Preparing CS Students for the Future: How Can a Required Cyber Security Course Better Prepare Undergraduate CS Students

CS4991 Capstone Report, 2024

Aaron Alem
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
ata8w@virginia.edu

ABSTRACT

With an estimated $10 billion lost yearly due to cyber attacks, cybersecurity has become an important issue in the United States. However, it seems that workers are not adept when it comes to this. To combat this, cyber security needs to become more prominent in computer science education. I recommend that a new cybersecurity training course be required as a part of the UVA Computer Science (CS) curriculum. In it, students would learn the basics of cybersecurity such as phishing awareness, securing sensitive information, etc. This would enable students to gain a better understanding of threats and the skills needed to create safer software. To do so, a new syllabus must be developed and data should be collected from the students to determine the effectiveness of the new course.

1. INTRODUCTION

With the rising threats of cyber attacks and the increasing amount of personal data being stored online, the importance of cyber security has only increased in recent years. With this growing challenge it is important that students at UVA are properly equipped with the skills to combat this threat. However, the current UVA CS curriculum does not require students to gain experience in his field. This means many future employees are susceptible to common cyber security attacks. A significant number of organizations that require handling sensitive information do not provide cyber security training for their employees. For the ones that do, many employees forget their training and leave their organization open to potential breaches. This makes it all the more important that CS students are exposed to cyber security training in school, while they are still learning.

2. RELATED WORKS

Dupuis (2017) explored the idea of requiring a cybersecurity introductory course for non-technical majors. He identifies the importance of "educating the masses" on cybersecurity, as he sees how it affects everybody. As Dupuis sees it, even people at home engaging in online behavior poses a cybersecurity risk as they do not have the knowledge or skills necessary to stay safe online. In his proposed course, students would learn technical topics like components of computer networking, cryptography, and encryption while also learning about more general ideas like the concept of privacy, and the risks and benefits of social networks. Dupuis strives to provide foundational knowledge in technical concepts without straying too far from the big picture of why cyber security and privacy are important to the students. To do so, no more than 3 class sessions are spent on any one topic. Instructional methods mainly consist of lectures and videos with activities, assignments and projects to help keep students engaged. Additionally, Dupuis examined the proposed course in the context of Bloom's taxonomy which is a set of learning outcomes that students set for their students. Dupuis

lastly explores the benefits of such a course to stakeholders. He explains how this type of course can benefit schools as it introduces students into cyber security topics. This can end up bringing more women into STEM majors. Additionally, more people being educated in cyber security generally benefits society as these people are less likely to be a security risk for organizations.

Ahmad, et al. (2022) also looked to implement cybersecurity education, but this time for all levels of education. With the rise of social networking sites, more personal information is being shared at a global scale. This has opened the possibility of people being impacted socially and financially by bad faith actors. Additionally there has been a huge increase in internet-based systems in people's homes, leading to growth in security vulnerabilities. Ahmad, et al. observed that most computer- and security-related programs in universities are mostly technical and require some background in computer science. They believe the study of cybersecurity should contain three main topics: 1) the day-to-day functioning of the information security task; 2) the management of the cybersecurity function; and 3) the transfer of knowledge to cybersecurity professionals and users. In the proposed courses, Ahmad, et al. are attempting to do the third topic, transfer knowledge to cybersecurity professionals and users. In this transfer of knowledge to the users, they want to teach students to assess risk and protect their information. To do so, they believe that students should be exposed to this information throughout all their years of school so they will be comfortable in dealing with cyberthreats.

3. PROPOSAL DESIGN

The first step in creating a new cyber security course would be to design the curriculum. As this course would be designed as an introduction to cybersecurity to teach students online security, topics will be discussed more generally. This course will be split into five main sections, each covering a different topic: Malware, Web Security/Networks, Cryptography, Ethics, Forensics, and Human Factors.

The “Malware” section will cover how to identify and differentiate between different types of malware (viruses, worms, trojans, etc.) Additionally this section will discuss what each type of malware does and what to do in response if encountered. The “Web Security/Networks” section will discuss the basics of computer networks and basic network security (firewalls, Wi-Fi encryption). Different types of web vulnerabilities should also be discussed, such as SQL injection attacks, cross site scripting, and cross site request forgery. The “Cryptography” section of this course will teach students what encryption is and different types of encryption such as hashing, and RSA. The “Ethics” section will discuss some of the ethical problems and dilemmas one might face when it comes to cybersecurity. Students will be taught different ethical frameworks and ideas so when put in tough situations in the future they will have a better understanding of what to do. The “Forensics” section will look at the history and different techniques used in digital forensics. Students will be able to learn and use some of the different digital forensics tools often used. Last, in the “Human Factor” section, students will explore how human behavior and psychology affect cybersecurity. Students will learn how to take the perspective of a threat and a defender so in the future they will be prepared to most effectively counteract the threat.

The proposed course will be ordered as shown in Figure 1 with each topic taking two to three weeks to complete. Similar to the cybersecurity courses currently offered at UVA, no textbook will be assigned, as

information on cybersecurity is constantly changing. This course will be taught through weekly lectures from the professor with weekly projects to supplement the lectures. Additionally a quiz will be held at the end of each section to assess students' comprehension of the material.

Week Number	Course Topic
1	Unit 1: Human Factors
2	Unit 1: Human Factors
3	Unit 2: Ethics
4	Unit 2: Ethics
5	Unit 3: Malware
6	Unit 3: Malware
7	Unit 3: Malware
8	Unit 4:Web Security/Networks
9	Unit 4:Web Security/Networks
10	Unit 4:Web Security/Networks
11	Unit 5: Cryptography
12	Unit 5: Cryptography
13	Unit 6: Forensics
14	Unit 6: Forensics

Figure 1: Schedule of Course Topics

4. ANTICIPATED RESULTS

With CS students required to take a cyber security course, we should expect to see an increase in the awareness of students. As students are more educated on potential cyber risks, they are less vulnerable to security risks. Additionally we should expect to see students form better habits and participate in better practices that create safer software.

Since students are more aware of all the different ways hackers can take advantage of vulnerabilities in their software, students will put more effort into making safer software. Additionally, students will be more knowledgeable about what to do if a cyber attack does happen. This will greatly help students in their future endeavors as they will be able to save companies more money if a security breach is to occur.

5. CONCLUSION

Cybersecurity is a very important part of CS regardless of what field students choose to go into. As this course is not too focused on going in depth on the technical side of many of these topics, students will be able to get a good broad understanding of cybersecurity in general. A required cybersecurity course will not only make students more secure online, but it will also enhance their skills, making them better computer scientists, giving UVA CS students an advantage for the future.

6. FUTURE WORK

In order to create this new course, it would need to be proposed to and reviewed by the CS program in addition to a committee in charge of reviewing all undergraduate and graduate curricular proposals. This proposal must contain a CCI form, syllabus of the course requirements, a schedule that lays out all work and activities assigned by the course, and a Core Competencies form. After this is done, should this course come into existence it would need to be tested. Attempting to get heavy student feedback the first few times the course is taught will be very important to help improve the effectiveness of this course.

REFERENCES

Dupuis, M. J. (2017). *Cyber Security for Everyone: An Introductory Course for Non-Technical Majors. 2017*(1), 3.

Ahmad, N., Laplante, P., Defranco, J., & Kassab, M. H. (2021). A Cybersecurity Educated Community. *IEEE Transactions on Emerging Topics in Computing*, 10(3), 1456-1463. https://doi.org/10.1109/tetc.2021.3093444