Security Awareness in Action: A Case Study

Julie M. Haney, *National Institute of Standards and Technology*
Wayne G. Lutters, *University of Maryland*

Abstract

A critical role and force-multiplier in security adoption is the cybersecurity advocate. Cybersecurity advocates are security professionals who attempt to remedy implementation failures by actively promoting and facilitating the adoption of security best practices and technologies as an integral component of their jobs. These advocates not only have technical skills, but also must possess the ability to educate, persuade, and serve as organizational change agents for cybersecurity adoption.

A prior interview study of a diverse set of cybersecurity advocates advanced the definition of the cybersecurity advocate role [1]. However, the study was limited in that it was a one-sided self-report view through the lens of advocates. Additional empirical evidence of cybersecurity advocates working "in the wild" (within an actual work context) is needed to validate the findings. To obtain a more comprehensive look at cybersecurity advocacy in practice, we are conducting an in-depth case study of a security awareness team at a mid-sized U.S. federal government agency.

Security awareness professionals are a type of cybersecurity advocate who are responsible for developing and executing security awareness programs within their own organizations. Prior insight into the day-to-day work and challenges of these professionals reveal that the majority of respondents perform security awareness duties on a part-time basis with little budget, with many lacking sufficient background and soft skills (e.g., communications, relationship-building, and marketing) that are needed to effectively engage the workforce and key departmental stakeholders such as the finance and operations departments [2,3].

The in-progress case study will allow for examination of a security awareness team from several perspectives via a multi-faceted approach involving: 1) interviews of security awareness team members, managers in the team's chain-of-command, and agency employees who receive the security awareness information, 2) field observations of four in-person security awareness events, and 3) review and analysis of security awareness materials distributed to the agency's workforce.

Preliminary qualitative analysis reveals a passionate, creative team willing to try new approaches to attain their goal of making security awareness entertaining and informative rather than a mandatory burden. We will discuss the techniques and approaches of the team and how their efforts are viewed by others at their agency. Examples of the team's approaches include: ensuring security awareness information is timely and topical to the season, world events, or current organizational concerns; providing employees with security awareness information that is not only relevant to their jobs, but also to their personal life; introducing humor and gaming when appropriate; and soliciting feedback from others in the organization about what topics to address in future events. We will also discuss challenges security awareness professionals face, including lack of resources and employee attitudes and time constraints.

As a complement to the prior cybersecurity advocate interview study, the case study will provide better insight into real-world security advocacy techniques and which are most effective. These practices may then inform the design of security interfaces and training. In addition, the project allows for a deeper examination of professional characteristics of advocates, and how those are viewed by advocates' target populations. The identification of these characteristics can aid in the creation of professional development resources to aid people in becoming successful advocates.

References

[1] J. M. Haney and W. G. Lutters. "It's Scary…It's Confusing…It's Dull": How cybersecurity advocates overcome negative perceptions of security. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 411-425, 2018.

[2] SANS. 2018 Security Awareness Report. https://www.sans.org/sites/default/files/2018-05/2018%20SANS%20Security%20Awareness%20Report.pdf, 2018.

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

Workshop on Security Information Workers, USENIX Symposium on Usable Privacy and Security (SOUPS) 2019. August 11, 2019, Santa Clara, CA, USA.

.