Exploring Government Security Awareness Programs: A Mixed-Methods Approach

Jody L. Jacobs, Julie M. Haney, Susanne M. Furman, and Fern Barrientos
National Institute of Standards and Technology

Abstract

Organizational security awareness programs are often underfunded and rely on part-time security awareness professionals who may lack sufficient background, skills, or resources necessary to manage an effective and engaging program. U.S. government organizations, in particular, face challenges due to strict security awareness requirements that often result in success being measured by training completion rates rather than impact on employees' attitudes and behaviors. However, no prior research has explored security awareness in the government sector. To address this gap, we are conducting an in-progress, mixed-methods research effort to understand the needs, challenges, and practices of U.S. government security awareness programs. This understanding will inform the creation of resources for security awareness professionals, including examples of successful practices and strategies, lessons learned, and suggestions for building a team having the appropriate knowledge and skills. While focused on the U.S. government, our findings have implications for organizational security awareness programs in other sectors.

1 Introduction

Despite an abundance of cybersecurity guidance and technologies, organizational employees continue to fall prey to cyber attacks, putting both themselves and their organizations at risk. Security awareness training is a first step towards helping employees recognize and appropriately respond to security issues, with a goal of achieving long-term behavior change [20].

Workshop on Security Information Workers, USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8, 2021, Vancouver, B.C., Canada.

Unfortunately, security awareness efforts face significant challenges. Security awareness programs in organizations of all sizes may be underfunded and rely on part-time security awareness professionals who may lack sufficient background, skills, tools, or resources necessary for managing an effective program [18, 21]. U.S. government – also known as federal – agencies are likewise affected by these challenges as they are mandated to conduct annual security awareness training for all employees [1, 16]. While mandates enforce a minimum baseline for security awareness, when viewed simply as a "check-the-box" exercise, organizations may begin to measure program success simply in terms of compliance metrics, like training completion rates. However, these metrics reveal little about the effectiveness of the training in changing and sustaining workforce attitudes and behaviors [10].

To address the lack of studies about security awareness issues within the U.S. government, we are performing mixed-methods research to better understand the needs, challenges, practices, and necessary competencies of federal security awareness teams and programs. Our research is being conducted in two phases. We held focus groups with federal security awareness professionals to inform the development of a subsequent, online survey that will be sent to a broader population. In this paper, we summarize preliminary results from the focus groups and then briefly describe the planned follow-on survey and potential contributions of our research for both government and non-government organizations.

2 Related Work

Prior research and industry surveys revealed challenges faced by security awareness programs. Programs may receive insufficient attention and funding within their organizations, and security awareness duties are often performed on a part-time, ad-hoc basis [18, 21]. Frequently recruited from the technical security ranks, security awareness professionals may also lack the professional skills (e.g., interpersonal and communication skills) needed to be successful in their role [18].

From a workforce perspective, security awareness training

may be viewed as an inconvenient, boring, "check-the-box" exercise with little relevance to day-to-day work [5, 11]. To counter these challenges, researchers [2, 4, 5, 7] recommend that programs better engage employees by communicating how security impacts the organization, tailoring communications to various audiences, and implementing creative ways to disseminate awareness information. In addition, programs should continuously provide training refreshers throughout the year to help make security a habit both at work and home.

Measuring program success is an important but often overlooked aspect of security awareness programs. For a holistic assessment, recommendations point to organizations using a combination of measures, such as security incident trends and reporting, views/engagement with security awareness materials, and feedback from stakeholders [4, 10].

Although evidence of security awareness challenges and recommendations abound, it is currently unknown whether these apply to programs within the U.S. government sector and if government organizations experience additional issues. Our research addresses this gap.

3 Methodology

We are undertaking an exploratory sequential mixed methods research approach (qual → QUAN) [8], with focus groups informing a broader survey. In this paper, we describe the completed focus group study phase and briefly describe our future plans for the survey.

