

A Cybersecurity Camp for Girls

Ms. Cariana Cornel, Brigham Young University

Ms. Caralea M. Cornel, Brigham Young University

Caralea Cornel is a sophomore in the information technology program at Brigham Young University. She is currently working as a research assistant in the cybersecurity research lab and hopes to continue to learn more about what cybersecurity has to offer.

Dr. Dale C. Rowe, Brigham Young University

Dr. Rowe has worked for nearly two decades in security and network architecture with a variety of industries in international companies. He has provided secure enterprise architecture on both military and commercial satellite communications systems. He has also advised and trained both national and international governments on cyber-security. Since joining Brigham Young University in 2010, he has designed a variety of courses on Information Assurance, Cyber Security, Penetration Testing, Cyber Forensics and Systems Administration and published over a dozen papers in cyber-security.

Samuel Moses, Brigham Young University

Samuel Moses is a Security Analyst at Brigham Young University Office of Information Technology. He earned his Bachelors in Information Technology August 2015, emphasizing in the fields of System Administration and Cyber Security. Currently Samuel Moses is working on his Masters in Technology emphasis in Cyber Security.

Cybersecurity Camp - A Call for Awareness

Abstract

The demand for cybersecurity analysts and awareness is increasing, the employment of information security analysts is projected to grow 37 percent from 2012 to 2022, much faster than the average for all occupations. Today, women represent just 10 percent of the cybersecurity workforce. Thus, to increase the amount of people going into cybersecurity, primarily women, we must start at the base: schools. There, we can emphasize the need for being cyber savvy and also address the need to have balanced teams of men and women.

In 2015, we hosted a Girls Cybersecurity Camp for years 9 through 12 that was primarily planned and hosted by female undergraduate students. With 38 attendees, student mentors and faculty prepared a series of workshops, seminars and activities designed to educate and inspire girls to consider potential career paths in cybersecurity. Due to the success of this project, we are planning a bigger and more significant event for the summer of 2016 along with a supplemental series of workshops for STEM teachers at middle and high-schools.

In this paper we discuss the methods and implementation of our 2015 summer camp. We look at the perceived strengths and weaknesses of our approach to identify successful aspects and recommend improvements for the coming year. By including data from entry and exit surveys, we are able to comprehensively analyze both the perceived impact of our camp from the attendee's perspective. We also acknowledge and thank Microsoft and Facebook for their generous financial support of this effort.

Introduction

Last year, a local middle school teacher contacted our research laboratory to request a cybersecurity awareness presentation to her computer class. With two groups of students in an elective course, the presentation was held twice. Between the two classes there was one girl in attendance. During the discussions following the presentation, both students and teachers had an interest in cybersecurity, but felt they lacked sufficient training and suitable subject matter materials. In discussions with other local schools, and independent research discussed later in this paper, we note also that the gender ratio observed is symptomatic of a larger problem in cyber-security.

We summarize these observations as follows: insufficient educator training in cybersecurity, insufficient resources to provide a cybersecurity education, lack of females in cybersecurity.

An undergraduate student in the laboratory with her faculty mentor applied for a small research grant to hold a week-long summer camp in an attempt to address the latter two of these concerns. This resulted in the first Brigham Young University Girls Cybersecurity Camp (BYU-GCC), hosted in July, 2015. The camps objectives were to increase awareness of cybersecurity, educate young women in online safety and increase interest in the cybersecurity discipline. A longer term objective is to increase female enrollment in higher-education cybersecurity majors although for now, this is beyond the scope of this paper.

The Information Technology (IT) industry demand for skilled cybersecurity analysts is increasing. The "employment of information security analysts is projected to grow 37 percent from 2012 to 2022, much faster than the average for all occupations"¹. Today, "women represent just 10 percent of the cybersecurity workforce".² In the same article, David Shearer, CEO of the

International Information Systems Security Certification Consortium (ISC²) stated: “The information security field is expected to see a deficit of 1.5 million professionals by 2020 if we don’t take proactive measures to close the gap,” He added “Knowing this, it is rather frustrating to realize that we do not have more women working in the industry” (ibid).

It has been our experience, and that of other researchers that there is a significant lack of comprehensive cybersecurity education in the middle and high school age ranges. Yet research has shown that middle-school and high-school are effective age ranges for recruiting to STEM fields.³ Thus the focal age range of the summer camp was set to target girls aged from 14 to 18 years.

