Developing the Cyber Defenders of Tomorrow With Regional Collegiate Cyber Defense Competitions (CCDC)

Anna Carlin
acarlin@csupomona.edu

Daniel Manson
dmanson@csupomona.edu

Computer Information Systems Department
College of Business Administration
California State Polytechnic University
Pomona, CA 91768 USA

Jake Zhu
jzhu@csusb.edu
Information and Decision Sciences Department
College of Business and Public Administration
California State University
San Bernardino, CA 92407 USA

ABSTRACT

With the projected higher demand for Network Systems Analysts and increasing computer crime, network security specialists are an organization's first line of defense. The principle function of this paper is to provide the evolution of Collegiate Cyber Defense Competitions (CCDC), event planning required, soliciting sponsors, recruiting personnel for the operations, red, white and blue teams. Information on one school's preparation will be provided with a review of what could have been improved to prepare their team for the competition.

Keywords: cyber defense, student competitions, security education, intrusion detection, security, network security

1. INTRODUCTION

The Bureau of Labor Statistics identified Network Systems and Data Communication Analysts as the fastest growing occupation with a percentage increase of 53.4% by 2016. In 2006 there were 262,000 Network Systems and Data Communication Analysts positions nationally with a projected increase to 402,000 by 2016. The most significant source of postsecondary education or training is a Bachelor's degree (Bureau of Labor Statistics, 2006).

The Computer Crime and Security Survey indicated that the previous five years showed a decrease in cybercrime losses but this year respondents reported a significant increase. In addition, the number of reported intrusions was 29% (CSI Survey, 2007). The Los Angeles County District Attorney, Steve Cooley, stated that "theft of

proprietary information, personal identifiable information, and intellectual property is the fastest growing category of crime in the U.S."

With the projected higher demand of Network Systems Analysts and increasing computer crime, Network Analysts can become critical to an organization's security defenses. Network Analysts job duties include not only the selection, setup, and maintenance of networks, but also the monitoring of the network for unusual or suspicious activity. Network Analysts are typically an organization's first line of defense against intruders.

With the increasing demand for network professionals with a Bachelor's Degree coupled with increasing computer crime, universities are looking for ways to educate students in security issues. In the academic environment, it can be difficult providing real-world experiences when dealing with issues like security over your computer resources. Universities are concerned that students may use tactics demonstrated in class for their own personal gain that violates the law. High school students have broken into computer systems to change grades and AP test scores to improve their college admission acceptances (Top Tech News, 2008).

One way that universities are training students to be the cyber defenders of tomorrow is through Collegiate Cyber Defense Competitions (CCDC). Competitions such as these teach students to be defenders, rather than attackers. Students must understand the security vulnerability, how it can be exploited, and ways to minimize the risk to an organization. This paper provides a description of CCDC, the university's participation in such a competition, and learning experiences.

2. EARLY CYBER DEFENSE COMPETITIONS

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.

A trophy is awarded to the team determined to be most successful by the NSA. "The trophy is a tangible reward for the winning team, but ultimately, experience is the win for every student and NSA. At the end of the day, we've created a new crop of information assurance torchbearers who have an understanding of the strategic imperative of safeguarding the nation's security." (NSA Press Release, 2006)

3. REGIONAL COLLEGIATE CYBER DEFENSE COMPETITIONS

Seeing the success of the U.S. 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 at the University of Texas, San Antonio in April of 2005. (National Collegiate Cyber Defense Competition website)

Teams

The template that a regional competition follows includes three main teams named using patriotic colors of red, white, and blue. Student teams are assigned the color blue and are segregated from all other teams in their own classroom/lab. Each team is required to have a faculty advisor from their school and a designated team captain. They are provided hardware and software to setup their network and secure it before the red team begins their exercises approximately 2 hours later. Software installed on some servers may not be current and may have known security vulnerabilities that the blue team needs to evaluate and address.

The red team consists of industry representatives that will attempt to infiltrate or disrupt each blue team's daily network operations throughout the competition. The red

team will use all their technical skills to compromise their network and disrupt business, in addition to, using social engineering to gain valuable information. 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 to lose service.

