have creative ways to present it so it doesn't feel like they're just taking the same thing over and over again and they're just clicking through without actually reading through the information." (N12)

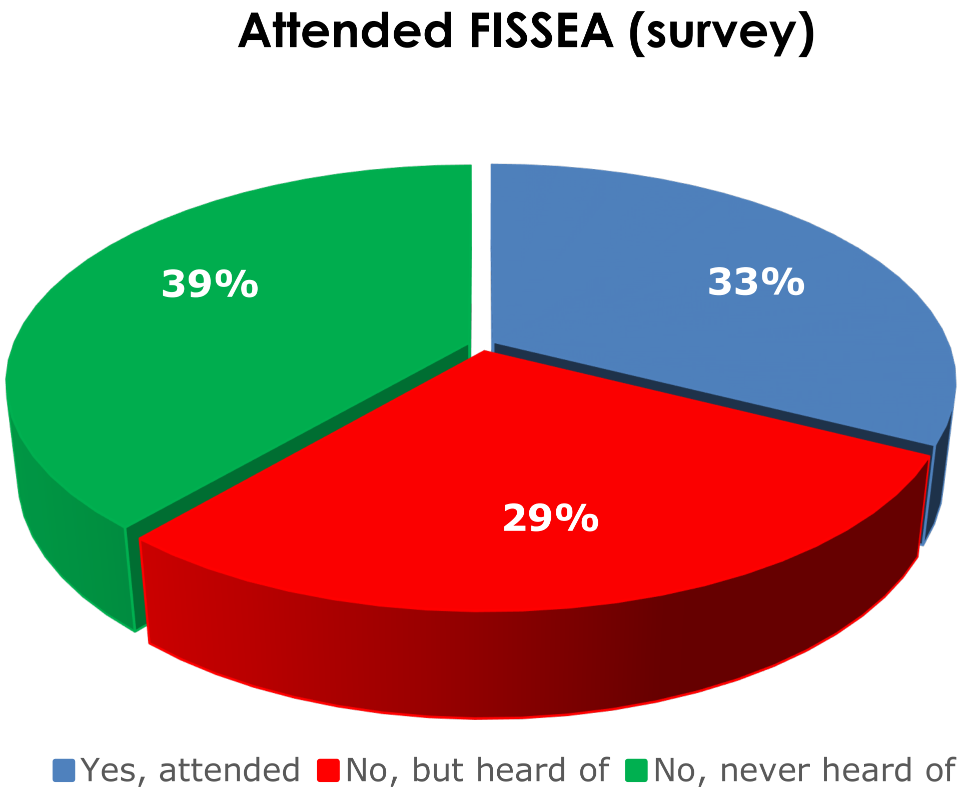
Informing Content

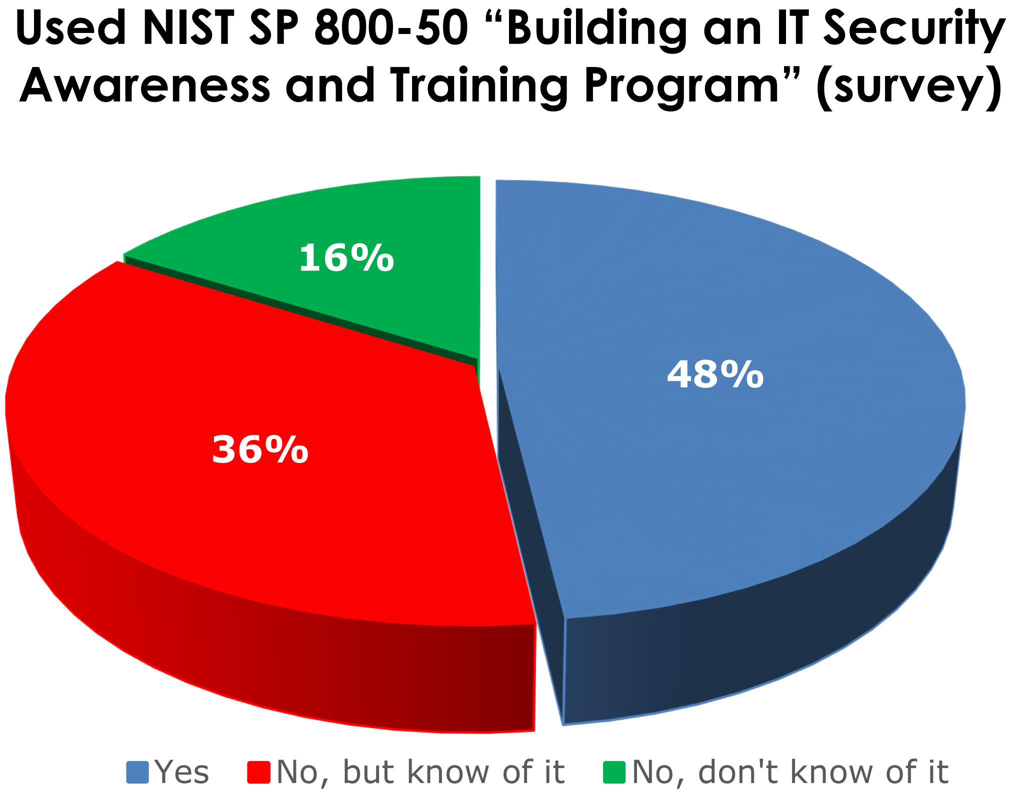
- Autonomy levels varied for program development and content customization
- Security awareness is a collaborative effort within the organization
- Internal and external sources informed content coverage and sources





