2018 ASEE Zone IV Conference: Boulder, Colorado Mar 25

Effective Competitions for Broadening Participation in Cybersecurity

Dr. John Y Oliver, California Polytechnic State University, San Luis Obispo

Dr. Oliver is an associate professor of Electrical Engineering and is the director of the Computer Engineering program at Cal Poly, San Luis Obispo. Dr. Oliver is also a program director for the California Cyber Training Complex (CCTC). His field of expertise is in computer architecture, system performance analysis and digital forensics. His teaching activities focus on embedded systems, digital circuit design, sustainability issues with electronics and computer forensics.

Cassidy Elwell,

Effective Competitions for Broadening Participation in Cybersecurity

Dr. John Oliver
Associate Professor
Cal Poly, San Luis Obispo
California Cyber Training Complex

Cassidy Elwell
Undergraduate Student
Cal Poly, San Luis Obispo
California Cyber Training Complex

Introduction

This nation has a critical shortage of professionals in cybersecurity. This need is amplified due to the lack of gender and racial diversity in the cybersecurity workforce. NIST's National Initiative for Cybersecurity Education (NICE) working group has made it strategic plan objective to increase participation by women, minorities and veterans in cybersecurity[1.]

Cybersecurity competitions have been promoted as a way to increase participation in cybersecurity-related fields amongst high school students. Typical cybersecurity competitions at the secondary school level currently focus on a very narrow set of computer-technical related activities. These competitions are rewarding to students who have traditionally been attracted to computer-related fields. However, these participants of the competitions are not typically diverse in gender or race[2]. The lack of diversity in cybersecurity competitions is a large problem if we want to increase the diversity of the cybersecurity workforce because one good indicator of career interests for adolescents is their choice of leisure and extra-curricular activity[3].

Tangentially, we also recognize that while computer-skills are critically important to a cybersecurity professional, professionals in cybersecurity also are required to have a wide breadth of skills. This broader set of skills include critical thinking, teamwork, communication as well as being well versed in privacy, ethics, and legal aspects of cybersecurity.

To expand demographic participation in cybersecurity and the diversity of the cybersecurity workforce, we believe that cybersecurity competitions at the formative ages should focus on a broader set of cybersecurity activities including: critical thinking, teamwork, communication skills, and ethics. By casting a wider net, we believe that cybersecurity competitions can capture a larger, more diverse audience and promote greater involvement in cybersecurity competitions. The theory plays out like this: a high school student who is a neophyte in "computer-skills" may find the ethical implications of cybersecurity to be very interesting and these ethical dilemmas can serve as a hook for this student into the more technical portions of the realm of cybersecurity. Meanwhile, neophyte students who participate in traditional cybersecurity competitions in high school may be so intimidated by these technology-focused competitions that they are discouraged from participating in future cybersecurity-related competitions.

To address these issues, the California Cyber Innovation Challenge (CCIC) was held in June of 2017, sponsored by the California state governor's office and hosted by Cal Poly and the California Cyber Training Complex (CCTC). The CCIC features an immersive cybersecurity competition where competitors had to work in teams to search and seize both digital and physical evidence, perform digital forensics and other cybersecurity-related challenges, create a criminal timeline, and present their findings to a panel of law enforcement professionals.

The remainder of this paper describes our observations of high school-level cybersecurity competitions, and how this led to the development and design of the CCIC. Lessons learned from the CCIC in 2017 will be shared as well as future improvements for the CCIC in 2018.

Observations from high school cybersecurity competitions

Prior to the design of the CCIC, members from the CCTC observed and/or designed six high school cybersecurity competitions in the state of California. We are very impressed with cybersecurity competitions and the competitors appear to enjoy these events while learning many cybersecurity fundamentals. At these competitions, we have made several observations that are also supported by others who have designed and/or observed prior high school cybersecurity competitions[4567]. The following observations are generalizations of the competitions observed. We recognize that there is high variability in the objectives and outcomes of competitions, but the observations apply nearly universally to all high school cyber security competitions that we attended.

Observation 1: Many competitions are arranged where students are organized into teams (typically 3-6 students) and teamwork is highly encouraged. However, we observed that many teams are really co-working by contributing to a team score rather than exhibiting high-levels of teamwork. As a result, many competitions observed don't show tell-tale signs of collaboration, such as having animated discussions or students working on the same problem at the same time.

