**How can a Different High School Curriculum Attract New Talent and Benefit the Future Cybersecurity Workforce: An Interdisciplinary Analysis**

Deep Patel

IDS 300 W Interdisciplinary Studies

Dr. Pete Baker

Old Dominion University

Abstract

We all use the internet and intelligent internet-connected devices as part of our daily lives. The increase in internet usage has led to a tremendous rise in cybercrime. All our information is available online and stored in a database or server. There is a considerable lack of a cybersecurity workforce. The usage of smart devices is constantly increasing. If this issue is not resolved in a timely manner, the cybersecurity field will get overwhelmed and face numerous challenges as the increase in cybercrime will get out of control. As students progress through their K-12 journey, they learn about their strengths and weakness. K-12 is a constant learning phase for students. In most cases, it is a foundation of what they become in the future. Students learn about various careers in High school, which helps them choose a college major and a career path. This research analyzes how a different High School curriculum can attract more students to pursue the cybersecurity field and ultimately fill the gap in the critical need for a robust cybersecurity workforce and talent.

**How can a different High School Curriculum Attract New Talent and Benefit the Future Cybersecurity Workforce: An Interdisciplinary Analysis**

Cybercrime has been increasing exponentially, and cybercriminals are constantly coming up with new ways to exploit systems. In today's society, with more data available online than ever before, we must be prepared to protect our information and all related resources. There is a massive demand for a cybersecurity workforce and talent. Cybersecurity is a newer field, and it is much different from the traditional degrees and careers out there. Kids in high school are not getting the opportunity to learn about the cybersecurity field due to the lack of resources. Many critical jobs are unfilled due to the lack of cybersecurity talent. Research and a comprehensive understanding of this issue through the interdisciplinary lens are essential to solving the shortage of cybersecurity workforce. High schools are not staying up to date with the constant changes in the field and the job market. This paper will draw on insights from multiple disciplines to answer how a different high school curriculum can attract students to pursue the cybersecurity field and bridge the gap in the cybersecurity workforce.

The problem of cybersecurity talent and workforce shortage is complex. Therefore, it requires insights from multiple disciplines to solve the problem. The cybersecurity field involves various disciplines such as criminal justice, business, law, computer science, and more. Information security is needed in every field. Consequently, critical thinking and analytical skills are essential in cybersecurity. An interdisciplinary approach will provide relevant insights that will show an analysis of how a different high school curriculum and education approach will attract more talent to the cybersecurity field. To get a comprehensive understanding of the problem, this research paper will use insights from three relevant disciplines. Insights from cybersecurity, education, and economics disciplines will provide a solution to this complex problem.

The cybersecurity discipline focuses on protecting information systems, networks, stopping hackers, preventing unauthorized access, and ensuring data are always available. The cybersecurity field requires people with specialized skills. In this field, professionals must constantly keep learning and stay updated as cybercriminals find new sophisticated ways to gain access. Cybercrime is a subdiscipline of cybersecurity. Cybercrime costs U.S business millions of dollars. Attacks on individuals and their personal computers are on the rise. IT security professionals are struggling with new attacks as they are non-traditional, and their severity is determined by the technical means used in the attack (Stanciu, & Tinca, 2017, p. 613).

Education is vital in ensuring students learn about the cybersecurity field and create a strong cyber workforce. The education discipline involves K-12 education, college education, certifications, and training. According to DeCrosta, the responsibility for fostering interest and awareness in a career like cybersecurity during K-12 plays a critical role in creating a robust cyber workforce (DeCrosta, 2021, p. 11). Students will gain interest in the fields and careers they get exposed to during K-12. Upon graduation, they choose their educational and career path. STEM education in schools focuses on traditional STEM fields. Specialized fields like cybersecurity are not part of the programs. Thus, preventing prospective students from pursuing the cybersecurity field and bridging the gap in the workforce.