The white team also consists of industry professionals responsible for monitoring the network, implementing scenario events, and refereeing. A White Team member will verify service functionality prior to competition scoring commences. The scoring is based on keeping required services up, controlling/preventing unauthorized access, and completing business tasks requested by the white team throughout the competition. Typical business tasks called injects may be to add new users, backup data, and add a network printer. Points will be awarded for keeping required services up and inject requests completed. Points will be deducted for required services being down and successful penetration by the red team. The team with the highest number of points wins the competition.

The scoring model involves giving points for successful completion of injects, taking points away for failure to maintain required business services, and deducting points for successful red team exploits.

Injects involve business requests such as account updates, blocking AIM and P2P, and Network Redesign. Most injects are scored by a White Team member observing the system change. A few injects may also require a written report or presentation. 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.

While we have not included Easter eggs and treasure hunts as part of the current competition, these added activities are under consideration for future events.

Regional competitions are permitted to define additional color teams for infrastructure needs at the university hosting the competition. The operations team ensures that all the needed hardware and software is available and ready for each blue team. For each red team, the necessary network resources are available and ready. And most importantly that the all blue teams are connected to a central router and scoring system for the white team. While all this is going on, the operations team needs to ensure that the hosting university's network services are not impacted.

National Competition

Universities became excited with the experience gained by students in competitions like these that regional competitions are now held and the regional's top team is sent to the National Collegiate Cyber Defense Competition at the University of Texas, San Antonio. Today there are 6 regional competitions held in the Mid-Atlantic, Midwest, Northeast, Southeast, Southwest, Northwest and the Western. See Figure 1 below for years of 1st Regional Competitions.

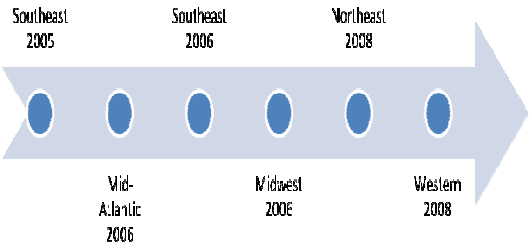

Figure 1: 1st Regional Competitions Held in Each Region

When a region covers more than one state with too many teams to accommodate, state competitions are held where the winner of each state competition competes to be the regional winner that proceeds to the national competition in Texas.

The Western Region includes California, Nevada, and Arizona. The Southeast Region includes Kentucky, Tennessee, South Carolina, Mississippi, Alabama, Georgia, and Florida. The Southwest Region includes New Mexico, Texas, Oklahoma, and Arkansas. The Northwest Region includes Alaska, Oregon, Idaho, and Washington. The Mid-Atlantic Region includes Pennsylvania, Virginia, West Virginia, Maryland, Delaware, and New Jersey. The Northeast Region includes New York, Connecticut, New Hampshire, Massachusetts, Maine, Vermont, and Rhode Island. The Midwest Region includes Minnesota, Iowa, Michigan, Wisconsin, Illinois, Indiana, and Ohio. The Central Region consists of Utah, Colorado, Nebraska, Missouri, Montana, North Dakota, South Dakota, and Wyoming. See Figure 2 below for regional groupings.

