The Cybersecurity Competition Experience: Perceptions from Cybersecurity Workers

Colin Wee
University of Illinois Urbana-Champaign
603 E. Daniel St,
Champaign, IL 61820
+1 (217) 333-6423
jwee2@illinois.edu

Masooda Bashir
University of Illinois Urbana-Champaign
501 E. Daniel St, MC-493
Champaign, IL 61820
+1 (217) 244-1139
mnb@illinois.edu

Nasir Memon
New York University
10 MetroTech Center,
Brooklyn, NY 11201
+1 (646) 997-3970
memon@nyu.edu

ABSTRACT
How do workers within the field of cybersecurity perceive cybersecurity competitions? This study aims to address this question and investigate if competitions left a positive mark on the information security workers who participated in them. In this paper, we report on an online survey of current employees of the cybersecurity industry who had once participated in Cybersecurity Awareness Week, one of the most established cybersecurity competitions in the world. We examine their perceptions of the competition in general, the skills they learnt from the competition, and whether they felt the competition was beneficial to them. Data from 89 cybersecurity workers showed that competitions taught them useful skills related to their job, especially skills related to reverse engineering and analytic skills. Their competition experience was also a major influence in their career-decision making.

Keywords
Cybersecurity Workers; Information Assurance; Human Factors; Cybersecurity Competitions.

1. INTRODUCTION
Cybersecurity attacks are a looming threat that is a major concern for the United States. The U.S. government emphasized the importance of national cybersecurity by passing four bills aimed at developing a plan to increase the number of information security professionals in the workforce [1]. One of the ways that the government promotes cybersecurity is through the sponsorship of cybersecurity competitions. The Department of Homeland Security and the National Security Agency often sponsor major competitions such as the National Collegiate Cyber Defense Competition (NCCDC) and New York University's Cybersecurity Awareness Week (CSAW). These contests are typically organized by schools and targeted towards high school- and college-aged students. Competitions such as the University of Santa Barbara's International Capture the Flag competition raise awareness of contemporary cyber threats and teach participants best network safety practices through live exercises. Participants also learn to apply problem solving strategies from classes and labs in real-world scenarios [2].

Schools benefit from cybersecurity competitions because they can evaluate their computer security syllabi and foster teamwork among their students. Industries benefit from cybersecurity competitions because they are places for professional networking and scouting of young talent [3]. But, how do workers within the cybersecurity field perceive cybersecurity competitions? Did workers who participated in cybersecurity competitions derive positive benefits from that experience? The present research aims to address these questions.

1.1 Related Work
Past research on cybersecurity competitions has shown that they are effective at piquing student interest on the subject of cybersecurity [4] and directing them towards a career in cybersecurity [5]. However, not much research has looked at competitions from a retrospective viewpoint of an employee working in the cybersecurity field. It is important that the people who transition from competitions to the cybersecurity workforce take-away positive skills and experiences from the competition, and have the opportunity to apply these skills in their working lives. Yet there have been only a handful of studies which looked at the skills required in cybersecurity jobs and none of them compared them to the skills learned in cybersecurity competitions. Previous research on the cybersecurity workforce included a study on cybersecurity workers in Australia which showed that the broad skills valued within field included technical expertise, experience, teamwork, and presentation skills [6]. The specific types of technical expertise would vary depending on the type of job of the worker. A study on women employees in the cybersecurity field also showed that problem solving skills, analytical skills, and technical skills were crucial for early career advancement [7]. The present study builds on the research on skills required in the cybersecurity workforce by connecting it to the skills learnt during cybersecurity competitions. Using a U.S. sample of cybersecurity employees, the present research investigates the extent to which skills such as teamwork, analysis, hacking, and reverse engineering are taught by competitions. By classifying information security workers into different job roles such as analyst, engineer, and researcher, we further investigate if the skills taken away from competitions differ between specific occupations. We thus have two main research questions for this study:

RQ1: What skills are learnt during competitions and do cybersecurity employees find the skills taught in competitions useful for their job?

RQ2: Does the perception of skills learnt and competition effectiveness differ depending on the occupation of the cybersecurity employee?