Observation 2: Student competitors learn much in preparation for the competition about the use and design of computer-related technologies as well as computer system vulnerabilities and threat vectors. However, students often are not applying critical thinking skills during the competition. At some competitions observed, students at the competition are either completing a prescribed checklist of exploits to close; or even more simply, using the internet to search for answers. We classify these competitions on the static-side of the spectrum.

Some competitions include more dynamic components of the competition, for example active adversarial components, such as a "red team." We believe that these dynamic components result in higher levels of critical thinking in cybersecurity competitions. However, through our research

and participation in the cybersecurity competitions, we have concluded that dynamic competitions appear to be the exception at the secondary school level.

Observation 3: Some competitors are very advanced in their knowledge of cybersecurity, even at the high school level. This results in some very lopsided competitions. We view this as a threat to novice players. Our conclusion is that the disparity of skills in an unbalanced game environment creates a hostile, inaccessible environment for students with budding interest in cybersecurity who have limited computer-technical skills.

Observation 4: Many competitions do not emphasize the tangential competencies of cybersecurity careers such as ethical, legal, and privacy concerns inherent to cybersecurity. Additionally, most competitions also don't explore the need for demonstrating good communication skills as part of the competition. Ethical, legal, and communication skills are necessary for any proficient cybersecurity professional. One could argue that one of the biggest challenges of cybersecurity is to find a way to effectively communicate the threats of cybersecurity to an increasingly cyber-based population who do not possess a good command of computer systems.

Observation 5: Most competitions involve a room full of competitors sitting around tables working constantly on computers for three hour blocks at a time with little collaboration. In addition, parents, mentors, and coaches must leave the facility to ensure fairness among teams and therefore are unable to observe the competition themselves.

Observation 6: Competitors are ranked by an automated scoring system in real time and sole success being recognized to the teams or individuals who have already mastered such technical skill sets. Most competitions were found to be technical-only resulting in critical thinking, intuitiveness, communication, and presentation skills not being considered criteria in scoring. Additionally, new teams and individuals interested in improving their computer technical skills are often intimidated and discouraged due to these criteria.

When considering the problem of diversity in cybersecurity competitions we argue that stakeholders should think more completely about the students who *don't* compete in competitions and how to attract those students. Furthermore, we should also recognize that many of the competitors of cybersecurity competitions *will not* pursue cybersecurity post-secondary school. Therefore, understanding the characteristics of these students would also be helpful in building a pipeline to cybersecurity careers from K-12 schools. We believe that if cybersecurity competitions, especially at the high school level, could address these observations, not only would the students who are currently "good cybersecurity competitors" benefit through the cultivation of a broader set of skills, but the competitions would open new pathways for inclusion of a more diverse set of students. Given the need for trained professionals in all realms

of cybersecurity, it is important that we engage a broader set of youths in cybersecurity in a welcoming and holistic manner.

The design and implementation of the California Cyber Innovation Challenge (CCIC)

The authors of this paper were designers of the California Cyber Innovation Challenge (CCIC) in 2017, which is sponsored by the California state governor's office and can be considered the "state championships" of high school cyber competitions. This competition was held on the California National Guard Base, Camp San Luis Obispo. The 2017 competition was designed with two parts, a CyberPatriot portion as well as an immersive cyber-physical experience in the digital forensics challenge (DFC) which the authors created. In the CCIC 2017, 16 teams of high school students participated, each team consisting of approximately six high school students. Half the schools were given automatic entries to the CCIC through virtue of placing in the top-two teams in their regional high school competitions. The remaining eight teams were selected by the governor's office to ensure both geographical as well as gender/racial diversity.

The well codified CyberPatriot event has teams of students closing known exploits in a variety of operating systems. CyberPatriot is sponsored by the US Air Force whom provides both the images of the operating systems and the live scoring system. As student teams close exploits, the teams earn points. For an official CyberPatriot event, teams have a total of six hours to close exploits. Exploits can range from very simple activities, such as reducing user permissions to the minimum acceptable level, to more complicated activities, such as closing unused ports for installed programs. Some CyberPatriot competitions have "red teams" where a team of "hackers" are trying to open exploits within the operating systems that the student teams are trying to protect. However, experienced "red teams" are not common. Competitors are not allowed to use scripts for closing exploits, and the exploits must be closed manually. Well prepared teams will come in with written checklists of steps and will partition the activities equally amongst all team members. CyberPatriot is the benchmark cybersecurity competition for by which all other cybersecurity competitions are measured for high school students.