The summer camp ran for a week and involved eight student mentors, one faculty mentor and 38 attendees. Our experience was successful based on exit survey data, informal feedback from attendees and the perceptions of the student mentors and faculty. Assuming continued efforts to procure funding are successful, we anticipate holding a camp annually for a larger number of girls.

Past Research

Recent research has highlighted the benefits of mixed-gender cybersecurity teams.⁴ The Credit Suisse Research Institute reported that over a period of six years, companies with a gender-diverse environment outperformed a dominantly male environment by 26 percent. As the movement to increase recruitment gains attention, organizations are becoming more proactive in their support and recruiting of female cybersecurity professionals.

Researchers at Mississippi State University (MSU) published a paper in 2012 detailing their efforts and findings.⁵ Their overall objective was to increase women’s interest in Information Assurance as a career field. MSU’s Department of Computer Science and Engineering promotes computer security through the involvement of students in research even as undergraduates. To improve the recruitment and retention of women in technology in their program, MSU implemented a three phase project:

- Phase 1: The goal of this phase is directed in capturing girls’ interest in Information Assurance through educational activities during a summer camp. The camps have been successful over a number of years. Through the camp the researchers learned that women were more likely to pursue fields where they feel they could make a positive difference in society.
- Phase 2: This phase focused on a program to help feed women into Information Technology fields. This allowed women as freshman and sophomores to gain experience and knowledge in information assurance fields like digital forensics.
- Phase 3: The women that showed an aptitude and interest in Information Assurance careers will be invited to job fairs and introduced to potential employers. This assisted the women in showcasing their skills and positive attitudes to help them get summer internships. Researchers stated that once students are exposed to the work the students get excited and work hard to prepare for the demands of the job.

In England, the research project *Computer Clubs for Girls* also showed some promise. This was an all-girl environment aimed to motivate young girls (ages 10 to 14) to pursue interest in IT. The club attempted to complete this goal by tailoring the subject matter to stereotypical girl interests such as fashion or music. However, many of the girls reported having no motivation in

continuing any interest in IT as a career. The researchers concluded that weaknesses contributing to the club results were a lack of technical depth and a narrowed perspective of girls.³

Our own research laboratory has gained experience in successfully cultivating a gender balanced environment. In our studies, we have found that the majority of women that joined the cybersecurity field migrated from other technical fields they were unsatisfied with. Through a variety of recruitment opportunities these women gained awareness of IT as potential field of study. Interviewing a subset of women engaged in cybersecurity research revealed that 70% of the women at our facility attributed their joining the IT program and subsequently cybersecurity research to one or more encounters with another female student at a recruiting event. Though we have found it harder to recruit women who do not have a pre-affinity and strong interest in technology, we theorize that reach out activities to pre-college aged girls will inform women of the information technology and cybersecurity opportunities available and result in increased enrollment.³

Our own findings in a mixed-gender environment that has approached gender equality have supported the ISC² findings. We have noted a significant increase in student research publications, class performance, and performance in cybersecurity competitions. Since 2011, the ratio of female to male students has increased from 1:4 to 2:3. Now in 2016, the ratio has drastically changed to 4:1. (It should be noted that the 4:1 female to male student ratio in the cybersecurity research laboratory is in part due to funding limitations impeding the employment of new researchers and a parent IT program that did not graduate any women between 2014-2015). Student opinion suggests that encouragement to interact, ask questions, and seek mentorship plays a strong role in the retention of undergraduate women in cybersecurity. Additional factors include: a collaborative and unified work environment; opportunities to discover and attend conferences; participation in cybersecurity competitive events and other outreach opportunities; and social activities. Additionally, the Information Technology program, which the CSRL and the Cybersecurity emphasis is under, has seen an overall rise in female enrollment due to this success.³

As part of looking into past research, we reviewed the value of single-sex versus coeducational schooling. There have been good arguments on both sides as they both take into consideration the advantages and disadvantages of each environment. The research has shown that younger females benefit from single-sex education. Students at single-sex schools have demonstrated higher academic achievement and educational aspirations with females completing more homework and achieving more in stereotypical male courses, like math and science. Single-sex schooling leads women to higher career aspirations and accomplishments. It was noted that a consideration for the higher career aspiration and accomplishments may also be attributable to a student's ability to access to same-sex mentors. While a deeper analysis displayed strengths and weaknesses in both single-sex and coeducational schooling, it is evident that there is a role for single-sex learning for the target age-range.⁶

