World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:10, No:1, 2016

Cybersecurity Awareness through Laboratories and Cyber Competitions in the Education System: Practices to Promote Student Success

Haydar Teymourlouei

Abstract**—**Cybersecurity is one of the greatest challenges society faces in an age revolving around technological development. With cyber-attacks on the continuous rise, the nation needs to understand and learn ways that can prevent such attacks. A major contribution that can change the education system is to implement laboratories and competitions into academia. This method can improve and educate students with more hands-on exercises in a highly motivating setting. Considering the fact that students are the next generation of the nation's workforce, it is important for students to understand concepts not only through books, but also through actual hands-on experiences in order for them to be prepared for the workforce. An effective cybersecurity education system is critical for creating a strong cyber secure workforce today and for the future. This paper emphasizes the need for awareness and the need for competitions and cybersecurity laboratories to be implemented into the education system.

Keywords**—**Awareness, competition, cybersecurity, laboratories, workforce.

I. Introduction

EVERY computer user is aware of the potential harm that comes from an increased use of the internet. A greater knowledge of cybersecurity and its implementation has the potential to protect against data thefts, cyber-crime, and other potential threats on the internet. Many users do not realize that a computer with or without internet can still be a risk of cybersecurity concern. For example, a machine could get infected through unknown external devices (e.g., CD, USB, or DVD). A user needs only to plug a USB embedded with spyware or malware into his or her system, and the system will become infected, potentially leading to the cyber-criminal stealing the user's data, capturing keystrokes, deleting documents, and corrupting the system.

Private data is being exposed due to the evolution of cyber-attacks, which inflict negative impacts against usage of technology. These threats have emphasized the importance of education in cybersecurity and the need for competitions and training laboratories. According to Bucci, a lack of education, awareness, and workforce planning is a root cause that hinders progress in improving the nation's cybersecurity posture. The development of an adequate cyber workforce begins with improvements in STEM education. These improvements need to span from kindergarten through high school and into higher education [1].

H. T is with the Computer Science Department, Bowie State University, Bowie, MD 20715 USA (e-mail: hteymourlouei@bowiestate.edu).

An education system that is enhanced with cybersecurity labs and competitions will teach students skills required in the workforce and spread the awareness of cybersecurity to every user. This will prepare students to implement all of the techniques and tools to protect the confidentiality and reliability of information. With the growing concern over cyber-threats, the government, professional organizations, and universities have to strengthen their efforts to recruit and hire qualified professionals in the field of cybersecurity. To meet what is characterized as an explosive growth in the need for cybersecurity professionals, it is essential to broaden participation in the field. According to the Florida Center for Cybersecurity, even when compared with other high-demand IT jobs, the demand for cybersecurity jobs is growing more than three times faster. Business leaders say they cannot hire skilled cybersecurity workers fast enough, and our nation's military and homeland security agencies are looking for help in navigating the constantly changing world of cybersecurity research [2]. Educators need to prepare and encourage posterity to join the cybersecurity field to ensure a trained and diverse workforce in the years to come.

II. Discussion

A. Cybersecurity Awareness

A cyber-threat occurs when an individual attempts and/or gains unauthorized access to a computer maliciously and either damages the system or steals valuable information from the computer. Cyber-threats lead to fraud, identity theft, and many other crimes. Cybersecurity involves protecting sensitive and personal data through detection, prevention, and defending against cyber incident. The increasing volume and sophistication of cybersecurity threats include phishing scams, data theft, and other online vulnerabilities-demand that we remain vigilant about securing our systems and information [3]. If a computer is connected to the internet and it does not have proper security controls, it is vulnerable for cyber-attacks. By integrating cybersecurity training into early education, students will have the understanding and technical skills needed to reduce the effects of cyber-attacks. If the future generation does not have at least a basic understanding of cybersecurity, it will be a major hindrance to the success of the nation.

