UVA CS Department Cybersecurity Focal Path: A Different Approach

A Technical Report submitted to the Department of Computer Science

Presented to the Faulty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

Yazmeen Younus Imam

Spring 2024

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Rosanne Vrugtman, Department of Computer Science

UVA CS Department Cybersecurity Focal Path: A Different Approach

CS4991 Capstone Report, 2024

Yazmeen Imam
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
yyi2yeu@virginia.edu

ABSTRACT

The University of Virginia (UVA) Computer Science (CS) Department has one focal path CS students can take: the National Center of Academic Excellence in Cyber Defense (NCAE-CD) Cybersecurity Focal Path at UVA. Cybersecurity is a great and important field and the students learning it need to feel prepared for their future work to protect everyone's data and privacy. The Cybersecurity Focal Path at UVA feels underdeveloped and insufficient. I have explored gaps within the existing Cybersecurity Focal Path that inadequately prepares students for the workforce after graduation and for the emerging threats in the cybersecurity field. After completing the Focal Path myself, I propose a solution that includes the integration of advanced courses on cybersecurity trends, hands-on labs with real-world simulations, and collaborations with industry companies to ensure the curriculum's relevance and comprehensiveness. The method includes a comprehensive curriculum review compared to other universities' curriculum, a review of the CS department's lack of concentrations as a whole, and the addition of feedback mechanisms from alumni to address any emerging gaps. Anticipated outcomes include a marked improvement in student preparedness for cybersecurity roles, a higher rate of post-graduation employment in the field, and a review feedback loop for ongoing curriculum improvement. Future work will concentrate on reviewing the impact of these changes, identifying areas for further improvement, and exploring opportunities for expanding the concentration to meet emerging cybersecurity needs.

1. INTRODUCTION

Cybersecurity was created out of necessity, as it safeguards people and organizations against cyber attacks and theft or loss of sensitive and private information. As the internet and private information become even more integral to modern society, there is a higher demand for skilled cybersecurity professionals. This demand means that academic institutions play a critical role in preparing the next generation of experts who will defend against cyber threats. However, with the speed at which the cybersecurity field changes, educational programs have trouble keeping up, especially in higher education. These programs must not only teach foundational knowledge but also adapt to reflect the current and future challenges in cybersecurity.

Because of this, colleges and universities play a key role. Like UVA, they offer specialized concentrations or course paths in cybersecurity in their departments. UVA's Cybersecurity Focal Path is comprised of ten cybersecurity courses that a Computer Science major can take that, once completed, award the student with a Letter of

Completion. This Focal Path does not effectively equip students with the requisite skills and knowledge to navigate the cybersecurity field. As a student in the Focal Path, I do not know how to use what I have learned in my courses in real life applications at companies or other organizations. Students who complete the Focal Path do not feel well prepared enough for the jobs they can get after graduation, having to learn more on the job, rather than in classes. To address this, there would have to be curriculum updates and incorporation of real-world applications to align coursework with industry standards.

2. RELATED WORKS

UVA's Computer Science Department has a website of the NCAE-CD Cybersecurity Focal Path. This document provides UVA's explanation and guidelines for the courses needed and how to apply for the completion of the focal path. This website explains where the Focal Path is from, its learning outcomes, the required courses, and the form to obtain the Letter of Completion. It is a simple course lineup that has no barrier to entry for a Computer Science major that teaches the fundamentals and principles of cybersecurity.

Towhidi and Pridmore (2023) provide an approach to curriculum redesign in higher education that addresses the global cybersecurity talent shortage. Their model is based on a backwards course design set to align with industry standards to show the importance of adaptive educational programs. This is important, so students will be well prepared and meet evolving industry demands.

3. PROPOSAL DESIGN

UVA's Cybersecurity Focal Path currently does not adequately prepare students for the ever changing field of cybersecurity. While this path is a good foundational guide for students interested in pursuing cybersecurity as a career, there is a big difference between the class curriculum's theoretics and the job applications and practicality. As a student in the current Focal Path, I have observed how this path structure is limiting for students. I do not know how to use what I have learned in my courses in real life applications at companies or other organizations. Also, there is not enough guidance about what to do with the Certification of Completion. Students would be better off with a full-fledged concentration. The UVA CS department should transform this focal path into a dedicated concentration.

3.1 Curriculum Enhancement

The UVA Cybersecurity Focal Path curriculum now consists of courses such as Introduction to Cybersecurity, Computer Networks, Defense against the Dark Arts, and Database Systems. These are great, informative classes, but they fail to equip students with skills and knowledge for real-life applications and jobs. From my personal experience, I felt this gap between class teachings and its real-world application. Towhidi and Pridmore (2023) introduce a model that emphasizes the integration of advanced courses, real-world simulations, and partnerships with industry leaders to prepare students for cybersecurity careers effectively which I have used to design curriculum changes.

