Cybersecurity Workforce

Instructor: The Internet and systems and data that operate in cyberspace are relied upon for a wide range of critical services. This dependence makes vulnerabilities to disruptive and destructive threats devastating if realized. There is a vital need for a skilled workforce prepared to protect and defend in cyberspace.

There have been challenges with cultivating a robust cyber workforce. Surveys like the annual I-S-C square Cybersecurity Workforce Study indicate the shortage in the cybersecurity workforce has grown to almost 3 million globally, with close to a half million vacant cyber-related positions in North America alone.

A contributing factor to the shortage is awareness. Cybersecurity as a career field simply hadn't been advocated by schools or occupation-guidance sources. There are now many outreach initiatives to introduce cyber fields to students earlier and provide hands-on(and internship) opportunities. Additionally, as more facets of everyday life increasingly rely on technology and more younger individuals are becoming proficient operating and troubleshooting mobile and smart devices, the lack of awareness problem may be cured via osmosis.

Compounding lack of awareness are vaguely described cybersecurity careers. Clear details of what cybersecurity work entails, as well as the training or experience to pursue it, has been lacking. Position descriptions for cybersecurity jobs are typically broad and list industry certifications and education credentials as requirements for a qualified candidate versus specific skills needed to be successful in the role. Solid candidates could be overlooked.

The lack of clearly defined work roles also makes career progression-planning difficult. Retaining staff is difficult without a clear path for promotion and professional growth. Coupled with competitive wages from private industry, experienced staff can be lured away.

An initiative to help solve some of these issues through standardizing a structure and definition is the NICE Cybersecurity Workforce Framework. Detailed in NIST Special Publication 800-181, the NICE Framework is a national resource that categorizes and codes cyber work across seven categories, identifies specialty areas within each, followed by work roles each with corresponding knowledge, skills, abilities (KSAs) and tasks.

The NICE framework is leveraged and customized by other entities to organize and manage their specific workforce needs. For instance, the DoD Cyber Workforce Framework is an adaptation where mission -

essential positions with their core and critical tasks and KSAs are coded and categorized.

Ideally a framework using standard terms for common work, will establish an important building block for a capable and prepared cyber workforce through Skill gap analysis, Targeted recruitment, Retention strategies, Identifying training needs, Developing career paths, Aiding in effective position descriptions.

While work roles will vary across organizations depending upon size and objective, some functional needs are prudent with a cybersecurity program component (such as executive managers who set the overall enterprise strategy and business managers who focus on the impact of specific functions). Operational personnel are the day-to-day workforce that has specific duties in support of the mission. Asset owners are concerned about the data or the hardware and services behind it. Certification agents examine configurations and security practices to authorize a component's use. And then auditors verify compliance from a cybersecurity perspective up through management.

Management at the executive level increasingly includes specialized officers to give critical concentrations dedicated attention. The chief executive officer (CEO) remains the most senior person in an organization, while delegating focused areas like information

security, risk management and technology to their own branch and senior leadership; bridging strategy and implementation.

Strategic alignment that ensures security supports and operates in concert with an organization's goals requires coordination of many work roles. As the cyber landscape continues to evolve, a skilled workforce to protect and defend the enterprise is crucial. While a concerning shortage of talented candidates has hindered the cultivation of an essential cyber workforce, the needs of current business environments and cyber workforce development initiatives - for awareness, training and defining work-role requirements - are shaping the way forward.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution. This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu. Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

DM18-0098