Awareness of FISSEA and NIST SP 800-50





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

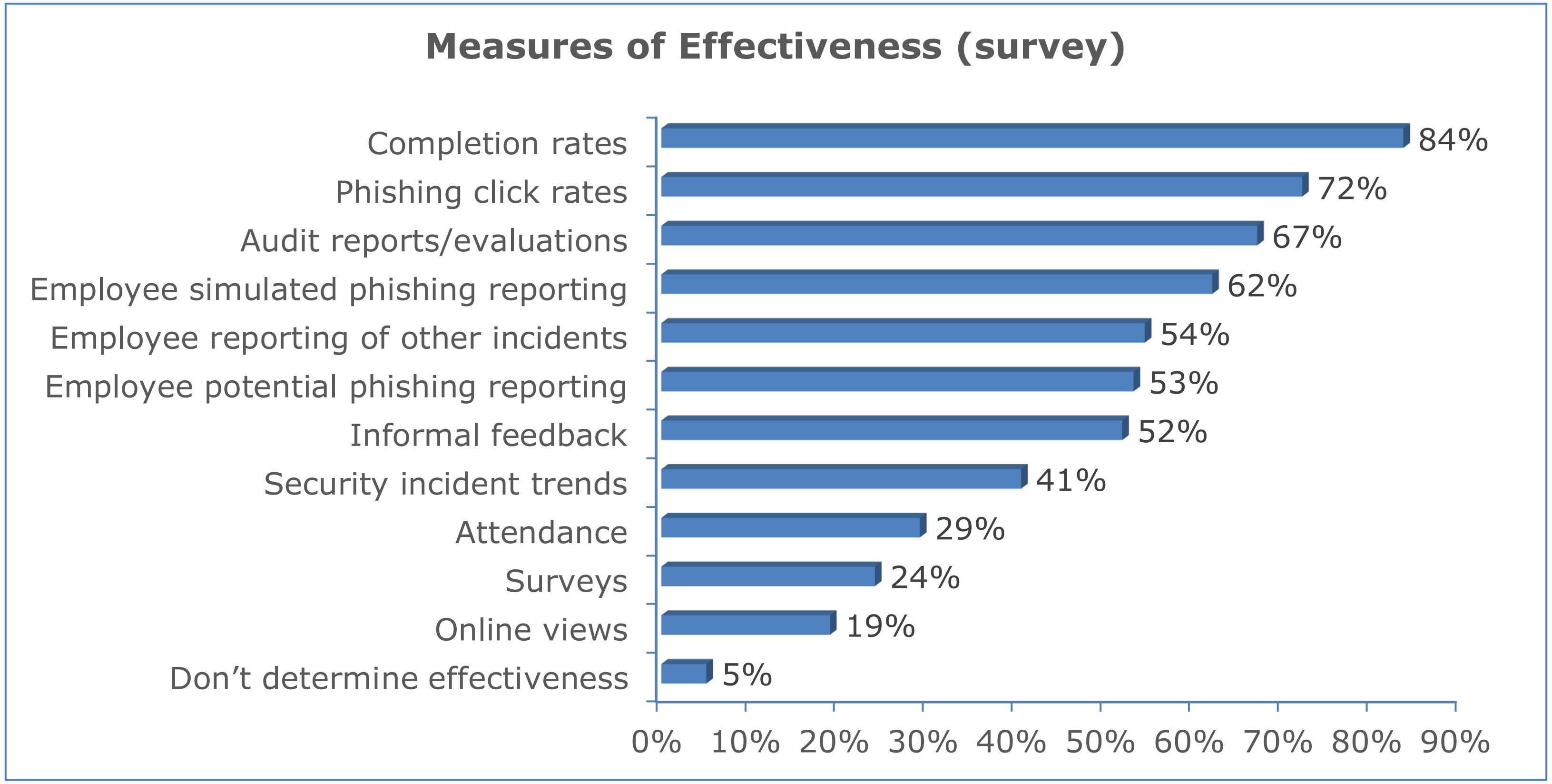
Informing Content Challenges

27% Collaborating with other federal security awareness professionals

33% Finding external sources of information relevant to organization

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

Measures of Effectiveness (MOEs)



- MOEs used for multiple reasons
  - 78% - Demonstrate compliance
  - 71% - Improve/inform program
  - 58% - Show value of program to leadership