Implementation

Our approach involved studying past researcher findings to learn from similar efforts. We decided to design our camp with what we believed to be an improved outreach methodology, focusing on gender-neutral technical topics⁷ while also addressing current issues and trends in cybersecurity gender balance.⁴ Lab activities were designed to provide: familiarization with a wide variety of platforms and technologies; hands-on technical experience; conceptual

understanding of topics such as networking; online awareness; knowledge on dealing with difficult or sensitive issues pertaining to security and privacy. From our review of single-sex versus coeducational schooling we saw advantages of keeping the camp exclusive to females only. We also sought primarily female mentors and speakers in line with evidence showing that same-sex mentors were a part in the consideration of the women reaching high aspirations and accomplishments. Eighty percent of student mentors were female as were all keynote speakers. The faculty mentor was male (our program does not yet have a female faculty member), but is a successful recruiter and mentor to many female students within our program. He created the cybersecurity research laboratory in 2011 which is now a female-dominant research facility in part due to funding and grants available from the colleges Women in Engineering and Technology (WIET) initiative.

Girls were recruited from local middle and high schools. Communication methods that were used included: flyers at reach out events; social media posting; and e-mails to local schools and teachers. In total, 38 girls attended. The week began on Monday evening with a parent-and-daughter dinner with the purpose of learning more about the week's events and activities. This opportunity was also used to collect signed waivers which included a trigger warning on the topic of cyber-bullying. Surveys were also given to the girls before and after the camp to measure their knowledge, interest and motivation in cybersecurity.



	Tuesday	Wednesday	Thursday	Friday
8:00am	Arrive and Breakfast			
	Sponsor Keynote:	Talk: Thriving as a Woman	Keynote:	Keynote:
8:30am				
9:00am	Daily Briefing - What to Expect			
9:30am	Introduction and Welcome	Longevity of Data & Social Engineering Activity	Password Security Workshop	Forensics
10:00am	Learning Pi with Py			Maintenance and Protection
Profe				Cybersecurity Research Lab Q&A
11:00am				Professional Group Photo
11:30am				
12:00pm	Lunch – CTB Lounge Area			
12:30pm				
1:00pm	Outdoor Activity - Networking	Tour - BYU Datacenter & CAEDM Supercomputer	Tour - BYU Datacenter & CAEDM Supercomputer	Wrap up and closeout
1:30pm				
2:00pm	Morse Code Transmitter	Sponsor Keynote: Facebook	Web Password Cracking	Pick Up
2:30pm		Staying Safe Online	Password Security Workshop	
3:00pm		Cyberbullying		
3:30pm	Finalize and Finish up - help those struggling to make sure they finish day's goals			
4:00pm	Daily Wrap-Up			
4:30pm	Fun with Pi's - Other Projects	Fun with Pi's - Other Projects	Fun with Pi's - Other Projects	
5:00pm	Pick Up			

Figure 1: Schedule of the Girls Cybersecurity Camp

The camp ran for four days from Tuesday through Friday and included topics such as coding in Python, networking, online safety, and social engineering. Team activities included a social engineering scavenger hunt, Morse and code-breaking circuit boards, and a password security

workshop. Each event was run by CSRL students who mentored the girls in the technical and educational aspects of the event.

Each day commenced with a Keynote speaker from a professional woman working in IT or cybersecurity. Speakers from Microsoft, Facebook, BYU Office of IT and LDSTech presented a day in their own life, thriving as a woman and the benefits of mixed-gender cybersecurity environments.

Thanks to generous support from Microsoft and Facebook, who provided significant sponsorship funding, the camp was not only free for attendees, it provided each girl with a Raspberry Pi 2. During the week, the girls used their Pi's for a variety of cybersecurity related activities, and were able to take them home for use as a personal computer at the end of the event.

One of the highlights of the week was a spy scavenger hunt. Participants had to solve multiple challenges involving forensics, social media reconnaissance and penetration testing to reveal the mission and location of a spy. Once at the location, they had to social engineer the target using pre-determined code-words and phrases from their research. If successful, the stolen data was retrieved and the mission completed.