The present research uses a sample of information security workers who participated in New York University's Cyber-Security Awareness Week (CSAW) one or more times. CSAW is an annual on-site competition with an 11-year history. The competitions within CSAW vary from Capture-the Flag, Policy-making, and embedded systems. Although CSAW is just one competition and workers drawn from this competition may not necessarily represent the entire population of cybersecurity workers, we feel that this compromise had to be made. It is difficult to access a broad sample of workers from mailing lists of different competitions as many competition institutions were reluctant to share their contact lists of their participants to researchers. Secondly, CSAW is one of the most established and a prestigious international competition, which annually recruits over 10,000 participants from around the world. There have also been several previous studies that have used CSAW competition participants as their sample to study cybersecurity competitions [5]. Thus, surveying a sample of cybersecurity workers who had participated in CSAW could produce a more representative sample of the cybersecurity workforce than originally thought.

2. Method

2.1 Participants

We used an email-list of past participants of New York University's Cybersecurity Awareness Week (CSAW) Capture-the-Flag competition to recruit respondents to our online survey on Cybersecurity Competitions. The survey was described as a questionnaire to learn more about the types of people attracted to the field of cybersecurity and help to improve future cybersecurity competitions. Respondents who completed at least 80% of the survey were rewarded with a $10 Amazon gift card for their time. A total of 408 people from the mailing list clicked on the survey link, and 235 consented to complete the survey for monetary compensation (Response rate of 57.6%). Two quality control items (e.g. Please select the 'strongly disagree' option) were used to flag careless responders (e.g. those who responded the same for all questions). The final sample comprised 217 For the purpose of this study, the sample was constrained to only current employees working within the field of cybersecurity ($N = 89$).

2.2 Survey Design

The present survey was part of a much larger survey about the psychological profiles of cybersecurity competition participants, their perceived efficacy in carrying out different cybersecurity tasks, and their satisfaction with the job. For the current study, we used data from 16 multiple-choice questions asking about participants' perceptions about cybersecurity competitions. These questions were answered on a scale of 1-5, with 1 representing 'strongly disagree' and 5 representing 'strongly agree'. Items in the survey covered the topic of participants' perceptions of the positive impact of cybersecurity competitions (e.g. "The skills I learned from cybersecurity competitions were useful", "Cybersecurity competitions increase the appeal of the field to the general public") as well as the negatives of cybersecurity competitions (e.g. "Cybersecurity competitions take up too much time"). The survey also contained questions asking participants to rate the skills learned during the cybersecurity competition. These skills were grouped under 8 categories (reverse engineering, cryptography, hacking & penetration testing, network security, operating systems, teamwork, steganography, and analytic skill). The categories were agreed upon by two content experts in the field of cybersecurity education. Items were set on a scale of 1-4 from "None" to "A lot". The survey also included two open ended questions asking if participants what other unlisted skills they learned from the competition, and if they had any suggestions on how to improve future cybersecurity competitions.

The demographic variables collected in the survey included the number of times participants participated in CSAW, the furthest they reached in the competition (finals vs. qualifying rounds), their gender, ethnicity, age, income, occupation, and highest level of schooling obtained.

2.3 Demographics

Of the 217 people that provided useable results, 89 reported that they were currently employed within the field of cybersecurity. The occupations that these people held ranged from security analysts/consultants ($N = 21$), penetration testers ($N = 9$), security engineers ($N = 20$), researchers ($N = 13$), interns ($N = 5$), and government/military workers ($N = 4$). The average age of the employed subsample was 25.44 ($SD = 5.31$). 64.0% of the sample was White, 22.5% was Asian, 7.9% were Hispanic, 1.1% were African American, and 4.5% specified 'other'. 84 people identified as male, 3 identified as female, and 2 as other. This gender distribution was similar to our previous studies conducted within the same population of CSAW participants, and unfortunately limits the ability to compare results between genders. The education background of the employed workers was varied. 19 had the equivalent of a high school or general education diploma, 44 had a bachelors' degree, and 20 had a masters' degree. Two people reported having professional or PhDs as their highest level of education obtained. 47 people reported majoring in computer science, 11 people majored in engineering, 11 in computer and information security, and 3 in physics. 77.5% of the cybersecurity employees had taken an academic course in cybersecurity before ($N = 69$).

2.3.1 Competition-related Demographics

Our sample of cybersecurity employees were generally frequent participants of cybersecurity competitions. 78.7% reported having participated in more than 3 competitions outside of CSAW and 14.6% have participated in CSAW more than three times. 25.8% ($N = 23$) of the employed sample reached the finals of CSAW; this is relatively higher than the complementary sample of participants no currently employed within cybersecurity—only 9.8% ($N = 10$) reached the finals of CSAW. Team composition was extremely varied within the sample, ranging from individuals participating alone and teams of 43. The average team size was 5 people. 73.0% of the sample ($N = 65$) reported working in all-male teams, 19.1% ($N = 17$) reported teams with a minority of females.

