Instilling Cybersecurity Professional Skills in Undergraduate Computing Students

Dr. Rajendran Swamidurai, Alabama State University

Dr. Rajendran Swamidurai is a Professor and Coordinator of Computer Science at Alabama State University. He received his BE in 1992 and ME in 1998 from the University of Madras, and PhD in Computer Science and Software Engineering from Auburn University in 2009.

Dr. Uma Kannan, Alabama State University

Dr. Uma Kannan is Associate Professor of Computer Science at Alabama State University, where she has taught since 2017. She received her Ph.D. degree in cybersecurity from Auburn University in 2017.

Instilling Cybersecurity Professional Skills in Undergraduate Computing Students

Abstract

Cyberspace and the Internet provide the backbone of any country's modern economy and national security. In 2024, there are approximately 400 million small businesses worldwide, with 33.3 million in the United States and 1.29 million in Canada. This represents over 99.8% of all businesses in both nations. Because of the COVID-19 pandemic, all companies had to go online and must now adapt to the "always-on" world in order to stay connected with their customers. These businesses cannot be successful until their customers possess confidence in the security of their web applications. Cyberattacks are increasing at an alarming rate every year. Reports are indicating that the cost of cybercrime may rise to $23 trillion by 2027. It is crucial to employ the right cybersecurity personnel with knowledge and abilities to protect the nation's critical infrastructures, such as its energy, communication, water, food, and healthcare. But the public and private sectors are facing a substantial challenge in acquiring a sufficient number of skilled security personnel, and the cybersecurity workforce gap is increasing by 19% every year. In order to deliver the next generation of cybersecurity professionals for entry-level and junior-level positions, we modified our undergraduate computing curriculum by infusing cybersecurity modules from Fall 2020 to Spring 2024 that include those that focus on cybersecurity professional skills. Our external evaluation data shows that students demonstrated particular confidence in their ability to solve problems, persevere in seeking solutions, and acquire knowledge in cybersecurity. They also expressed confidence that they will be able to understand what they learn about cybersecurity.

1. Introduction

Cyberspace and the Internet serve as the foundation of any country's modern economy and national security since they have become part of the country's homeland, much like cities, mountains, and coastlines, and practically all of our daily activities, such as shopping and banking, take place in cyberspace [1]. Because a breach or attack will inflict severe financial loss on its stakeholders, which can range from national governments to small enterprises and individuals, cybersecurity is an essential component in the process of preserving a nation's economic and financial stability [2].

Cyberattacks are increasing in frequency and severity at an alarming rate. During a U.S. Senate hearing in March 2013, leading intelligence officials cautioned that "in the future, the cyber threat will be the paramount threat to the nation," surpassing terrorism [3, 4]. This assertion was reiterated in a 2019 survey of 200 global CEOs and 100 senior investors of billion dollars or more conducted by management consultancy EY [2, 5]. The U.S. Agency for International Development Assessment indicates that the cost of cybercrime is $8 trillion in 2023 and may rise to $23 trillion by 2027 [2].

Barracuda Networks, a cloud security company, conducted a year-long study in 2021 that revealed small businesses with fewer than 100 employees are three times more likely to be targeted by cybercriminals than their larger counterparts [6]. The U.S. Agency for International Development Assessment indicates that within six months of being subjected to a cyber attack,

as many as sixty percent of micro, small, and medium-sized enterprises (MSMEs) go out of business [2]. MSMEs are the backbone of all economies, including developed countries such as the US and Canada. In 2024, there are approximately 400 million small businesses worldwide, with 33.3 million in the United States and 1.29 million in Canada. This represents over 99.8% of all businesses in both nations [7, 8]. Because of the COVID-19 pandemic, all companies had to go online and must now adapt to the "always-on" world in order to stay connected with their customers [9]. These businesses cannot be successful until their customers possess confidence in the security of their web applications.

It is crucial to employ the right cybersecurity personnel with knowledge and abilities to protect the nation's critical infrastructures, such as its energy, communication, water, food, and healthcare. But the public and private sectors are facing a substantial challenge in acquiring a sufficient number of skilled security personnel. The first look at the ISC2 cybersecurity workforce study 2024 [10] reveals that the size of the cybersecurity workforce gap in 2023 was 4 million, and in 2024 it is 4.8 million globally, an increase of 19% every year.

