The motivation for this project is based on the large fairly complex corpus of frameworks used throughout industries. There seems to be a lack of frameworks dedicated to cybersecurity workforce (CSW) development. The goal of this project is to identify and analyze the differences and similarities of CSW frameworks while providing clarity to the literature.

Homeland Security Challenge

Strengthen the overall security posture of the nation by better preparing the current and future cybersecurity workforce.

Motivation & Goal

The motivation for this project is based on the large fairly complex corpus of frameworks used throughout industries. There seems to be a lack of frameworks dedicated to cybersecurity workforce (CSW) development. The goal of this project is to identify and analyze the differences and similarities of CSW frameworks while providing clarity to the literature.

Approach / Methodology

Surveyed a large portion of the available literature related to frameworks. Initial collection was intentionally broad to ensure those frameworks that may be applied toward CSW development were analyzed. Initially, 16 CSW related frameworks are identified and reduced to six based on the major functions and their popularity.

These six provided met the established criteria for this project, being focused on CSW development. The frameworks identified as relating to both cybersecurity and workforce development are 181 & 181r, DoDD 8140, CCM, NCAE, and COBIT.

Outcomes / Results

Frameworks were analyzed based on four key elements; publishing organization, goal/objective, audience, and mapping components and summarized in Table 1. The volume of text was large, but the analysis was conducted manually by hand. The effort involved in automated text analysis was reserved.

Through the initial identification resulted in a wide assortment of frameworks we are confident the resulting analysis incorporates many relevant frameworks.

Table 1: CSW Framework Analysis Summary Results

<table>
<thead>
<tr>
<th>Framework Name</th>
<th>Initiative organization</th>
<th>Goal/Objective</th>
<th>Main Audience</th>
<th>Mapping Components</th>
<th>Highlights</th>
<th>NICE Frameworks and NIST SP 181/181r in 2020</th>
<th>DoD 8570/8140 Cyber Workforce</th>
<th>National Centers of Academic Excellence in Cyber Defense/Cyber Operations (CAE-CD/CO)</th>
<th>Cybersecurity Competency Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>NICE Cybersecurity Workforce Framework (NCWF)</td>
<td>NIST (National Institute of Standards and Technology)</td>
<td>Describes and categorizes cybersecurity work and identifies sample job titles, tasks, and KSA’s (Knowledge, skills, and Abilities)</td>
<td>Employers, current and future cybersecurity workers, training and certification programs, educators, technology providers</td>
<td>7 Categories (Security, Innovation, Program, and Practice, Governance, Cybersecurity, Information and Technology)</td>
<td>181r provides a simplified and flexible approach to describe cybersecurity work</td>
<td>No NIST standard components valid until further publication</td>
<td>DoD 8140.01 Manual not released yet</td>
<td>100% Academia focused</td>
<td>Information Systems Audit and Control Association</td>
</tr>
<tr>
<td>NICE CYF - NIST SP 800-181r in 2020</td>
<td>NIST</td>
<td>Provides the foundation for identifying education, training, and certification requirements to support cybersecurity personnel qualification</td>
<td>Students and those looking to enter the field</td>
<td>53 Area of Expertise</td>
<td>Small target audience</td>
<td>181r.01 Manual released yet</td>
<td>3 Focus areas: DevOps, IT Risk, Security</td>
<td>NICE Cybersecurity Workforce Framework Analysis</td>
<td>ISACA COBIT</td>
</tr>
<tr>
<td>DoD 8570/8140 Cyber Workforce Framework</td>
<td>DoD (Department of Defense)</td>
<td>Military, civilian, and contractor cybersecurity personnel</td>
<td>Students and those looking to enter the field</td>
<td>33 Speciality Areas, 52 Work Roles</td>
<td>Able to be usable by a wide range of users</td>
<td>3 Federal Guidelines, 3 Core Technical KUs</td>
<td>3 Focus areas: DevOps, IT Risk, Security</td>
<td>NICE Cybersecurity Workforce Framework Analysis</td>
<td>ISACA COBIT</td>
</tr>
<tr>
<td>National Centers of Academic Excellence in Cyber Defense/Cyber Operations (CAE-CD/CO)</td>
<td>NSA</td>
<td>Education, training, and certification efforts involved in automated text analysis were reserved.</td>
<td>Students and those looking to enter the field</td>
<td>53 Area of Expertise</td>
<td>Able to be usable by a wide range of users</td>
<td>3 Federal Guidelines, 3 Core Technical KUs</td>
<td>3 Focus areas: DevOps, IT Risk, Security</td>
<td>NICE Cybersecurity Workforce Framework Analysis</td>
<td>ISACA COBIT</td>
</tr>
<tr>
<td>Cybersecurity Competency Model</td>
<td>Department of Labor</td>
<td>Provide a comprehensive overview of cybersecurity workforce competencies, including roles, training, and career paths for job seekers.</td>
<td>Students and those looking to enter the field</td>
<td>33 Speciality Areas, 52 Work Roles</td>
<td>Able to be usable by a wide range of users</td>
<td>3 Federal Guidelines, 3 Core Technical KUs</td>
<td>3 Focus areas: DevOps, IT Risk, Security</td>
<td>NICE Cybersecurity Workforce Framework Analysis</td>
<td>ISACA COBIT</td>
</tr>
</tbody>
</table>

Discussions

There are similarities among the reported six frameworks. All the frameworks exhibit a goal of developing a cybersecurity workforce. They all utilize some variation of knowledge, skills, and tasks. They also share a common foundation in or contain and large component of the NICE Framework.

We have developed a simple yet effective template for which future iterations of and new published frameworks can be quickly evaluated by audiences to gauge the relevance of a particular framework or update.

Comparing the cybersecurity workforce frameworks provides the ability to better understand the current frameworks and their application. This subjacent project constructed the foundation for continued research whereby knowledge, skills, and tasks were extracted from job postings and compared to the NICE Framework.

Acknowledgements

This research was performed under an appointment to the U.S. Department of Homeland Security (DHS) Science & Technology (S&T) Directorate Office of University Programs Summer Research Team Program for Minority Serving Institutions, administered by the Oak Ridge Institute for Science and Education (ORISE) through an interagency agreement between the U.S. Department of Energy (DOE) and DHS. ORISE is managed by ORAU under DOE contract number DE-AC05-00OR22725. All opinions expressed in this paper are the author’s and do not necessarily reflect the policies and views of DHS, DOE or ORAU/ORISE.

Selected References


Authors: Jordan Bernot & Max Douglas
Faculty Advisor: Dan J. Kim