6-30-2015

The Benefits of Hosting the NECCDC at Your Institution

George Markowsky
University of Maine

Peter Lutz
Rochester Institute of Technology

Daryl Johnson
Syracuse University

Bill Stackpole
Rochester Institute of Technology

The Benefits of Hosting the NECCDC at Your Institution

G. Markowsky[1], P. Lutz[2], D. Johnson[2]
W. Stackpole[2], R. Soucy[1], and B. Attaie[3]
[1]School of Computing and Information Science, University of Maine, Orono, Maine, USA
[2]Department of Computing Security, Rochester Institute of Technology, Rochester, NY, USA
[3]School of Information Studies,Syracuse University, Syracuse, NY, USA

Abstract— *The Northeast Collegiate Cyber Defense Competition (NECCDC) [2] is a regional competition that feeds the National Collegiate Cyber Defense Competition (CCDC) [1]. Since RIT organized the first NECCDC in 2008, the NECCDC has selected a representative to compete in the CCDC. It has been relatively successful and has produced the national champion twice and the runner up three times during its eight years of existence. The NECCDC has been hosted on a rotating basis by one of the universities in the northeast and has become a popular event for both the hosting schools and for the students. We feel that the NECCDC has continued to be an exciting event in part because it has been hosted by different universities which have all made important contributions to the event. This paper describes some of the benefits that come from hosting. Our hope is to convince other universities to host the NECCDC and similar competitions.*

Keywords: CCDC, NECCDC, cybersecurity competitions

1. Introduction

Cyber competitions have been found to inspire the students and help faculty put together better courses. One well-established competition is the National Collegiate Cyber Defense Competition, also known as the National CCDC, NCCDC or simply the CCDC [1]. The following material comes from [1]:

> *The mission of the Collegiate Cyber Defense Competition (CCDC) system is to provide institutions with an information assurance or computer security curriculum a controlled, competitive environment to assess their students' depth of understanding and operational competency in managing the challenges inherent in protecting a corporate network infrastructure and business information systems.*

1.1 History of the CCDC

The following material comes from [1]:

> *On February 27 and 28, 2004, a group of educators, students, government and industry representatives gathered in San Antonio, Texas, to discuss the feasibility and desirability of establishing regular cyber security exercises with a uniform structure for post-secondary level students. During their discussions this group suggested the goals of creating a uniform structure for cyber security exercises might include the following:*
>
> 1) *Providing a template from which any educational institution can build a cyber security exercise*
> 2) *Providing enough structure to allow for competition among schools, regardless of size or resources*
> 3) *Motivating more educational institutions to offer students an opportunity to gain practical experience in information assurance*

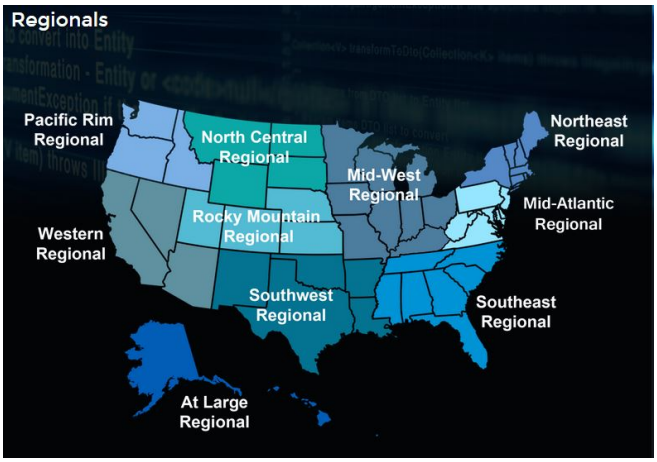

Fig. 1: The Regional Competitions that Feed the CCDC

1.2 Structure of the CCDC

The CCDC is fed by 10 regional competitions. Figure 1 shows these 10 regions. Regional competitions generally take place at a single physical location, but the At Large region is a virtual competition because of the great distances between competitors.

