Compliance or Impact?

Insights into How U.S. Government Organizations Determine the Effectiveness of Security Awareness Programs

Julie Haney
National Institute of Standards and Technology
March 2, 2023

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

Disclaimer

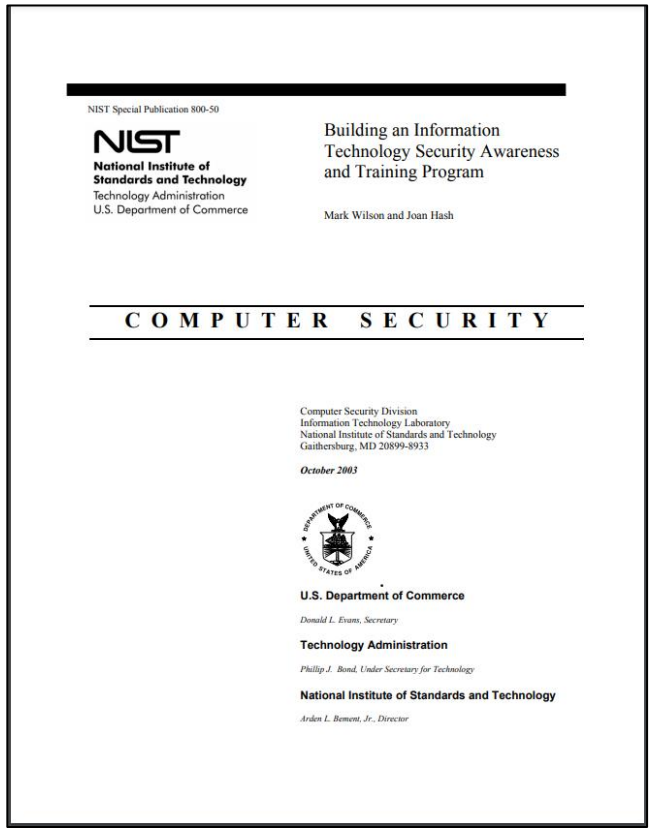
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Security Awareness in the U.S. Government

Challenges to Measuring Effectiveness

versus

Informing New Guidance


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

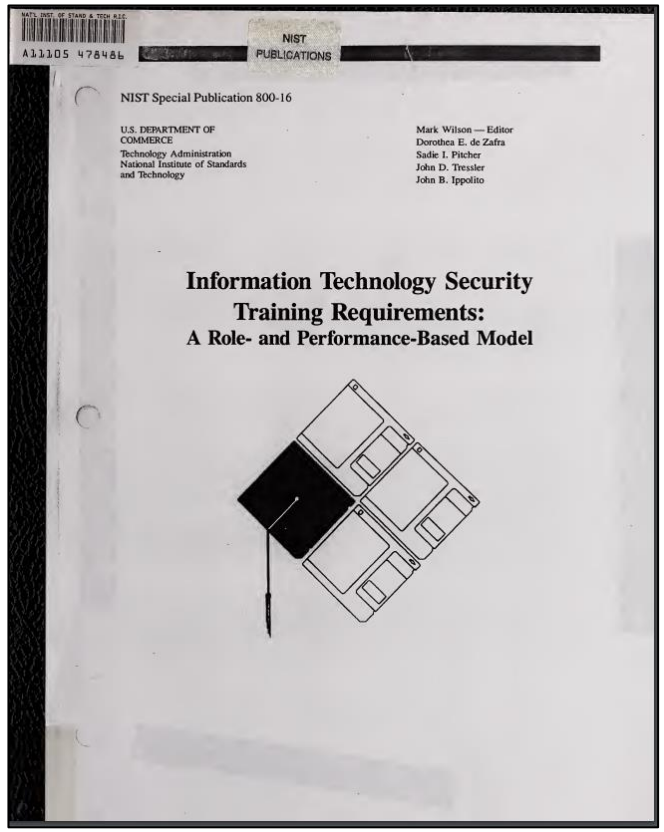
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8933

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



NIST Special Publication 800-16

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology

Mark Wilson — Editor
Dorothea E. de Zafra
Sadie I. Pitcher
John D. Tressler
John B. Ippolito

Information Technology Security Training Requirements:
A Role- and Performance-Based Model

New Special Publication Draft for Public Comment coming this Spring!
Tentative title: “Building a Cybersecurity and Privacy Awareness and Training Program”

Research Questions

1. How do U.S. Government organizations determine the effectiveness of their security awareness programs?
2. Which types of effectiveness data are most valuable to managers who oversee security awareness programs?
3. What are the challenges organizations face when trying to measure effectiveness?