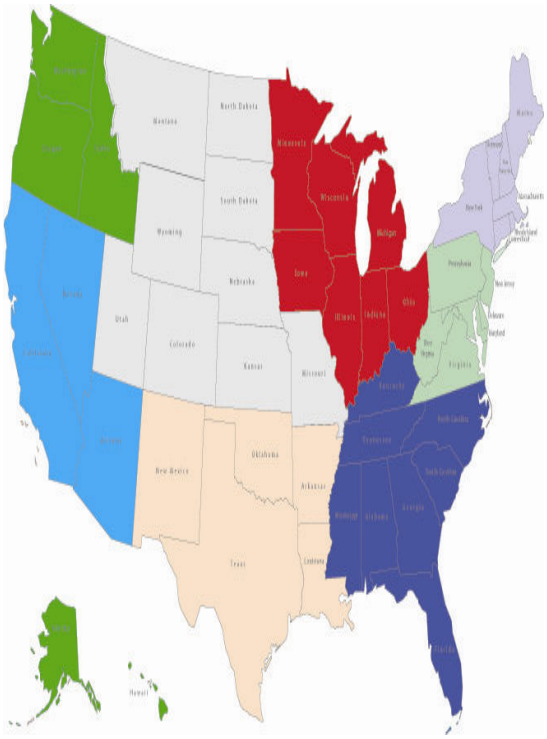

Figure 2: Regional CCDC Map

Since the first National Collegiate Cyber Defense Competition, several published papers have emphasized the value and potential of these competitions. Conklin (2006) mentions the "opportunity for active and collaborative learning." White and Dodge (2007) highlight the increase in security awareness and interest in computer security at schools involved in the competition. Mattson (2007) highlights the impact of "hands-on, real-world training these events provide". Chu, et. al. (2007) adds that even with current success, more work is needed to "promote student's creative design and problem solving skills." The Collegiate Cyber Defense Competitions "gives us the opportunity to put your brain power, your education, your experience and skills into this whole area of network security" (Cooley, 2008).

2. EVENT PLANNING

A Computer Information Systems (CIS) faculty from Cal Poly Pomona attended the 2006 CCDC Midwest Regional scoring workshop at Moraine Valley Community College and the 2007 CCDC Midwest Regional, also at Moraine Valley. Attending provided valuable experience and understanding of critical success factors to run a cyber defense competition. At the June 2007 Colloquium for Information Systems Security Educators, Dr. Greg White from the University of Texas, San Antonio presented findings on the recent 2006 National CCDC. After the presentation, Cal Poly Pomona committed to host the 2008 Western Regional CCDC.

In the spring of 2007, a Computer Information Systems Senior Project team assisted in early preparation for Cal Poly Pomona to host the 2008 Western Regional Collegiate Cyber Defense Competition (CCDC). The project involved students working with the computers and associated network equipment to test the equipment functionality needed to support the competition. In the summer of 2007, two additional Senior Project teams continued preparation efforts for the Western Regional CCDC. Both teams developed a Western Regional CCDC website, marketing materials, and prepared equipment for a mock competition. The website was critical to promoting the competition to students, white and red team members, sponsors and the media. The website included sections on registration, sponsorship, location, and a FAQ.

After the mock competition, it was clear that significant work was needed to prepare an adequate competition infrastructure. In the fall of 2008, James Schneider, a CIS student and Network Analyst at Cal Poly Pomona continued infrastructure research and development for the Western Regional

CCDC. One result of this research was the following network diagrams for the competition. Figure 3 illustrates the network design for the blue teams while Figure 4 shows the topology for the entire competition.

Each student team is provided the following:

- CISCO 1841 Router
- CISCO ASA Security Appliance for firewall, Unified Communications (voice/video) security, SSL and IP-sec VPN, intrusion prevention (IPS), and content security services
- CISCO switch
- 4 servers with Windows 2003, Windows 2000, Gentoo Linux, and Ubuntu Linux operating systems
- 2 local machines with Windows XP operating system