The CCDC is organized as follows. Teams of students from participating schools are called blue teams. Each blue team is treated as a replacement IT department for a company whose IT department was fired for incompetence. Thus,

each blue team inherits a system that has been compromised and will continue to be under constant attack during the competition.

The competition schedule generally looks like the following:

- Friday noon to 7 PM
- Saturday 8AM to 7 PM
- Saturday 7 PM Mixer and Recruiting Evening
- Sunday 8AM to noon
- Awards luncheon and keynote speaker Sunday afternoon

The competition staff is divided into three teams:

- *Red Team*: they provide all the attacks and compromises.
- *Black Team*: they design, assemble, operate and monitor the competition network
- *White Team*: they act as management and design the competitions "injects" (tasks), they judge the competition, and monitors blue teams directly to ensure compliance with the rules

Injects are tasks for the blue teams. For example, a blue team might be asked to scan the network for vulnerabilities, configure new machines, or rebuild a system after a server crash. Blue teams are judged on task performance, reporting and sometimes on the quality of oral presentations.

2. The NECCDC

The Northeast Collegiate Cyber Defense Competition (`http://neccdc.net`) is one of the feeder competitions for the CCDC. It is a very interesting and challenging 3 day competition that follows the format of the CCDC. The northeast region includes Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island and Vermont. Some New Jersey schools have also participated on occasion because of their proximity to New York City.

The NECCDC follows the CCDC very closely. The goal is to help the NECCDC winner to prepare for the CCDC so it follows all the CCDC rules as closely as possible. In particular, the NECCDC schedule is the same as the CCDC. Also, the terminology: Red Team, Blue Team, White Team and Black Team are the same. During the 2013 NECCDC, UMaine made a video of the competition [3] that gives a sense of the competition. The paper by Scaparra [4] gives a feel for the CCDC type of competition. For insight into how the CCDC competitions are scored and ideas on how the scoring can be improved see Markowsky [5].

Over the years, the NECCDC and similar competitions have generated papers on a wide variety of topics. These include such items as red team preparation (Johnson [6], Scaparra and Bullock [7]), blue team preparation (Engebretson, Pauli, and Bosma [8], Gourd [9], Pauli and Engebretson [10], Capalbo, Reed and Arpaia [11], Cavanaugh and Albert [12], [13], Cheung, Cohen, Lo and Elia [14], Glumich and Kropa [15], Casper and Papa [16], Mauer, Stackpole and Johnson [17]), resources for cybersecurity education (L. Markowsky [18]), and even how to run high school and middle school cyber competitions (Albert, Markowsky, Wallingford [19]).

The initial interest in hosting the Northeast regional CCDC started at least as early as 2006, when a group of RIT faculty visited the National CCDC event as observers. This was motivated by the chair of RIT's NSSA (Networking, Security and System Administration) Department, Luther Troell. The goal of the first visit was to better understand the components of the event as well as the commitment required to host the event. A second visit in 2007 was performed in order to obtain a commitment from the CCDC organizers for the first northeast regional competition to be hosted at RIT in Rochester, NY.

RIT's interests in becoming involved in the NECCDC focused mainly on having a venue within which students could compete and display their talents in the field of cyberdefense. As the field of cybersecurity was fairly new at the time, another benefit included promoting the development of cybersecurity programs in the northeast region. After hosting events in 2008 and 2009 it appears that these goals were met. Hosting the NECCDC, especially in the early years, when competitors and sponsors were hard to come by, was a huge effort for which there are no regrets. The effort expended to start this movement appears to have staying power, and has been evidenced by the performance of the teams in the Northeast region.

3. NECCDC I (2008)

There were many lessons learned at the first NECCDC that have influenced the delivery and execution of subsequent NECCDCs. Because of the importance of these lessons we will describe the first NECCDC in more detail than subsequent NECCDCs.

This first competition took place in the early spring of 2008 (February 29 - March 2) which corresponded with spring break at RIT that year. It was sponsored by McAfee, Harris RF Communications, and Cisco in addition to RIT's NSSA (Networking, Security and System Administration) Department. Competitors that year were Champlain College, Northeastern University, Norwich University, NYU Polytechnic, Rochester Institute of Technology, and Syracuse University. RIT was the winner the first year.