Throughout the event, a team of student mentors were present in the workshops to assist with any girls who may be struggling – and provide extra one-on-one mentoring for those who were not sufficiently challenged by the group's activities. The impact of this personal approach to mentoring were commented on by several girls and parents both during and after the event. We believe that this was a critical part of the camps success and would strongly encourage other groups considering hosting a similar event to adopt this approach to mentoring.

Results and Findings

As previously mentioned, our camp decided to focus on both technical and social aspects of cybersecurity. Research has shown that activities designed to be effeminate are often limited in their effectiveness and are not taken seriously. The girls thus experienced multiple aspects of cybersecurity that were designed to educate, build confidence and provoke interest.

Survey data showed an overall doubling in the number of girls expressing a strong or very strong interest in cybersecurity (33 girls took the pre-camp survey with 29 girls completing the post-camp survey); 94% of attendees expressed an interest in cybersecurity after the event.



Figure 2: Interest in cybersecurity before and after GCC2015

We believe this indicates that the camp was a success. Exit surveys also collected feedback comments which were reviewed in detail to identify strengths and weaknesses of the week's activities. These will be re-reviewed in planning committees of the 2016 summer camp.

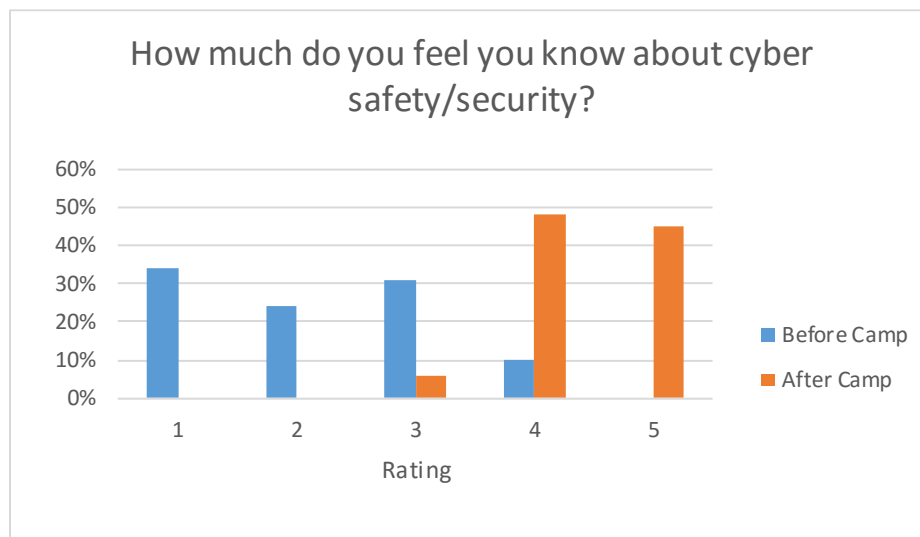


Figure 3: Self assessed knowledge in cybersecurity.

In another question from the survey, inquiring how much they feel they know about cyber safety/security (Figure 3) based on a scale from 1 - 5, the outcome displayed an increase in how much they feel they know about cyber safety/security. Self-assessed knowledge in cybersecurity on a scale of 1-5 shifted from an average of 2.17 to 4.39. This implies that the camp led girls to feel more confident in their knowledge of cybersecurity.

Overall, the survey results indicate the camp was a significant success and we are hopeful that this will generate increased interest and consideration of cybersecurity as a field of study for those who attended. In addition to this, the comments indicated that the camp was a fun and enjoyable experience in learning the various topics and understanding what future opportunities

are available to women in the field. In the final question, 100% of attendees said they would return again to similar summer camps. This positive feedback suggests that camp such as this are helpful in spreading awareness in a fun, relaxed and educational way.

Future Plans and Objectives

Based on our efforts last year, we are looking to expand our outreach efforts over the coming year. To date, students from the CSRL have hosted two Capture the Flag events for girls in the same age range at local groups of DigiGirlz and SheTech. These has resulted in over 70 new girls registering an interest for this year's summer camp.

In addition to the GCC, next year, we are looking to host an eight week evening school for teachers that will occur two nights a week. This is being designed to equip the teachers with the knowledge, resources and skills they need to not only tackle their own online safety, but educate their students and potentially become coaches for local cyber patriot groups. (Cyber Patriot is a national cybersecurity youth program affiliated with the US Air Force Academy <https://www.uscyberpatriot.org/>).