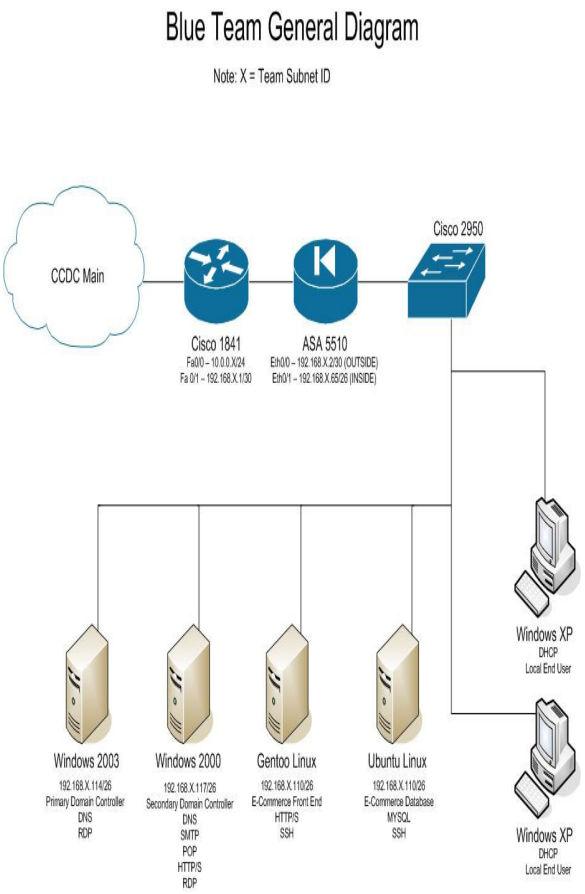

Figure 3: Blue Team Diagram

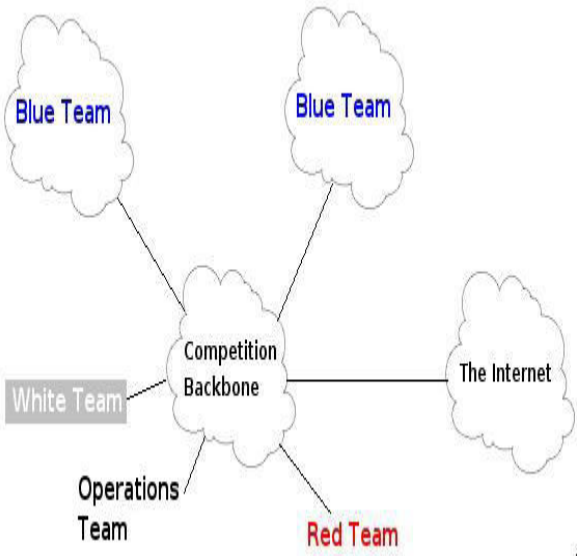

Figure 4: Competition Topology

Because Cal Poly Pomona had never held a contest requiring a dedicated network infrastructure and multiple computer networks, testing became a priority. In addition, students were encouraged to become part of the testing process to create interest in the competition. Weekend testing in a computer lab/classroom first occurred the weekend of 12/7 and 12/8/2007. Testing continued on 12/23, 1/26 and 1/27, 2/9 and 2/10, 2/16 and 2/17, 2/23 and 2/24, and weekend of 3/8 and 3/9. A final test was held with Red Team members on 3/15.

In January 2008 the following call for competitors was e-mailed to 2 and 4 year schools in Southern California. "I would like to invite you and your students take part in a new event we are hosting this Spring. We are hosting the first Western Regional Collegiate Cyber Defense Competition (CCDC) on March 28th, 29th and 30th. We are very interested in a student team from your school. The CCDC is the first competition that specifically focuses on the operational aspect of managing and protecting an existing "commercial" network infrastructure." (Western Collegiate Cyber Defense Competition website).

While most student and faculty feedback was positive for competing in a cyber defense competition, there were strict limits on who could compete as stated in the following rule from the National CCDC. "Each team

member must be a full-time student of the institution the team is representing and must not be currently employed in the IT industry (security operations, network administrator, system administrator, programmer, network operations, help desk, etc.) as a salaried employee or as an hourly employee for more than 20 hours per week. Team members must qualify as full-time students as defined by the institution they are attending - typically this means the team member must be enrolled in 12 or more semester credit hours for undergraduates and 9 or more semester credit hours for graduate students during the semester the competition is held." (National Collegiate Cyber Defense Competition website).

Because we could not allow less than full-time students and students working more than half-time in IT, we struggled to receive commitments from students for the competition. What finally enabled us to have four teams competing was our sponsor support. A month before the competition, we were able to make the following statement to student teams. "Because of our sponsors, we should be able to provide entry fee, meals, and two nights lodging (double occupancy) for teams competing in the CCDC."

Sponsors

Obtaining sponsors was just as critical as student teams for the competition. One successful way to obtain sponsors does not exist, but many avenues do exist. Cal Poly Pomona faculty had existing relationships with several audit and security related professional associations. Face-to-face presentations and meetings with local chapters of the Institute of Electrical and Electronics Engineers (IEEE), Information Systems Security Association (ISSA), Information Systems Audit and Control Association (ISACA), and High Technology Crime Investigation Association (HTCIA) all resulted in monetary sponsorships for the Western Regional CCDC.

Additional sponsorships were found through two other types of contacts. Ernst and Young and Aerospace Corporation both recruit CIS graduates, and committed to sponsoring the competition. Microsoft and McAfee have strong vendor relationships with our schools, and became sponsors. McAfee's strong relationship with the California State University System help secure them as a title sponsor for the competition.

