



Chapter 9

Cybersecurity Workforce Development Through Innovative High School Programs


Aikyna Finch

 <https://orcid.org/0000-0002-0078-1973>
American Public University, USA


Darrell Norman Burrell

 <https://orcid.org/0000-0002-4675-9544>
Marymount University, USA


Calvin Nobles

 <https://orcid.org/0000-0003-4002-1108>
Illinois Institute of Technology, USA

Kevin Richardson

 <https://orcid.org/0009-0002-3212-8669>
Edward Waters University, USA

Horace C. Mingo

 <https://orcid.org/0000-0002-2395-2990>
Marymount University, USA


Jennifer Ferreras-Perez

Marymount University, USA

Philip Shen

Marymount University, USA

Laura Ann Jones

 <https://orcid.org/0000-0002-0299-370X>
Capitol Technology University, USA

Katrina Khanta

Marymount University, USA

ABSTRACT

In 2022, there were more than 4,100 data breaches that were brought to public attention, which resulted in nearly 22 billion people's information being compromised. When compared to 2021, when the number of cybersecurity specialists stood at 2.72 million, this shows a significant rise in the severity of the problem. Many businesses run the danger of having their organizations put at a "moderate" or "severe" risk of being attacked by cybercriminals due to a lack of workers. This study explores the value of cybersecurity skill and workforce development programs in high schools, especially those on Native American reservations, rural areas, urban areas, and low-income areas.

DOI: 10.4018/978-1-6684-7207-1.ch009

INTRODUCTION

In 2022, more than 4,100 data breaches were brought to public attention, resulting in nearly 22 billion pieces of information being compromised (Cooker, 2022). Because healthcare firms often handle and retain a wide array of essential data, criminals have been focusing on these organizations for a significant time (Cooker, 2022). The stakes have been significantly higher over the past several years because these attacks may benefit cybercriminals in numerous ways (Cooker, 2022). Personal information is like a data goldmine for a hacker since they may demand lucrative ransom payments and then market the illegally obtained data to commit financial fraud using it (Cooker, 2022). As a direct consequence, hackers have committed themselves to finding and exploiting weaknesses in healthcare network security (Cooker, 2022). Compared to 2021, when the lack of cybersecurity specialists stood at 2.72 million, this shows a significant rise in the severity of the problem. Many businesses run the danger of having their organizations put at a “moderate” or “severe” risk of being attacked by cybercriminals due to a lack of workers (Cooker, 2022)

The lack of qualified cybersecurity workers is a significant issue. In 2018, there were more than 4 million openings for positions in the field of cybersecurity (Muncaster, 2019). In addition, allies of the United States in Europe witnessed similar decreases in the number of cybersecurity professionals during the same period. Career opportunities in the field of cybersecurity expanded from 142,000 to 291,000 on a worldwide scale (Muncaster, 2019). Rogers (2019) says that the assessed firms need more cybersecurity professionals and need more experience in basic technological security measures. The inefficiency of ongoing efforts to alleviate the impact of this crisis will result in an indefinitely increased danger of personnel shortages (Rogers, 2019).

The need for educational programs to promote professions in technology is the cause and the impact of the current scarcity of qualified cybersecurity professionals (Rogers, 2019). This study will focus on how the cybersecurity sector may inherit novel tactics, educate, promote, and establish a pipeline of cybersecurity specialists to enhance a positive outcome. This focus will continue throughout this paper and will be the primary topic of this study. We must push for new educational techniques to create a healthy talent pipeline to prepare the next generation of cybersecurity experts. Regarding employment requiring modern technology, diverse populations have been overlooked and devalued on a systemic level.

The establishment of public charter high schools in areas that are predominantly minority, have high unemployment rates, are economically deprived, and are located in urban, rural, or Native American reserves is one potential option. Students in these communities would be able to earn experience in a subject with a massive workforce development deficit while still in high school if these schools had a hands-on academic focus on cybersecurity. This is possible because these schools concentrate on cybersecurity (Burrell et al., 2015).

Problem Statement

Cybersecurity is a critical component of national security in the United States. It is essential for protecting the country’s networks, systems, and data from malicious actors, both foreign and domestic. However, the cybersecurity workforce shortage is a significant challenge threatening the security of the United States. According to the Center for Cyber Safety and Education (2020), there are currently nearly three million cybersecurity job openings in the United States, with an expected job growth of 32% by 2028. This is even though only about 500,000 cybersecurity professionals work in the United States. This shortage of

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/cybersecurity-workforce-development-through-innovative-high-school-programs/321018

Related Content

Fuzzy Approach for Monitoring Projects Success in the IT/IS Industry

Jose L. Salmeron and Cristina Lopez (2012). *Measuring Organizational Information Systems Success: New Technologies and Practices* (pp. 120-135).

www.irma-international.org/chapter/fuzzy-approach-monitoring-projects-success/63450

Characteristics of IDCM Systems

Len Asprey and Michael Middleton (2003). *Integrative Document and Content Management: Strategies for Exploiting Enterprise Knowledge* (pp. 86-133).

www.irma-international.org/chapter/characteristics-idcm-systems/24073

Software Solutions Construction: An Approach Based on Information Systems Architecture Principles

Sana Bent Aboukacem Guetat and Salem Ben Dhaou Dakhli (2013). *Sociotechnical Enterprise Information Systems Design and Integration* (pp. 215-232).

www.irma-international.org/chapter/software-solutions-construction/75883

COTS Software Procurement Methodology

Seema Al-Mahmood and Mansoor Al A'ali (2011). *E-Strategies for Resource Management Systems: Planning and Implementation* (pp. 288-305).

www.irma-international.org/chapter/cots-software-procurement-methodology/45111

Methodological Issues in the Evaluation of System Analysis and Design Techniques

Andrew Gemino (2005). *Business Systems Analysis with Ontologies* (pp. 305-321).

www.irma-international.org/chapter/methodological-issues-evaluation-system-analysis/6127