The RIT organizer was Peter Lutz, the Black Team leader was Bruce Hartpence, the Red Team leader was Daryl Johnson, the White Team was led by Larry Hill, and the RIT blue team coach role was shared by Sharon Mason and Bill Stackpole. All of these people were faculty in the NSSA Department.

In this first year of the competition, a major problem was simply recruiting competitor institutions. Competing turned out to be a major undertaking for each institution,

and while sponsors helped to cover the costs of running the competition, there was no financial support available to provide competitor institutions any relief. RIT contacted someone at each of the NSA CAEIAE's in the region, as well as announced it at the yearly colloquium. After the competition RIT worked on having a better plan for reaching potential competitors for future NECCDCs. After review, a plan to reach more institutions was devised, and the following year a more organized and robust approach was followed. In particular, mining the web for institutions with coursework in information assurance (IA) was a fruitful way to discover potential participants outside of the CAEIAE community.

Another major problem was in creating an ongoing event without the impression that RIT had an unfair advantage. During the first event, a meeting of all coaches was held on Saturday to discuss this issue. All attending expressed an interest in continuing this competition into the future. However, the other institutions indicated that the resources required would be beyond them. As a result, RIT chose to host it a second time.

In all NECCDCs, team coaches form an oversight panel that is privy to the operations of the White Team and all judging. As questions arise, the White Team captain suggests how particular problems should be resolved and the panel discusses the problems and suggested resolutions. After the discussion, the panel votes (ties to be broken by the White Team Captain) and the vote is binding. The team coaches also decide policy for the competition and decide where future NECCDCs will be held. One policy decision that has been made is to automatically qualify the hosting school for the NECCDC regardless of how they perform in the qualifying round.

3.1 White Team Notes

The White Team experienced myriad issues, questions, decisions during the competition. In particular, the White Team members stationed in blue team rooms tended to make judgments of their own, based on their understanding of the competition rules. The result was that, during the first day, inconsistent rulings were given to the teams. New procedures were adopted on the second day of the competition requiring that White Team members in the blue team rooms refer all questions to the White Team captain, who served as the final judge. This has been the standard operating procedure in all subsequent NECCDCs. It was also discovered that having group White Team meetings and standard forms for injects and incident reports were very helpful to keep the competition moving quickly.

Unlike the NCCDC, the NECCDC allowed and still allows teams to bring alternates to the competition. This is because between the regionals and the nationals the final team composition might need to be altered because of illness, personal emergency, etc. and we did not wish to hamper the NECCDC winner before the NCCDC even began.

At the 2008 NECCDC, blue teams were provided disaster recovery DVDs for each system. These were bootable DVDs with disk images that would restore a system to its pre-competition state. These were in addition to the distribution CDs/DVDs for each OS. The experience at the 2008 NECCDC suggests that these DVDs should be kept by the Black Team who would be the only ones authorized to use them so that any recovery activities would result in a blue team penalty. The blue teams could, of course, create their own disaster recover CDs/DVDs, if they so desired.

During the competition, the blue teams asked frequently about retasking workstations to specific purposes. In general, this was allowed, but in future NECCDC limits were imposed on how many machines could be retasked in this way. At the outset, blue teams had 4 servers and 4 workstations. An inject required the retasking of one workstation. It would be a mistake to lose all workstations in this manner, so it is recommended that at least two workstations be maintained throughout the competition.

The machines at the 2008 NECCDC had three NICs in them, but there were no rules determining whether and how additional NICs could be used. Some blue teams wanted to use the extra NICs to turn servers into a routers/firewalls, while the organizers wanted to force the blue teams to use the PIX firewalls provided. As much as possible we recommend that rules be in place to deal with any extra hardware that might make its way to the blue teams.