Study Methodology

Focus Groups
(29 participants)

Survey
(96 participants)

Participants were U.S. Government employees who have security awareness responsibilities in their organization or manage/oversee the security awareness program.

Survey Participants

Represented different roles

- **44%** were program leads or duel leads/managers
- **9%** were managers or executives

Mostly worked on security awareness part-time

- **55%** spend less than ¼ of time

Were experienced in security awareness

- **74%** had more than 5 years experience

Had diverse educational backgrounds

- **56%** had at least one computing degree
- **51%** had a degree in a non-STEM field

Organizations and Teams

Different levels of the U.S. Government

- **About a third** each from Departments, sub-components, and independent agencies

Diverse program sizes (# employees covered)

- **About a quarter** each from small, medium, large, very large programs

Varying security awareness team sizes

- **34%** had 1-2 people assigned to security awareness
- **30%** had 3-5 people


Results

Determining Effectiveness

Most popular measures

- **84%** annual training completion rates
- **72%** phishing simulation click rates
- **67%** audit reports

Over half considered employee reporting rates

41% looked at security incident trends

24% conducted employee surveys

4% said they don't try to determine effectiveness

> For all of our virtual events and at the end of our training, we have surveys…And it gives them a rating scale and asks them, was the training effective? Was the content effective? Was the delivery or the presenter's delivery effective?

Use of Effectiveness Data

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

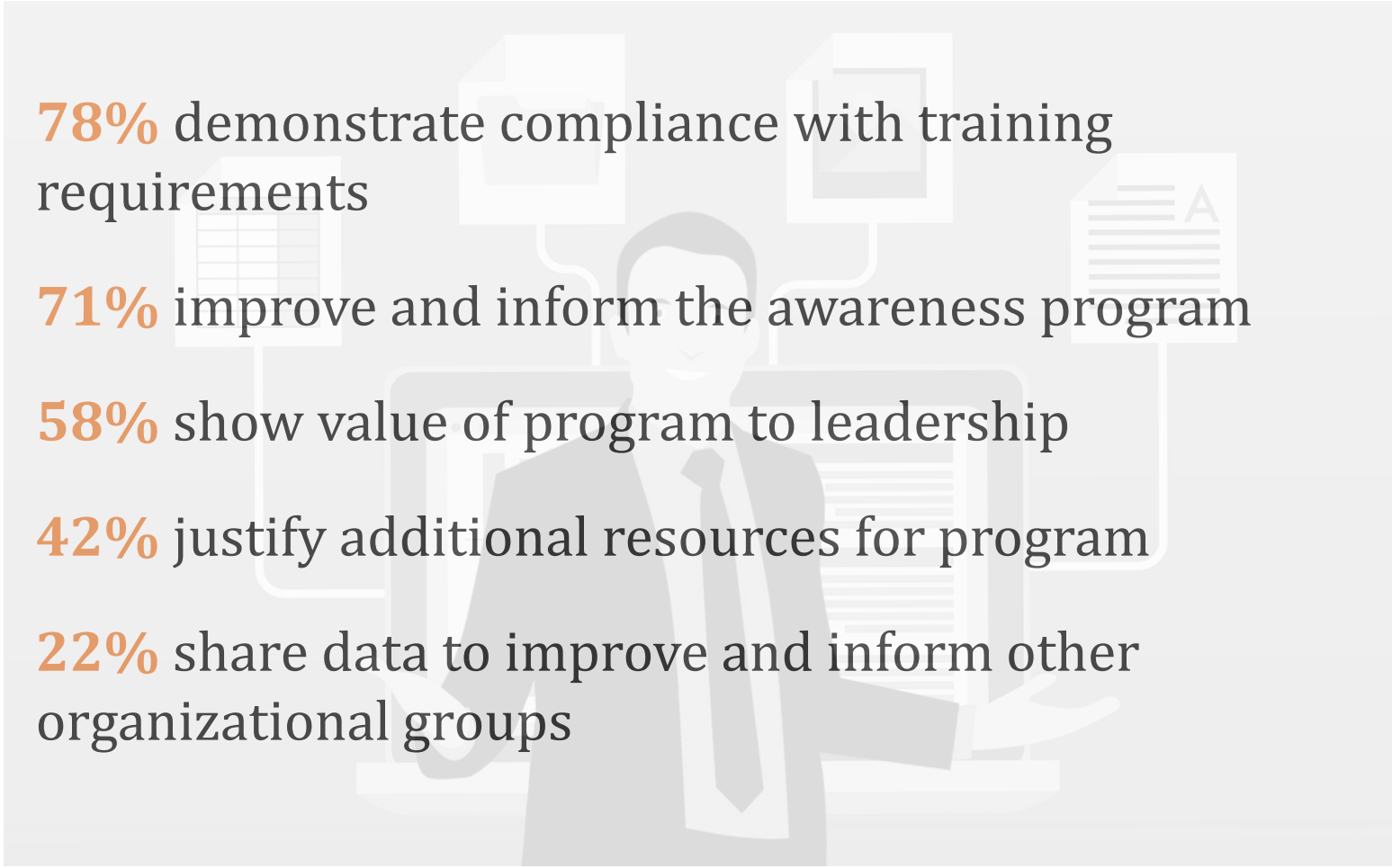
78% demonstrate compliance with training requirements