Economics is a social science field that focuses on how people use resources and consume goods and services. The internet is growing rapidly, changing how we live and do things. Cybercrime and cyberattacks disrupt our economy by stealing valuable and confidential data. Cyber-attacks cause substantial losses to our economy. To secure our future, we need a cyber workforce that is prepared to combat any cyber-attack. The lack of talent and workforce ultimately cost organizations a considerable amount of financial loss. The economic impacts of cyber-attacks go much further than just the loss of valuable data. Cybersecurity is in every field and used in every industry in some form. Therefore, it is critical we bridge the workforce gap to ensure a safe and secure economic future for the United States.

All the fields discussed face similar issues of increasing cyber-attacks and the workforce talent shortages to combat and stop attacks. An interdisciplinary approach will analyze similarities and differences in the disciplines to create a common ground. Furthermore, utilizing the insights from each discipline will provide a deeper understanding of the various reasons causing the problem and help create a solution. The usage of multiple disciplines will offer a solid solution to the problem as such a complex problem cannot be solved by any single discipline. The disciplinary conflicts and parallels provide valuable contributions in identifying a solution on how a different cybersecurity curriculum can lead to a robust future cybersecurity workforce that can combat any cyber threat.

Insights from each discipline’s perspective must get evaluated to gain a deeper understanding of the problem and develop a solution. Cybersecurity focuses on protecting electronic data against criminal or unauthorized access. This also includes combating cybercriminals and placing proper security measures to protect data and infrastructure. Cybersecurity as a discipline provides insights established on how humans use, interact, and communicate with technology. Communications between networks, devices, and the usage of cyber applications, security tools, data, and devices affect modern cybersecurity. Education is about teaching, learning, and beyond. Education is used in every field, and the discipline will provide insights on proper education and how to approach problems using education (teaching people) and the education system. Lastly, the economics discipline will contribute by giving insights on market trends and how our economy is affected by cyber-attacks. The shortage of the cybersecurity workforce and its economic impact will help understand the problem using a different approach. Ultimately the results will provide a solution to approach the problem and how a different high school curriculum can lead to a robust cybersecurity workforce. Cybersecurity discipline relative to workforce shortage is causing difficulties for many companies and organizations. The issue of cybercrime and cyberthreats is across both public and private sectors. The scale of cybercrime is under-reported due to the fear of negative exposure and the lack of resources available to law enforcement (Clough, 2011). Although there is a lot of awareness about cybersecurity, people are still uncertain about many aspects of it. According to DeCrosta, the education system fails in many areas, including early education and post-secondary education (DeCrosta, 2021). Cybersecurity is a constantly changing field. Therefore people must continuously keep learning to stay updated. “The 2016 Symantec Internet Security Threat Report emphasizes that there are over one million web attacks against people each day in 2015, and a new zero-day vulnerability is found every week” (Stanciu, & Tinca, 2017, p. 615). The urgency to bridge the workforce gap is evident. There is a lack of females and minorities in the cybersecurity field. The early stages of cybersecurity workforce development occur in K-12 STEM programs. The number of educational programs, projects, and career enrichment activities during K-12 positively influences students to pursue a cybersecurity-related career.

The Department of Defense Science Board’s report on the cyber task force concluded that United States’ adversaries would far exceed the country’s ability to defend against threats to critical infrastructure (Coulson, Mason, & Nestler, 2018). The United States government lacks a sufficient workforce to combat the continuously growing number of cyber threats in the cyberspace. Cybersecurity education in K-12 is a big part of filling the workforce gap. However, education at post-secondary schools fail to change their curriculum to meet the workforce talent demands. Education programs are placing emphasis on theoretical knowledge. Reading textbooks does not provide skills or prepare students for real-world cybersecurity jobs. Students in high schools should get exposed to different parts of cybersecurity and real-world applications. High schools should use resources provided by the federal government agencies on what to teach about cybersecurity. This provides a guideline on what is currently happening in the cybersecurity field. A gap exists in the literature regarding professional certifications available. A gap is also noted in what is being taught versus what skills actually get used in the workforce (McBride, 2021).