In order to deliver the next generation of cybersecurity professionals for entry-level and junior-level positions, with the support of the US National Science Foundation, we modified our undergraduate computing curriculum by infusing cybersecurity modules from Fall 2020 to Spring 2024 that include those that focus on cybersecurity professional skills. The cybersecurity-infused courses are Networking Fundamentals, Information Security, Data Communication and Networking, Introduction to Operating Systems, Software Engineering, and Special Topics (Digital Forensics).

2. Infusing Cybersecurity Skills in UG Computing Curricula

Due to the complexity of cybersecurity, the curriculum for cybersecurity needs to place an emphasis on how to apply security concepts to a wide variety of computer science courses. These classes need to cover a wide range of topics, including but not limited to: software engineering, web development, database administration, safe coding, operating systems, low-level programming, computer literacy, cryptography, and networking. [11-18]

To facilitate active learning, we segmented the cyberattacks and defenses training course modules into two parts. The first part focuses on the theoretical and conceptual foundations of the methodologies examined, whereas the subsequent phase entails practical experimentation. From Spring 2019 to Spring 2021, we included cybersecurity principles into the following courses: CSC315 Data Communication and Networking, CIS310 Networking Fundamentals, CIS341 Information Security, CSC414 Introduction to Operating Systems, and CSC280 Software Engineering. In the spring of 2021, we presented the generated course modules and laboratory experiments to an external curriculum advisory committee, received their feedback, revised the courses, and implemented the revised courses beginning in the academic year 2021/22.

Beginning in Fall 2021, we will offer a new course each Fall semester, CSC 491 Special Topics (Information Security and Digital Forensics), derived from the curriculum revised in summer 2021.

In Spring 2022, we created two new security course modules: Operating Systems Security and Network Operating Systems Security, which were subsequently integrated into CSC 414 Operating Systems and CSC 315 Data Communication and Networking courses, respectively. Following the course's deployment, the external evaluator obtains feedback from the students through surveys and the findings are presented in the results section below.

Data Communication and Networking: It is absolutely necessary to have a solid understanding of the principles of data communication and computer networks in order to be able to establish network security. The objective of the modules added to this existing course is to place an emphasis on developing an understanding of the essential concepts that are required to comprehend computer attacks and defenses from the point of view of a network. The topics that are essential for network and cybersecurity such as network protocols and standards, network commands that are widely used in network and cyber security, and network simulation using GNS3 were introduced in this course.

Operating Systems: This course covered a variety of security principles and provided clarification on the many approaches that may be used to protect the operating system from potential dangers. In this course, the students learned about the following topics: 1) command line usage (both Linux and DOS), 2) common administrative functions using Microsoft PowerShell, 3) system security, 4) threats to both the system and the network, 5) the use of cryptography as a security measure, 6) the implementation of security defenses, which includes security policy, vulnerability assessment, intrusion detection, virus protection, auditing, accounting, and logging, 7) methods to harden an operating system (either Windows or Linux), 8) firewalling, and 9) practical experiments that make use of operating system tools for security purposes.

Information Security: This course emphasizes the integration of information technology aspects pertinent to network and application layer security, while providing students the opportunity to obtain Security+ certification and/or Certified Ethical Hacker (CEH) certification. This revised course encompasses topics included in the Security+ and CEH examinations. Included are network scanning, denial-of-service attacks, SQL injection, cryptography, penetration testing, threat management, identity management, identification and mitigation of security risks, and network access control.

Digital Forensics: This course covers topics such as hashing and validations, data erasure, file carving, file signatures, slack space, string search, regular expressions, forensic discovery, analyzing system times, file system analysis, systems and subversion, deleted file system persistence, and system processes. This course leveraged topics typically found in ISC2 (Association for Inspiring a Safe and Secure Cyber World)’s CHFI (Certified Hacking Forensics Investigator).

3. Results

This result summarizes feedback from student surveys taken in the Spring 2022 and again in the Spring 2023 semesters. Information was gathered about the types of students, the coursework they had completed and were still working on, their persistence, their 21st-century skills, how they thought the course went, and how ready they felt for a career.

Project Objectives: Students were asked to indicate the extent to which they agreed with each of the following statements related to the project goals and objectives. Overall, responses were positive with the overall scale averaging 4.03 in 2022 and 3.79 in 2023. Students most strongly believed that their experiences at ASU enhanced their problem-solving skills (M=4.25 in 2022 and M=4.0 in 2023) and they became more competent in developing working solutions to defend cyberspace and computer networks (M=4.17 in 2022 and M=4.0 in 2023).

