Communications of the IIMA

Volume 11 | Issue 2 Article 1

2011

A League of Our Own: The Future of Cyber Defense Competitions

Daniel Manson
California State Polytechnic University

Anna Carlin
California State Polytechnic University

A League of Our Own: The Future of Cyber Defense Competitions

Daniel Manson
California State Polytechnic University, Pomona, USA
dmanson@csupomona.edu

Anna Carlin
California State Polytechnic University, Pomona, USA
acarlin@csupomona.edu

ABSTRACT

Numerous cyber defense competitions exist today for individuals and teams to test their cyber security skills where each team has to "win or go home." What is missing from these competitions is a league allowing head to head competitions over the course of a season, much like a sport. Teams playing several hours every week during a ten-week season have the opportunity to improve their cyber security skills. This paper provides an overview of cyber security competitions, and how a National Cyber League can greatly expand the number of and participants in these competitions at a much lower cost leveraging virtual technologies.

INTRODUCTION

According to a 2010 survey of 45 different companies, cybercrime costs an average of $3.8 million per organization per year (Whitney, 2010). Experts state that only 1,000 people in the United States have the sophisticated skills needed for the most demanding cyber defense tasks (Evans & Reeder, 2010). To meet the computer security needs of U.S. government agencies and large corporations, a force of 20,000 to 30,000 similarly skilled specialists is needed (Gjelten, 2010). One way this need is being addressed is through computer security competitions. These competitions can foster innovation and educate students in a highly motivating setting (Childers, et al., 2010).

One example is students from the Los Angeles Unified School District's (LAUSD) Locke High School, who competed in 2010 and 2011 in a cyber defense competition. During this time, Morris Phillip's high school cyber defense team practiced for many hours, every week. Competing for the first time in a national competition against several hundred other high school teams, they advanced through the first round. In the second round last December, they played in an auditorium with teams from LAUSD's Locke High School, Kennedy High School, Los Angeles High School and Franklin High School along with teams across the country (Air Force, 2010). They advanced through the second round, and on March 31 and April 1, 2011 played for the National Championship against eleven other high school teams in CyberPatriot, billed as the world's largest high school cyber defense competition (The Street, 2011). While Locke did not win the competition, they gained valuable experience and exposure to colleges and companies sponsoring the event.

If this sounds like a team competition sport, it is. The sport is cyber defense, a "mind sport" that involves several hours to several days of running, maintaining, and defending a simulated commercial network from attack by security professionals (Manson & Carlin, 2011). Cyber defense competitions provide a hands-on, active learning experience enabling students to apply theoretical concepts in a physical environment (Conklin, 2006). From high school to community college to universities, cyber defense competitions are becoming an annual ritual for kids who play for much more that trophies and bragging rights. Cyber security competitions develop skills that industry and government desperately need, and provide a path to college and careers. Students who do well receive scholarships, internships and full time positions that jumpstart careers in cyber security.

THE IMPORTANCE OF CYBER SECURITY AS A TEAM COMPETITION SPORT

Team competition sports are important to young people for good reasons. A 1989 Michigan State survey of 28,000 boys and girls around the country listed the top three reasons as "to have fun" followed by "to do something I am good at" and "to improve my skills" (Hyman, 2010). Cyber security competitions are increasingly popular for the same reasons as other sports When cyber security is viewed as a team competition, it drives interest in computer science, computer engineering, information technology, computer information systems and other Science, Technology, Engineering and Math (STEM) disciplines. After the dot-com collapse in 2000, these areas all suffered significant enrollment declines for several years. Now STEM programs are starting to see enrollment gains, one reason being cyber security is viewed as an exciting and growing profession.

