Prioritizing Cybersecurity Education

Mackenzie Coleman

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Dr. Saltuk Karahan & Professor Bora Aslan

January 30, 2022

Cybersecurity Education

Nowadays it is almost impossible not to have some sort of smart device. From smart phones to smart toothbrushes, technology has truly taken over the world. The demand for the cybersecurity workforce is only expected to increase over the next few years. But we come to the question, what is cybersecurity? Cybersecurity is the protection against criminal or unauthorized use of electronic data or devices. It is important to recognize the demand for cybersecurity education and training throughout governments, private organizations, and companies.

Many times, companies and organizations run into security problems due to careless behavior with employees. Careless behavior such as downloading unidentified links, visiting corrupt website through company computers, and even setting their passwords to something too simple like their birthday. This behavior is often unintentional and without thinking about the potential consequences of a simple click. These simple mistakes are why the need for proper cybersecurity education and training is crucial in the world we live in today.

In these times, all organizations require the use of technology, but many do not know how to manage and handle such advancements. As far as cybersecurity is concerned, this means that they have no methodology for detecting cyber incidents (Frayssinet, M., Escnarro, D., Juarez, F.E., Diaz, M. 2021). The National Institute of Standards and Technology (NIST) developed an initiative called NICE. NICE is the National Initiative for Cybersecurity Education and was developed in 2010 as a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development (Frayssinet Delgado, M., Esenarro, D., Juárez Regalado, F. F., & Díaz Reátegui, M. (2021). This strategy is set in place to ensure that cybersecurity training and education is being offered and taught throughout the country. Many jobs and workforces are now requiring employees to go through

the necessary cybersecurity training to ensure safe practices while using devices. The NICE Cybersecurity Workforce Framework serves as a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization (Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). The framework resources are there to enhance cybersecurity protocols already in place within an organization and possibly give guidance as to where to start when enforcing cybersecurity training and education within the workforce.

The idea behind the NICE framework is a great plan, however, everything has room for improvement. Online courses for certifications and training have become more frequent, especially over the last two years. A survey was done on 35 of the free online cybersecurity courses back in 2018 by Lorena Gonzalez-Manzano and Jose M. de Fuentes. This study was conducted to show the areas that need improvement based on what the students are learning and how it is applicable in a realistic cybersecurity setting. Following the NICE framework, a list of recommendations were proposed to make online courses and training more effective. Two of the issues that stood out was topic choice and level choice. During this study, based off the NICE framework, most issues have received less attention like cyber operational planning courses are lacking (Manzano, de Fuentes, 2018). During these free online courses, different levels are offered from intermediate and advanced levels but no beginner levels (Manzano, de Fuentes, 2018). With these two issues alone, there are changes that need to be made to the online cybersecurity courses offered.

The NIST NICE framework is a great resource for organizations to use to better their cybersecurity protocols. At some point, these policies that the NICE initiative is creating should

become a part of the cybersecurity education and training norm. The more awareness that is spread regarding the importance of cybersecurity, the safer our information and we, as a nation, will be.

Reference:

Frayssinet Delgado, M., Esenarro, D., Juárez Regalado, F. F., & Díaz Reátegui, M. (2021). Methodology based on the NIST Cybersecurity Framework as a proposal for cybersecurity management in government organizations. *3C TIC: Cuadernos De Desarrollo Aplicados a Las TIC*, *10*(2), 123–141. https://doi.org/10.17993/3ctic.2021.102.123-141

González-Manzano, L., & De Fuentes, J. M. (2018). *Design Recommendations for Online Cybersecurity Courses*.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. https://doi.org/10.6028/nist.sp.800-181