	Spring 2022		Spring 2023	
	Mean	**SD**	**Mean**	**SD**
I am well-versed in the practical elements of cybersecurity to be attractive to potential employers	4.08	.900	3.75	.965
Through my experiences at ASU, I am being exposed to cybersecurity practices regularly used in industry.	4.00	1.044	3.83	1.115
My experiences at ASU are enhancing my problem-solving skills.	4.25	.754	4.00	.739
I am becoming more competent in developing working solutions to defend cyberspace and computer networks.	4.17	.835	4.00	.739
The cyber range has been a valuable asset in my cybersecurity training.	4.00	.953	4.08	.793
The cybersecurity course/modules have helped me acquire critical concepts and industry skills.	4.08	.900	3.92	.793
I am being well-prepared for the cybersecurity certification examination (e.g. Security+ and/or Certified Safe Hacker)	3.83	1.193	3.67	.985
I believe that I am prepared to pass the cybersecurity certification examination.	3.83	1.193	3.17	1.193
I have learned cutting-edge cybersecurity practices at ASU	4.00	1.044	3.58	.996
My experiences at ASU will help me get a job in the cybersecurity field.	4.08	.900	3.82	1.079
TOTAL SCALE	**4.03**	**.93**	**3.79**	**.78**
Scale (SD, D, N, A, SA)				

Cybersecurity Engagement and Self-Efficacy: We asked the students to respond to the 15 items adapted from the Cybersecurity Engagement and Self-Efficacy Scale (CESES) [19]. Students were highly confident in their abilities, with all items averaging above 4.0 and overall scales averaging 4.45 in 2022 and 4.51 in 2023. Students demonstrated particular confidence in their ability to solve problems, persevere in seeking solutions, and acquire knowledge in cybersecurity. They also expressed confidence that they will be able to understand what they learn about cybersecurity.

Longitudinal Assessment of Engineering Self-Efficacy (LAESE):
We asked the students to respond to the 23 items from the LAESE [20] and overall, students were very confident in their abilities with all items averaging above 4.0 (using a 5-point agreement scale)

Academic Efficacy: When asked to respond to items related to their confidence in their ability to succeed academically, students expressed high levels of confidence with all items averaging above 4.0 each year. More specifically, they believed they would learn if they worked hard, they will learn, it was important to learn new things in class, they believed they could do all the work required in classes and their goal was to learn as much as they could.

21st Century Skills: Students were also very confident in their 21st century skills with all items averaging above 4.0. They strongly believed in their ability to set their own learning goals, work with students from different backgrounds and respect the differences of their peers, make changes when things do not go as planned and produce high quality work.

Career Readiness: Students expressed great confidence in their career readiness skills with each competency averaging above 4.0.

Persistence: When indicating their intentions to persist in their degree and career, students were very positive with all items averaging above 4.0 in 2022 and all above 3.75 in 2023. They strongly believed they would complete their degree in their current major (M=5.0 in 2022 and M=4.67 in 2023), get a job in the field major (M=5.0 in 2022 and M=4.67 in 2023, and working in the field for at least 5 years (M=4.92 in 2022 and M=4.67 in 2023). When asked specifically about cybersecurity, students planned on taking more cybersecurity courses (M=4.92 in 2022 and M=4.25 in 2023), seek opportunities for internships (M=4.83 in 2022 and M=4.08 in 2023), and get a job in cybersecurity (M=4.83 in 2022 and M=4.0 in 2023)

Student Perceived Change – Outcomes: At the conclusion of each semester, students were asked to indicate the extent to which they changed using a 5-point scale (1=much worse, 3= about the same, and 5=much better). Overall, they indicated that they improved over each semester with all items averaging above the scale midpoint of 3.0. The greatest improvements were reported in terms of their problem solving skills, ability to develop working solutions to defend cyberspace and computer networks, and their understanding of critical concepts and industry skills.