Many schools today include cyber defense exercises as part of their curriculum (Augustine, De Looze, Monroe, & Wheeler, 2010; Hoffman, Rosenberg, Dodge, & Ragsdale, 2005; Mullins, Lacey, Mills, Trechter, & Bass, 2007; Sherman, Roberts, Byrd, Baker, & Simmons, 2004). While teaching cyber defense through hands-on exercises is a valuable learning experience by itself, team development to competition level requires many hours of practice in addition to classroom experiences. Students that succeed in cyber defense competitions commit the same time, energy, and enthusiasm that high school and college athletes commit to baseball, basketball, football and other traditional sports. A class or lab project is merely a starting point. Table 1 summarizes different types of well-known cyber defense competitions, which will be covered on the following pages.

Table 1: Summary of Well-Known Cyber Security Competitions.

Competition	Eligible to Compete	Student Offense	Level of Virtual Technology
Defcon	Anyone	Yes	Medium
iCTF	Anyone	Yes	Medium
CDX	U. S. Service Academies	No	Medium
National CCDC	U. S. Colleges and Universities	No	Medium
CyberPatriot	U. S. High Schools and ROTCs	No	High

TYPES OF CYBER DEFENSE COMPETITIONS

Def Con®

The first DEF CON® hacker convention took place in Las Vegas in 1993 and has grown to become one of the world's largest hacker conventions ("Def Con," 2011). Capture the Flag (CTF) began at DEF CON® in the 1990s and has become an annual conference highlight. In CTF, teams attempt to defend their own electronic "flags" and capture flags on opposing teams' machines. A definition of CTF is "an educational exercise to give participants experience in securing a machine, as well as conducting and reacting to the sort of attacks found in the real world." ("Capture the Flag," 2011). Advanced skills in penetration testing, reverse engineering, and network security are required to play in the DEF CON® CTF.

International Capture the Flag

An international version of Capture the Flag (iCTF) was started at the University of California, Santa Barbara (UCSB) in 2004. The latest UCSB iCTF was held December 3rd, 2010 and involved 72 teams and 900 participants from 16 countries. In a 2011 IEEE Security and Privacy article, Brian Pak, an undergrad student at Carnegie Mellon University and leader of the of the winning iCTF competition team Plaid Parliament of Pwning, described the value of the competition as follows. "We study crypto, we study reverse engineering, but competitions are where we actually test and use them" (Vigna, 2011).

U. S. Service Academies Cyber Defense Exercise

In 2001 the United States Military Academy at West Point challenged the five United States service academies to an inter-academy Cyber Defense Exercise (CDX) (Hoffman et al., 2005). U. S. Service Academies for the Air Force, Army, Navy, Coast Guard, and Merchant Marine began a competition to test the network defense skills of their students. Each team was responsible for setting up and maintaining a closed, secured computer network. A group of National Security Agency (NSA) specialists graded each team on their ability to maintain their network services while detecting, analyzing, and responding to potential intrusions (Hoffman et al., 2005).

The CDX has also grown and evolved over the years to consist of a "Red Cell" of attackers, a "White Cell" of judges, and a "Blue Cell" of competing teams. The 2010 CDX theme, "Survival Strategies in a Hostile Network Environment", emphasized a strategy of mitigating vulnerabilities rather than trying to simply avoid them. Another innovation in 2010 was creation of a "gray cell" in which 12 personnel played the role of users on the blue cell network ("Fact Sheet," 2011).

National Collegiate Cyber Defense Competition

Seeing the success of the United States Military Academy's competition in preparing students to be defenders, a group of government, academics, students, and industry representatives decided to create uniform cyber defense exercises for post-secondary education in February of 2004. The

group decided that a uniform structure would allow any university to hold a challenge regardless of size or resources available. The primary goal was to encourage more universities to offer students real-world experience in information assurance. The first Collegiate Cyber Defense Competition (CCDC) was hosted by the Center for Infrastructure Assurance and Security (CIAS) at the University of Texas, San Antonio in April of 2005 ("History of CCDC," 2011).

The National Collegiate Cyber Defense Competition now hosts state level and nine regional competitions. Winners from state level competitions advance to a regional; and, regional winners advance to the National CCDC held in April at the University of Texas, San Antonio.