One contentious issue that came up was whether reconnaissance is considered an attack. The Red Team did reconnaissance at periods when they were prevented from attacking, and some blue teams questioned this practice. As the NECCDC has evolved we have adopted the position that the NECCDC is not a contest between blue teams and the Red Team - it is an event that tests the abilities of blue teams and to get a good measure of these abilities, it is important to push the blue teams as much as possible during the competition. To make the trial as challenging as possible it is desirable for the White, Black and Red teams to work together.

It was also discovered during the competition that it is a good idea to place staplers and paper clips in each blue team room. The paper clips are ideal for resetting routers and switches.

3.2 Black Team Notes

The Black Team benefited greatly from its detailed knowledge of the the scoring engine. It became clear during the competition that the White Team would benefit greatly from a better understanding of how SLAs and the injects were scored. In subsequent NECCDCs effort has been devoted to improving pre-competition communication between these two teams to minimize doubts about scoring.

An open question is how much detail about the scoring should be communicated to the blue teams. For example, simply telling them that having services down would cost them points, and more points the longer they were down, is one approach. Another is to tell them that they receive points for services being up every 5 minutes of play. If services go down, they stop receiving these points. If services are down for long enough (an hour or more) points are deducted. The goal is to make the scoring system essentially invisible to the blue teams so they can focus on cyber defense.

In this NECCDC we captured only packet headers. In subsequent NECCDCs full packet captures were collected.

3.3 Red Team Notes

The Red Team members were from seven different organizations and for the most part were not familiar with each other before the event. A Google group was created for the red team to get acquainted ahead of time. They used the forum to begin to discuss what tools they were bringing, what strengths they had, what similar experiences they had and to discuss strategies. The Red Team expressed that this interaction was helpful and recommended it for future red teams.

The Red Team members brought their own hardware and software for the competition. We provided a single Linux file server with 750 GB of storage that they could use as needed. They ended up using it for three purposes. First, it was connected to the projection system and projected the overall blue team summary of service availability. Second, it was used to type up the exploit reporting forms and print them to be given to the white team. Third, they installed a wiki that the red team members used to share exploit and strategic information about the blue teams' and the red team's activities. Occasionally, they also used it to display a document or information that they wanted to display to the group at large.

This NECCDC forced the competition organizers to deal with social engineering practiced by the Red Team. The competition staff have extraordinary access to team rooms, and the blue teams are not empowered to prevent this access. One of the staff roamed among all of the team rooms taking pictures of the event and the participants. One of the Red Team members asked the staff member for copies of the pictures and was given a download. The pictures included whiteboard and monitor shots that revealed network and account information. The White Team judge disallowed the attack and the Red Team did not use the information gained. It was decided that social engineering the competition staff gives the Red Team an unrealistic advantage. It is suggested that the rules more explicitly prohibit this kind of attack.

The Red Team made a major phishing attack at the outset of the competition with great success. They were able to get several blue teams to execute a Trojan that installed remote control software on one of their systems. The Red Team then used that access to shut down services. However, this raised the level of awareness among the blue teams who quickly shut down Red Team access. Several blue teams failed to protect their Cisco hardware from remote access. The Red Team was able to take full control of several routers and switches. They proceeded to lock the blue teams out of their own equipment. This tipped off the blue teams and they took corrective action.

3.4 Conclusion

The 2008 NECCDC was conducted much like the nationals, but with some local tweaks. In the future, the tweaks would be greater and lessons learned would be applied. Overall, it was a good experience, and RIT hosted again in 2009.

4. NECCDC II (2009)

The second competition took place in the spring of 2009 (February 27 - March 1). It was sponsored by Harris RF Communications and M&T Bank. The competitors that year were the University of Buffalo, Champlain College, the University of Maine, Northeastern University and Rochester Institute of Technology. The winner was Northeastern University. Many of the lessons learned from the 2008 NECCDC were applied to the 2009 NECCDC which ran quite smoothly. Communication with the blue teams was much improved, but there was still the problem of having teams show up for the competition. At least one team said that they were coming, which caused another team to be turned down, but then the original team backed out of the competition at the last minute. At the competition, the University of Maine indicated a willingness to host the 2010 NECCDC and plans were made for bringing the NECCDC to the University of Maine. Pete Lutz again was director of the competition and White Team Captain, Daryl Johnson was the Captain and organizer of the Red Team and Bo Yuan was the Captain of the Black Team. All were members of the RIT faculty.

