An Examination of the Vocational and Psychological Characteristics of Cybersecurity Competition Participants

Masooda Bashir
University of Illinois at Urbana-Champaign

April Lambert
University of Illinois at Urbana-Champaign

Jian Ming Colin Wee
University of Illinois at Urbana-Champaign

Boyi Guo
University of Illinois at Urbana-Champaign

Abstract

The demand for cybersecurity professionals grows each year, and so do efforts to attract students to cybersecurity. Competitions are a popular way to address the shortage of cybersecurity professionals, but are competitions actually effective at attracting talent into the cyber security workforce? To date there has been little empirical evidence of the effectiveness of cybersecurity competitions, but this paper presents the results of an extensive survey of cybersecurity competition participants. These results provide a profile of the demographic, psychological, cultural, and vocations characteristics of competitions participants and may inform efforts to develop effective competitions and tools for identifying promising cybersecurity students.

1. Introduction

The demand for cybersecurity professionals grows each year, and so do efforts to attract students to cybersecurity. In late 2014, the United States Congress passed several bills aimed at increasing the nation's cybersecurity. One of these, the Cybersecurity Workforce Assessment Act of 2014 (Pub.L. 113-246), required the U.S. Department of Homeland Security to assess the current status of the government's cyber security workforce and to develop a plan for recruiting and training cyber security professionals. Another of the bills passed enhances the pay scales for government cyber security employees in an attempt to attract and retain needed talent (and compete with the private sector). (Pub.L. 113-277). These efforts join the ranks of other government programs intended to increase the cybersecurity workforce and train these professionals, such as the Federal Cyber Service: Scholarship for Service Program, which awards scholarships to promising students interested in working for government upon graduation. Despite these efforts, both government and industry continue to struggle to fill professional cybersecurity positions.

Another method of attracting promising students into cybersecurity careers has been the sponsorship, by both industry and government agencies, of cybersecurity competitions. These contests, held around the United States typically for high school- and college-aged students, aim to train the next generation of cybersecurity specialists using hands-on competition and to enhance the interest of a cybersecurity career for those already expressing some interest in the field. Competitions have generally been seen as great tools for cybersecurity recruitment and great effort has gone into developing the best competitions and experiences for students (NICCS; Tobey, Pusey, and Burley, 2014).

This enthusiasm for competitions as an effective tool for attracting participants to the cybersecurity field, however, has, to date, little empirical evidence to back it up. While there has been work done by the cybersecurity education community to develop the "best" competitions, there has been almost no empirical research done to explore whether competitions really are effective recruiting tools and to explore the characteristics of the students who compete and then do go on to a cybersecurity career. Our project begins to try to fill this empirical lacuna by assessing the demographic, personality, cultural, and career interest characteristics of hundreds of participants in one of the largest and longest-running cybersecurity competitions, which is associated with the Cyber Security Awareness Week (CSAW) conference held annually at New York University Polytechnic School of Engineering. Using several well-developed psychological, cultural, and vocational measures, we developed an extensive profile of those who participate in cybersecurity competitions. Participants in this study include both students and graduates, some of whom who are currently employed in the cybersecurity field, providing data about competitors at different stages in their education and careers. The data that we have gathered in this project can be the initial step towards the development of effective cybersecurity competitions—effective both at teaching students and at

attracting them to the cybersecurity profession—and potentially the development of an assessment tool for identifying students well suited for the cybersecurity profession.

2. Related Work

While there has been almost no empirical work done assessing the effectiveness of competitions for attracting students to cybersecurity competitions, two recent papers have begun to explore this issue. Tobey, Pusey, and Burley (2014) explored the engagement levels of students participating in one season of the recently formed National Cyber League, concluding that competitions seemed best suited for reinforcing the interests of those already with high-level cybersecurity skills. Cheung and colleagues (2012) assessed changes in interest levels and self-reported skills in a small set of students who participated in a series of workshops and lectures leading up to a competition, concluding that knowledge levels were a significant barrier for using competitions to recruit students into cybersecurity careers. Additionally, Turner and colleagues (2014) have assessed high school students using several psychological measures before, during, and after a "cyber science" residential camp program to determine whether their interest in and perceived value of the subject changed.