To help resolve the current issues, I propose the following courses: Cybersecurity Ethics, Cybersecurity in Government, Hands-on Cybersecurity Labs, and Emerging Technologies in Cybersecurity. Cybersecurity Ethics will address the complex legal and ethical issues surrounding cybersecurity, preparing students about the moral means of security. The Cybersecurity in Government course will go into the cybersecurity policies within the US

government. This course will cover how government policies are changing the field of cybersecurity and vice versa. Hands-on Cybersecurity Labs are practical labs that will simulate real-world cybersecurity challenges, allowing students to apply theoretical knowledge in industry situations. Emerging Technologies in Cybersecurity will be a course focused on new technologies such as AI, quantum computing, and blockchain, exploring how they affect and revolutionize cybersecurity. These proposed courses would offer a more comprehensive and practical education in cybersecurity.

3.2 Adding Hands-on Labs and Real-world Simulations

Hands-on Labs and real-world simulations will provide students with the practical experience essential for understanding the complexities of cybersecurity. These exercises show students what to expect in the cybersecurity field, especially in topics where the traditional classroom instruction inadequately prepares students. These hands-on labs will include case studies, company and employee reviews, and examining current security threats. This will allow students to apply their learning in these practical scenarios.

The real-world simulations will be of current cybersecurity challenges, giving students the opportunity to test and refine their skills in a controlled, realistic assessment. Other hands-on approaches include collaborating with Industry partners. Partnerships with leading cybersecurity firms will bring direct interaction between students and professionals. This will be a great time for students to gain insights into current practices and emerging technologies and to understand what jobs are like in the cybersecurity field.

3.3 Comprehensive Curriculum Review and Feedback

An ongoing review and feedback mechanism would be important to implement to continuously improve the curriculum. Feedback from alumni, industry partners, and current students will be essential to making the program as well-suited as possible for both students and professors. This approach aims not only to update the curriculum but also to instill a culture of continuous improvement. Additionally, benchmarking against other universities' curriculum and consulting with cybersecurity experts will ensure UVA's program exceeds cybersecurity academic and industry standards.

4. EXPECTED RESULTS

These proposed changes to the Cybersecurity Focal Path at UVA are expected to significantly improve the quality of cybersecurity education and prepare graduates more effectively for future jobs in the field. The introduction of advanced courses and immersive labs should result in a more engaged learning experience and promote a deeper understanding of cybersecurity principles in their application, rather than just in theory.

Also, having continuous feedback from industry partners, alumni, and current students will ensure the program is responsive to the evolving demands of the cybersecurity field. This process is not only proposed to enhance the Cybersecurity Focal Path but also to lay the groundwork for future curriculum evaluations across other sectors within the CS department. The success of these reforms could lead to the development of additional concentrations in the major, addressing emerging areas in IT and enriching student learning at UVA.

5. CONCLUSION

The proposed improvements to the Cybersecurity Focal Path at UVA are expected to transform the current educational program for students pursuing careers in

cybersecurity. From my own experiences within the CS department's existing program and informed by models of Towhidi and Pridmore, I present a proposal designed to ease the issue that the current curriculum presents: the lack of practical application in the classroom. By integrating advanced courses, including Hands-on Cybersecurity Labs and Cybersecurity Ethics, the curriculum will provide a more rounded education that is also more industry-relevant. Real-world simulations and hands-on labs, in collaboration with industry leaders, will ensure that students not only learn but also know how to apply their knowledge in contexts mirroring the challenges they will face in their professional jobs.

Establishing a feedback loop to allow the proposed program to grow and change in the future will help those who most benefit from it: the students. This mechanism promises a dynamic program that can adapt to the rapidly evolving field of cybersecurity, which will ensure the students are getting the best education for their futures.

Anticipated results from these proposed changes include not only improved educational topics and better-prepared graduates but also a potential model for larger curriculum changes within the CS department. If these reforms succeed, they can contribute to the field of cybersecurity as a whole by preparing graduates to become capable of defending against emerging threats and safeguarding our personal data. This proposal, while rooted in the specific context of UVA, offers valuable insights and a template for curriculum development that could also influence cybersecurity education in other universities.

6. FUTURE WORK

The future work will focus on creating new syllabi for the proposed classes, comprising data and reviews on how the proposed changes will be beneficial to new graduates, and also creating and cross referencing other universities' curricula to model these changes after. These are the first steps for this proposal, as it will create the foundation for the proposed changes in UVA's Cybersecurity Focal Path.

REFERENCES

University of Virginia. Department of Computer Science Cybersecurity Focal Path. Cyber Innovation at Virginia. https://cyberinnovation.virginia.edu/department-computer-science-cybersecurity-focal-path

Towhidi, G., & Pridmore, J. (2023, January 1). Aligning Cybersecurity in Higher Education with Industry Needs. Journal of Information Systems Education, 34(1), 70 - 83.