3. Results

3.2 Skills Learned

Overall, cybersecurity competitions were considered a very positive experience for workers within the information assurance field. 89.9% ($N = 80$) agreed or strongly agreed to the statement that the skills they learned from cybersecurity competitions were useful. 58.4% ($N = 52$) agreed or strongly agreed that their experience in cybersecurity competitions influenced their decision to enter a cybersecurity career. 50.6% ($N = 45$) disagreed or strongly disagreed to the statement that cybersecurity competitions take up too much time. Cybersecurity employees also perceived that competitions had a positive impact to the field of cybersecurity. 68.5% ($N = 61$) of the employed sample agreed or strongly agreed that competitions were effective at recruiting people into cybersecurity careers. 64.1% ($N = 57$) agreed or

strongly agreed that cybersecurity competitions increase the appeal of the field to the general public.

With regards to the specific types of skills taken away from cybersecurity competitions, information security workers reported that reverse engineering and analytic skills were the most learned and tested skills within the competition (Figure 1). Since previous studies found analytical skill and technical expertise to be among the most demanded skills for career advancement in cybersecurity [6, 7], it is advantageous that these are the main skills learned from the cybersecurity competition. Qualitative analysis of the open-ended question regarding additional skills learned from cybersecurity competitions showed that exploitation was a common skill not covered by our original 8 categories. 8 people stated that binary exploitation was a useful skill they learned from these competitions. From the above analyses, the answer to research question 1 is that employees learn a variety of skills in cybersecurity competitions, of which reverse engineering and analytic skills are most prominent, and they find them to be useful and applicable in their current jobs.

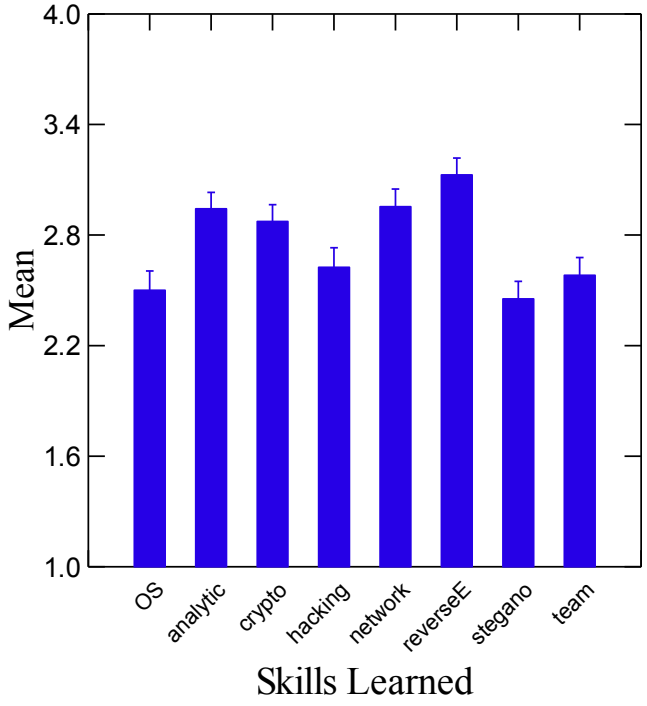

Figure 1. Skills learned from cybersecurity competitions. Categories are: operating systems (OS), analytic skills, cryptography, hacking and penetration testing, network and web security, reverse engineering, steganography, and teamwork. Question was on a scale of 1 to 4.

An analysis of variance was used to investigate if there were specific occupations which showed differential learning of skills from competitions. The ANOVA showed that there was a significant difference between occupations in learning cryptography. Cybersecurity employees working as researchers differed from analysts and engineers in skills learned. Researchers reported that they learned a lot more about cryptography from competitions (M = 3.54, SD = .519) while analysts and engineers reported significantly less learning in cryptography (2.45 and 2.70; $t(31)$ =-4.87 and -3.34, $p < .01$). There were no other significant differences between occupations in terms of learned skills. Thus, our answer to research question 2 is that the skills learnt in cybersecurity competitions are mostly unaffected by the type of occupation that the information security worker is from.