The template that a competition follows includes three main teams named using colors of red, white, and blue. Student teams are blue and are separated from the other blue teams with their own workspace. Each team is required to have a faculty advisor from their school and a designated team captain. Blue teams are given hardware and software to setup their network and secure it before the red team is unleashed. Software installed on the equipment usually is not current and has known security vulnerabilities (Manson & Carlin, 2011).

The red team consists of industry cyber security professionals that will try to penetrate or disrupt each blue team's network. The only attack barred from the competition is a denial of-service (DOS) attack as it was felt that blue teams may not react timely and result in all the blue teams' networks losing service.

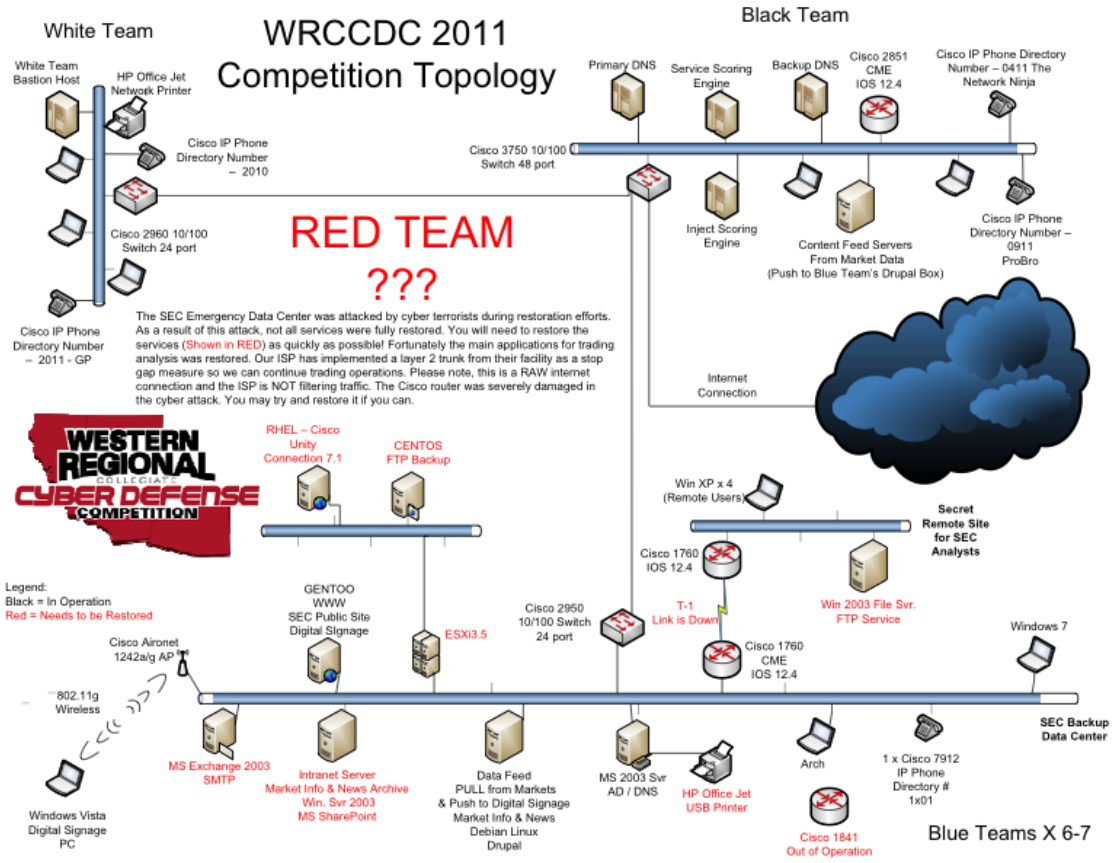
The white team also consists of industry professionals responsible for monitoring the network, implementing scenario events, and refereeing. A white team member verifies service functionality prior to competition scoring commences. The scenario events are typical business tasks called injects that could require the student teams to add new users, backup data, and add a network printer.