B. Cybersecurity Education

Cybersecurity education is not only restricted to technical studies, but also includes network security, application

security, and operating system security. In order to create a secure computing environment and protect data, users and security professionals need to understand the concepts and intentions of cyber-attacks. In order to spread cybersecurity awareness, educators and professionals need to pursue a universal approach that combines a variety of strategies to encourage more participation in the cybersecurity field. Increased collaboration with research laboratories will give students more knowledge to implement different technologies and practice what they learn in the classroom. National Centers, including CyberWatch and the Center for Systems Security and Information Assurance, are focused on increasing cybersecurity awareness and the size of the workforce through curriculum development, faculty development, and student development. Activities include training faculty in topics such as ethical hacking, forensics, and network defense [4].

1. Workshops for Educators and Students Educators

Workshops can meet the need for cybersecurity education for the current education system, in which both students and professionals can participate. The objective of workshops is to bring together many experts and government officials to share the current state of cybersecurity with educators. A computer security workshop is designed to instruct other post-secondary instructors who want to start a course or laboratory exercise sequence in computer security [5]. These workshops provide cyber education, identify various exercises, and illuminate the technical, legal, and ethical knowledge for educators. Participation in workshops will increase the number of faculty members endowed with the capability to teach cybersecurity courses. It will also enable educators to develop new courses and hands-on exercises that will teach students cybersecurity concepts. Educators need to persistently update and improve their skills by attending workshops. In prior to this research, it is assumed most of the educators would be aware of the cybersecurity topic, but this hypothesis was wrong. A survey result for a workshop that was held at Bowie State University appears below. The workshop's aim was to address issues and new research topics in cybersecurity, provide hands-on training, and share methods to ensure a secure network infrastructure. This workshop had leading researchers from academia, industry, and the government for a comprehensive update on cybersecurity research and development issues. After the workshop, a survey was conducted to assess the effectiveness of the training. Participants were asked ten questions regarding the effectiveness of the workshop. A total of twenty educators responded to the survey. Table I shows the evaluation of the workshop and how much participants learned on a rating scale of 1 to 5, with 1 meaning disagree and 5 meaning agree.

a. Students

Workshops are a combination of theory and practice in a variety of core cybersecurity issues. By attending workshops, students will be aware of the concepts, practices, tools, and tactics of cybersecurity. Students will also learn the attacking strategies to help them understand the mindset of an attacker. Many universities often lack the facilities to expose students' to the hands-on challenges where they can learn major technical skills required in workforce. These workshops will not only help students to solidify their knowledge about cybersecurity, but also teach them leadership and teamwork skills. Workshops provide an opportunity to learn current information about the field and provide students with networking opportunities. Moreover, the hands-on experience students gain at these events is essential to fortify their knowledge in areas such as penetration testing, intrusion detection, and malware analysis. These experiences will increase student participation in competitions since they will be equipped with the required skills to qualify for competitions. In participating in competitions, students are afforded valuable opportunities to interact with such professionals and experts and to learn about the cybersecurity profession. According to Ronald, lectures and workshops increased student interest in cybersecurity. Many students reported further interest in taking more university courses in security and knowing more about the cybersecurity profession...many students began inquiring about a career in cybersecurity after participating. Fig. 1 shows the results from a workshop which was held in Bowie State University. A total of thirty students completed the survey before and after participation. The scale goes from 1 (low) and 5 (high). Fig. 1 shows different aspects of cybersecurity workshops participation by students and their own interest ratings.

TABLE I
WORKSHOP EVALUATION RESULT

Evaluation Questions	Average Rating
This workshop helped me to gain experience with computer security tools and techniques.	4.7
This workshop focused on tools and techniques that, in my opinion, are important in computer science.	4.8
The workshop focused on tools and techniques that are of interest to me.	4.7
The presentation (PPT slides, handouts, and workshop discussion) of the material related to the tools.	4.6
The exercises related to the tools and techniques were valuable and informative.	4.7
I could use the workshop presentation materials (PPT slides and handouts), as is, within my own classroom.	4.9
I could use the workshop exercises, as is, within my own computing program.	4.9
The workshop time devoted to hands-on use of the tools was valuable.	4.7
This workshop was of value to me.	4.7
I would recommend this workshop to others.	4.7

Results show that students found the workshop helpful for learning about cybersecurity; many students began inquiring about a career in cybersecurity after participating in the workshop.