3.1 Study Design

Focus groups can be valuable when used as a precursor to quantitative surveys of larger samples as they can facilitate the development of survey questions by providing an understanding of how people talk about specific topics and what concepts are most important [12, 14]. We selected focus groups, rather than interviews, for several reasons. Since one of the goals of our study was to identify potential ways in which information could be shared more effectively across the community, it was valuable to observe how ideas emerged during group discussion, which is not possible in individual interviews. Focus groups also served a practical purpose as we had an abbreviated timeline in which to collect and analyze data. We hoped that our study results could inform the revision of a federal security awareness guidance document [20] set to commence around the same time as our study. Wanting to provide input earlier rather than later in the revision process and factoring in the time to design and execute a follow-on survey, focus groups were deemed a more efficient way to collect data as compared to individual interviews.

When designing the focus group study, we consulted seven federal security awareness subject matter experts (SMEs). The final protocol consisted of 11 questions covering topics such as approaches, successes, challenges, measuring effectiveness, wish lists, and necessary knowledge and skills for security awareness teams. We selected a multiple-category design, which involves focus groups with several types of participants to allow for comparisons across or within categories [12]. Based on SME discussions, we decided on three categories: 1) department-level organizations (e.g., U.S. Department of Labor), 2) sub-component agencies, which are semi-autonomous organizations under a department (e.g., Bureau of Labor Statistics under Department of Labor), and 3) independent agencies, which are not in a department. In the Executive Branch of the U.S. Government, there are 15 departments, over 200 sub-components, and just over 100 independent agencies.

Potential focus group participants were selected via a purposeful approach to identify information-rich cases and represent diversity of agencies. We identified participants via several avenues: recommendations from the SMEs; researchers' professional contacts; a mailing list of small and micro agencies; previous speakers and participants from the last three years of the Federal Information Security Educators (FISSEA) conference [15]; and LinkedIn and Google searches. Participants had to have knowledge of the security awareness programs in their organizations either because they had security awareness duties or oversaw the programs.

3.2 Data Collection

Between December 2020 and January 2021, we conducted eight virtual focus groups with 29 total participants: 2 groups with 6 department-level participants, 3 with 12 participants from independent agencies, and 3 with 11 participants from sub-components. Group sessions lasted 60-75 minutes, with each having 3-5 participants. We found that, given the virtual nature of the groups, smaller numbers of participants worked best [19]. All groups were audio recorded and transcribed. Participants also completed an online survey to gather demographic and organizational information.

The study was approved by our institution's Research Protections Office with informed consent required for all participants. To ensure anonymity, each participant was assigned a reference code, with individuals from independent agencies identified as N01 – N12, department-level organizations as D01 – D06, and sub-components as S01 – S11.

3.3 Data Analysis

For data analysis, initially, each member of the four-person research team individually coded a subset of three transcripts (one from each category) using an *a priori* code list based on research questions and open coded for additional concepts as needed. We met several times to discuss codes and develop a codebook. In accordance with the recommendation of qualitative methodologists [6, 13], we focused not on calculating

agreement scores but rather on how and why disagreements in coding arose and the insights afforded by subsequent discussions. When disagreement occurred, we discussed as a group to reach consensus.

Coding continued until each remaining transcript was coded by two researchers. The coding pair then met to discuss code application and resolve differences. The entire research team convened to discuss overarching themes identified in the data.

4 Participant Demographics

The 29 participants represented 28 unique federal organizations (one agency had two people participate). Among those, 22 led their respective security awareness programs, three were security awareness team members, and four were managers or Chief Information Security Officers (CISOs). All but two were part-time in their security awareness duties (average 46%). Twenty had been involved in security awareness for more than five years, with the others involved 1-5 years. Eleven of the 23 who provided formal education information had at least one degree in a technology-related field.

Fifteen participants were male and 13 female, with one participant not disclosing gender. One participant was in the 18-29 years-old age range, 5 were 30-39, 9 40-49, 9 50-59, and two 60 + (3 did not disclose age).

