International Journal of Information Technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.43.1.8

Bridging the Gap: Aligning Cybersecurity Education with Industry Needs

Oluwatosin Islamiyat Yusuf*

[*]Department of Computer Science, Stephen F. Austin State University, Texas, United States.

Corresponding Email: [*]oluwatosinyusuf85@gmail.com

Received: 28 November 2023 **Accepted:** 14 February 2024 **Published:** 01 April 2024

Abstract: As technology has revolutionized every facet of the world and the rate of cyber-attacks is continuously increasing, the need for cybersecurity professionals has also been on the rise. However, there has been little match between the industry needs and the skills exhibited by the students of cybersecurity. This paper identifies some issues as well as gaps associated with the mismatch between the industry needs and the education pipeline designed to fulfil these needs. The paper also provides recommendations and guides to follow to tailor the cybersecurity curriculum design.

Keywords: Cybersecurity Curriculum, Education.

1. INTRODUCTION

Over the years, as technology is advancing, there has been a huge rise in cyber-attacks. The wide adoption and acceptance of the Internet of Things and Bring Your Device has introduced a lot of security challenges thereby making systems and organizations vulnerable to cyber-attacks. Studies have shown that based on the interdisciplinary nature of cybersecurity, many educational institutions face challenges and issues when designing the cybersecurity curriculum. This is because some institution's curricula are generic and more theoretical than specific and practical. Furthermore, there are cases in which some curricula do not incorporate a cyber training space that captures real-world scenarios. Thereby contributing to the wide skill gap which we have in the cybersecurity industry today. To address this challenge, graduates must be equipped with the right knowledge and skill set that matches with industry needs to produce highly skilled professionals capable of protecting against cyber-attacks and as well as safeguarding corporate assets.

According to cybersecurity ventures, the number of unfilled global cybersecurity jobs levelled off in 2022 and remained at 3.5million in 2023 and is expected to remain through by 2025 with more than 750,000 of those positions in the US [1].

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information Technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.43.1.8

Over the past few years, the cybersecurity curriculum has undergone a significant change. Cybersecurity used to be a set of computer science courses. Today, cybersecurity is a sophisticated and constantly expanding field that is crucial to shielding businesses of all sizes from cyberattacks. The curriculum for training new cybersecurity experts to succeed in the market must expand along with the discipline of cybersecurity. This study explores the literature on cybersecurity curriculum to identify the gaps in the curriculum and proffer solutions to mitigate gaps.

2. RELATED WORKS

Stephanie Redman, Kate Yaxley and Keith Joiner's research on how to enhance undergraduate cybersecurity education through the development and implementation of advanced practical reinforcement laboratories. These laboratories, the study shows, aimed to integrate practice, content, logical reasoning, and interpretation more effectively as part of a broader curriculum and pedagogical reform. The goal was to make cybersecurity more tangible and valued by students, highlighting the significance of well-constructed laboratories in the educational landscape of this emerging field [2]

Student feedback on the new laboratory program indicated substantial improvements in satisfaction and confidence compared to previous setups. Quantitative data from surveys showed increased positive responses and a significant decrease in neutral and negative feedback, demonstrating the program's effectiveness in boosting students' confidence and willingness to engage with cybersecurity topics. However, responses also shifted concerns towards instruction quality, suggesting a need for pedagogical improvements to fully optimize the new program's impact.

The revamped laboratory program incorporated several key elements to foster student engagement and enhance learning outcomes, including focusing on relatable topics, encouraging discussion, aligning with industry frameworks, offering practical hands-on experience, and mapping content to ensure effective concept teaching. These components were designed to address diverse student needs, make the subject matter more accessible, and align educational experiences with real-world applications and industry standards, thereby preparing students for future cybersecurity roles more effectively [2] [3].

Another study also explores the challenges instructors encounter in preparing students for the Security+ Certification exam, emphasizing the knowledge gap between instructors' solid foundation in network and security concepts and students' limited exposure and experience. It also points out the constraint's students face, including their previous knowledge, motivation, study time, and financial resources, which hinder their ability to follow the instructors' practices closely. Additionally, the lack of financial resources compels instructors to adopt labor-intensive methods to gather study materials, like manually compiling free online practice questions into quizzes. The paper underscores the need for instructors to adopt thoughtful and resourceful teaching strategies that incorporate hands-on practice and ongoing assessment to effectively bridge these gaps and prepare students for the exam [4].

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information Technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.43.1.8

3. METHODOLOGY

The research utilizes secondary data sources from numerous journals, periodicals, and databases to answer the research questions. There is a need to critique the existing research on the curriculum of cybersecurity by consolidating the work of existing scholars. Secondary data such as published research works, government reports, industry publications, and periodicals are valuable resources that can generate insight into the status of the cybersecurity curriculum and the loopholes in the curriculum that can be improved upon. This study analyzed the relevant data to draw its conclusion and findings [2].