There is also a growing body of research into how to best develop cybersecurity competitions (Capalbo, Reed & Arpaia, 2011; Patriciu & Fortuna, 2009) and how to use competitions to further cyber security education (Cheung, Cohen, Lo & Elia, 2011; Conklin, 2005; Werther, Zhivich, Leek & Zeldovich, 2011). This research is typically guided by personal experience with competitions and the idea that the most effective competitions are those that most effectively teach cybersecurity skills. Thus, this body of literature focuses on the design of the competition exercises with the hope that the result will be more skilled cybersecurity students and professionals.

While these above approaches are much needed and developing the best competitions is an important part of the solution, our research focuses on another key part: identifying *who* is best suited for recruitment. Though it is highly important to develop programs that will effectively teach the best cybersecurity skills, we believe that understanding who the learners are, including their interests in and capacities for undertaking cybersecurity careers is also important. The data presented in this paper begins to do that.

3. Methodology

To obtain respondents for this survey, 8,000 participants of CSAW, one of the largest and longest running cybersecurity competitions, held annually at New York University Polytechnic School of Engineering, were emailed a link to an online survey. CSAW is a capture-the-flag type competition in which teams of students compete in regional rounds culminating in a national finals round. There is a high school track and an undergraduate track, and each school forms their own team(s). An incentive of a $10 Amazon gift card was offered to each participant who completed at least 70% of the survey. On average, the 229-question survey took 30-40 minutes to complete. The survey asked for a range of information about the participants, including (1) demographic information, (2) competition experience, (3) hacking practice, (4) intentions or actuality of pursuing a cybersecurity career (depending on age), and (5) responses to several standard psychological, career inventory, and cultural measures. Some sections of the survey were dynamic, so depending on their responses regarding age and employment and education status, participants were asked different questions relevant to their current situation. For example, respondents who indicated that they were currently in cyber security careers were asked about their work experiences, while students were asked about their academic and career plans. We recognize that this survey reached only those who already have expressed *some* interest in cyber security, as it includes only those with a connection to the CSAW competitions, and therefore may be limited. However, we believe these results provide some guidance for determining how to motivate those who come to competitions to pursue cyber security careers.

In addition to the questions developed for this survey, which included demographic information, competition experience, experience and intentions regarding cybersecurity careers, and other hacking experience, several standard measures were administered. To assess vocational interests, respondents were asked to complete a truncated version of Holland's (1997) interest classification to assign a vocational personality type. This model, often referred to as RIASEC, assumes six vocational personality types and work environments—**R**ealistic, **I**nvestigative, **A**rtistic, **S**ocial, **E**nterprising**,** and **C**onventional. The best fit or congruence for workers and workplace occurs when a workers' RIASEC code matches that of his or her workplace.

Participants were also asked to complete a 44-question version of the Big 5 personality inventory, the dominant personality measure used today (Goldberg, 1990). This measure provides a personality profile across five factors: openness to experience, conscien-

tiousness, extraversion, agreeableness, and neuroticism. Of these the factor that proved most notable for our participants, as described below, was neuroticism, which refers to the tendency to experience unpleasant emotions easily and to a degree of emotional stability and impulse control.

Also included were questions related to attachment dimensions, which are individual differences in "attachment style" that emerge from experiences in relationships. (Fraley, Waller & Brennan, 2000). We assessed two dimensions of adult attachment style: attachment anxiety and attachment avoidance. Respondents were also asked two questions to assess their perception of their own self-efficacy towards cybersecurity tasks, which is the strength of one's beliefs in one's own ability to complete tasks and achieve goals (Rottinghaus, Larson & Borgen, 2003).

Another measure included in the survey was a version of Triandis' cultural measure (2001), which assesses cultural orientation in two dimensions: horizontal–vertical and individualism–collectivism. The horizontal–vertical dimension measures differences in preferences for equality or hierarchy, and the individualism–collectivism dimension assesses preferences for independent or interdependent self-constructions, relationships, and goals.

In this paper we use two main statistical methods: (1) t-test and (2) correlation coefficient. The t-test is used to determine if two sets of data are significantly different from each other. The correlation coefficient is a measure of the linear correlation between two variables. The correlation coefficient can range between -1 and +1 inclusive, where +1 is total positive correlation, 0 is no correlation, and -1 is total negative correlation.

