

Cyber Defense Competitions - Educating for Prevention

Raymond T. Albert
Professor of Computer Science
University of Maine at Fort Kent
23 University Drive
Fort Kent, ME, 04743
(207) 834-7696
ralbert@maine.edu

JoAnne L. Wallingford
Associate Professor of Business/MIS
University of Maine at Presque Isle
181 Main Street
Presque Isle, ME 04769 (207) 768-9432
joanne.wallingford@umpi.edu

Abstract

Information security remains a critical topic in today's information driven societies. Societies, and especially educational institutions, have been called to action to help raise information security awareness. Cyber Defense Competitions are an attractive option for raising awareness and interest in information security while simultaneously educating for prevention. Different approaches exist to implement Cyber Defense Competitions but the goal remains the same – to educate. Universities are ideally positioned to orchestrate such competitions for the betterment of current and future students and to contribute to the best preparation of future information workers and leaders. The purpose of this paper is to clarify the importance of information security and the role education organizations have been called to play, identify the goals and benefits of Cyber Defense competitions within this context and especially with respect to educating for prevention, and share the advantages/disadvantages of different approaches to implementing such competitions.

Introduction

Information security remains a critical topic in today's information driven societies. Our educational organizations and nation are collectively facing increased risk resulting from the prolonged dearth of information security practitioners and low level of information security awareness in our general population. Educational organizations are, however, "... uniquely and ideally positioned to significantly contribute to the best preparation of future information workers and leaders through the advancement of safe and sensible educational computing practices" (Albert, R., 2009, p. 1). Through better education, personal and "... community involvement, appropriate information security practices will supplant those that are inappropriate and society will be better for it." (p. 8)

Societies, and especially educational institutions, have been called to action to help raise information security awareness. In early 2009, President Obama ordered a 60-day, comprehensive,

“clean-slate” review to assess U.S. policies and structures for cybersecurity. One of the observations contained in the report that resulted from the review was that changes are needed in education, among other sectors, that require strong vision and leadership. The relationship between what must be done and which organizations should be involved is clearly portrayed in the report.

“The United States should initiate a K-12 cybersecurity education program for digital safety, ethics, and security; expand university curricula; and set the conditions to create a competent workforce for the digital age... To help achieve these goals, the Nation should:

- Promote cybersecurity risk awareness for all citizens;
- Build an education system that will enhance understanding of cybersecurity and allow the United States to retain and expand upon its scientific, engineering, and market leadership in information technology;
- Expand and train the workforce to protect the Nation’s competitive advantage; and
- Help organizations and individuals make smart choices as they manage risk. “ (NSC, 2009, p. 13)

The report includes specific near- and mid-term action plans including initiation of “... a national public awareness and education campaign to promote cybersecurity.” (p. 37), expanding “... support for key education programs and research and development to ensure the Nation’s continued ability to compete in the information age economy... [and development of] ...a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government. “(p. 38)

The importance of securing the cyberspace world of the 21st century is underscored by the change in the United States Air Force (USAF) mission statement. On December 7, 2005, the USAF changed its mission statement to include the cyber security concept. It now reads, “The - mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests -- to fly and fight in Air, Space, and Cyberspace.” (USAF, 2005)

The private sector too has acknowledged the considerable and growing need for skilled information security practitioners. For example, the Center for Strategic and International Studies (CSIS) has established “a national talent search and skills development program. Its purpose is to identify 10,000 young Americans with the interests and technical computer skills to fill the ranks of cyber security practitioners, researchers, and warriors. In particular, the search is looking for the people who can become the top guns in cyber security” (CSIS, 2010). When the government and private sector needs are combined, the impetus for educational organization action becomes very clear. The question that naturally follows is, ‘Exactly what can educational organizations do to respond?’

The authors’ experience in this field has yielded anecdotal evidence consistent with that of others (e.g., Jacobson, D. & Rursch, J.) that supports the notion that Cyber defense competitions are an attractive and effective option for raising awareness and interest in information security while simultaneously educating for prevention. Of the competitions reviewed in this paper, there are

two major categories that can be distinguished based on their goals. For the first type of competition (e.g., CyberPatriot and NetWars), achievement of the competition goals naturally leads to prevention of the negative consequences associated with the United States being unable to adequately defend its cyber infrastructure and resources (hereafter referred to as defense-based competitions). For the second type of competition (e.g., IT-Adventures and NCCDC), achievement of the competition goals naturally leads to prevention of the negative consequences associated with the US being unable to adequately compete in an increasing technological global marketplace (hereafter referred to as development-based competitions). Thus, education for prevention is a theme that all approaches share in common.