5 Preliminary Results

5.1 Required Annual Training

U.S. government organizations are mandated to implement annual, mandatory security awareness training programs for their workforce. In executing these programs, security awareness professionals encounter several challenges. Employees may perceive the training as a "check-the-box" exercise with boring, unchanging content and are often overwhelmed by having to complete numerous other mandatory organizational training courses. As one participant mentioned, "You've got IT security, physical security, personnel security, etc. And they have their own training requirements... So to me, it's inefficient for our user base not to have one course that meets all the needs" (S11). In addition, programs often have challenges tracking training completion of contractors supporting the organization or seasonal staff due to them not having the same system access as government employees.

We noted that enforcement of awareness training completion varied among organizations. Nine participants indicated that their organization took a zero-tolerance approach by disabling accounts of employees who failed to complete the training by the appointed deadline. One participant described how enforcement, while having its merits, also resulted in additional challenges for his organization: "They [employees] put it off... Even though we're giving them messages throughout the year, they'll wait. And then when we had to come up with this big, long list of people we're disabling accounts, then it becomes a political nightmare" (N08). Conversely, five participants expressed that they had not received the organizational support necessary to enforce training completion, especially when leaders themselves are guilty of not completing the training: "Our biggest problem is with our executives. They are the ones who are more than likely not to have taken the training in a timely manner, and we can't exactly lock them out" (S03).

5.2 Approaches

The programs represented in our focus groups delivered their required, annual cybersecurity training via standard online, computer-based or instructor-led training. Furthermore, most organizations went above-and-beyond mandatory training and disseminated security awareness information throughout the year via a variety of methods, including newsletters, cybersecurity tips of the month, broadcast emails, posters, speaker events, and webinars. Phishing simulation exercises – in which employees are sent emails that mimic real-world phishing attempts to train them to recognize and appropriately respond to phishing emails – were particularly popular. Several organizations took novel approaches to deliver information – for example, escape rooms and virtual reality – with the intent of boosting employee engagement. Programs also hold awareness campaigns in line with annual National Cybersecurity Awareness Month themes [9].

With the variety of security awareness delivery methods, participants noted that they were highly sensitive to the amount, relevancy, and conciseness of information they distributed to their workforce as they did not want to overwhelm employees. Participants expressed challenges in ensuring their delivery methods are adaptable to a variety of learning styles, skill levels, and work roles. They also discussed difficulties they face in meeting various accessibility and assistive technology requirements, especially when implementing novel techniques such as virtual reality.

When asked what is working well for their programs, three participants mentioned that they have incentive programs to engage users and reward them for good security behaviors. One organization incorporated a multi-level gamification approach where individuals could advance as their security awareness increased. Another gave employees a certificate to hang in their office or added a "badge" in their email signature stating they were a "phish hunter" when they successfully reported a phish during a scheduled phishing exercise. These incentive programs resulted in "a lot of internal, healthy competition" (N01) and encouraged engagement with security awareness information.

5.3 Security Awareness Content

We found that organizations have no single resource from which to obtain security awareness training materials. Nineteen participants indicated that their organization outsourced at least some content development to an external entity (e.g., contractor, training vendor, or other federal organization), while others developed content in-house. Eight participants from sub-component organizations stated that they received complete or partial training materials from their parent department, with most having the autonomy to customize the training to fit their organizations' unique needs. Programs determined which security topics to cover in a variety of ways, often utilizing external sources (e.g., SANS, national news outlets) or internal sources (e.g., their organization's security operations center, workforce feedback) to identify pertinent security topics and trends. Participants felt that their workforce responded positively when training topics were relevant and relatable to both the organization and employees' daily lives.

