# Engaging students in cybersecurity through co-curricular student organization participation

Vamsi Gondi
vkgondi@bsu.edu

David Hua
dhua@bsu.edu

Biju Raja Bajracharya
bajracharya@bsu.edu

Ball State University
Muncie IN

## Abstract

Cybersecurity is an upcoming area in the field of information technology. The growth in this area is expected to create an estimated million job openings in the next three years. Cybersecurity is a very complex concept where students need to know the depth and breadth of information technology areas. Recent university graduates are not well equipped to work in this area. This lack of preparation has resulted in many of these recent graduates to opt-out of working in cybersecurity. Industry experts indicate that there is a strong need for students to participate in co-curricular student organizations which align to their interests. Keeping this in mind, faculty need to develop student organizations to equip them with all the necessary tools to excel when they enter into industry. The Computer Technology Student Organization at Ball State University is a co-curricular activity designed to support and extend what is being taught in information technology, information systems, and computer science courses at Ball State University. The current initiatives to focus these activities around cybersecurity will be highlighted.

**Keywords:** Computer Science Education, Cybersecurity, Student Organization, Retention Rate, Student Engagement, Project Development, Ethics in computing, Certification.

### 1. INTRODUCTION

The area of information technology is an ever changing and challenging field. Students need to acclimate to these changes and challenges to meet industry standards before they graduate.

Cybersecurity is an area which has huge potential to secure high paying jobs that are unlikely to be impacted by downturns in the economy. According to the Department of Homeland Security (DHS), cybersecurity is termed as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" (Sinha et al., 2015). In the United States, critical infrastructures such as food, water, electricity, transportation, security, policing, and healthcare are dependent upon cyber infrastructures. These infrastructures are vulnerable to both physical compromises and cyber-attacks by the hackers backed by the terrorist organizations and rogue nations. It is of utmost importance to safeguard these infrastructures; prevent the theft of intellectual property; the disruption of the economy; or threats to democracy. To achieve this, countries and the corporations need an army of

cybersecurity experts (Finkle & Randewich, 2012).

There is a high need for cybersecurity professionals in the coming years (Kessler & Ramsay, 2013). In 2019, the DHS estimated that there were half a million vacancies open in public and private space (Finkle, J., & Randewich, N. (2019)) (Department of Homeland Security, 2015; Finkle & Randewich, 2012).

The National Security Agency (NSA), DHS, and other government bodies work with universities and established cybersecurity programs to develop the workforce needed by those agencies (Nakashima, 2013; National Initiative for Cybersecurity Careers and Studies, 2019). The NSA established the National Center of Academic Excellence program which certifies colleges and universities that meet their standards in cybersecurity education (National Security Agency, 2019).

Cybersecurity is one such field in the information technology domain where students need to comprehend various concepts: hardware, software, operating systems, networking, databases, wireless communication, access controls and cryptography (Roussey, 2018). To master cybersecurity, students need to go through rigorous training and have a hands-on experience on implementing cybersecurity across the information technology domain. Students also need to work in groups and have experience of working and leading projects. Cybersecurity education requires more than just technical skills. Students need an understanding of the ethics associated with cybersecurity technologies and practices.

This paper will also provide an overview of the Computer Technology Student Organization (CTSO) as an example of how co-curricular activities can support and enhance the knowledge and skills students are learning in their information technology, information systems, and computer science classes. A framework outlining three levels of cybersecurity activities provided through the student organization. Apart from these activities, the paper will also detail how students are involved in ethics; working in the groups; managing projects; and developing leadership skills.

## 2. CTSO PROGRAM AND CYBERSECURITY

The Computer Technology Student Organization was formed in 2009 to operate as a co-curricular student group to expand their knowledge of information technology and its role in society. Additionally, CTSO was intended to promote professionalism through leadership, fellowship, scholarship, and a philosophical foundation for future information technology professionals. CTSO was originally developed for students majoring in the undergraduate Computer Technology program. It has since reached out to both information systems and computer science students to participate in its activities.