5. NECCDC III (2010)

The 2010 was held March 5th through 7th at the University of Maine's flagship campus in Orono. There were a total of 9 schools represented: Alfred State College; Champlain College; Harvard University; Northeastern University; Polytechnic Institute of NYU; Rochester Institute of Technology; Stevens Institute of Technology; SUNY Oswego; and The University of Maine. Northeastern University was the 1st place winner, and would continue to win 1st place at the National CCDC for 2010. The University of Maine placed 2nd, and Rochester Institute of Technology 3rd.

The Director of the NECCDC was George Markowsky, Professor of Computer Science of the University of Maine. The Captain of the White Team was former RIT competitor Thomas Vachon, the Red Team captain was Daryl Johnson

of RIT, and the Black Team captains were Ray Soucy and Andrew Moody from the University of Maine.

2010 marked major changes in the NECCDC to raise the profile of the regional, including increased focus on clear rules for competitors and judges, better communication for attendants, and aggressive pursuit of sponsorship from companies like Trustwave, Boeing, Black Hat, Game Logic, and Fairpoint, as well as public sector support from the Department of Homeland Security.

In 2009, the NECCDC suffered from having no-shows. For the 2010 NECCDC it was decided to institute a $750 fee for all schools wishing to participate. The stipulation was that any school that attended the NECCDC would receive a $750 travel assistance grant. Any school not showing up would not receive a travel grant. This mechanism prevented no-shows and has been used since 2010.

Overall, the majority of feedback for the 2010 NECCDC was the lack of information and activities for non-competitors. The request to see team standings or points in real time was very popular, as well as the request to have a non-scored team setup for coaches to gain hands-on experience with the event and better insight into what their teams are exposed to. There was also feedback requesting more information ahead of the competition on how to prepare, particularly for new competitors.

Because of the enlarged scope of the 2010 NECCDC, fund raising became a big concern. Fortunately, we were able to get a $10,000 grant from the Department of Homeland Security. Douglas Maughan, of the Department of Homeland Security attended the 2010 NECCDC and as a result DHS has been funding all the regionals at the rate of $15,000 per event.

Northeastern University won the 2010 NECCDC and went on to win the CCDC. One blue team was disqualified from the competition because of its behavior and using resources of other blue teams. This is the only time in the history of the NECCDC that a team was disqualified during the competition.

6. NECCDC IV (2011)

For 2011, the NECCDC was hosted by Northeastern University at an EMC training facility to accommodate the growing number of competitors.

A total of 11 teams participated: Alfred State College; Champlain College; Harvard University; Northeastern University; Pace University (NY); Polytechnic Institute of NYU; Rochester Institute of Technology; Stevens Institute of Technology; University of Maine; University of Massachusetts Boston; and University of New Hampshire. The winner for 2011 was RIT, with 2nd place going to Stevens Institute of Technology, and 3rd to Champlain College.

The Head Judge was Thomas Vachon, white team co-captain Ray Soucy, Red Team captain Daryl Johnson, and Black Team Captain David LaPorte of Northeastern University,

The majority of the feedback for 2011 centered around the physical security restrictions of the facility, lack of wireless access for non-competitors, and vendor presentations being the wrong choice for the spirit of the event.

7. NECCDC V (2012)

NECCDC V was hosted by Northeastern University at the EMC training facility, with 12 teams representing: Alfred State College; University of Buffalo; Champlain College; Harvard University; The University of Maine; University of Massachusetts Boston; University of New Hampshire; Northeastern University; Pace University; Rochester Institute of Technology; Stevens Institute of Technology; and Worcester Polytechnic Institute. The winner for 2012 was RIT, with 2nd place going to UNH, and 3rd to The University of Maine.

The Head Judge was Marc McLaughlin, and Black Team captain Chris Mills, both from RSA. The Red Team captain was Daryl Johnson.