2. Curriculum Development

Integrating a cybersecurity program into a curriculum will address deficiencies of the knowledge and skills needed at the higher education level and in the workforce. National Centers

of Academic Excellence (CAE) designation promotes research and a pipeline of professionals in the field of cybersecurity starting in colleges and universities. Courses integrate the knowledge areas as determine by the Department of Homeland Security that are needed to ensure that students are well-trained and have the cybersecurity skills necessary to promote the growth of the cybersecurity workforce [7]. The development of relevant curriculum materials, such as laboratory modules, courses re-design, and new courses will give students in-depth knowledge on several topics. Topics such as emerging security threats, new countermeasure with computing technology to prevent these threats, cybersecurity principles and policies, and other security related issues are all important. Curriculum developments such as new courses, new tracks/concentrations as well as new programs in cybersecurity also seem to engage students in cybersecurity [8]. Also, incorporating cybersecurity into the curriculum will give and encourage students to do research/projects in cybersecurity field.

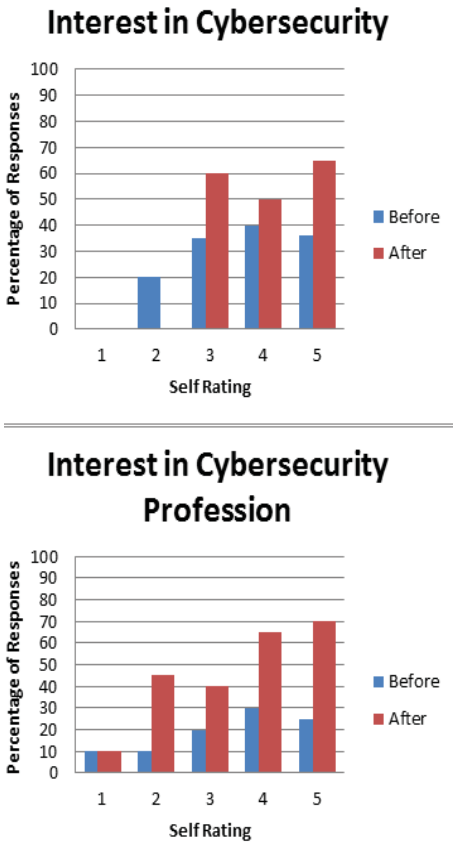

Fig. 1 Student's self-ratings in various aspects of cybersecurity

C. Cybersecurity Competitions

Academic institutions are the main suppliers of workers in the cybersecurity field. Cybersecurity competitions are becoming an increasingly prominent part of cybersecurity education. They engage individuals and teams in addressing real security risks in real-time. Specifically, competitions can be used as a means to stimulate interest and enhance experiential learning within and outside the classroom. For example, the CyberPatriot Competition, which is a national high school competition created by the Air Force Association, encourages high school students to pursue careers in cybersecurity and more generally computer science, information technology, and other STEM-related fields. Cyber competitions have great potential to spark an interest in cybersecurity and have implemented a variety of strategies to expose students to the field. Competitions are usable as a tool for studying several aspects related to cyber space and as a platform for experimentation in the area. According to Sommestad, competitions may have several different goals, for example to offer a challenge, train, test the competence or increase the awareness of the participants [10]. Also, by participating in competitions students are able to build their network through discussions with security professionals, learn techniques to secure network, and speak to company recruiters.

Cybersecurity competitions teach students current techniques and tools in network security and also allow them to engage in local, regional, national, and international competitions where they will have the opportunity to test their skills in realistic scenarios, similar to those that exist in the private or public sector. Ronald states …all students who participated in the study benefited greatly from the CBL experience. These benefits included knowledge gained by networking with industry professionals, improving computer and security skills, and applying these skills in a practical, real world environment [6].