4. Discussion

The present study sought to study the usefulness of cybersecurity competitions in the eyes of employees within the field of cybersecurity. By focusing on employees who had experienced one or more cybersecurity competitions, we learned that they perceived cybersecurity competitions to be a good way to recruit people into cybersecurity careers, and that the majority of them had their career decisions influenced by their experience in cybersecurity competitions. The technical and analytical skills that they learn through their experiences in cybersecurity competitions overlap with the skills high in demand within the field of cybersecurity. With the exception of cryptography (which researchers reported learning more of), cybersecurity competitions teach a broad set of skills that generally do not favor a specific occupation within the information assurance field.

4.1 Limitations and Future Directions

The main limitation for this study on cybersecurity competitions was its reliance on retrospective self-report data for participants of past CSAW competitions. The competition duration, quality, and overall experience would have been quite different from year to year. However, assessing multiple competitions together is a good way to find out the aggregate perceptions of information security workers on competitions in general. We also had to settle for retrospective self-report data because it is difficult to acquire a large sample of cybersecurity specialists who have been in different competitions above and beyond CSAW. Another limitation to our current methodology was that we did not survey the perceptions on cybersecurity competitions from workers within cybersecurity who did not participate in any competition before. These people might share a different, negative opinion on the cybersecurity competition experience and what they can learn from it. There have been studies showing that the barrier to entry to participating in competitions is very high in terms of skill and knowledge, and this could be an intimidating factor that deters some workers within the cybersecurity field [8]. One final limitation is that our sample, like most of the cybersecurity workforce, is predominantly male. In our survey we had asked participants if they felt cybersecurity competitions appealed to men more than women, and 47.2% of respondents agreed. Women might perceive competitions differently and their viewpoint should be keenly studied to find ways to reduce the gender disparity within the field. Future studies should be conducted within cybersecurity employees, with additional efforts to recruit more women in the sample, who have never participated in competitions to gather their viewpoint about the utility of the competition experience.

4.2 Conclusion

This brief study examined the skills learnt from cybersecurity competitions by information security workers. Research on cybersecurity competitions is still in its nascent state and we are slowly but surely contributing more evidence of the effectiveness of these teaching and recruitment tools. Replication with different competition samples and further study into the cybersecurity competition experience is essential to reinforce findings from this growing field.

5. ACKNOWLEDGMENTS

Our thanks to the CSAW and its participants for being an accessible research sample.

6. REFERENCES

[1] ISACA, 2015 Global Cybersecurity Status Report, available at http://www.isaca.org/pages/cybersecurity-global-status-report.aspx

[2] Vigna, G., Borgolte, K., Corbetta, J., Doupe, A., Fratantonio, Y., Invernizzi, L., Kirat, D. and Shoshitaishvili, Y. 2014. Ten Years of iCTF: The Good, The Bad, and The Ugly. In *Proceedings of the USENIX Summit on Gaming, Games and Gamification in Security Education (3GSE)*, San Diego, CA.

[3] Gavas, E. and Memon, N. 2012. Winning cybersecurity one challenge at a time. *IEEE Security & Privacy*, vol. 10(4), 75-79. DOI= http://dx.doi.org/10.1109/MSP.2012.112

[4] Cheung, R. S., Cohen, J. P., Lo, H. Z. and F. Elia, 2011. Challenge based learning in cybersecurity education. In *Proceedings of the 2011 International Conference on Security & Management*, Las Vegas, Nevada,

[5] Bashir, M. Lambert, A., Wee, J. M. C., Guo, B. and Memon, N. 2015. An examination of the vocational and psychological characteristics of cybersecurity competition participants. *In 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*, Washington, DC.

[6] Potter, L. E. and Vickers, G. 2015. What skills do you need to work in cyber security?: A look at the Australian market. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research* (SIGMIS-CPR '15). ACM, New York, NY, USA, 67-72. DOI= http://dx.doi.org/10.1145/2751957.2751967

[7] Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J. and Chai, S. 2010. Women in cybersecurity: A study of career advancement. In *IT Professional*, vol. 12(1), 24-31. DOI= http://dx.doi.org/10.1109/MITP.2010.39

[8] Cheung, R., Cohen, J. Lo, H., Elia, F. and Veronica C.M. 2012. Effectiveness of Cybersecurity Competitions. In *Proceedings of the International Conference on Security and Management*, Las Vegas, Nevada.