The growing interest in cybersecurity among students and demand for professionals with such skills has prompted another evolution of CTSO. Adopting a focus area in cybersecurity has mobilized faculty and students to develop a game plan of what can be done outside of class to help prepare students for potential careers in the field. This section will provide an overview of the framework that was developed, detail of some of the activities, and identify the learning outcome of the activities.

In 2018, CTSO identified five focus areas: cybersecurity, robotics, Linux, game development, and community outreach. For cybersecurity, a total of 15 students participated during the first year. A total of 3 faculty with varied backgrounds in the areas of security, networking, database, programming, embedded systems and ethics collaborated to develop the content and lead the activities and labs. CTSO met twice a week to explore cybersecurity. The cybersecurity activities were divided into three different levels: Entry, Medium and Expert.

**Year 1 – Entry Level**

During the first year the students were introduced to cybersecurity. In the fall semester, faculty presented operating system security and the Kali OS. Kali is a Linux-based operating system which incorporates the tools used for information security assessment and penetration testing. Students started by learning the tools used for information gathering and enumeration of target systems. The theory behind malware and intrusion detection were also presented. Students used the tools in Kali to create and detect malwares and intrusion as a part of the training.

During the spring semester the students learned about software security. Concepts of buffer overflow were simulated in the lab. Concepts of network security were also discussed during this semester. Labs associated with network security (DNS poisoning, DHCP man in the middle attack, ICMP redirect, ARP poisoning, network scanning, DOS attack, packet sniffing and packet spoofing) were conducted during this period.

**Year 2 – Medium Level**
During the fall semester of the second year the students will be introduced to theory and labs associated with access code, authentication, and firewalls. The theory behind the Database Security and the SQL injection techniques were taught during this semester.

In the spring semester, students will learn about wireless security and breaking WPA/WPA2 using brute force attack. Sessions covering the concepts of symmetric encryption and public key cryptography (RSA and Diffie-Hellman) will be discussed.

**Year 3 – Expert Level**
In the final year during both semesters, the students will be working on simulation projects. Students will also be made aware of computer security laws, the need for ethics within cybersecurity and web security, and implementing it in the lab sessions.

The final project will be a live attack/defend scenario. Students will be divided into red and blue teams. Students on the blue team will build and secure a set of networked resources. Those on the red team will be tasked with attacking those network resources.

## 3. PROGRAM OUTCOMES

**Content Knowledge on Cybersecurity**
The primary goal of this aspect of this aspect of the student group is to promote content knowledge in the cybersecurity domain. This will be fostered by encourage independent research, hands-on activities, and guest speakers. Through these activities, students will learn the tools and techniques needed for safeguarding cyber infrastructures.

**Certifications**
There are many industry certifications the cover different aspects of the cybersecurity domain. Examples of the organizations that sponsor these certifications include the SANS Institute, $(ISC)^2$, CompTIA, Cisco, EC-Council, the Information Assurance Certification Review Board (IACRB), and Offensive Security.

Students will have the opportunity to prepare for the entry level certifications in the cybersecurity domain. Faculty will mentor students as they work through sample questions and activities related to the SANS Institute's Global Information Assurance Certification (GIAC) - Security Essentials certification (SANS Institute, 2019), EC-Council's Certified Ethical Hacker (CEH) certification (EC-Council, 2019), and the CompTIA Security+ (CompTIA, 2019a) and PenTest+ (CompTIA, 2019b) certifications. After the successful completion, students can register separately and get certified on their own.

**Cybersecurity Competitions**
To validate their applied and conceptual understanding, CTSO will participate in student cybersecurity competitions. Similar to the cybersecurity certifications, there are competitions designed for varying skill levels and experience within the realm of cybersecurity. As the collective knowledge and experience of the members is developed, they will be encouraged to participate in competitions of increasing difficulty.