Despite 2011 feedback on the restrictions of the EMC training facility being the wrong fit, there were no alternatives to accommodate 12 teams. There was also a growing concern expressed that the academic focus of the event was being lost.

8. NECCDC VI (2013)

For 2013 there was an effort to address the concerns of the 2011 and 2012 competition by hosting the event once again at the University of Maine. To make this possible, a virtual qualifier was held for the first time to narrow the competition from 14 interested schools to the top 10.

The 10 teams represented: Alfred State College; Champlain College; Northeastern University; Rochester Institute of Technology; SUNY BUffalo; SUNY IT; Syracuse University; University of Maine; University of New Hampshire; and Worcester Polytechnic Institute.

The winner for 2013 was RIT, with SUNY IT placing 2nd, and both Worchester Polytechnic Institute and Northeastern University placing 3rd.

The Head Judge was Ray Soucy, with Red Team captain Daryl Johnson, and Black Team captain Andrew Moody. For more information about the 2013 NECCDC see [20], [21], [22].

9. NECCDC VII (2014)

The 2014 NECCDC was held at the University of New Hampshire, which was hosting it for the first time. The Director of the competition was Kenneth Graf. Ken Graf developed a good relationship with industry sponsors and is interested in hosting the 2018 NECCDC again at UNH.

10. NECCDC VIII (2015)

Syracuse University (SU) began its participation in NECCDC back in 2008 when a team of graduate students from the School of Engineering traveled to RIT for the inaugural NECCDC. Unfortunately no one had checked the rules which only permitted a maximum of two graduate students per team and as a result the team was not able to compete. It wasnâĂŹt until 2013 when SU was able to field another team this time consisting of a small group of graduate and undergraduate students from the School of Information Studies (iSchool). The team was able to make it through the virtual qualifier and traveled to the University of MaineâĂŹs Orono campus (UMaine) for the 2013 NECCDC. The students had an exceedingly positive experience and when they learned that NECCDCC was looking for other schools as future hosts of the event they urged their coach to investigate it. After careful deliberations it was decided to shadow the 2014âĂŹs host in order to gain more experience so that a determination could be made for 2015.

The iSchool was able to form a full team for the 2014 NECCDC as a result of increased interest generated from the previous yearâĂŹs engagement and the team advanced through the qualifier to the 2014 regional at the University of New Hampshire (UNH) in Durham. Shadowing UNH in 2014 was very helpful as it facilitated a behind the scenes access to the event and seeing how it was organized was a key factor in the iSchoolâĂŹs decision to adventure into hosting the event for 2015.

Several other factors were equally instrumental in finalizing the decision to host the 2015 NECCDC. The sponsorship made available by National CCDC through a grant from Homeland Security and other CCDC sponsors was critical to establishing a sound financial foundation which helped to secure commitments from the DeanâĂŹs office. Equally critical was the never ending encouragement, support and advice from previous hosts UMaine, RIT and UNH making it a family affair.

The list of benefits that can be attributed to hosting the NECCDC is lengthy and includes both long term and short term benefits. Some of the short term gains were enhanced student interest and pride and a nice set of good publicity. Long term gains included the formation of an Information Security Student Club and proposal to add an Ethical Hacking Course to the curriculum as well as research opportunities in cybersecurity and other areas such as the effectiveness of NECCDC as a recruitment tool for cybersecurity talents versus traditional forms of recruitment.

11. NECCDC IX (2016)

At the 2015 NECCDC a new hosting university was selected for the 2016 NECCDC. In July 2015 the university selected indicated that because of budget cuts and staff changes it would no longer be able to host the 2016 NECCDC. George Markowsky indicated that the University of Maine would be willing to host the 2016 NECCDC. After some discussion among the various schools, it was decided to accept the University of Maine's offer. The University of Maine hopes to build on all the successes that the NECCDC has had to this point and is looking to an exciting NECCDC.

12. NECCDC X (2017)

RIT indicated a strong interest in hosting NECCDC X in light of its role in starting the NECCDC. All the schools involved in the NECCDC agreed that the honor of hosting NECCDC X should go to RIT in recognition of their pioneering work in establishing the NECCDC.