When asked what resources might best help their programs, participants offered suggestions. Because finding or developing awareness content was viewed as a challenge, 15 participants expressed that security awareness programs would benefit from having a single, federal-level security awareness course to fulfill mandatory training requirements. The training would include core materials common to all organizations while allowing programs to customize some content for their current environment and organizational mission. A standardized course would ensure the delivery of consistent security awareness information and reduce the burden on federal security awareness programs. A participant who supported this idea stated, "There are... probably 80% of the topics everybody needs to know about. So, why are we buying that over and over again at each agency as opposed to give us the 80% solution and let us pay for the other 20%? That would be more efficient" (D01).

Other participants suggested a repository where organizations could share awareness materials to augment other programs' offerings. One participant said:

> "if there was a central repository within the federal government... of various trainings and awareness pamphlets, flyers, presentations... that the various agencies could actually share and leverage back and forth, I think that would definitely better help us make use of what limited resources we do have" (S01).

Participants also desired to have more government-specific, detailed guidance regarding security awareness training content/topics and delivery methods and tools. Without clear direction, many programs have had to interpret federal polices and directives on their own, leading to marked differences in training quality across organizations. As one participant said, "I think that's something that we could use more guidance on. 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" (S04).

Only five participants noted that they are involved with security awareness working groups and online forums where the latest security developments and training approaches are shared. To encourage more cross-organizational collaboration, participants suggested that a real-time sharing platform for federal security awareness professionals would be beneficial. This platform would create an environment where lessons learned, trend analysis, training opportunities, and approaches could be shared. One participant stated, "if we... share the results, we can help each other build more efficient programs for our respective agencies" (D02).

5.4 Measures of Effectiveness

Participants employed a variety of methods to determine the effectiveness of their security awareness programs. Training completion rates were a popular metric, but some participants acknowledged that these do not demonstrate long-term attitude or behavior change, which should be the real goals of security awareness training. Participants mentioned other indicators of success, such as: security awareness event attendance; employee feedback, including formal (e.g., via surveys) and informal (e.g., via personal interactions); and program audit reports. Six participants indicated that they review user-generated security incidents, security operations trends, and reporting to help determine whether certain security topics are being effectively taught and translated into action by the workforce. Participants also use click and reporting rates collected during their phishing simulations to determine the effectiveness of phishing-related training.

Although all programs make at least some attempt, 13 participants are still unsure how to gauge effectiveness. As one participant said, "We run security awareness campaigns and... we really have no idea how much of it is absorbed" (S04). Participants expressed a desire for more government guidelines on ways to measure effectiveness. One security awareness professional spoke of the benefits of standardized measures that could help "determine whether or not the programs that are out there are effective or what parts need to actually be focused on" (S01).

5.5 Team Knowledge and Skills

We asked what knowledge and skills a security awareness professional should possess. Sixteen participants stated that technical knowledge was highly important, but others felt that this knowledge could be outsourced to other security staff in the organization. Additionally, non-technical, professional skills such as interpersonal, communication, creativity, and collaboration were mentioned as being just as, if not more, important as a technical background.

Participants agreed that finding a single individual who possesses all desired knowledge and skills would be ideal, but may be difficult to achieve. Therefore, building a multidisciplinary team can be beneficial. As one participant shared, "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). However, some programs do not have the resources for an entire team and instead must rely on one person to run the entire program. In these cases, it becomes especially important to work closely with other components of the organization (e.g., human resources, communications, and the training group) to assist with activities such as outreach and training material development.

6 Future Work and Implications

Our analysis of the focus group data identified areas of interest that will inform the development of an online survey to be sent to a larger population of federal security awareness professionals. We will synthesize the qualitative focus group data with the largely quantitative survey data to capture a deeper understanding of the state, challenges, and experiences of U.S. government security awareness programs.

It is our hope that insights gained from our research will lead to the creation of multiple resources for federal security awareness training professionals, including: examples of successful practices and strategies; lessons learned; suggestions for building a team with appropriate core competencies; and the creation of information sharing platforms, such as an online forum, working group, or central repository. In addition, results will inform government-wide guidelines to aid federal organizations in the development of effective security awareness training programs.