III. Methodology

A cybersecurity lab should be housed in an isolated environment and have its own private local area network (LAN). An advantage of having an isolated network is that it gives students the freedom to perform any test or security measure without affecting other networks. For example, students can locally scan network through packet sniffer software to capture unencrypted data. If such testing measure runs on a regular network, it can cause a potential threat to the entire network. In addition, a lab that is housed in an isolated environment is not a controlled environment where one is not limited to install or configure program, has administrative privileges, generates certain traffic, etc. By having a cybersecurity lab, students can learn an abundance of tools and techniques without having an influence on the outside network, which could alter testing results. Fig. 2 shows cybersecurity lab's infrastructure.

Fig. 2 shows the equipment needed to setup a cyber-security lab. Each desktop machine needs to be connected to the switch with a network cable. The lab network consists of three subnets: an attack domain, a defense domain, and an administrative domain. Each domain has a separate switch that connects to the main router or switch that gives the proper IP address to the machines.

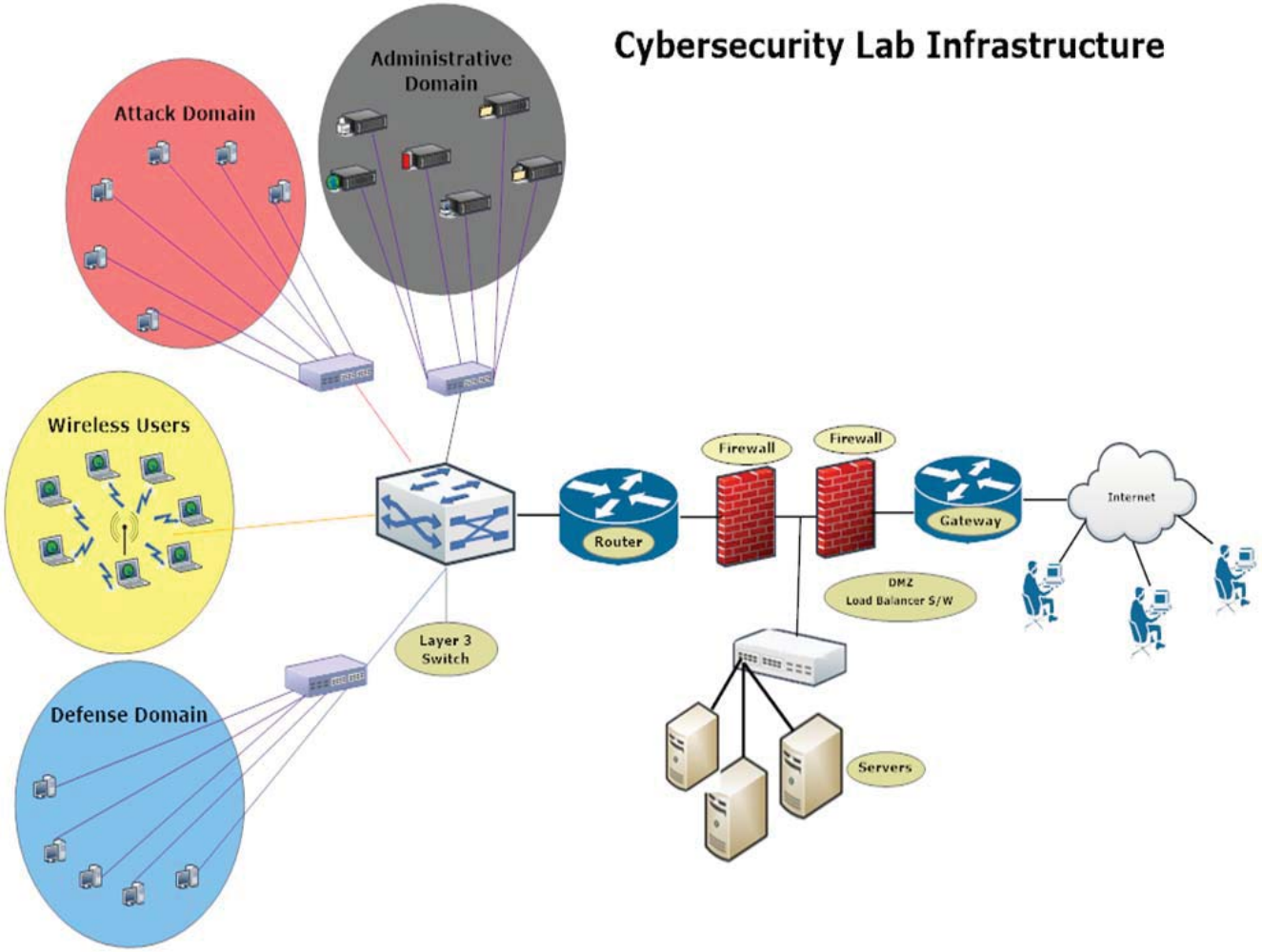

Fig. 2 Cybersecurity Lab Infrastructure

The attack domain (red team) consists of computers that launch attacks at the defense domain machines. The ultimate goal of the red team is to take control of the blue team using a variety of available tools to seek, destroy, and tear down the blue team defenses. Once the red team finds vulnerability, it needs to exploit and obscure it so that defending team cannot detect it; thus the attack could be more destructive. Here is the list of some actions that the Attack Domain will take against the Defense Domain:

- Exploit vulnerabilities in Windows, Linux, and UNIX operating system
- Produce and modify exploit in order to penetrate a network attack