CyberPatriot exhibits many of the observed shortcomings of cybersecurity competitions. While the competitors are working on teams, they are really "co-working" rather than having a meaningful teamwork experience. The activity is devoid of critical thinking for teams that are well prepared. Teams that are well prepared tend to do very well and make the event very intimidating for less experienced teams. Finally, CyberPatriot is very focused on the technical aspects of computer security and does not emphasize the larger set of cybersecurity competencies.

To address these issues, the authors developed a digital forensics competition (DFC) as part of the CCIC 2017. Figure 1 displays the skills and competition elements associated with building

each skill significant to a cybersecurity professional. For example, critical thinking is an important skill built through completing a crime investigation without a prescribed checklist and making inferences based on forensic analysis findings. A digital and physical evidence trail was created for competitors to discover. This evidence was hidden amongst "non-evidence" in a vehicle, where each team was allocated a separate vehicle to search and seize evidence. Teams were tasked to perform forensic analysis to collect evidence, place the evidence on a criminal timeline, and then present their findings to a panel of law enforcement professionals (assistant DA, forensics examiners, CIA and FBI agents, etc.). As an example, the team would find a laptop in the vehicle, IoT devices, a flash drive, an invoice, and perhaps a post-it note with a password scribbled on it. This password could be used to unlock an encrypted evidentiary file on the laptop. Email and Skype logs could contain evidence, etc. To facilitate the student teams, training from the California Department of Justice was repurposed to use open-source and freeware tools and hosted on the web prior to the competition. Additionally, practice forensics exercises were provided online, as well as instructional videos.

Development of the Digital Forensics Challenge (DFC)

There were a number of stages necessary to successfully create such a digital forensics competition as the California Cyber Innovation Challenge to ensure the inclusion of both technical and soft skills and a realistic digital forensics investigative scenario:

Stage 1: Create forensics training materials

With the goal of the competition to attract a broader representation of participants and emphasize investigative skills, critical thinking, and teamwork, it is crucial for participants to prepare. Therefore, the materials provided should assist the students in establishing the proper skill sets in conjunction with a step-by-step guide of how to use particular tools to accomplish forensics analysis. In the materials created for 2017, training material was obtained from the California Department of Justice that was based on a specific vendor's tools. This training was refactored to use open-source and freeware tools to ensure accessibility to all high school students. This training walked students through a Windows-based digital forensics investigation, and provided three additional training scenarios, each with a decreasing amount of scaffolding for self-guided education. Additionally, training videos were also created to assist in the dissemination of Windows-based digital forensics training. This training is now freely available at: https://cctc.calpoly.edu/events/ccic/2017.

Stage 2: Establish realistic, engaging scenario

For students to successfully build technical and soft skills significant to a cyber professional and to supply excitement and interest to the field, the scenario behind the evidence must be concrete and realistic. A sense of drama and importance was deemed necessary to captivate the competitors.