Red and White Team Formation

Simultaneous with obtaining sponsorships was the creation of a Red Team of professional security experts and a White Team of competition referees. Our first Red Team member, Rodney Kocot, and our first White Team member, Michael Felker, were recruited at an ISACA Meeting. Attending the 1/29/2008 Quarterly meeting of the Los Angeles Electronic Crimes Task Force was a turning point in creating a Red Team. At the meeting Jimmy Garcia, Supervising Investigator of the High Technology Crimes Investigation for the Los Angeles District Attorney's Office committed to being part of the Red Team for the competition. Jimmy was a major reason for the success of the competition, as he brought Donn Hoffman, Dave Maupin and Justin Pheffer from his office as Red Team Members, and made possible Mr. Steve Cooley, Los Angeles County District Attorney, to be our opening keynote speaker.

In addition to testing, numerous conference calls were held. The conference calls enabled formation of the Red and White Teams, discussion and agreement of competition rules, schedule and logistics. We were also able to share documentation from prior National and Regional Collegiate Cyber Defense Competitions, including injects (service requests) that were to be assigned to the student teams during the competition. As the competition drew near, the White team held separate conference call to finalize injects.

The actual competition had a few glitches, none of which kept the competition from being viewed as a success. After the keynote speaker, Blue Teams were supposed to have two hours to secure their systems before Red Team attacks began. Due to network issues, the Red Team attacks were delayed by 90 minutes. White team injects were adjusted throughout the competition.

3. COMPETITION OUTCOMES

A survey of participants after the competition confirmed its value. Typical comments included:

- "Not bad, but better if there were more faculty present"
- "Given the constraints, I thought it went very well"
- "Love this stuff, but as you noticed it is difficult to mockup"
- "I would do this again"

As a participant university of the 2008 Western Regional Cyber Defense Competition, several benefits deserve mentioning in the areas of knowledge integration, applying classroom learning to the real world, teamwork, faculty participation, equipment, university administration support, student leadership, training, and preparation. Each area is discussed in more detail below.

Knowledge integration is the key to successful college learning. One of the major problems of an MIS program is that pieces of knowledge/skill sets are learned through different classes and one capstone course usually helps students to put everything together; but not nearly enough to have the depth students need to be a successful IT professional. This competition allowed students to demonstrate their understanding of network security at a detailed level.

While putting everything together is important, bridging the gap of classroom learning and real world IT is another hurdle in student learning. An instructor could easily explain to students we are doing real IT (networking in this case); but it would very difficult to explain well to them the only difference is that we are somewhat structured in class while the real IT is less structured where more random variables need to be considered. With this competition, it made it easier to tell the difference.

Teamwork is a somewhat paradoxical word in college classrooms. We all do it in our projects and assignments; yet most students hate it. They suffer when they are stuck with an underperforming team in the classroom. The competition made them work as a team without thinking of it. As a matter of fact, one cannot do all that is required in this competition. They learned to leverage each others' strength and learn together.

While participating in the cyber defense competition, a few lessons were learned in several areas:

- Training for faculty – faculty may not have managed a real network, nor defended a problematic one. If trained in setting up and securing a network, faculty would be able to form a balanced student team with critical skill sets to compete well. In addition, faculty could hold their own mock competitions and would not be dependent on traveling to regional mock competitions to practice.
- Equipment – With the state budget shrinking, most schools cannot afford state-of-the-art network equipment for classes to experiment. Instead, a very minimal number of old networking devices are used.
- A competition of this scale needs the involvement from more than one faculty member for each team. With multiple Operating System environments, selection of tools, vendor specific requirements, hacking defense and business analysis skills, it is unrealistic that one faculty member can master everything needed to ensure your team's success in the competition. Even though faculty are not directly involved in the competition itself, departmental or even a college's expertise should be leveraged during training.
- Administration support – Deans and chairs may not know what you are doing unless you win something, but not everyone is a winner. We feel every team needs the financial and resource support from their administration.
- Release time for faculty – This is the only way to have a sustainable program like the regional collegiate cyber defense competition. Release time would enable the faculty advisor(s) to spend ample time and energy to prepare their team for the competition.
- Student leader – Without one, it is not going to happen; the faculty member's role is to identify, encourage and support students to participate in competitions such as these.