4. RESULT AND DISCUSION

There is a gap between the industry domain and the education cybersecurity domain as studies revealed that graduates who are produced do not have the technical skills as well as the hands-on skills to tackle the cyber security challenges faced in the real world.
Early researchers on cyber security education conceptualized it from different perspectives. Some researched it from purely industry perspective and practicability; theoretical and educational angle; and lastly, defense and security perspective. These three approaches were the dominant approaches documented in the literature [3] [4].

A. The Industry Approaches

The technological boom and digitization of everyday life have increased the potential of the cybersecurity market. The 2018 Global Risks Report affirms that attacks on businesses have increased exponentially within half a decade turning the hitherto extraordinary events into daily occurrences [5]. These anomalies have a deleterious impact on the global financial system. Some of these cases are related to ransomware with over three hundred thousand computers in more than one hundred and fifty countries being affected with the prominent being the WannaCry attack that cost about three hundred million dollars. The report also highlights the deliberate attack on key infrastructures in strategic sectors leading to catastrophic consequences [5]. This has resulted in the increasing need for experts in the field.
The cybersecurity curriculum not only serves the educational need but also blocks industrial bleeding. The 2023 report of the World Economic Forum on cybersecurity outlook indicates that electronic-based service delivery platforms such as hospitals, electricity, and payment are facing a deficit in terms of cybersecurity experts [6]. The global market requires over three million cybersecurity experts to augment the existing labor force in the field. To further compound the problem, the growth of language modelling AIs, despite its numerous advantages, increased the potential of cyberattacks.
To bridge this gap, some scholars have advocated for a solution such as certification of the existing professionals in the field [2] [4]which in the short term can upskill those in the field. But in the long term, there is a need for a holistic incorporation of modern reality into the cybersecurity curriculum of institutions of higher education. This is Germane because the need for certification arises primarily because of the quality of education received by those on the field at the institution. [4] argued that most institutions teaching cybersecurity failed to meet the ABET standard in their curriculum.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information Technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.43.1.8

No doubt, many institutions globally have incorporated cybersecurity curricula in their programs. An example is the University of Maryland, and the University of Oxford, to mention but a few with courses such as Master of Professional Studies in Cybersecurity and similar others that are recognized globally.

The biggest lacuna in the industry perspective of the cybersecurity curriculum lies in the mismatch between industry needs and educational output. Most graduates lack the required skills to make a meaningful impact in the industry. A conscious decision must be made by the educational institution to prepare graduates ready for the job market. Emphasis has been laid on the theoretical angle of the course jettisoning the practical aspect that can match industry needs. The industry expects ready-work graduates with minimal supervision. The cybersecurity curriculum must factor in the need of industry to bridge this gap. Considering the industry requirement, the cybersecurity curriculum should be unbundled with major specializations focusing on specific areas of interest to the industry [7].

B. The Educational Institution Perspective

At the heart of the debate on cybersecurity curriculum design needs lies the centrality of the role of educational institutions and their nature of training. Yes, the industry might dictate the labor market requirement but what better way to measure the qualification of a recruit than through the class of degree earned? A study investigated this phenomenon and found that the majority (84%) of recruiters in the role of cybersecurity look for people with degrees [8]. This buttresses the fact that beyond any other professional certifications, earning a university Degree is the benchmark for recruitment. What then is the fate of graduates going into the labor market if the Universities' curricula are not designed to prepare them for the job market?

The solution is multimodal. Some universities have incorporated certification courses into their curriculum. Certifications such as CEH, CISM, CISSP, and CISA have been incorporated into cybersecurity curricula to help prepare graduates for the job market [9]. There have also been efforts globally to enhance cybersecurity education. This gave birth to the United States Cybersecurity Enhancement Act of 2014, which was amended in August 2022. Before that, the National Initiative for Cybersecurity Education (NICE) was established in 2010. NICE is a global cybersecurity education initiative that aims to provide a common language and standard for cybersecurity curriculum design. The framework outlines a set of cybersecurity work roles, knowledge, skills, and abilities required for each role, and suggested training and certification requirements for each role [10]. These are all in a bid to promote cybersecurity literacy. Europe formulated The European Union Agency for Cybersecurity popularly known as ENISA to address this brain definite on the continent. All these agencies and policies were created to promote and enhance cybersecurity education and training to build the capacity and competence of the new entrants into the workforce.