The defense domain (blue team) consists of the computers that prevent outbreaks from attack domain. The essential goal of the blue team is to develop an effective network defense for their network to prevent attacks from the red team. They need to determine what kind security measures to take for different types of attacks, efficiency of proposed security measures, and check sufficiency of such measures after implementation. Once the blue team determines where the attack originates and configures, this can be extremely beneficial because it will prepare them to pursue countermeasures, by updating their machines including firewalls. Some of the actions that that the Defense Domain will take against the Attack Domain include:

- Understand rules of network communication (such as traffic flow, packet filtering, proxy firewalls, network intrusion detection, and more) to prevent such type of attacks
- Restrict Windows firewall for TCP port access, harden IIS web server, take control over admin access to limit compromise of such attacks

The administrative domain consists of three servers that include: AD/DNS/DHCP, File Server, VMs Storage, and WSUS role. Each server domain includes necessary support features and management/monitor systems to manage the attack and the defense domain separately. Each server has a/an AD/DNS/DHCP to setup domain for the team, create the user accounts, and allocate designated IP addresses to the computers. VMs Storage stores all pre-configured VMs to be used in the competition, which can be accessed anytime. WSUS' role is to push the latest Windows update to the host machines to make sure they are up-to-date at all times.

During the competition, the attack and the defense domain use various software developments, network monitoring, and hacking tools to complete their tasks. The STARS (Students & Technology in Academia, Research, and Service) Alliance provides a comprehensive approach to address declining enrollment and the need to broaden participation in computing [9]. Moreover, cybersecurity labs serve many educational functions such as offering courses, workshops, lectures, demonstrations, presentations, training, and competition practice. They also provide training in computer forensics, and serve as a center for next generation research in these areas. By utilizing cybersecurity labs, students can gain knowledge and skills to make a difference in society.