Universities are ideally positioned to orchestrate and host such competitions for the betterment of current and future students and to contribute to the best preparation of future information workers and leaders. The structure of most cyber defense competitions fosters the establishment of working relationships between industry partners and participating schools and these relationships are most often enhanced through university involvement. Industry partners often provide support in the form of sponsorship and/or human resources in exchange for the opportunity to meet and converse with top performers. Participating universities often provide information security curricula and degree options in addition to hosting those competitions not conducted entirely online. The effectiveness of such educational programs is greatly enhanced by the excitement and enthusiasm that is nearly universally experienced by competition participants.

Cyber-Defense Competition Goals and Benefits

The history of cyber-defense competitions is often cited as starting around 2001, with early information warfare exercises within and between military academies. The goals of these defense-based competitions remain in large part the same as those of subsequent competition formats that evolved after an early-2004 meeting of academicians and others in San Antonio, - Texas. One outcome of that meeting was the 2005 establishment of a collegiate cyber-defense competition (CCDC) by the University of Texas at San Antonio. The success of the CCDC competition in attracting participants has led to its evolution into a regionalized national competition (NCCDC). Other competitions have since been established based on the success of NCCDC model and now involve secondary education students.

The current incarnations of cyber defense competition formats differ in their degree of offensive tactics and level of network configuration involvement. At one end of the spectrum are capture the flag competitions (e.g., NetWars) where teams of students attempt to gain access to specific flag files on competitor computer systems. This type of competition favors those teams who employ significant offensive tactics. At the other end of the spectrum are purely defensive competitions (e.g., CyberPatriot, NCCDC) wherein teams of students compete to quickly remove as many vulnerabilities as possible from the preconfigured virtual machines and/or networked computer system they are provided. This type of competition favors those teams who employ significant defensive tactics. Between these two formats are competitions that are primarily defensive in nature but include an element of network configuration (e.g., ISU IT-Adventures). This type of competition requires students to build their own network and subsequently defend it during the competition while being simultaneously charged with supporting end users.

The competitive element of these events drives and compels all participants to more enthusiastically commit to and engage in active experimentation and learning. According to Conklin

(2006), “Participating students learn in a true active learning environment. Instructors are able to evaluate the thoroughness of their curriculum in its intended setting...In the end, everyone feels they had learned important lessons.” (p. 1) This level of commitment and drive are essential to most successful educational endeavors. The more motivated the student the more likely the educational goals will be achieved.

Since these competitions are relatively new and are enjoying significantly increasing levels of participant interest, assessment of their effectiveness in meeting their goals has for the most part not been formally pursued. This paper attempts to broach this subject by both providing a brief overview of each competition and identifying common traits and unique characteristics that may be considered (dis)advantages depending upon the context and goals of the host institution. The authors acknowledge that the identified traits are not the only ones available and that each institution must decide for itself that approach best matching its goals and ability to commit resources to successfully host such a competition.

Cyber-Defense Competition Approaches

There are fundamentally three types of approaches for cyber defense competitions involving post-secondary education participants. The first approach is focused mainly on offensive tactics where the students configure their own network environments and hack into competitors’ machines to capture the “flag”. The second approach is a purely defensive competition wherein teams of students remove vulnerabilities and harden their preconfigured systems before professionals attack them. The third approach is a hybrid approach which is defensive in nature but the teams must build and configure their own networks and provide end users with various services (such as email, web mail and web site) while thwarting off attacks. This section covers - some of the most successful implementations of cybersecurity competitions; what type of competition is it and how they did it. Table 1 summarizes a few key attributes.

