NISTIR 8420A

Approaches and Challenges of Federal Cybersecurity Awareness Programs

Julie Haney
Jody Jacobs
Susanne Furman
Fernando Barrientos

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

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

NISTIR 8420A

Approaches and Challenges of Federal Cybersecurity Awareness Programs

Julie Haney
Jody Jacobs
Susanne Furman
Fernando Barrientos
Information Access Division
Information Technology Laboratory

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

March 2022

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

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8420A
73 pages (March 2022)

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

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 NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

Organizational security awareness programs experience a number of challenges, including lack of resources, difficulty measuring the impact of the program, and perceptions among the workforce that training is a boring, "check-the-box" activity. While prior surveys and research have examined programs in the private sector, there is little understanding of whether these findings also apply within the U.S. government. To address this gap and better understand the needs, challenges, practices, and necessary competencies of federal security awareness teams and programs, NIST conducted a research study that leveraged both qualitative and quantitative methodologies. This companion document to NISTIR 8420 "Federal Cybersecurity Awareness Programs: A Mixed Methods Research Study" reports on a subset of study results focused on identifying the current approaches and challenges of security awareness programs within the federal government. Insights gained from these results are informing guidance and other initiatives to aid federal organizations in building effective security awareness programs. While focused on the U.S. government, findings may also have implications for organizational security awareness programs in other sectors.

Keywords

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

Executive Summary

Security awareness programs aim to help employees recognize and appropriately respond to security issues, with a goal of achieving long-term behavior change. Industry and research surveys have revealed that organizational security awareness programs face a number of challenges, including lack of resources, difficulty measuring the impact of the program, and perceptions among the workforce that training is a boring, “check-the-box” activity. However, it is unclear if these challenges also apply to security awareness programs in the United States (U.S.) government.

To better understand the needs, challenges, practices, and necessary competencies of federal security awareness teams and programs, we conducted a “mixed methods” research study that leveraged both qualitative and quantitative methodologies. We first conducted eight focus groups of federal employees who had security awareness duties or were managers or executives who oversaw the programs within their organizations. The focus groups then informed an online survey completed by 96 federal employees with security awareness responsibilities.

The research background and methodologies for these two phases are described in detail in NISTIR 8420 “Federal Cybersecurity Awareness Programs: A Mixed Methods Research Study.” This companion document reports on a subset of results focused on the approaches and challenges of federal security awareness programs. The following is a high-level overview of these results, with cited statistics from the survey.

Required Annual Security Awareness Training

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

Security Awareness Approaches

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

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

Informing the Security Awareness Program

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

Program Success and Support

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

make decisions about the security awareness program, while training completion and phishing click rates were mentioned by much fewer.

- Large majorities (70% and greater) thought that security was a priority for the organization, that security was understood by leadership and employees as important, and that leadership and employees supported the security awareness program. However, only 35% of survey participants thought the program had been provided adequate funding and staff.

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

Table of Contents

List of Appendices

List of Figures