4. Results & Discussion

4.1 Demographics

In all, 588 people responded to at least some part of the survey. Only 11.88% (n=67) identified as female. This is slightly less than the 15% female participation rate an Tobey, Pusey, and Burley (2014) found among National Cyber League participants. Some minority racial and ethnic groups were also underrepresented, with 48.40% (n=272) of the overall group identifying as white and 32.03% (n=180) as Asian. Only 2.49% (n=14) were African-American, 6.41% (n=36) were Hispanic/Latin American, and 0.18% (n=1) identified as Native American. The 2.85% (n=16) selected "other" for this question, 7.65% (n=43) preferred not to answer, and eight failed to provide any response. The mean age of the respondents was 24.26 years old.

Those currently in school constituted 72.27% (n=404) of the respondents, with 50.38% (n=199) of these currently undergraduate students. High school students account for 29.37% (n=116) of the student population, and graduate students another 16.96% (n=67). The remaining students were in professional degree programs (2.28%, n=9), other education institutions (1.01% n=4), or failed to indicate their level of enrollment (n=9). Undergraduate and graduate students were also asked to report their major or field of study. Again, the undergraduate students were less diverse, with 92.31% of those who reported (134 provided did not respond to this question) indicating that their major was computer or information science. Another 6.15% of the undergraduates were studying engineering. A single respondent indicated that their major was in the social sciences. At the graduate level, 80.33% (n=49) were studying computer or information science and 6.56% (n=4) engineering. Other responses included business, mathematics/statistics, physical sciences, and biology/life science.

Students were also asked a number of questions about their competition experience. Many of the students attend more than one competition per year; Table 1 shows how often each group participated in competitions. When asked their primary reason for attending competitions, the most popular reason was "for fun and enjoyment" (54.7%, n=150) followed by "to learn new skills" (26.6%, n=73).

	Less than 1	1	2 or 3	4 or 5	6 or more
High school students (n=87)	32.18%	40.23%	18.39%	3.45%	5.75%
Undergraduate students (n=138)	18.12%	23.19%	34.06%	7.97%	16.67%
Graduate students (n=50)	12.00%	22.00%	30%	18.00%	18.00%
Employed in cybersecurity field (n=88)	3.41%	13.64%	43.18%	18.18%	21.59%
Employed in different field (n=95)	16.84%	28.42%	28.42%	8.42%	17.89%

Table 1. Frequency of competition attendance (per year).

The respondents were also asked whether their experiences at the competition made them change their intended career plans, and if so, whether they were more or less likely to go into a cyber security career. More than half of the high school students said that the competition had affected their plans (53.49%, n=46), and of these 80.85% (n=38) said they were now more likely to pursue a cyber security group. Fewer undergraduate students (29.2%, n=40) and graduate students (28.00%, n=14) responded that the competition had changed their plans. Of those surveyed, 37.35% (n=161) are employed full time. Of these, 57.76% (n=93) are employed in a field related to cyber security. The rest (42.24%, n=68) are employed in non-cyber security positions. Of the cyber security employed group, 66.29% (n=59) were employed in the private sector, 19.10% (n=17) were employed in federal agencies, 3.37 (n=3) in the national labs, 4.49% (n=4) in state or local agencies, and 2.25% (n=2) in federally funded research and development centers. The remaining 4.49% (n=4) indicated "other" for this question. Employed participants responded similarly to students that they attended competitions primarily for fun and enjoyment (53.7%, n=58). Like the students, employed respondents were asked whether the competition changed their career plan and, if so, whether they were more likely to go into a cyber security-related career. Of those currently employed in a cyber security career, more than half responded that the competition had changed their career plans (51.09%, n= 47) making them more likely to go into a cyber security-related career. As for those in non-cyber security careers, only 28.88% (n=13) said that the competition had changed their career intentions positively towards a cyber security career.

4.2 Career Interests

This was an exploratory study investigating several individual difference variables assessed within a sample of cybersecurity competition participants, with the aim of better understanding the unique characteristics of people who are likely to become cybersecurity professionals. More specifically, we identified the interest and personality profiles of cybersecurity competition participants and examined if the relationships found between interests, personality and other measures could be corroborated by existing scientific literature.