13. The NECCDC Red Team

It is not difficult to get volunteers for the Red Team. It is much more difficult to get good Red Team members. By this we mean finding people who see the goal and purpose of the Red Team as "assessing the skills and talents of the blue teams and determining the best team to move on to the NCCDC". Often Red Team members want to see the opportunity to play on the Red Team as a test of their attacking skills. While serving on the Red Team is challenging, Red Team members need to be committed to being fair and launch the exploits against all the teams to provide a thorough test of the blue teams. Slogging through the repetitions requires dedication to the ideal of the Red Team as a challenger of blue teams.

Over the years, one of the greatest changes that has come about is the realization by the NECCDC White Team that the Red Team should not be considered "the bad guys" who need to be keep in the dark, but rather as an integral part and member of the competition. This paradigm shift has allowed the competition to grow and expand its areas of coverage in assessing the blue teams' strengths and weaknesses. The Red Team is now participates in the design, operation, and grading of the event. This change strengthens the competition by making the best utilization of all of the talents available.

Fairness and equity in the attention that each blue team receives from the Red Team is critical to making sure that the winning blue team is indeed the best. Our primary tenant is "no Red Team success can be scored unless it has been tried on every other blue team first." This organizes the Red Team by discipline or skill. A common alternative in cyber competitions is to assign Red Team members to a specific blue team. This is likely to create situations where a very good Red Team member is pitted against a very weak blue team and an exaggerated score is achieved compared to the rest of the blue teams. Potentially, worse is if a weaker Red Team member is pitted against a weaker blue team. This might lead the weak blue team to get a very good score and win the competition, which could cause the NECCDC

to supply a weak team to the NCCDC. Clearly, making sure that every exploit is tried against every team permits us to have some confidence in the results.

14. Conclusions

The benefits to the students of the host institution are that the attention and stature that their institution garners reflects on them and their degree. The benefits for the blue team are obvious but now add the esteem of the host. For those students not on the Blue team there can be opportunities for exercising their skills and learning new ones is aiding and assisting the host in making preparations. This can come if the form of volunteering for the various teams supporting the event. Getting ready involves every aspect of security from building networks, systems, and services, to solving the associated problems with making 10 of duplicate copies, to scoring and monitoring the event, and on to creating and enforcing the rules. All of these pieces can provide growing and enriching opportunities for faculty, staff, and students.

The benefits to an institution for hosting an event such as NECCDC are many. The first impact realized would be the commitment of your administration to your security program through their support, but also the commitment of your faculty and staff to the effort. An event such as this can often galvanize and motivate your faculty to push their limits and bring them together as a team. A common goal is a powerful motivator. The exposure of your programs and curriculum outside of your institution can help expand your visibility and recognition in the field. A fair amount of media coverage can be garnered because of the event. The attention acquired through media and sponsorship efforts can help realize long term relationships with vendors and employers that pay off over the long haul. The preparations for the event can provide a challenge for the host. It is through those challenges that the host institution can grow both their capability and capacity but also find out what hidden talent and capabilities they already have. A host might discover resources, skills, or facilities dormant or hidden at home that they were not aware of.

It can be said of the host institutions over the years, that every one of them has benefited from the experience. They have struggled with various aspects but always persevere and come out of it stronger and more confident of the work they are doing. After the experience, one will often hear comments such as "I wasn't sure we could pull it off but we did!" with pride and a sense that now they are better. It is interesting that another surprise from hosting is the discovery of skills and resources that the host had but did not recognize or fully appreciate. This often opens up new opportunities for the host in terms of curriculum, recognition, support, and associations. For the host it can also spur and encourage the faculty to broaden their course offering by creating new courses supporting the material needed by the blue teams.

References

[1] National Collegiate Cyber Defense Competition Website, http://www.nationalccdc.org/.

[2] Northeast Collegiate Cyber Defense Competition Website, http://neccdc.net/wordpress/.