  - 42% - Justify additional resources
- “Compliance is most important indicator of success”
  - Among leadership - 56% Agree, 22% Disagree
  - Among respondents - 47% Agree, 28% Disagree

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

Measures of Effectiveness Challenges

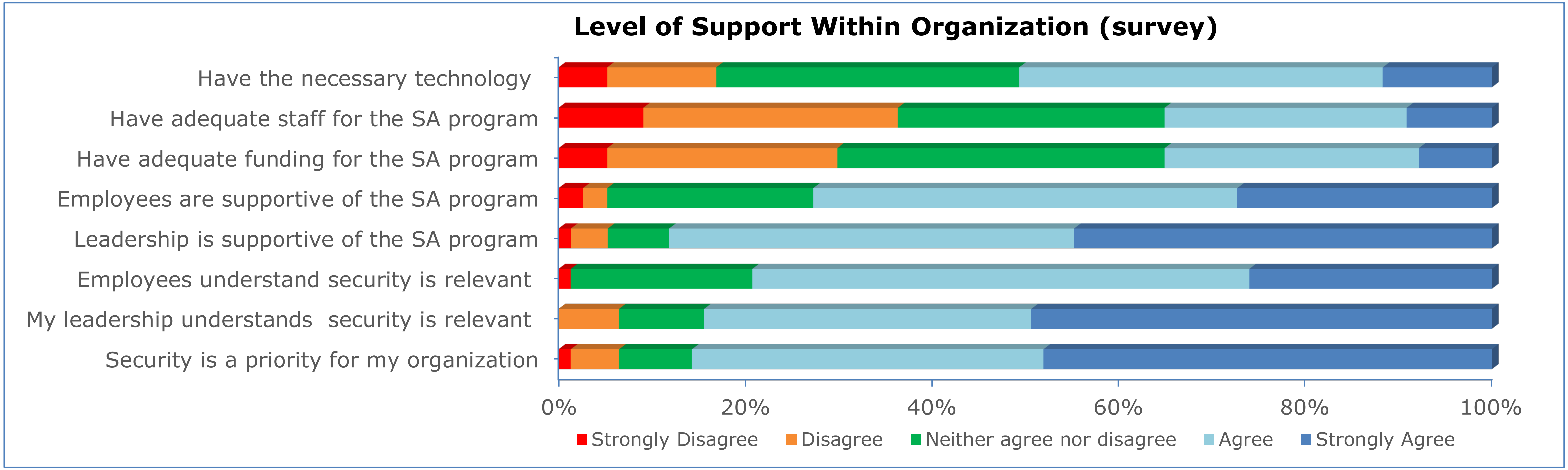
- 44% What/how to measure
- 37% Effectively presenting data to leadership
- 48% Integrating security awareness data with data from other groups
- 56% Benchmarking program against other federal organizations