Of the six dimensions of Holland's (1997) interest classification, those interested in cybersecurity on average scored highest on Investigative (M = 3.33, SD = .94), Social (M = 2.90, SD = .93), and Artistic (M = 2.87, SD = .96). See Figure 1. An analysis of variance followed by paired t-tests showed that individuals scored significantly higher on Investigative interests

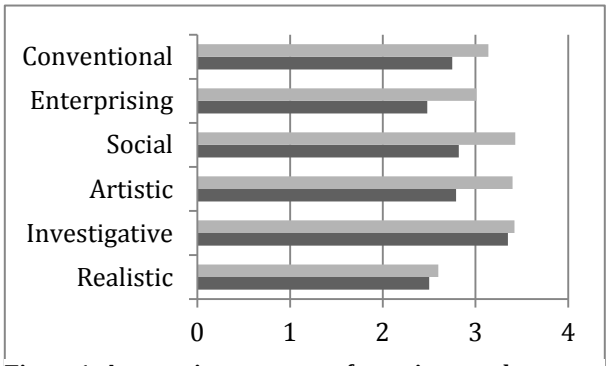

Figure 1. Average interest scores for entire sample (n=372) by gender.

than any other interest (F = 4.65, p < .05). Social and Artistic scores were not significantly different from each other, but they were significantly higher than the Enterprising, Conventional, and Realistic interests. Further dividing the sample into participants already employed in cybersecurity versus those who wish to pursue a career in cybersecurity revealed that the interest profile of aspiring cybersecurity workers did not significantly differ from those who are already employed in the field. From these comparisons of mean level interest scores, we can infer that among those surveyed aspiring cybersecurity workers and current employees of cybersecurity can be characterized mainly by their interests in puzzle-solving and scientific pursuits, followed by an interest in helping others and enjoyment of creative endeavors.

The survey included a behavior-based measure of intentions for those who were not yet employed in a cybersecurity job. This provided the unique opportunity for a regression analysis to be conducted to investigate if interest scores could predict whether or not the individual declares intention to pursue a job in cybersecuri ty after his or her experience in the hacking competition. A discriminant function analysis was performed using the six RIASEC scale scores to predict if participants would answer "yes" or "no" to pursuing a cybersecurity career. The discriminant function was significant (Λ = .95, χ^2 = 14.81, p = .02), suggesting that there was a significant difference in interests between the two groups. Univariate ANOVAs showed that "yes" responders scored significantly higher in the investigative scale (M_1 = 3.38, M_2 = 3.06; F = 4.49, p = .04). Through examining the correlations between the variates and the discriminant score, high scores on the discriminant function are mainly associated with participants reporting high investigative interests. The discriminant function was better at predicting the correct response from participants than random assignment and matching (82.9% hit rate vs. 50-71% hit rate).

		1	2	3	4	5	6	7	8	9	10	11
1.	Self Efficacy											
2.	BFI Extraversion	**.23**										
3.	BFI Agreeable-ness	.03	**.17**									
4.	BFI Conscientious	**.26**	**.22**	**.35**								
5.	BFI Neuroticism	**-.21**	**-.35**	**-.37**	**-.39**							
6.	BFI Openness	**.33**	**.27**	**.19**	**.23**	**-.16**						
7.	Realistic	-.01	-.03	-.03	.01	.09	**-.12**					
8.	Investigative	**.12**	.06	.02	-.02	.01	**.26**	**.26**				
9.	Artistic	.05	**.15**	-.01	-.07	.09	**.26**	**.39**	**.42**			
10.	Social	.06	**.17**	.13	.08	.05	.07	**.41**	**.31**	**.56**		
11.	Enterprising	-.04	**.11**	-.07	-.05	.07	.05	**.48**	**.30**	**.61**	**.57**	
12.	Conventional	-.07	-.05	-.05	.03	.17	-.10	**.57**	**.21**	**.28**	**.40**	**.43**

Table 2. **Intecorrelations between personality and interest variables. Significant correlations in bold. $p <$.**

The relationship between interest scores and other variables assessed in the survey generally agreed with established studies conducted in the past. The inter-relationships among select variables can be found in Table 1. Two meta-analyses summarizing the bulk of studies comparing interests and personality showed moderate to large correlations between Artistic scores and the Openness trait (r = .41-.48), Investigative interests and Openness scores (r = .21-.25) and Enterprising intersts and Extraversion (r = .40-.41; Larsen, Rottinghause & Borgen, 2002; Mount et al., 2005). In support of past findings, we obtained signfificant Investigative x Opennes and Artistic x Openness correlations (r = .26 for both), as well as smaller albeit significant relationships between Enterprising and Extraversion (r = .11). There were only several observed intercorrelations that contradicted meta-analytic findings. We expected larger relationships between Social interests and Openness scores and Conventional interests and Conscientiousness scores, but failed to find significance. Meta-analyses showed that they were correlated .19 and .22 respectively.

