June 27-29, 2019

fissea FEDERAL

CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

How to Measure the Effectiveness of Cybersecurity Training and Awareness Programs

Michael Adams, NuCrest, LLC
President/CEO

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

BACKGROUND

Organizations often struggle with determining and measuring how effective their implementation of a comprehensive cybersecurity training and awareness program is for their workforce.

This presentation explores the measures that organizations can use in determining if they have implemented a successful cybersecurity training and awareness program leading to security protections of their data, networks, and personnel.

MEASURES

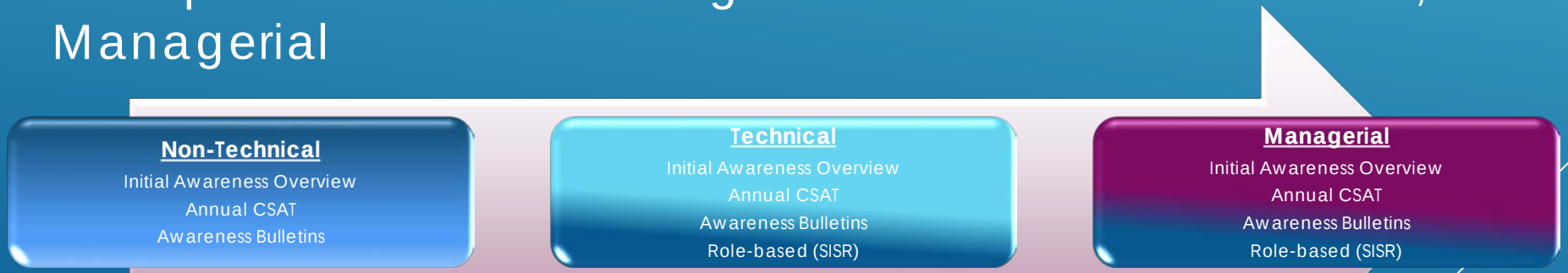
- Top-Down Leadership buy-in
- Workforce Training Measures
- Risks, Vulnerabilities, POA&M Measures & Cybersecurity Compliance

MEASURE 1: TOP-DOWN LEADERSHIP BUY-IN

- One of the key factors to successfully measuring the effectiveness of a Cybersecurity Training and Awareness Program is through leadership (executives, managers, supervisors) support throughout the organization. Leaders serving as champions for organizational security training and awareness program efforts, directly influences employee participation in the program. When employees see the leaders reiterating mandated security awareness, they are more inclined to respond to ensuring security requirements are met themselves.
- The implementation of C-Suite Cyber Security Training model will provide an organization's leadership with the right knowledge and resources to make informed decisions regarding the need for a comprehensive Cybersecurity Awareness and Training Program throughout their organization

MEASURE 2: WORKFORCE TRAINING MEASURES

- Cybersecurity Awareness and Training should not be an “implement and forget solution” for an organization. There should be a continuous cycle of training conducted throughout the organization for end-users, privilege users, and managerial staff.
- This training should be measured to ensure that the staff was trained on current security trends, securing technology, security labs and exercises, and workforce assessments conducted.
- Example of effective training to measure: Non-Technical; Technical and Managerial



MEASURE 3: RISKS, VULNERABILITIES, POA&M REDUCED & CYBERSECURITY COMPLIANCE

- As security control assessments (SCAs) are conducted during the RMF Assessment and Authorization (A&A) process, security controls that have been properly implemented by Privileged Users (ISSOs, SAs, DBAs, WebApp Admins, and Network Engineers) with risks should be captured, analyzed, and measured.
- Vulnerabilities on the network from the result of a vulnerability assessment scans should be measured and tracked
- Risks and Vulnerability measures captured can determined what security control implementation that Privileged Users need to be trained on to help reduce risks and vulnerabilities from security controls not properly implemented thus reducing the number of POA&Ms on the network
- Cybersecurity Compliance measures captured can show that a successful cybersecurity awareness training program has been implemented that enables the organization to understand and meet FISMA requirements

CONCLUSION

Our presentation explored the measures that organizations can use in determining if they have implemented a successful Cybersecurity Training and Awareness program which will help lead to improved security protections of their data, networks, and personnel.

QUESTIONS?
COMMENTS?

ADDRESS

613 Maccubbin Lane, Gambrills, MD 21054

PHONE

703-375-9308

EMAIL

michael.adams@nucrest.com and info@nucrest.com

Follow us on Social Media

FACEBOOK

TWITTER

LINKEDIN

NuCrest

www.nucrest.com