71% improve and inform the awareness program

58% show value of program to leadership

42% justify additional resources for program

22% share data to improve and inform other organizational groups



Compliance as Indicator of Success

56% agreed or strongly agreed with the statement "Among ***leadership***, compliance is the most important indicator of success."

47% agreed or strongly agreed with the statement "***I*** think compliance is the most important indicator of success."

> Management pays attention to things with compliance…Now, that doesn't identify effectiveness…but it does help increase management awareness and attention to supporting these programs.

Manager Preferences

59% security incidents

31% phishing data

24% training completion rates

21% employee feedback

21% other demonstrations of employee behaviors

> …incidents more granularly analyzed and categorized as to the types of human actions/inactions that contributed, and who, so we can adjust both general training and targeted follow-up training with individuals.

Challenges

> How do determine whether or not it is effective?...How are we making a difference when we educate our workforce?

44% determining what/how to measure is very/moderately challenging

37% effectively presenting data to leadership

48% synthesizing data from multiple groups to inform awareness program

56% benchmarking against other government organizations

Overall Program Success

34% rated their security awareness programs as ***very successful***

43% rated their security awareness programs as ***moderately successful***

19% rated programs as ***slightly successful***

4% rated programs as ***very unsuccessful***


Takeaways

Supporting Security Awareness Programs

Develop measurement standards & guidance

"[We need] something standard that all the departments and agencies could actually end up measuring…to really determine whether or not the programs that are out there are effective."

Facilitate benchmarking & sharing

"We could judge apples to apples to know where we are, how we stand up to someone else, and where we could focus our training."

Emphasize impact over compliance

"Completion of training is one statistic, but that doesn't really tell you whether anything's sunk in. It tells you that they got through the course."

What Programs Can Do

Develop & document a plan

"Document what it is that you want the program to do and how you want it to work…so that you can brief senior leadership on that, because if you don't have their buy-in, then your program is probably not going to go anywhere."

Synthesize data from multiple sources

"Annual [training]…and phishing click data graphed with the network monitoring data and helpdesk reporting data …to compare between user knowledge and actions."

Automate data collection

"Automation is key because [otherwise] the level of effort – for particularly, smaller agencies where they may not have access to tools or there's a single person – is really impactful and inefficient."

THANK YOU

julie.haney@nist.gov

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