The scoring model involves awarding points for successful completion of business injects, taking points away for failure to maintain required business services, deducting points for successful red team exploits, and awarding points for a corresponding incident report. Most injects are scored by a white team member observing the system change. A few injects may also require a written report or presentation to executive management who may not have a technical background. The number of points given for injects vary; for example, configuring SSH access on a system may be worth a total of 50 points, creating/enabling new user accounts 100 points, and installing new infrastructure hardware 100 points.

The scoring engine tracks whether HTTP, HTTPS, SSH, POP and other required services are up or down, with points given for services being up during measured intervals. When a red team member succeeds with an exploit against one team, the same exploit must be attempted against all teams and scored accordingly. Student teams can recoup points due to a successful exploit by completing an incident report. The incident report should clearly identify the attack and what the team did to mitigate the risk to the organization. The team with the highest number of points wins the regional competition and advances to the national competition (Carlin, Manson & Zhu, 2010).

Although there are common rules that must be followed by all state, regional and national competitions, the length of time and infrastructure can vary from one competition to another. The 2011 Western Regional CCDC held March 25-27 at Cal Poly Pomona included approximately 22 hours of competition time over three days using the following competition infrastructure.

Figure 1: WRCCDC 2011 Competition Topology.



CyberPatriot

In 2008, the Air Force Association (AFA) partnered with CIAS at the UTSA to create a three-phase approach to a national high school cyber defense competition called CyberPatriot (White, Williams, & Harrison, 2010). In fall 2010 and early 2011, CyberPatriot was expanded to full national competitions in "All Service" and "Open" high school divisions. (op. cit.) The first in-person championships of both high school divisions took place March 31 and April 1, 2011 in Washington, D.C., at the AFA's CyberFutures Symposium and Technology Exposition (Cyberpatriot, 2011).

CyberPatriot is now open to high school students between the ages of 13 and 18. High schools must be an accredited public or private institution or a registered home school association. Students in Civil Air Patrol (CAP) units are also eligible. CyberPatriot is designed to provide students with hands-on, practical knowledge in cyber security that develops their interest and desire for degrees and careers in cyber security and related areas. It is common knowledge that the United States does not produce enough graduates with degrees in science, technology, engineering and mathematics (STEM), it is hoped that CyberPatriot can help address this need as part of a larger national effort (Air Force, 2011).

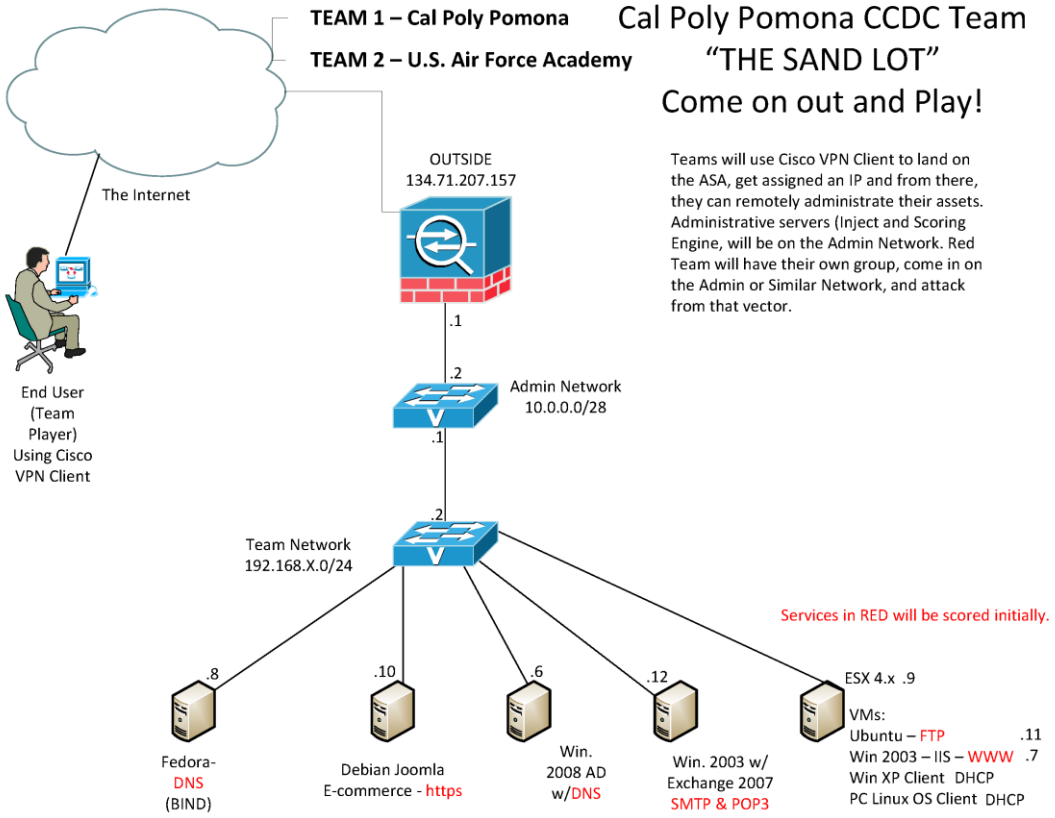
CyberPatriot registration opens in summer and closes around October 1st. An entry fee of $350 covers all direct costs and provides licenses for the Microsoft Academic Alliance Developer software package. Mentoring opportunities are available through the CyberPatriot website ("CyberPatriot Mentor," n.d.).

