International Journal of Education and Social Science; Vol. 11 No. 1; April 2024
ISSN 2410-5171 (Online), 2415-1246 (Print)
Published by Research Institute for Progression of Knowledge

"Public Service and Cybersecurity: Preparing Next Generation Career Opportunities"

Dr. Deborah LeBlanc
Professor
College of Law and Public Service
National University, San Diego, CA
United States of America

Abstract

The general public needs assistance in understanding and protection within the Cybersecurity Landscape. As of 2024, the world has over 3.5 million unfilled Cybersecurity jobs. The cyber-skills and talent shortage continues to widen at an alarming rate. – Half of the smallest organizations by revenue say they either do not have or are unsure as to whether they have the skills they need to meet their cyber objectives. – Only 15% of all organizations are optimistic that cyber skills and education will significantly improve in the next two years. – 52% of public organizations state that a lack of resources and skills is their biggest challenge when designing cyber resilience. Cybersecurity is public service, and we must work together collaboratively.

Blueprint for a Comprehensive Cybersecurity Approach

Next generation career opportunities in all areas of public services will demand comprehensive approaches to cybersecurity. "At the intersection of policy, technology and human behavior is the blueprint for a comprehensive cybersecurity approach," according to public administration experts (Centralsquare,2024). The general public needs assistance in understanding and protection within the Cybersecurity Landscape. Cybersecurity is quickly becoming an essential element of public administration. Cybersecurity is public service; therefore, gaining a keen understanding of the landscape of Cybersecurity is critical to public safety and protection.

"*No country or organization is spared from cybercrime, yet many are direly underequipped to face the threats effectively, and we cannot have effective global response mechanisms without closing the capacity gap. Key stakeholders must work collaboratively towards immediate, strategic actions that can help ensure a more secure and resilient global cyberspace." –* ***Jürgen Stock***, Secretary-General of ***INTERPOL (World Eco Forum, 2024)."*** Reports from the 2024 Annual Meeting of the World Economic Forum (WEF) revealed the following key points: (1) Worldwide Cybercrime is on the rise – expected to be $10.55 Trillion in 2025. (2) As of 2024, the world has 3.5 million unfilled Cybersecurity jobs. (3) Ransomware damage costs are predicted to exceed $265 Billion by 2031.And (4) Women are predicted to 30% of global Cybersecurity jobs in the workforce by 2025. Further point, 'every IT position is a Cybersecurity position now.'

Role of Law Enforcement

Law Enforcement is a huge part of public service; and as such, they play a vital role in working with public and private agencies towards greater achievement of local, state, and national goals and objectives in Cybersecurity. Law Enforcement can better fortify the public with useful, current and relevant information on Cybercrimes. Greater public awareness is needed in the ever-evolving world of Cybersecurity crimes.

Law Enforcement agencies are in a good societal position to shed light on the following four areas for the public: (1) Types of Cybersecurity crimes, (2) Profiles of Cybersecurity criminals, (3) Reporting agencies, i.e. ICE/HSI Center and (4) Training and awareness for community and other agencies. All levels can be beneficial within the landscape of Cybersecurity.

Framework for Cybersecurity

The role of Law Enforcement is to 'protect and serve' our citizenry from local to globally. Speaking of global, Law Enforcement must continue explore and expand connectivity to two chief reasons: (1) to assist in raising public awareness of Cybersecurity crimes, and (2) to assist in the ever-increasing effort to protect against ransomware pandemic. "The National Institute of Standards and Technology (NIST) has updated the widely used Cybersecurity Framework (CSF), its landmark guidance document for reducing cybersecurity risk. The new 2.0 edition is designed for all audiences, industry sectors and organization types, from the smallest schools and nonprofits to the largest agencies and corporations — regardless of their degree of cybersecurity sophistication" (Nist,2024). The original NIST was established in 2014. The Cybersecurity Information Sharing Act (CISA) was introduced by the late U.S. Senator Diane Feinstein and signed in law by former President Barack Obama on December 18, 2015; and it served as a taxonomy of Cybersecurity outcomes, which identified (5) Five major functions: Identify, Protect, Detect, Respond, and Recover. These (5) Five functions were subdivided into (23) Twenty-three categories and outcomes; thus, ending with (108) One hundred-eight subcategories in total.

In May of 2023, "the Cybersecurity and Infrastructure Security Agency (CISA) joined government partners across the nation to celebrate and thank all of those who have dedicated their careers to public service. While their service may not always make headlines, public servants play a vital role in making our communities safer, healthier, and more secure." According to CISA, it is a good place to work with an effective mission. CISA" agency has a unique and important mission, responsible for protecting the nation's critical infrastructure from cyber threats, physical attacks, and other hazards." Further, they help protect those assets and systems that most citizens take for granted and 'don't often think about-from turning on a light switch to opening a faucet. From ensuring the security and resilience of their election systems to protecting their physical infrastructure and the information technology and operational technology that they depend on, CISA's work is essential to our national security. From their work on protecting soft targets such as stadiums and commercial buildings to their work on bombing prevention and emergency communications, CISA does all the aforementioned. Agencies in Public Administration, like the Cybersecurity and Infrastructure Security Agency (CISA) are always seeking to grow their team and hire talented individuals who are passionate about public service and their mission are encouraged to join their team.

Cyber skills and talent Shortage

Research shows that there is a need to hire more, however, 'the cyber-skills and talent shortage continues to widen at an alarming rate. – Half of the smallest organizations by revenue say they either do not have or are unsure as to whether they have the skills they need to meet their cyber objectives. – Only 15% of all organizations are optimistic that cyber skills and education will significantly improve in the next two years. – 52% of public organizations state that a lack of resources and skills is their biggest challenge when designing for cyber resilience' (Weforum,2024).

Conclusion/Recommendations

Our world is digitally connected. 'An increasingly connected world brings along with it many challenges, as well as many unprecedented career opportunities. There are daily occurrences of data breaches, ransomware and malware attacks causing significant disruption of key infrastructure. The good news is that there is an overabundance of career and job opportunities for all who have the skills and passion for Cybersecurity, especially for students in law enforcement and public administration. It is highly recommended that students expand knowledge and skills in the landscape of Cybersecurity.

References

"Insights from WEF's 2024 Cybersecurity Report and Strategies for ...." https://www.cigniti.com/blog/world-economic-forum-2024-cybersecurity-report-cyber-inequity/.

"Widening Disparities and Growing Threats Cloud Global Cybersecurity ...." 11 Jan. 2024, https://www.weforum.org/press/2024/01/wef24-global-cybersecurity-outlook-2024/.

"Essential Cybersecurity Practices for Public Administration." 01 Mar. 2024, https://www.centralsquare.com/resources/articles/essential-cybersecurity-practices-for-public-administration.

"Cybersecurity as a Public Service: 3 Ways Local Governments ... - Tenable." 16 Jul. 2019, https://www.tenable.com/blog/cybersecurity-as-a-public-service-3-ways-local-governments-can-change-the-conversation.

Make a difference in Public Service – Join CISA! | CISA

"NIST Releases Version 2.0 of Landmark Cybersecurity Framework." 26 Feb. 2024, https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework.

"Insights from WEF's 2024 Cybersecurity Report and Strategies for ...." https://www.cigniti.com/blog/world-economic-forum-2024-cybersecurity-report-cyber-inequity/.

"Global Cybersecurity Outlook 2024." https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.