Cyber Defense Competition Approaches				
Approach	Competition/Organization	Environment	Host University Resource Demand	Participating School Resource Demand
Defense-based competitions - prevention of the negative consequences associated with the United States being unable to adequately defend its cyber infrastructure and resources				
Defensive Remove Vulnerabilities	CyberPatriot/AFA	Pre-configured Virtual Machine Images or Remotely Accessed Computer Network	Time: Medium Cost: High	Time: Medium Cost: High
Offensive "Capture the Flag"	NetWars/SANS	Pre-configured Virtual Machine Images used to Access Online Environment	Time: Low Cost: Low	Time: Low Cost: Low
Development-based competitions - prevention of the negative consequences associated with the US being unable to adequately compete in an increasing technological global marketplace				
Hybrid Offense and Defense	IT-Adventures/ Iowa State University	Remotely Configured Computer Network with User Support	Time: High Cost: Medium	Time: High Cost: Low

Table 1: A few key attributes of predominant cyber defense competition formats.

CyberPatriot

CyberPatriot (<http://www.highschoolcdc.com/>) is a defense-oriented cybersecurity competition recently sponsored by the Air Force Association (AFA) in 2008 and technically offered by Science Applications International Corporation (SAIC). The AFA created a “truly national high school cyber defense competition” in an attempt to meet the growing need for cyber security talent in the United States. The initial phase (called CyberPatriot I), was designed to prove that a “National High School Cyber Defense Competition could excite and motivate students...” (AFA, 2009). The CyberPatriot I culmination competition was held in conjunction with the Air War Symposium in Orlando in February 2009, and included AFJROTC (Air Force Junior Reserve Officer Training Corps) and CAP (Civil Air Patrol) high school students in the state of Florida.. The Air Force Magazine reported on the success of CyberPatriot I and remarked “One thing CyberPatriot is not meant to be is a training ground for hackers. Hackers are searching for one chink in a computer system’s armor; defenders have to mount a broader effort that takes into account all the different ways hackers might work.” (Grier, P., 2009)

The participants in the first CyberPatriot competition were so excited and motivated by the activity-based real world scenarios of the competition that the AFA implemented CyberPatriot II during the 2009-2010 academic year. This competition was open to all AFJROTC and CAP units. Of the 225 participating units across the United States and overseas DoD high schools, -

eight teams advanced to the finals and competed on February 18-19, 2010 in Orlando. This was an important phase as it proved that a geographically diverse competition could successfully be orchestrated to narrow the field down to the final competitors. The third phase has as its goal, to open the CyberPatriot competition to any high school student.

The AFA accomplished their success through the help of the Center for Infrastructure Assurance and Security (CIAS) of the University of Texas – San Antonio. This partnership provided them a link to the National Collegiate Cyber Defense Competition through the CIAS director, Dr. Greg White and gave them access to educational resources that had been previously created by the graduate students from the university. The AFA also worked with the Science Applications International Corporation (SAIC) – developers of the CyberNEXS Cyber Defense Trainer. Through SAIC, the Air Force Association only needed minor modifications to an established and proven industry leader in cybersecurity training software. This saved them valuable time and money in creating an environment that would support their needs for multiple rounds of competition.

For CyberPatriot II, any high school with an AFJROTC or CAP group was encouraged to register. Once the team registered, they gained access to the training materials (videos, website links, training manuals, etc.) and the schedule of rounds. The student teams studied for the competition by reviewing the training materials and investigating how to secure a network by focusing on the task of removing operating system vulnerabilities. SAIC through their CyberNEXS (pronounced cyber nexus) software offer two options for game day.

The first option is a distributed game, where the contestants connect remotely and download VMware images to their own equipment. All teams receive the same image on the same day. After downloading and installing the VMware image, it connects to the CyberNEXS server and the teams view a real-time scoreboard of the vulnerabilities that they have removed. The major

processing burden is on the local machines, so this distributed option is very scalable and thus a great way to conduct qualifying rounds for the final competition.

The second option is a centralized game where the teams interact with the CyberNEXS environment. The teams connect to the server and assume control of their systems where they need to quickly begin hardening their system by removing vulnerabilities. They are given a window of time to fix as many problems as possible before a team of hackers tried to take over their system. The teams are expected to document all trouble tickets and the status of their systems throughout the competition. This option is usually reserved for the final round of competition (8-10 teams) as it does not scale well as it is resource intensive (centralized processing and hackers).