Students provided suggestions to improve future competitions:

- Add a Traffic Generator so that Red Team activity is masked with normal consumer activity on the website.
- Require website access for White Team to also act as a consumer.
- Blue Teams should not be allowed to block everyone except the scoring engine.
- Red Team members should be allowed to perform social engineering as this is a common ploy used by would-be hackers.
- Allow anyone access to the room which forces teams to be diligent of the physical perimeter.

For the team when preparing for the competition:

- Plan to train early, usually six months before the competition.
- Train by reserving a student lab for a couple hours, two to three days a week.
- Provide training for the team in Cisco, networking, Linux, computer forensics, Active Directory, Email/Exchange, LDAP, Unix and Cisco ASA Firewalls to ensure that the team is well rounded to compete successfully.
- Hacking Tools – teams should create their own toolbox to aid in the detection of suspicious activity (i.e., websites to use, tools you want to download, etc.).

When the blue team is competing:

- Install the Service packs first.
- Get the services up and running (DNS, Active Directory, Email both Exchange or open source, etc.).
- Install critical updates.
- Windows 2000 Machines should be backed up and then deleted. Keep the business data and load it into Windows 2003 Server machines.

4. CONCLUSION

Regional Collegiate Cyber Defense Competitions were developed to protect what the government, organizations, and individual's value. Regional Collegiate Cyber Defense Competitions do prepare students to defend a network while under attack. As evidenced by the end-of-competition feedback, members of all teams felt that the competition was well worth the time and energy expended. Suggestions from all teams on ways to improve the future competitions are instrumental in planning the next competition.

Universities that want to provide real-world experience to their students should categorically consider conducting mock competitions on their campus and competing at a Regional Collegiate Cyber Defense Competition. The competition provides experience that can't be taught in the classroom and provides skills that are marketable upon graduation.

The Los Angeles County District Attorney Steve Cooley summed it all up by saying, "The Collegiate Cyber Defense Competitions gives us the opportunity to put your brain power, your education, your experience and skills into this whole area of network security. Develop an attitude, have the ethics, develop the techniques, learn from one another so you can be defenders of our great system".

5. REFERENCES

Bureau of Labor Statistics, Fastest Growing Occupations 2006-2016, www.bls.gov/emp/mlrtab2.pdf. Last accessed July 17, 2008.

Chu, Be-Tseng, Ahn, Gail-Joon, Blanchard, Steven, Deese, James, Kelly, Richard, Yu, Huiming, and Young, Ashika. "Collegiate Cyber Game Design Criteria and Participation". 6th Annual IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007). Montréal, Québec, Canada December 9 - 12, 2007.

Conklin, Art. "Cyber Defense Competition and Information Security Education: An Active Learning Colution for a Capstone Course". Proceedings of the 39th Hawaii International Conference on Systems Sciences. January 4-7, 2006. Koloa, Kauai HI.

Mattson, Jeffery A. "Cyber Defense Exercise: A Service Provider Model". IFIP International Federation for Information Processing, Volume 237 Fifth World Conference on Information Processing, eds. Futcher, L., Dodge, R. (Boston, Springer) pp. 81-86.

Los Angeles County District Attorney, Steve Cooley, Keynote speech at Western Regional Collegiate Cyber Defense Competition, 2008.

National Collegiate Cyber Defense Competition website at http://www.nationalccdc.org/history.html. Last accessed July 17, 2008.

NSA Press Release, *National Security Agency, Academies Partner to Mold New Generation of Cyber-Defenders,* April 6, 2006. http://www.nsa.gov/releases/relea00103.cfm. Last accessed July 17, 2008.

Post-Competition Survey Results for Western Regional Collegiate Cyber Defense Competition, April 25, 2008.

Richardson, Robert, *2007 CSI Computer Crime and Security Survey,* GoCSI.com. Last accessed July 20, 2008.

Student Charged with Hacking into School Computer, http://www.toptechnews.com/story.xhtml?story_id=12000DGCVA4O, June 20, 2008. Last accessed July 21, 2008.

White, Gregory. "The National Collegiate Cyber Defense Competition: What are the next steps?" Proceedings of the 11th Colloquium for Information Systems Security Education. Boston University, Boston, MA, June 4-7, 2007.