Summary and Conclusions

To produce the next generation of cybersecurity professionals for entry-level and junior positions, we revised our undergraduate computing curriculum, incorporating cybersecurity modules from Fall 2020 to Spring 2024, with an emphasis on professional skills in cybersecurity, supported by the US National Science Foundation. The courses incorporating cybersecurity are Networking Fundamentals, Information Security, Data Communication and Networking, Introduction to Operating Systems, Software Engineering, and Special Topics (Digital Forensics). The external evaluation data on 15 items indicates that students exhibited significant confidence in their abilities, with all things averaging above 4.0 and total scales averaging 4.45

in 2022 and 4.51 in 2023. Students exhibited notable confidence in their problem-solving capabilities, persistence in pursuing solutions, and acquisition of information in cybersecurity. They conveyed assurance in their ability to comprehend the information acquired regarding cybersecurity.

References

1. Jeh C. Johnson, Let's pass cybersecurity legislation, http://thehill.com/opinion/op-ed/217151-lets-passcybersecurity-legislation
2. KC Nwakalor, "Cybersecurity: ECONOMIC GROWTH AND TRADE (EGAT)," USAID / Digital Development, https://www.usaid.gov/sites/default/files/202310/Cybersecurity%20Briefer_Economic%20Growth.pdf
3. Cyber Security and Network Reliability, https://www.fcc.gov/encyclopedia/cyber-security-and-networkreliability
4. Cyber Security Primer, http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm
5. Chloe Taylor, "Cybersecurity is the biggest threat to the world economy over the next decade, CEOs say," https://www.cnbc.com/2019/07/09/cybersecurity-biggest-threat-to-world-economy-ceos-say.html, Published Jul 9 2019, Updated Mar 13, 2020.
6. Edward Segal, "Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report," https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/?sh=19392c0c52ae, Mar 16, 2022.
7. Kelly Main, "Small Business Statistics Of 2025,"https://www.forbes.com/advisor/business/small-business-statistics/#sources_section, Jan 31, 2024.
8. Alana Cameron, Bay of Quinte Small Business Week Oct. 21-25, Belleville, ON, Canada / Quinte News, https://www.quintenews.com/2024/10/03/bay-of-quinte-small-business-week-oct-21-25/
9. 2 stores, 100M hacks. Where's cybersecurity? Our view, The Editorial Board, 7:42 p.m. EDT September 14, 2014, http://www.usatoday.com/story/opinion/2014/09/14/home-depot-target-data-breach-credit-card-editorialsdebates/15642867/?utm_source=feedblitz&utm_medium=FeedBlitzRss&utm_campaign=news-opinion
10. "Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen," ISC2 Research 2024 Cybersecurity Workforce Study First Look, https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen
11. George I. Seffers, "National Security Agency Program Fills Critical Cyber Skills Gaps," Signal Magazine, June 1, 2014, https://www. afcea.org/content/national-security-agency-program-fills-critical-cyber-skillsgaps
12. Chris Krebs, "Why So Many Top Hackers Hail from Russia," Krebs on Security, June 22, 2017, https://krebsonsecurity.com/2017/06/why-so-many-top-hackers-hail-from-russia/
13. 13. Intelligence and National Security Alliance, Cyber Intelligence: Preparing Today's Talent for Tomorrow's Threats (Arlington, VA: September 2015),

https://www.insaonline.org/wpcontent/uploads/2017/04/INSA_Cyber_Intel_PrepTalent.pdf
14. Workforce Intelligence Network for Southeast Michigan, Cybersecurity Skills Gap Analysis (Michigan: July 2017), https://winintelligence.org/wp-content/uploads/2017/07/FINAL-Cybersecurity-Skills-Gap-2017-Web-1.pdf
15. Laura Lee, “Circadence responses to NIST RFI on Cybersecurity workforce education or training,” August 2, 2017, https://www.nist.gov/sites/default/files/documents/2017/08/02/circadence.pdf
16. Gregory White, “Security across the curriculum: using computer security to teach computer science principles,” January 1996, USAF Academy, CO.
17. Ambareen Siraj, Blair Taylor, Siddarth Kaza and Sheikh Ghafoor, "Integrating Security in the Computer Science Curriculum," ACM Inroads 2015 June, Vol. 6, No. 2
18. Ambareen Siraj, Blair Taylor, Siddarth Kaza and Sheikh Ghafoor, "Integrating Security in the Computer Science Curriculum," ACM Inroads 2015 June, Vol. 6, No. 2
19. https://sites.google.com/site/amoceses/home
20. http://aweonline.org/efficacy.html#desc