The major potential benefits of the Cyber Patriot II approach to the AFA are that the software and resources already exist to begin this type of regional competition in your area. This competition format still requires that it be orchestrated (organized, publicized and managed), but the technology aspects are virtually a turnkey solution. Aside from the logistical benefits, this defensive approach mirrors the real world situations these students are likely to face. CyberNEXS is a professional training and evaluation system used to train cybersecurity professional and as such can be used to provide certifications in various areas of security. The -

practice rounds give students the experience and confidence they need to compete during the final rounds. All students who participate in any of the rounds will benefit from the awareness of cybersecurity measures. The final round fosters application of critical thinking skills as the students are protecting their systems from live and dynamic attackers trying to break into their systems.

NetWars

NetWars (<http://www.sans.org/netwars/>) is an offensive-oriented cybersecurity competition that is conducted entirely online and made available to high school students through post-graduate students. It is an online game where the purpose is to break into systems to gain access to a file or files (the flag) to prove that you successfully penetrated the defenses. The NetWars game is conducted by SANS Institute. It is a major player in the training and certification of cyber security professionals in the United States. SANS claims they “develop, maintain, and make available at no cost the largest collection of information security research documents and whitepapers about various aspects of information security and operate the Internet's early warning system - the Internet Storm Center.” (SANS, 2010) Besides the training materials, they provide links to other resources. Participants may play the game either as individuals or as members of a team. NetWars might lend itself to building bridges between the high school students and the universities if utilized to the fullest. In and of itself, NetWars is not as well suited to being hosted by a college or university. SANS has regularly announced the availability of a new round of the competition for participants to engage in. Participants work in an offensive fashion to break into systems and capture flags for points.

Perhaps the greatest potential benefit of the NetWars approach is that it requires the least time and monetary resources of all of the competitions. This is due to that fact that no host organization, other than SANS of course, need be involved. Individuals and teams are free to participate at no cost and they only need access to an Internet attached computer in order to play the game.

Iowa State University's IT-Adventures

IT-Adventures Cyber Defense competition (<http://www.it-adventures.org/cdc.html>) is a hybrid defensive- and offensive-oriented cybersecurity competition that Iowa State University (ISU) developed and created for Iowa State high school students. IT-Adventures was created in re-

sponse to the realization that enrollments are continuing to drop in the science, technology, engineering, and mathematics (STEM) disciplines while the need for information technology workers increases yearly (especially in the area of information and cyber security). The creators realized that in Iowa, many high schools do not offer computer science or networking classes and counselors were steering students away from careers in information technology. To combat this phenomena, the computer science department created an after school extra-curricular activity to allow students to “explore information technology in a non-threatening, non-graded environment.” (Jacobson, D., 2008, p 60)

ISU’s approach encourages inquiry-based learning. It began in 2006, when they sponsored a cyber defense competition for the high schools in the state of Iowa. In 2007, they included the formation of extra-curricular high school clubs that met for several months before the competition. This enabled the students to study and learn together before having to compete, much like a sports team has months of training before their first competition. The clubs discuss security issues and work through hands-on learning modules.

This type of competition begins with the formation of a team of high school students managed by a team advisor with access to a mentor (who is typically an IT professional). For this approach, the high schools had little out of pocket costs as ISU provided each club with the necessary equipment and training materials to participate in the program. The schools needed to form a club with an advisor to receive the equipment. ISU undergraduate and graduate students developed most of their training materials including demonstrations and lectures.

High schools received their equipment several months before the competition to ensure ample time to learn about cybersecurity concepts. The clubs in the ISU competition had to configure and setup their own network to support end users and their needs. The specifications were sent to the teams one month before the competition. Teams participated in attack and defend competitions while simultaneously maintaining their network services (e.g., email, file sharing, web) for their clients.

The competitions are held at the university where students bring their equipment and set up their networks. During an 18-hour competition, the teams try to defend their networks while minimizing downtime of services for their customers and plan capture the flag attacks on other competitors’ networks.

In more recent years, ISU has expanded the venue to include robotics and game design, but have retained cyber defense as the predominant component of the competitions. This year the culmination of the IT-Adventures experience is a two-day competition called IT-Olympics situated on the ISU campus. In an attempt to attract more young women to the competitions, ISU also added an information technology community service project for all competing teams. In reply to a reported overwhelmingly positive response, the “Community College Cyber Defense Competition (CCCDC) was created as a bridge between Iowa State University and the 15 community college districts in the state of Iowa.” (Rursch, 2010, p. 1)

One of the major potential benefits of this approach is the considerable emphasis on educating all participants through a well-crafted organizational structure and collection of educational resources. An equally important potential benefit is the establishment of post-secondary and university partnerships that help to raise awareness and interest of students in information technology as well as other STEM disciplines.