Virtual Competitions

Up to now, almost all regional and national collegiate cyber defense competitions have been face-to-face competitions, with all competitors and support personnel in the same location. Major obstacles to expanding these cyber defense competitions exist, including cost, scalability, and inclusion of high school students. Virtualization enables the creation and deployment of computer security lab exercises while minimizing the associated configuration time and the associated hardware requirements. A topology that we successfully used for a six hour virtual competition between Cal Poly Pomona and the Air Force is shown in Figure 2.

The 2011 National Collegiate Cyber Defense Competition included nine regions with approximately 100 schools. The National CCDC is a cyber defense version of "March Madness" where each team has to "win or go home". The same is true for CyberPatriot. All high school teams have to win to advance in the competition.

Figure 2: Virtual Cyber Defense Competition Topology.



THE CASE FOR A NATIONAL CYBER LEAGUE

What is missing for both the National CCDC and CyberPatriot is a league allowing head to head competitions over the course of a season. A National Cyber League (NCL) would allow teams to play for several hours every week for a season. The expectation is that all participants would improve their cyber security skills in a competition mode using this extended period of time. Table 2 shows the current timeline for CyberPatriot and National CCDC, and how a virtual NCL would compliment both competitions.

The CDL can be a training ground for both the CCDC and CyberPatriot teams by providing several opportunities to identify team deficiencies/inadequacies and benchmarking their skills against their competitors. Between rounds, the team can obtain personnel with the required skills and training on their deficiencies. Through each round, the teams can see whether their recruitment and training efforts are paying off.

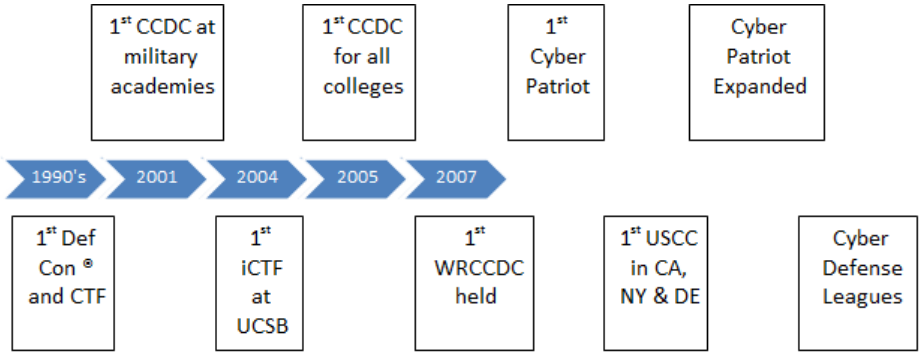
Table 2: Proposed 2012 National Cyber League Competition Season.