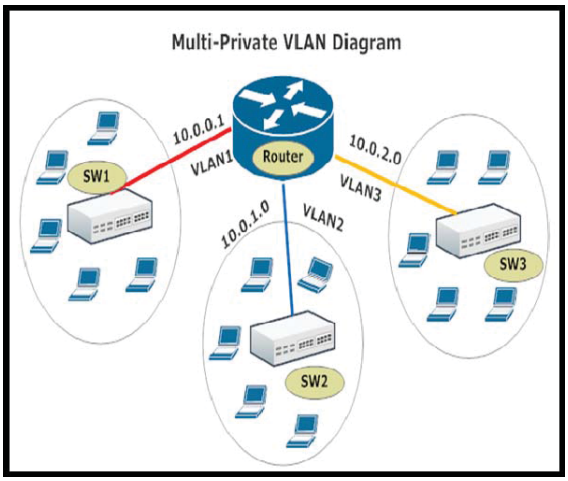

Fig. 3 Multi-Private VLAN Diagram

The main router/switch can create up to many different VLAN allowed in a device as shown in Fig. 3. Each line serves as a connection residing on a separate VLAN in the device. Each switch needs to connect to its respective VLAN port on the router/switch to give out the specific IP addresses to the machines.

IV. Conclusion

The rapid rate of change means there is a continuous need to stay aware of current trends to limit breaches by cybercriminals who try to maximize their gains as they leverage new technology to identify and exploit vulnerabilities before solutions are deployed or become well-known. Many specialists and nations have acknowledged the need for cybersecurity education due to the security issues relating to cyber-attacks. Security has become an essential and challenging issue in this technology driven world. It is vital to educate our future generation about the cyber-threats and prepare them for workforce. The combination of workshops, curriculum development, competitions and cybersecurity laboratories can increase student interest in the cyber field. Additionally, institutions of higher education need to incorporate these approaches into their education system. Competitions challenge, educate, and train students to use their knowledge, skills, and technology to solve real-world problems. The workshops have been effective in communicating the cybersecurity concepts, skills, tools, and techniques to faculty and students. The education system should integrate cybersecurity labs and conduct cyber competitions into the curriculum. The objective of this paper is to promote cybersecurity awareness via multidisciplinary approaches which encourage students to take interest in cybersecurity fields and to participate in competitions. University collaboration with cybersecurity laboratories and participation in competitions will enable students to overcome the obstacles necessary to learn about cybersecurity.

References

[1] Bucci, S. (2013). A congressional guide: Seven steps to U.S. Security, Prosperity, and Freedom in Cyberspace. Retrieved from http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace

[2] Florida center for cybersecurity. (2013). University of Florida, Retrieved from http://www.usf.edu/pdfs/final-cybersecurity-report.pdf

[3] Why is cyber security important. (2010). State of New Jersey. Retrieved from http://old.citationmachine.net/index2.php?reqstyleid=2&mode=form&reqsrcid=APAUnivDocOnline&srcCode=22&more=yes&nameCnt=1

[4] Ate Centers Impact 2014, Patton, Madeline, ED. Tempe, AZ: Maricopa Community Colleges, 2014. Retrieved from http://www.atecenters.org/wpcontent/uploads/PDF/ATEIMPACT_2014.pdf.

[5] Wagner, P. (2006). A portable computer security workshop. University of Wisconsin, Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.101.9059&rep=rep1&type=pdf

[6] Cheung, R. (2011). Challenge based learning in cybersecurity education. Retrieved from http://josephcohen.com/papers/cbl.pdf.

[7] Spidalieri, F. (2014). Professionalizing cybersecurity: A path to universal standards and status. Retrieved from http://www.salve.edu/sites/default/files/filesfield/documents/Professionalizing-Cybersecurity.pdf.

[8] D. W. Evans and C. L. Chatmon, "Increasing Minority Participation in Information Assurance," in ITHET 6th Annual International Conference. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1560322

[9] Dahlberg, T. (2007). The stars leadership model for broadening participation in computing. Retrieved from http://www.uncg.edu/stars/doc_stars/STARS Leadership Model.pdf

[10] Sommestad, T. (2012). Cyber Security Exercises and Competitions as a Platform for Cyber Security Experiments. Retrieved from http://www.sommestad.com/teodor/Filer/Sommestad,%20Hallberg%20-%202012%20-%20Cyber%20security%20exercises%20and%20competitions%20as%20a%20platform%20for%20cyber%20security%20experiments.pdf