Focus Groups: Compliance vs. impact on behavior change

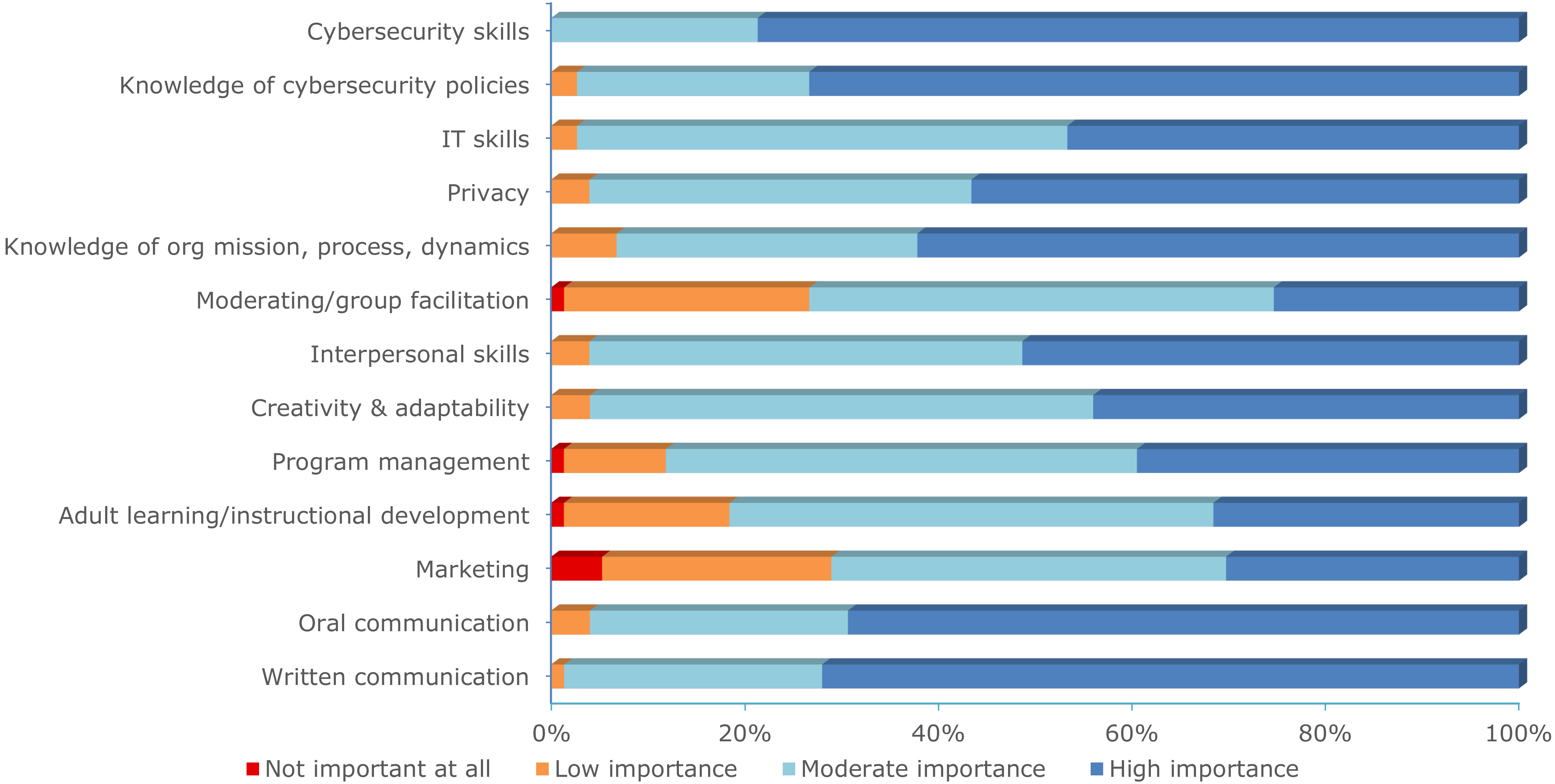
> "How do we determine whether or not it is effective? We have not come up with that solution yet…How are we making an impact? How are we making a difference when we educate our workforce?" (N04)