Economic impacts of cybersecurity go far as business or resource downtime causes a lot of damage. Cyberattacks cost U.S organizations millions of dollars annually. "The Ponemon Institute’s 2017 Cost of Data Breach Study showed it takes and an average cost of $2.4 million and an average of 50 days to address a typical malicious insider’s attack, and an average of 23 days to resolve a ransomware attack (6)” (Farahbod, Shayo & Varzavdeh, 2020, p. 65). This goes to show much damage and financial loss a cyber-attack causes. An organization's reputation also gets damaged due to its failure to secure its systems. There is a shortage of cybersecurity talent caused due to the differences in cybersecurity education at different levels. However, McBride asserts Shortages for skilled jobs occur due to the inability to hire and fill (McBride, 2021). Summer camps and competitions help students gain a unique experience and inspire them to pursue the field. Students gain analytical and problem-solving skills during such programs. The education system is not preparing the future cybersecurity workforce with the skills required to start working upon graduation.

Cybersecurity, education, and economics have some differences in opinions or disciplinary bias. Still, all agree on the importance of a curriculum that includes different aspects of cybersecurity and focuses more on real-world applications. The key is ensuring programs are relevant, current, and changing as needed. Graduates are coming out unprepared to meet the expectations of businesses (McBride 2021). Students need to know about professional cybersecurity certifications available and used in the job market. Outreach and extracurricular activities increased motivation in students. Outreach programs can foster confidence in students and inspire them to innovate (Wolf, Burrows, Borowczak, Johnson, Cooley, & Mogenson, 2020). A more inclusive cybersecurity curriculum and education will benefit the cybersecurity workforce. Economic impacts of cyber-attacks can be reduced with a strong, skilled, and prepared workforce.

The cybersecurity workforce development begins during high school, as many students are exposed to STEM fields and get the freedom to explore and learn about various careers that interest them. Better curriculum and outreach programs during K-12 education expose students to real-world cyber applications. The more exposure and experience students get with cybersecurity and related careers in school, the more motivation they get. An applied learning method is best for a field like cybersecurity. In the workforce, practical and hands-on skills are necessary to stop, and combat cyberattacks. Early and focused cyber education will lead to a more inclusive and diverse cyber workforce. Incorporating cyber camps, career enrichment, and other interactive programs into their educational journey will inspire students to pursue and excel in the field. A skilled cyber workforce can combat any attack and keep our data and resources safe. This paper took an interdisciplinary approach to the lack of a talented cybersecurity workforce and answered how a different high school curriculum could attract and retain cyber talent. The ten interdisciplinary steps focused this research on identifying key issues and providing solutions to the problem. A better cybersecurity education will benefit everyone and ensure a strong, skilled cyber workforce is ready to combat any cyber threats.

References

Wolf, S., Burrows, A. C., Borowczak, M., Johnson, M., Cooley, R., & Mogenson, K. (2020). Integrated Outreach: Increasing Engagement in Computer Science and Cybersecurity. *Education Sciences*, *10*(12), 353. <https://doi-org.proxy.lib.odu.edu/10.3390/educsci10120353>

Stanciu, V., & Tinca, A. (2017). Exploring cybercrime – realities and challenges.*Accounting and Management Information Systems, 16*(4), 610-632. http://dx.doi.org/10.24818/jamis.2017.04009

DeCrosta, J. (2021, August). *Bridging the Gap: An Exploration of the Quantitative and Qualitative Factors Influencing the Cybersecurity Workforce Shortage*. ProQuest

Coulson, T., Mason, M., & Nestler, V. (2018). Cyber Capability Planning and the Need for an Expanded Cybersecurity Workforce. *Communications of the IIMA*, *16*(2), 1–11.

McBride, D. Y. (2021). An Analysis of Cybersecurity Curriculum Designs, Workforce Readiness Skills, and Applied Learning Effectiveness (Order No. 28414562). Available from ProQuest Dissertations & Theses Global. (2532559250). <http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/analysis-cybersecurity-curriculum-designs/docview/2532559250/se-2?accountid=12967>

Clough, J. (2011). Cybercrime. Commonwealth Law Bulletin, 37(4), 671-680.

Kamy Farahbod, Conrad Shayo, & Jay Varzandeh. (2020). CYBERSECURITY INDICES AND CYBERCRIME ANNUAL LOSS AND ECONOMIC IMPACTS. Journal of Business and Behavioral Sciences, 32(1), 63-71.

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security, 75(C), 24-35.