In a bid to standardize the cybersecurity curriculum, the International Organization for Standardization's strive to "provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information Technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.43.1.8

infrastructure protection (CIIP)" [11]. The ISO also addresses the model security practice for professionals in the field. This covers "an overview of Cybersecurity, an explanation of the relationship between Cybersecurity and other types of security, a definition of stakeholders and a description of their roles in Cybersecurity, guidance for addressing common Cybersecurity issues, and a framework to enable stakeholders to collaborate on resolving Cybersecurity issues." [11]

In Africa, the Malabo Convention of 2014 signals the readiness of the African Union to also tackle the challenges of cybersecurity. The purpose of this was to develop a legal framework for cybersecurity and data protection in Africa. The resolution suffered so many setbacks until 2021 when implementation began in earnest [12]. The debate about whether the policy has translated to meaningful progress is still ongoing.

Many solutions have been proffered towards better ways of ensuring educational institutions provide the needed skills to students. One study shows that mentorship and internship programs have shown a tremendous improvement in the skills of the students [13]. Others also identified a lack of communication skills among graduates of cybersecurity which is fundamental in the corporate world [14]. This also speaks to the fact raised earlier about the need for industry and academic collaboration. This will go a long way in mitigating the challenges in the curriculum of many institutions. A commendable example is the collaboration between Texas A&M University and the business community where students are trained, and professionals retrained through certification [15]. This partnership provides students with first-hand experience of scenarios of the job environment and how to blind into the corporate working environment.
For universities to design a cybersecurity curriculum in tandem with global best practices and churn out graduates ready for the labor market, there is a need for the incorporation of ABET and ISO/IEC 27032:2012 standardized certification courses, provision of real-world practical experiences, adoption of experiential learning. Aside from the curriculum, the human and material angles should also be addressed. Relevant equipment and textbooks, adequate funding and support, industry-experienced faculty, and upskilling of faculty are sacrosanct.

Technical knowledge, communication skills, and business skills, among others, should form the core of the cybersecurity curriculum so that graduates will be able to address real-world risks and security threats. Knowledge of the IT infrastructure, computer crimes, forensics, networks, and security and embracing a multidisciplinary approach will go a long way.

C. The Defense and Security Perspective

The Defense and Security Perspective

Exploring the cybersecurity curriculum design from a national security or defense perspective is primarily tailored toward designing the curriculum in such a way that the education system churns out graduates with strong technical knowledge of IT infrastructure, problem-solving, and analytic skills, critical thinking, and the capacity to operate and manage complex networks and security apparatus. Understanding the ethicality and legal implications of their professions is also sacrosanct. That explains why the US government left no stone unturned [16]. This response led to the establishment of NICE. The Department of Homeland Security (DHS) also

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information Technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.43.1.8

set up the Cyber Skills Task Force, a joint operation involving government officials and industry experts. Although they worked separately to map out pathways for the government, none of their recommendations proved to be actionable in the education sector [16] [4].
However, another effort yielded profit through the NSA initiative with later collaboration with DHS. This gave birth to the Centers for Academic Excellence in Information Assurance Education (CAEIAE). CAEIAE "established criteria for two-year institutions, four-year institutions, and research schools. Currently, the NSA is leading an effort to revamp and modernize its curriculum-based approach to the CAE program [16].
Furthermore [17] [18]analyzed the educational needs of the DHS staff. The study intends to find out the right academic course to be offered by undergraduate students. Terrorism and Fundamentals of Homeland Security were the two courses chosen by the staff to form the core of the curriculum. General education courses, including Critical Thinking/Analytical Skills, Ethics, Technical Writing, English Composition, and Informational and Oral Communication were also considered important.

No doubt, the quality of the cybersecurity curriculum has an impact on the overall national security architecture of a country. For a country so invested in its national security, being subjected to cyberattacks and readiness to combat such attacks are non-negotiable. Therefore, the curriculum must cover not only IT skills but also be a multidisciplinary curriculum inculcating topics such as communication skills, psychology, management, business analytics, etc. Early detection of risks, vulnerabilities, breaches, and possible ways to tackle them should be at the front burner of the curriculum. National security also involves ethical and legal issues, all these must be mainstreamed into the curriculum. The cybersecurity curriculum must be multi-faceted and train students in courses beyond IT skills [19].

D. The Future Outlook

Several studies have highlighted the need for cybersecurity education [13] [7]. These studies were carried out in different contexts and curriculums of different universities. The dominant direction of the literature regarding the status of cybersecurity curriculum has improved from its state over a decade ago when [2]argued that cybersecurity curricula are generally theoretical based. Even [13] also advocated for the incorporation [15] [3]of hands-on application, ethical training, and instructor-led peer discussion to further fast-track the actualization of industry needs.

