Prioritizing Cybersecurity Education

Paper 5

Mackenzie Coleman

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Dr. Saltuk Karahan & Professor Bora Aslan

April 15, 2022

By now we all should understand the importance of implicating cybersecurity education and training in the work force, schools, and a part of our everyday is ultimately to give individuals the knowledge and skills to protect their privacy and information in cyberspace. Cyber-attacks such as DDoS attacks, ransomware, phishing emails, trojan horses, and many other types of cyber-attacks are happening to people every day. For example, this past January, the International Committee of the Red Cross's systems were compromised, resulting in hacker's gaining access to data on more than 500,000 people and disrupting service around the world. Some studies show that attacks of this nature on organizations are becoming increasingly common and have doubled in the recent years (Fernando, R. M., Demetrio Antonio Da, S. F., Georges Daniel, A. N., Rafael Timoteo de, S. J., & Rafael, R. N. (2021).

In 2010, The National Institute of Standards and Technology (NIST) developed the NICE initiative. NICE is the National Initiative for Cybersecurity Education and was developed 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). Research of cybersecurity education in higher forms of education in Europe and the United States was conducted using the NICE Cybersecurity framework. Using this framework, the results were able to detect that in certain fields of study at universities in Europe and in the U.S, proves that cybersecurity education is carried out in all 7 of the categories, however, Collect, Operate, and Analyze were found to be the most absent (Karo, S., Jaakko, B., & Jarmo, N. (2020). With this analysis, using the NICE framework, this study was able to find where the improvements in the cybersecurity education workforce needed to be. This evaluation of the NICE framework was a great way to show how the information regarding cybersecurity is being taught and practiced.

Emphasizing the importance of cybersecurity education and training in everyday life will not stop these attacks from happening but can minimize the damage caused through preparing individuals and organization's systems and networks for potential attacks. The implication of Cybersecurity Education and Training policies in schools, work environments, and for individuals is critical. If the policies surrounding, or lack thereof, cybersecurity education and training were better enforced in schools and made as important as, let's say, math classes, there is already a potential for lowered cyber-attacks against youths. As mentioned before, research done by the New York Police revealed that almost 80% of sexual abuse cases [primarily teenagers] in the nation had been linked to a virtual friendship (Amankwa, E. (2021). Human and cultural risk factors must also be considered because they influence risk at each stage level of risk management (Fernando, R. M., Demetrio Antonio Da, S. F., Georges Daniel, A. N., Rafael Timoteo de, S. J., & Rafael, R. N. (2021).

Using the NICE initiative and the NIST cybersecurity framework, schools can evaluate their own cybersecurity standards within their own network of teachers and staff, while also creating a curriculum to teach students about the proper cybersecurity protocols and procedures. This not only will ensure that students enter the digital world with valuable knowledge and skills but also can also be relevant to them in their current lives while they use technology devices and social media sites every day.

I do believe that the cybersecurity education and training implementations would be successful in the workplace, schools, organizations, and the government. In today's world, you cannot escape the inevitable use of technology. We, as a society, should prepare ourselves the best we can to minimize the damage of cyber threats. Cybersecurity education and training will become one of the most important topics of any work environment dealing with technology.

References

Amankwa, E. (2021) Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of In- formation Security, 12, 233-249. https://doi.org/10.4236/jis.2021.124013

Fernando, R. M., Demetrio Antonio Da, S. F., Georges Daniel, A. N., Rafael Timoteo de, S. J., & Rafael, R. N. (2021). Evaluating the Performance of NIST's Framework Cybersecurity Controls Through a Constructivist Multicriteria Methodology. *IEEE Access*, *9*, 129605-129618. http://dx.doi.org/10.1109/ACCESS.2021.3113178

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

Karo, S., Jaakko, B., & Jarmo, N. (2020, October 26). *Old Dominion University Libraries*. Old Dominion University Libraries - Remote login. Retrieved April 6, 2022, from https://dl-acm-org.proxy.lib.odu.edu/doi/pdf/10.1145/3436756.3437041