Experience with all of these competition formats has confirmed their ability to pique students’ interests in STEM disciplines and more specifically the fields of information technology and in-

formation security. Less apparent however, is which approach is most appropriate to implement given the goals of the host university and intended participants. Any university desiring to implement their own cyber defense competition should carefully consider the resource demands of each approach, explore partnerships with other organizations for funding and other assistance, and ensure their goals are clearly identified.

Conclusion

Given the spotlight that the government and private sectors currently shine on cybersecurity, the number of organizations desiring to form partnerships that avail cyber defense competitions to high school students is expected to continue to grow. Colleges and universities are ideally positioned to foster such partnerships. The popularity of cyber defense competitions among high school and college students is evident. The growth reported by some universities borders on becoming viral in nature. It is acknowledged that competitions can be categorized in many ways. Three predominant competition formats were presented and contrasted along with potential advantages respective to each.

If your post-secondary institution is searching for a way to raise interest and awareness of students in STEM disciplines with relevance and excitement, then serious consideration should be given to stepping into the world of cyber defense competitions. Given that there are several cyber defense competition formats, it becomes a matter of determining which format will best help your organization to achieve its goals with the resources that are available.

While the golden standard of these formats, in terms of educational emphasis, is the Iowa State University IT-Adventures model, it is clearly the most resource demanding option for both the host university and participating high schools. While the least resource demanding and easiest approach to implement is clearly SANS NetWars, it does not have a development focus that helps to nurture the development of critical thinking skills essential to long-term success. CyberPatriot, on the other hand, may be the best format to utilize to host your inaugural year competition as it offers a moderate degree of education in exchange for a moderate investment in time and money. Overall, be sure to regularly check for changes in the formats of all of these cyber defense competitions as they are continuing to rapidly evolve.

References

- Albert, R. (2009). The “U” in Information Security. *Proceedings of the 2009 ASCUE Summer Conference*. Retrieved March 8, 2010 from http://www.eric.ed.gov/ERICDocs/data/ericdocs2sql/content_storage_01/0000019b/80/45/2f/85.pdf
- Center for Strategic & International Studies (CSIS) (2010). *US Cyber Challenge*. Retrieved March 3, 2010 from <http://csis.org/uscc>
- Conklin, A. (2006). Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course. *Proceedings of the 39th Hawaii International Conference on System Sciences – 2006*. Retrieved March, 2, 2010 from <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1579743&userType=inst>
- Grier, Peter, (2009). CyberPatriot Smack Down. Retrieved March 11, 2010 from <http://www.airforce-magazine.com/MagazineArchive/Pages/2009/June%202009/0609cyberpatriot.aspx>
- Jacobson, D. & Rursch, J. (2008). Engaging Millennials with Information Technology: A Case Study Using High School Cyber Defense Competitions. *12th Colloquium for Information Systems Security Education (CISSE) Proceedings*. Retrieved March, 2, 2010 from www.cisse.info/colloquia/cisse12/proceedings12/PDFs/TOC.pdf
- Rursch, J., Luse, A., & Jacobson, D. (2010). IT-Adventures: A Program to Spark IT Interest in High School Students Using Inquiry-Based Learning With Cyber Defense, Game Design, and Robotics. *IEEE Transactions on Education*, 53(1), 71-79. doi:10.1109/TE.2009.2024080.
- National Security Council (2009). 60-day Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. Retrieved March 10, 2010 from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
- SANS Institute (2010). Retrieved March 11, 2010 from http://www.sans.org/why_sans.php.
- United States Air Force (2005). Air Force Releases New Mission Statement. Retrieved March 10, 2010 from <http://www.af.mil/news/story.asp?id=123013440>

Acknowledgements

Special thanks to Rachel, Alexandra and Samuel for their patience and support and to all those cited above for their contributions to and promotion of information security.

Special thanks to Ken, my husband for his unending support for my interests and career and to Ray Albert for including me in this adventure.