Program Support and Success

- 77% of survey respondents think their program is moderately or very successful
- Varied views on level of support within the organization



Team Knowledge and Skills – Rating Importance



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

Mix of Skills/Knowledge

- 61% of survey respondents think they have the right mix of skills/knowledge for their programs
- **Focus groups**:
  - Discipline diversity is beneficial
  - Programs often enlist help from other organizational groups (e.g., communications, HR) to augment their team

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

Advice from the Field

The Big Picture

Seek out management support & guidance

“Establish and maintain a good working relationship with senior management because their support can make or break your program.” (N09)

First develop a strategy, then establish repeatable processes

“Assess your organization’s need before you jump into things.” (survey)

“documenting the steps that you took…so that you would have a program that's repeatable.” (N05)

Security awareness should not be “one-and-done”

“Have some other awareness campaigns that go on throughout the year just to try and keep it at the forefront of everybody's mind.” (S01)

Approaches

Use a variety of communication channels and methods to deliver security information

“Interactive programs have proven much more effective than slide show-based programs.” (survey)

“try to make it fun.” (N01)

Information should be relatable and tailored to the audience

“Use examples that the employees are likely to encounter in their daily work and personal experiences.” (survey)

“If you can't get that message across in a way that is understandable, you've lost.” (D01)

Reward positive behaviors

“Focus less on bad behaviors and highlight good behaviors -- help employees learn from model employees, not through negative examples.” (survey)

Security Awareness is a Team Effort

Use existing templates & guidance documents

“Really trying to make use of resources that are out there, …federal guidance that's been put out.” (D03)

“Borrow content from industry colleagues.” (survey)

Participate in related fed information sharing groups

“If we…share the results, we can help each other build more efficient programs for our respective agencies.” (D02)

Build a multi-disciplinary team or leverage other expertise

“You really got to have a team. There's no way one person can do it without a lot of backup.” (D06)

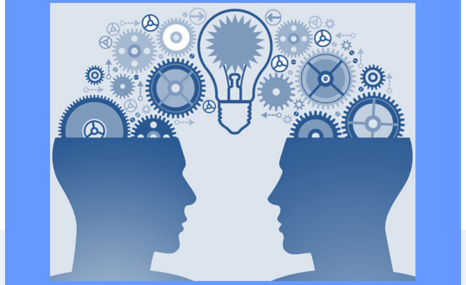
“Build relationships with offices within your organization.” (survey)

Next Steps

Exploring Government-wide Solutions

Federal-level Training

- Alleviate challenge in finding/creating content
- Allow for customization for each organization



Collaborative Forums

- Real-time & interactive
- Share tips, content, ideas with other federal security awareness professionals

NIST Special Publication 800-50

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

Building an Information Technology Security Awareness and Training Program

Mark Wilson and Joan Hash

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8933

October 2003

U.S. Department of Commerce

Donald L. Evans, Secretary

Technology Administration

Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology

Arden L. Bement, Jr., Director

Federal Guidance

- Inform revision of NIST SP 800-50 & NICE Framework
- Impact-focused MOEs
- Lessons learned

Professional Development

- Gaining support
- Empowering the workforce
- Developing engaging materials
- Risk communication

Thank you!

Full report on study results targeted for late Fall

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

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