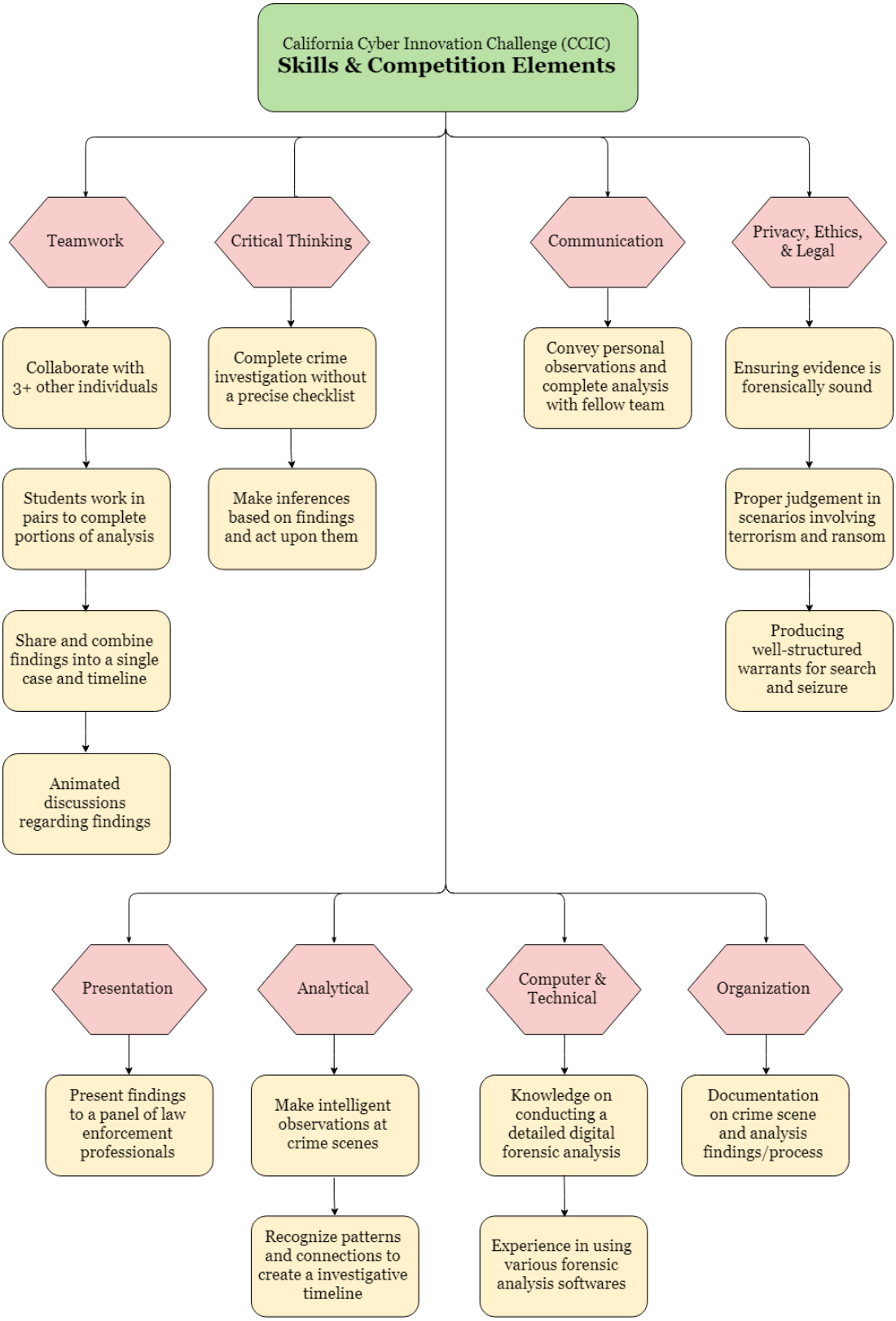

Figure 1: California Cyber Innovation Challenge Learning Skills Mapped to Corresponding Competition Elements

For the 2017 competition, the crime investigated by the competitors was a cyber threat against a municipal water supply. The crime included multiple criminals, with disparate motives. A non-linear evidence path was created where investigators (student teams) were led to believe that the initial suspect was the main criminal, but the mastermind of the crime was actually an accomplice whose digital evidence trail was more closely guarded. In the creation of this scenario, two criminal forensics examiners were consulted to ensure realism in the challenge.

Stage 3: Timeline and digital evidence creation

The digital evidence trail is time consuming to create as any activity on a computer system is logged by the computer so both evidence and other activities need to be entered real-time. First, an evidence trail for our crime had to be planned out. This included emails, Skype calls, web browsing, document creation, photos, and other such common activities on a computer. Some of these pieces of digital evidence were either hidden (placed on different hard drive partitions for instance) or encrypted (password protected .zip files for instance). Then, to create this digital evidence trail (two to three times daily) the authors had to use the computer for planting this evidence trail along with other "non-evidence" activities, such as sending emails to friends and family members. This process was implemented over a 3 week period. This would ensure a correct chronology of evidence events as well as make the search realistic. Five digital device evidence pieces were created in our implementation: a laptop, an external hard drive, an SD card, an Amazon Echo device and a Ring doorbell.