While we found success in our first year hosting this camp, we also discovered areas for improvement. While we had a theme (Codebreakers of World War 2) that we hoped to keep throughout the camp, we found it difficult to always tie everything back to the theme. This was largely due to limited preparation time caused by late funding and approvals to host the camp. We believe that a continuous theme would have provided a much more cohesive experience for the girls and intend to begin development for the next camp well in advance.

Last minute technical issues also resulted in several mentors with the faculty mentor spending excessive time making last minute corrections and testing rather than working with attendees. We will hence include more extensive testing for future events. Making certain everything is built and prepared beforehand will help mentors be able to focus on teaching and helping the students. This will be accompanied by more extensive training for mentors to ensure a higher quality of instruction and support throughout the camp.

Despite these minor difficulties, the overall consensus was that the camp was a great success. There was an excellent group of attendees and great sponsors, Microsoft and Facebook. We anticipate that these improvements for future camps will improve upon the overall quality of the experience while allowing mentors more interactions with attendees.

Conclusion

The Girls Cybersecurity Camp was set up in an effort to recruit and retain women in cybersecurity education, to teach internet safety, and to increase the amount of potential female employees in the field. The camp raised awareness by teaching those of a younger generation about potential cyber threats.

Internet safety is greatly applicable to today's youth as they spend up to 10 hours a day using various forms of media such as Facebook or Instagram.⁸ In combination with internet safety, cybersecurity is also an ever growing field. Because of this, "cybersecurity awareness is" necessary "for internet users like youngsters as a counter-measure strategy to combat silent privacy invasion".⁹ The camp taught participants about protecting their private information, opportunities available in the information assurance field and the encouragement to continue their cybersecurity education.

The GCC's goal is to address the concern that there is an insufficient number of women in the cybersecurity field. The camp helps to promote this by inviting speakers to talk about the different opportunities the cybersecurity has to offer. In conclusion, the camp was an overall success; the girls had a fun positive learning experience and reported that they would like to attend the camp.

Acknowledgements

We wish to express our sincere thanks to the sponsoring organizations; Microsoft and Facebook as well as LDSTech and the BYU Office of IT whose support made this camp possible.

Bibliography

1. US Department of Labor - Bureau of Labor Statistics. Information Security Analysts. 2014.
2. Zakrzewski C. Women Could Be The Solution To Fighting Cybersecurity Threats. TechCrunch. 2015 [accessed 2016 Mar 15]. <http://techcrunch.com/2015/09/28/women-could-be-the-solution-to-fighting-cybersecurity-threats/>
3. Winders W, Cornel C, Cornel C, Larson A, Cunha S, Moses S, Rowe D, Wilkinson L. Cyber War is not Gender War - Experiences of Creating a Productive Heterogeneous Environment in Cyber Security Research. In: 2015 ASEE Annual Conference and Exposition Proceedings. ASEE Conferences; p. 26.437.1–26.437.10. <http://peer.asee.org/23776>
4. Frost and Sullivan. Agents of Change: Women in the Information Security Profession. Mountain View; 2015. <https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/Women-in-the-Information-Security-Profession-GISWS-Subreport.pdf>
5. Dampier D a, Kelly K, Carr K. Increasing Participation of Women in Cyber Security. In: 2012 ASEE Southeast Section Conference. San Antonio, Tx: ASEE; 2012.
6. Single-Sex Versus Coeducational Schooling: A Systematic Review. 2005.
7. Fuller A, Turbin J, Johnson B. Computer Club for Girls: The problem with seeing girls as the problem. Gender and Education. 2013;25(4):499–514.
8. Moreno MA, Egan KG, Bare K, Young HN, Cox ED. Internet safety education for youth: stakeholder perspectives. BMC Public Health. 2013 [accessed 2016 Mar 22];13(1):543. <http://www.biomedcentral.com/1471-2458/13/543>
9. Rahim NHA, Hamid S, Mat Kiah ML, Shamshirband S, Furnell S. A systematic review of approaches to assessing cybersecurity awareness. Kybernetes. 2015 [accessed 2016 Mar 22];44(4):606–622. <http://www.emeraldinsight.com/doi/10.1108/K-12-2014-0283>