[3] University of Maine Video of the 2013 NECCDC, https://www.youtube.com/watch?v=V8A7wci81Yo. The video and photos are also available at https://www.flickr.com/photos/geomarkowsky/.

[4] Jeffrey C. Scaparra, "One Individual's Three Perspectives on the Collegiate Cyber Defense Competition," in *Proc. SAM'10*, 2010, pp. 307-313.

[5] George Markowsky, "Toward a More Perfect Scoring System for the NECCDC",*Proc. 2012 Inter- national Conference on Security and Management*, (SAM'12), Las Vegas, NV, July 16-19, 2012, pp. 230-235, http://www.gbv.de/dms/tib-ub-hannover/739342479.pdf.

[6] Daryl Johnson, "The Assembly and Provisioning of a Red Team," in *Proc. SAM'11*, 2011, pp. 530-534.

[7] Jeffrey C. Scaparra and Jeffrey R. Bullock, "Red Teaming for Education," in *Proc. SAM'11*, 2011, pp. 512-517.

[8] Patrick Engebretson, Joshua Pauli, and Joshua Bosma, "Lessons Learned from an Evolving Information Assurance Lab," in *Proc. SAM'10*, 2010, pp. 261-266.

[9] Jean Gourd, "Cyber Storm: The Culmination of an Undergraduate Course in Cyber Security," in *Proc. SAM'10*, 2010, pp. 300-306.

[10] Joshua Pauli and Patrick Engebretson, "A Cradle-to-Grave Approach to Retaining Students in Information Security Programs," in *Proc. SAM'10*, 2010, pp. 255-260.

[11] Nicholas Capalbo, Theodore Reed, and Michael Arpaia, "RTFn - Enabling Cybersecurity Education through a Mobile Capture the Flag Client," in *Proc. SAM'11*, 2011, pp. 500-506.

[12] Cory Cavanagh and Raymond Albert, "Goals, Models, and Progress towards Establishing a Virtual Information Security Lab in Maine," in *Proc. SAM'11*, 2011, pp. 496-499.

[13] Cory Cavanagh and Raymond Albert, "Implementation Progress, Student Perceptions, and Refinement of a Virtual Information Security Laboratory," in *Proc. SAM'12*, 2012, pp. 197-200.

[14] Ronald Cheung, Joseph Cohen, Henry Lo, and Fabio Elia, "Challenge Based Learning in Cybersecurity Education," in *Proc. SAM'11*, 2011, pp. 524-529.

[15] Sonja Glumich and Brian Kropa, "DefEX: Hands-On Cyber Defense Exercises for Undergraduate Students," in *Proc. SAM'11*, 2011, pp. 487-493.

[16] William D. Casper and Stephen M. Papa, "A Multi-Disciplined Security Engineering Education Approach," in *Proc. SAM'12*, 2012, pp. 243-248.

[17] Brandon Mauer, William Stackpole, and Daryl Johnson, "Developing Small Team-based Cyber Security Exercises," in *Proc. SAM'12*, 2012, pp. 213-217.

[18] Linda Markowsky, "An SELinux Sourcebook for Cybersecurity Education," in *Proc. SAM'10*, 2010, pp. 248-254.

[19] Raymond Albert, George Markowsky, and Joanne Wallingford, "High School Cyber Defense Competitions: Lessons from the Trenches," in *Proc. SAM'10*, 2010, pp. 280-285.

[20] George Markowsky, Daryl Johnson, Andrew Moody, Ray Soucy and William Stackpole, "The 2013 NECCDC - Lessons Learned", *Proc. 2013 International Conference on Security and Management*, (SAM'13), Las Vegas, NV, July 22-25, 2013, pp. 433-439, http://umaine.edu/scis/files/2013/07/The-2013-NECCDC-%E2%80%93-Lessons-Learned.pdf.

[21] 2013 NECCD Symposium Schedule. [Online]. Available: http://neccdc.net/wordpress/?page_id=99

[22] 2013 NECCD Media Release. [Online]. Available: http://neccdc.net/wordpress/wp-content/uploads/2013/02/NECCDCPhotoRelease2013.pdf