Stage 4: Hold dry-runs of the challenge and training materials

Following the completion of the evidence trails, the authors hosted dry-runs with local area high school students who were not participants in the CCIC. These dry-runs used the forensics images developed for the CCIC to identify any issues with realism and difficulty, receive feedback from students on the challenge set up and scenario, and estimate the amount of time taken for student teams to successfully analyze a majority of the evidence. Based on observations made and feedback provided from these dry-runs, the competition evidence may need to be adjusted and the time constraints of the competition may need to be modified. Fortunately, we didn't have to make any changes to the digital evidence trail as this process would have necessitated the complete rebuild of the digital evidence and the only changes made were in some of the non-digital evidence that was part of the competition and the training material provided.

Stage 5: Finalize and 'build' scenario setting

To continue with adding realism and excitement to the competition, teams were given a scenario setting to search and seize evidence from. The digital devices (or the evidence created) were then placed in a vehicle. We borrowed 16 vehicles from a local car dealership for the event. These devices were placed with "car garbage" purchased from our local Goodwill. The laptop was kept in plain sight on the passenger-side seat, while the rest of the digital devices were hidden in the

vehicle. The digital props placed in the vehicles need not be in working order (for more details, see Stage 6 below).

Stage 6: Deploy the scenario on competition day

Following the authors' announcement of the premise of student teams' need to act as digital forensics investigators, each team is given a box containing background information about the suspect, latex gloves, notepads, and flashlights to perform their search. Also included in the box was a USB drive with some pre-recorded (mp3) interviews with the initial suspects in the case. The teams were each provided a vehicle that was apprehended from the suspect to search and seize both digital and physical evidence. Upon discovering a digital device from the vehicle, student teams were instructed to go to the "forensics technician" table to exchange their digital device for a USB drive that contained a forensics image of that digital device. This was done to avoid having competitors create their own forensics images, as this is a time consuming process that could take several hours or even days.

The students then would perform digital forensics analysis and often the teams would have their members work in parallel: one student would look at the email evidence, while another would recover deleted files, while another would look at Skype chat logs. Student teams would put the evidence they found on a criminal timeline and then craft an argument of who committed the crime, what their motivation was, when and how the crime was committed, and what should be done to remediate. This argument was then presented by each team to a panel of judges. The judges ranged from CIA and FBI agents to the county's assistant district attorney and other forensics examiners. These judging panels were given a 30-minute training on the case and provided a scoring rubric and list of suggested follow-up questions to ask the student teams.

Analysis of the Digital Forensics Challenge (DFC)

Through this forensics exercise, it was clear that the level of engagement of the students as a whole was much higher than in CyberPatriot competitions. Teams were observed having (sometimes heated) discussions on the evidence found, and a larger proportion of the teams were actively engaged in the digital forensics. We believe that more of the team members had talents to lend to the team's performance be it through general critical thinking activities, presentation organization, or verbal communication skills. Teams were also observed to be making intellectual discoveries during their forensic analysis resulting in an additional search of their vehicle for an inferred digital device from other evidence, such as a mini SD card. Students were so engaged as part of the competition that some unexpected behaviors were also observed. Several students were observed using their smart phone's camera to photo-document the crime scene. One student was seen calling phone numbers found on some of the random pieces of "car garbage," expecting that the competition organizers staged actors on the other side of that phone number.

With the competition being more interactive, a different dynamic was observed within the competition room. Teams seemed inquisitive and engaged with the crime at hand. Parents, mentors, and coaches were able to watch their students obtain new skills and accomplish presenting their case to the panel of judges.

Competitor and spectator feedback for the DFC was overwhelming positive. Comments such as, "that was the most fun I've ever had at a cybersecurity competition" and "it was an excellent educational experience" were commonplace. Feedback following the CCIC 2017 was received through a coaches' survey as well. A common theme amongst the feedback was how positive of an educational experience the DFC was. An experienced team coach expressed his belief that "other competitions [have] something listed as Forensics, but really aren't [forensics while] the CCIC did forensics the right way." Unfortunately, our human subjects' approval for analysis of the CCIC did not allow us to obtain more meaningful feedback due to that the authors were working with minors.

The CCIC 2017 was such a success, the California governor's office has selected Cal Poly and the California Cyber Training Complex (CCTC) to host the CCIC in 2018. This year, each of the regional competitions (San Diego, Los Angeles, Fresno, Sacramento, and Bay Area) will also contain a CCIC challenge in preparation of the state-wide CCIC championships. Because of this unique opportunity of integrating the CCIC challenges into regional competitions we are confident that our assessment tools and tools for broadening participation in cybersecurity competitions will be adopted. Additionally, working with the regionals, the authors believe that they will have unique access to a large number of competitors to track their persistence in cybersecurity post-secondary school.