Initially, they will participate in purely online competitions like the competition offered by the National Cyber League (NCL). Students are bracketed into three skill levels based on their success during a mandatory preseason game (National Cyber League, 2019). The registration for the event will be covered by the funds generated from organizational events. All three faculty will serve as faculty mentors for the NCL events.

The plan is for students to participate at in-person competitions and use the skills to attack or safeguard more highly complex computing infrastructures. This will be attempted once the collective knowledge of the members has reached an acceptance level.

**Soft Skills**
Apart from technical knowledge, the student organization provides details on how soft skills, community engagement, and leadership qualities need to be incorporated into the learning process through student engagement.

Students are familiarized with Importance of ethics in computer science, they are actively involving in community development activities, students volunteer in providing technical support for schools in Muncie school district, organizing food drive events for supporting underprivileged. The students also attain project Handling experience and working in the groups as a part of the organization.

## 4. CONCLUSION

Cybersecurity is becoming more relevant in this computer age with trillions of dollars and millions of people's lives at stake. It is very crucial than ever before to develop a credible and

knowledgeable workforce to safeguard cyber infrastructures from hackers and rogue nations. We introduced cybersecurity in 2018 for a small part of the student organization and developed labs and content to sustain and develop them, and made aware of the cybersecurity as a career choice. The necessary skills, tools, techniques and concept is introduced and labs that are needed to develop the knowledge of the students are effectively implemented. The students are well prepared to take part of the cybersecurity competitions and certification process. Finally, interpersonal skills needed part of the employability is developed apart from the cybersecurity skills.

## 5. REFERENCES

CompTIA. (2019a). CompTIA Security+ Certification. Retrieved August 2, 2019, from https://certification.comptia.org/certifications/security

CompTIA. (2019b). PenTest+ (Plus) Certification | CompTIA IT Certifications. Retrieved August 2, 2019, from https://certification.comptia.org/certifications/pentest

Department of Homeland Security. (2015, September 1). Cybersecurity Jobs. Retrieved August 2, 2019, from Department of Homeland Security website: https://www.dhs.gov/cisa/cybersecurity-jobs

EC-Council. (2019). Certified Ethical Hacker | CEH Certification | CEH v10. Retrieved August 2, 2019, from EC-Council website: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

Finkle, J., & Randewich, N. (2012, June 13). Experts warn of shortage of U.S. cyber pros. *Reuters*. Retrieved from https://www.reuters.com/article/us-media-tech-summit-symantec-idUSBRE85B1E220120613

Kessler, G., & Ramsay, J. (2013). Paradigms for Cybersecurity Education in a Homeland Security Program. *Journal of Homeland Security Education*, *2*, 35–44.

Nakashima, E. (2013, January 27). Pentagon to boost cybersecurity force. Retrieved August 2, 2019, from The Washington Post website: https://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html?noredirect=on&utm_term=.868833057da7

National Cyber League. (2019). Preseason | National Cyber League. Retrieved August 2, 2019, from NCL | National Cyber League | Ethical Hacking and Cyber Security website: https://www.nationalcyberleague.org/preseason

National Initiative for Cybersecurity Careers and Studies. (2019). Workforce Development. Retrieved August 2, 2019, from https://niccs.us-cert.gov/workforce-development

National Security Agency. (2019). National Centers of Academic Excellence. Retrieved August 2, 2019, from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

Roussey, B. (2018, October 8). Must-have cybersecurity skills that make you an in-demand expert. Retrieved August 2, 2019, from TechGenix website: http://techgenix.com/cybersecurity-skills/

SANS Institute. (2019). GIAC GSEC Certification | GIAC Security Essentials Certification. Retrieved August 2, 2019, from https://www.giac.org/certification/security-essentials-gsec

Sinha, A., Nguyen, T. H., Kar, D., Brown, M., Tambe, M., & Jiang, A. X. (2015). From physical security to cybersecurity. *Journal of Cybersecurity*, *1*(1), 19–35. https://doi.org/10.1093/cybsec/tyv007