Month	NCL and CCDC Seasons	NCL and CyberPatriot Seasons
January	State CCDC	CyberPatriot
February	State/Regional CCDC	CyberPatriot
March	Regional CCDC	CyberPatriot
April	National CCDC	
May	Spring NCL	
June	Spring NCL	
July		Summer NCL
August		Summer NCL
September	Fall NCL	
October	Fall NCL	CyberPatriot
November	Fall NCL	CyberPatriot
December	Fall NCL	CyberPatriot

While budget cuts in high school and colleges increasingly impact traditional sports, creating virtual cyber competition "playing fields" will provide opportunities for tens of thousands of students to participate in virtual pickup games, exhibitions, and league play. Organizations can participate in the cyber league through sponsorship, red and white team participation, and combinations of industry and student teams, enabling students to learn side-by-side with cyber security professionals.

In addition, creating virtual cyber competition playing fields will help meet our nation's demand for tens of thousands of expert cyber defenders. The National CCDC and CyberPatriot have received sponsorship support from top cyber security, aerospace, defense and utility companies, as well as consulting firms, professional audit and security organizations and the Department of Homeland Security. These organizations see the value in developing cyber security talent through team competitions. Ongoing competitions could build on existing sports leagues and rivalries based on the NCAA and California Interscholastic Federation. As shown on the timeline below, cyber leagues can be viewed as the next evolution of cyber defense competitions.

Figure 3: General Evolution of Cyber Defense Competitions.



Organizational Support

Organizations can participate in the cyber league through monetary sponsorship, in-kind support and team participation. Industry sponsorship provides access to some of the best and brightest young cyber security talent. Added perks include the publicity associated with competitions, product awareness and product placement, as well as, the opportunity for cyber security professionals at their companies to gain hands-on experience themselves.

In the future, organizations could tailor competitions to their specific industry needs by testing out new products while gaining experience with specific vulnerability scenarios. Industry professionals provide a much needed "reality check" on the validity of cyber defense competitions. Competitions can also be used by the industry as an in-house training environment and a "virtual simulator" to assess employee cyber defense skills and competencies.

Support for cyber security "boot camps" are another way industry can promote hands-on cyber security learning and passion in young people. The U.S. Cyber Challenge (USCC) camps which began in 2010 are expanding. Students attending the camps not only gain in-depth skills and practice through Capture the Flag competitions, they leave the campus hungry for more opportunities to practice and further develop their abilities.

CONCLUSION

From high school through college and beyond, the cyber industry can make a huge difference by mentoring future experts. As schools deal with ongoing budget cuts, the ability of professionals to step in and work closely with faculty and students involved with these competitions can ensure that young talent is nurtured, not neglected.

REFERENCES

Air Force Association. (2010, December 22). *CyberPatriot, beyond the bell strive to further students' education experience*. Retrieved April 10, 2011, from http://airforceassociation.blogspot.com/2010/12/cyberpatriot-beyond-bell-strive-to.html

Air Force Association. (2011, August 11). *CyberPatriot FAQ*. Retrieved April 10, 2011, from http://www.uscyberpatriot.org/about/Pages/FAQ.aspx

Augustine, T. A., De Looze, L. L., Monroe, J. C., & Wheeler, C. G. (2010). Cyber competitions as a computer science recruiting tool. *Journal of Computer Sciences in Colleges, 26*(2), 14-21.