Ties to previous efforts and research

This project builds directly on existing research and scholarship of our team. Our previous work has shown that cybersecurity competitions that lack opportunities for novices resulting in high levels of attrition[2], and advocates for a more collaborative cybersecurity competition and better supports and engages novices[5]. Additionally, our team has previous experience in designing cybersecurity competitions, such as the CCIC, which was the state's high school cybersecurity championships in 2017.

Other research papers also cite that cybersecurity competitions are often designed for competitors well-versed in cybersecurity topics and that competitions don't aim to educate their participants[4]. Other competition designers have likewise noticed that many cybersecurity competitions lack realism, accessibility, and educational applications.

One interesting research paper created assessments for measuring the vocational and psychological characteristics of cybersecurity competition participants (Bashir 2015) and their measurements could serve as a starting point for our own demographic assessments proposed for this project.

We believe that our approach is promising because

- Creating and using assessment tools on the broader set of cybersecurity skills will likely make competition designers think more inclusively about the composition of their competition tasks.
- Positive increases in diversity in the California cybersecurity high school competitions will inform the nationwide competitions, such as CyberPatriot, on how to increase diversity of cybersecurity competitions nationally.
- High school cybersecurity competitions are formative and represent a key engagement point where the maximum number of pathways to cybersecurity careers should be emphasized.
- Focusing on a breadth of skills will help competitors feel integral to their teams and help developing students find their place in cybersecurity.
- Competitors that do not end up in cybersecurity will still learn valuable skills that are more broadly applicable.

Future work, CCIC 2018

There are several improvements planned for CCIC 2018. First, we plan on embedding links in the forensics data that would enable competitors to "unlock" pre-recorded interviews with key witnesses. This will enable the competitors to have a more realistic examination path. Second, we plan on using more than just a single location to hide evidence, enabling the teams to search multiple locations. Third, we want to continue to make the competition more realistic and the case to solve more dynamic by requiring competitors to bag-and-tag evidence items and complete Android forensics. By incorporating mobile phone forensics, the competitors would have the opportunity to utilize GPS location, Bluetooth connections, and phone call or message logs to piece together an even more detailed timeline. Finally, for future competitions we want to tie together the computer system cybersecurity event with the forensics event. For instance, in a hypothetical scenario, a healthcare organization tasks the student team to protect their computer system from intrusion. After that portion of the competition, the students will be told that the computer systems were hacked and now they will need to perform forensics analysis.

Conclusion

By broadening the scope of cybersecurity competitions, and not solely rewarding good computer competencies, we believe we can attract a wider array of students to the field of cybersecurity.

The computer forensics aspect of cybersecurity provides an interesting, multi-competency entry point for young adults to explore the importance of cybersecurity.

Bibliography

[1] Associates, NICE. 2017. "NICE Program Office Updates." In Minutes of the NICE Working Group monthly meeting. Skype, November.

[2] Portia Pusey, Mark A. Gondree and Zachary N. J. Peterson. 2016. "The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations." IEEE Security & Privacy. vol. 14, no 6, pp.90-95.

[3] Tobey, D. H., Pusey, P., & Burley, D. L. 2014. "Engaging learners in cybersecurity careers: lessons from the launch of the national cyber league." ACM Inroads. (1), 53-56.

[4] Eagle, Chris. 2013. "Computer Security Competitions: Expanding Educational Outcomes." IEEE Security & Privacy. vol. 11, no. , pp. 69-71.

[5] Mirkovic, Tabor, Woo and Portia Pusey. 2015. "Engaging Novices in Cybersecurity Competitions: A Vision and Lessons Learned at ACM Tapia 2015." 015 USENIX Summit on Gaming, Games, and Gamification in Security Education.

[6] Bashir, Masooda and April Lambert and Jian Ming Colin Wee and Boyi Guo. 2015. "n Examination of the Vocational and Psychological Characteristics of Cybersecurity Competition Participants." USENIX Summit on Gaming, Games and Gamification in Security Education.

[7] Dube, Clark Taylor and Pablo Arias and Jim Klopchic and Celeste Matarazzo and Evi. 2017. "CTF: State-of-the-Art and Building the Next Generation." USENIX Workshop on Advances in Security Education .