5. CONCLUSION

There is a need to align the cybersecurity curriculum with industry needs to fill the massive job roles available as well as produce graduates who are highly skilled to meet the industry's needs. The current state of cybersecurity curriculum design varies widely between educational institutions. Some institutions offer cybersecurity programs that are narrowly focused on technical skills, while others incorporate a broader range of topics such as policy, risk management, and governance. However, there is a consensus among cybersecurity educators that cybersecurity education should not only focus on technical skills but also emphasize the importance of critical thinking, communication, and collaboration. This is because

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information Technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.43.1.8

cybersecurity professionals must not only have technical expertise but also be able to work in teams and communicate effectively with stakeholders.

Recommendation

Ensuring that the education pipeline agrees with the industry needs will help to enhance students' opportunities at the end of their education as graduate students can fit in properly into the industrial environments with the right practical as well as technical skills. Below are a few recommendations that can be considered when designing the cybersecurity curriculum, as this will help the gap.

1. Cybersecurity curriculum design should be multidisciplinary in approach to improve soft skills for graduates.
2. Adequate funding should be provided for research and infrastructure to ease the actualization of curriculum goals. There should be a mentorship program designed to aid students in transit fully into the labor market.
3. Faculty members should be retrained and upskilled to improve and sharpen their knowledge as the hackers are continuously advancing their skills.
4. The cybersecurity curriculum should be designed in a way that students are exposed to the right branch of cybersecurity they want to concentrate on and get exposed to those practical skills as well as theoretical) on time.
5. There should be partnerships between education institutions, industry experts, as well as government standard bodies such as the National Institute of Standards and Technology. NIST frameworks, National Institute for Cybersecurity Education (NICE) to tailor the curriculum in ways that best match industrial needs.

6. REFERENCES

1. Steve Morgan, "Official Annual Cybercrime Report," Herjavec Group, 2023.
2. T. Smith, A. Koohang and R. Behling, "Formulating an Effective Cybersecurity curriculum," Issues in Information Systems, vol. xi, pp. 410-416, 2010.
3. H. Santos, T. Pereira and I. Mendes, "Challenges and reflections in designing Cyber security curriculum," in IEEE World Engineering Education Conference (EDUNINE), Santos, Brazil, 2017.
4. D. Mouheb, S. Abbas and M. Merabti, Cyberecurity Curriculum Design, Transactions on Edutainment, 2019.
5. "World Economic Forum," The Global Risks Report, Geneva, Switzerland, 2018.
6. "World Economic Forum," The Growth Summit 2023, 2023.
7. A. Bicak, X. M. Liu and D. Murphy, "Cybersecurity curriculum development: Introducing specialties in a graduate program. Information Systems Education Journal," Information Systems Education Journal, vol. vol 13, pp. 99-110, 2015.
8. J. Marquardson and A. Elnoshokaty, "Skills, Certifications, or Degrees: What Companies Demand for Entry-Level Cybersecurity Jobs," Information Systems Education Journal, vol. 18, no. 1, pp. 22-28, 2020.
9. K. J. Knapp, C. Maurer and M. Plachikinova, "Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance," Journal of Information Systems Education (JISE), vol. 28, pp. 101-114, 2017.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information Technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 03, April-May 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.43.1.8

10. National Institute of Standards and Technology, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," NIST Special Publication, 2020.
11. International Organization for Standardization, "Information technology - Security techniques - Guidelines for cybersecurity education," 2012.
12. A. UNION, African Union Convention on Cyber Security and Personal Data Protection, Ethiopia, 2021.
13. M. Erickson and P. Kim, "Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning," International Association for Computer Information Systems, vol. 22, no. 4, pp. 9-20, 2021.
14. N. S. Clair and J. Girard, "Judging Competencies in Recent Cybersecurity Graduates," vol. 8, 2020.
15. J. K. Nelson and B. L. Donham, "Partnership to Prepare Students for Careers in the Emerging Field of Cybersecurity," in ASEE Virtual Annual Conference, 2020.
16. W. A. Conklin, R. E. Cline and T. Roosa, "Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors," in 47th Hawaii International Conference on System Science, 2014.
17. C. D. Ramirez and G. A. Rioux, "Advancing curricula development for homeland security education through a survey of DHS personnel," Journal of Homeland Security Education, vol. 6, 2012.
18. A. Siraj, B. Taylor, S. Kaza and S. Ghafoor, "Integrating security in the computer science curriculum," Association for computing machinery, vol. Vol 6, no. 2, pp. 77-81, 2015.
19. I. W. Trabelsi Zouheir, "A Hands-on Approach for Teaching Denial of Service Attacks: A Case Study," Journal of Information Technology Education: Innovations in Practice, 2013.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)