Capture the flag. (2011). In *Wikipedia*. Retrieved April 10, 2011, from http://en.wikipedia.org/wiki/Capture_the_flag

Carlin, A., Manson, D., & Zhu, J. (2010). Developing the cyber defenders of tomorrow with regional collegiate cyber defense competitions (CCDC). *Information Systems Education Journal, 8*(14). Retrieved from http://isedj.org/8/14/index.html

Childers, N., Boe, B., Cavallaro, L., Cavedon, L., Cova, M., Egele, M., & Vigna, G. (2010). Organizing large scale hacking competitions. *Detection of Intrusions and Malware, and Vulnerability Assessmen: Lecture Notes in Computer Science*. Berlin, Germany: SpringerLink. doi: 10.1007/978-3-642-14215-4_8

Conklin, A. (2006). Cyber defense competitions and information security education: An active learning solution for a capstone course. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06),* Kauai, HI.

CyberPatriot crowns national championship winners. (2011). Retrieved April 20, 2011, from http://www.prnewswire.com/news-releases/cyberpatriot-crowns-national-championship-winners-119242769.html

CyberPatriot Mentor Registration. (n.d.). Retrieved April 10, 2011, from https://www.uscyberpatriot.org/_layouts/cyberpatriot/mentorregistration.aspx

Def Con. (2011). In *Wikipedia*. Retrieved April 10, 2011, from http://en.wikipedia.org/wiki/DEF_CON

Evans, K., & Reeder, F. (2010). *A human capital crisis in cybersecurity: Technical proficiency matters: A report of the CSIS Commission on cybersecurity for the 44th Presidency.* November, 2010. Washington, DC: Center for Strategic and International Studies

Fact sheet: NSA/CSS cyber defense exercise: After exercise. (2011). Retrieved April 10, 2011, from http://www.nsa.gov/public_info/_files/press.../cdx_fact_sheet.pdf

Gjelten, T. (Narrator). (2010, July 19). Cyberwarrior shortage threatens U.S. security. In NPR (Producer), Morning Edition [Radio program]. Listening location: http://www.npr.org/templates/story/story.php?storyId=128574055

History of CCDC. (2011). Retrieved April 20, 2011, from http://nationalccdc.org/index.php?option=com_content&view=article&id=47&Itemid=34

Hoffman, L. J., Rosenberg, T., Dodge, R., & Ragsdale, D. (2005). Exploring a national cybersecurity exercise for universities. *Security & Privacy, IEEE , 3*(5), 27-33.

Hyman, M. (2010, January 30). A survey of youth sports finds winning isn't the only thing. *New York Times*. Retrieved April 10, 2011, from http://www.nytimes.com/2010/01/31/sports/31youth.html?_r=2&ref=sports

Manson, D., & Carlin, A. (2011). Educating the next generation of security professionals. *Lydian Journal* (6). Retrieved from http://pymnts.com/educating-the-next-generation-of-security-professionals/

Mullins, B. E., Lacey, T. H., Mills, R. F., Trechter, J. M., & Bass, S. D. (2007). How the cyber defense exercise shaped an information-assurance curriculum. *Security & Privacy, IEEE, 5*(5), 40-49.

Sherman, A. T., Roberts, B. O., Byrd, W. E., Baker, M. R., & Simmons, J. (2004). Developing and delivering hands-on information assurance exercises: Experiences with the cyber defense lab at UMBC. *Information Assurance Workshop, 2004: Proceedings from the Fifth Annual IEEE SMC.*

The Street. (2011, April 20). *Registration for cyber patriot IV now open!* Retrieved April 20, 2011, from http://www.thestreet.com/story/11088208/1/registration-for-cyberpatriot-iv-now-open.html

Vigna, G. (2011). The 2010 international capture the flag competition. *IEEE Security and Privacy, 9*(1), 12-14.

White, G. B., Williams, D., & Harrison, K. (2010). The cyberpatriot national high school cyber defense competition. *Security & Privacy, IEEE, 8*(5), 59-61.

Whitney, L. (2010, August 5). The cost of cyber crime. *InfoTech Spotlight*, August 5, 2010. Retrieved April 10, 2011, from http://it.tmcnet.com/topics/it/articles/94247-cost-cybercrime.htm

This Page Was Left Blank Intentionally.