Even though we are focusing on federal security awareness programs in the U.S., our findings appear to have relevance to programs in other countries', e.g., [3, 17].

In addition, there are other sectors outside the government that implement security awareness training and are mandated to do so, like the health and financial communities. Therefore, we believe many of our findings may be transferable to non-federal organizations.

Disclaimer

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

References

[1] 113th Congress. Federal Information Security Modernization Act of 2014 (FISMA). https://www.congress.gov/bill/113th-congress/senate-bill/2521/text, 2014.

[2] Jemal Abawajy. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3):237–248, 2014.

[3] Raneem AlMindeel and Jorge Tiago Martins. Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. *Information Technology & People*, May 2020.

[4] Moneer Alshaikh, Sean B. Maynard, Atif Ahmad, and Shanton Chang. An exploratory study of current information security training and awareness practices in organizations. In *Proceedings of the 51st Hawaii International Conference on System Sciences*, January 2018.

[5] Maria Bada, Angela M. Sasse, and Jason R.C. Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour? https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf, 2019.

[6] Rosaline S. Barbour. Checklists for improving rigour in qualitative research: a case of the tail wagging the dog? *British Medical Journal*, 322(7294):1115–1117, 2001.

[7] Stefan Bauer, Edward W. Bernroider, and Katharina Chudzikowski. Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, 68:145–159, 2017.

[8] Vicki L. Plano Clark. Meaningful integration within mixed methods studies: Identifying why, what, when, and how. *Contemporary Educational Psychology*, 57:106–111, 2019.

[9] Cybersecurity and Infrastructure Security Agency. National Cybersecurity Awareness Month (NCSAM). https://www.cisa.gov/national-cyber-security-awareness-month, 2021.

[10] Tobias Fertig, Andreas E. Schütz, and Kristen Weber. Current issues of metrics for information security awareness. In *Proceedings of the European Conference on Information Systems*, 2020.

[11] Julie Haney and Wayne Lutters. Security awareness training for the workforce: Moving beyond "check-the-box" compliance. *Computer*, 53(10):91–95, 2020.

[12] Richard A. Krueger and Mary Anne Casey. *Focus Groups: A Practical Guide for Applied Research*. Sage, Thousand Oaks, CA, 5th edition, 2015.

[13] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. In *ACM on Human-Computer Interaction*, page 72, 2019.

[14] Sylvia C. Nassar-McMillan and L. DiAnne Borders. Use of focus groups in survey item development. *The Qualitative Report*, 7(1):1–12, 2002.

[15] National Institute of Standards and Technology. FISSEA – Federal Information Security Educators. https://csrc.nist.gov/projects/fissea, 2021.

[16] Office of Management and Budget. Circular A-130. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf, 2016.

[17] Eka Ayu Puspitaningrum, Ferizka Tiara Devani, Vidya Qoriah Putri, Achmad Nizar Hidayanto, and Ika Chandra Hapsari. Measurement of employee information security awareness: Case study at a government institution. In *Proceedings of the 2018 Third International Conference on Informatics and Computing (ICIC)*, pages 1–6, 2018.

[18] SANS. 2021 SANS security awareness report: Managing human cyber risk. https://www.sans.org/security-awareness-training/resources/reports/sareport-2021/, 2021.

[19] UXalliance. Conducting remote online focus groups in times of COVID-19. https://medium.com/@UXalliance/conducting-remote-online-focus-groups-in-times-of-covid-19-ee1c66644fdb, April 2020.

[20] Mark Wilson and Joan Hash. NIST Special Publication 800-50 - Building an information technology security awareness program. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf, 2003.

[21] Ben Woelk. The successful security awareness professional: Foundational skills and continuing education strategies. https://library.educause.edu/~/media/files/library/2016/8/erb1608.pdf, 2015.