The relationship between interests and self-efficacy was only significant for Investigative interests (r = .12). The self-efficacy questions in our survey pertained only to the job activities related to cybersecurity, thus finding a correlation between investigative interests and self-efficacy reinforces the importance of investigative interest scores in predicting membership in the cybersecurity field. Future studies could evaluate if the relationship between investigative interests and the decision to work in cybersecurity is driven by greater feelings of self-efficacy.

4.3 Personality Characteristics

The sample of cybersecurity competition participants showed a distinct profile on the Big 5 personality dimensions (Goldberg, 1990). Participants on average scored significantly higher on the dimensions of Openness (M = 3.67, SD = .55) and Agreeableness (M = 3.60, SD = .60), while scoring lowest on Neuroticism (M = 2.62, SD = .70). See Figure 2. This profile suggests that participants in cybersecurity tend to have openness and agreeableness as their dominant traits. One caveat for this generalization is that survey-takers were all participants of a group-based cybersecurity competition, which could introduce the alternative explanation that high agreeableness and openness is due to self-selection into group-based activities, rather than self-selection into cybersecurity. More research on this distinction would better distinguish the personality characteristics of cybersecurity personnel.

The inter-correlations between personality scores and other variables (see Table 3) agreed with past literature

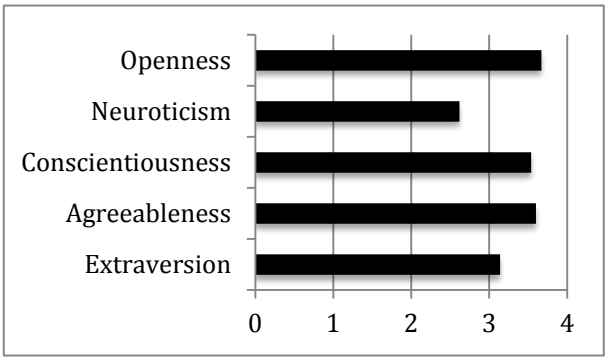

Figure 2. Average Big 5 personality scores for the entire sample (n=460)

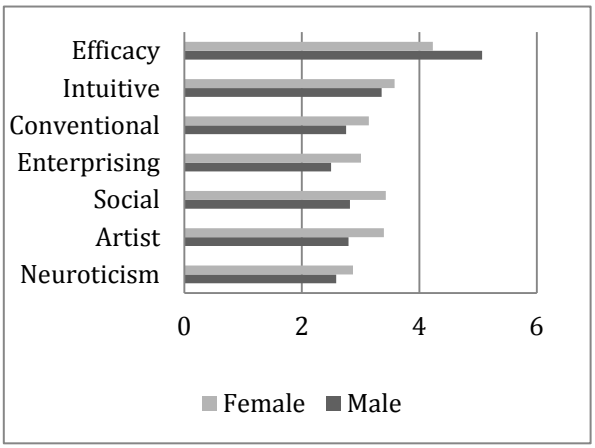

Figure 3. Significant differences between male and female participants (n=492).

on the same bivariate relationships. For example, Big 5 personality traits have been studied exhaustively in the context of attachment theory. With our short measure of attachment included in the survey, we observed significant correlations of -.34 between Attachment Avoidance and Extraversion, -.27 between Agreeableness and Avoidance, .39 between Neuroticism and Attachment Anxiety, and -0.18 between conscientiousness and attachment anxiety. Our results paralleled primary studies on attachment and the Big 5, which reported correlations of up to .42 between Anxiety and Neuroticism, and correlations of about -.22 between Avoidance and Extraversion as well as Agreeableness (Noftle & Shaver, 2006).

Our survey instrument included an individualism-collectivism measure by Triandis (2001). Collectivism scores generally showed larger and significant correlations with personality and interest scores compared to the individualism subscale. In particular, horizontal collectivism showed correlations of .47 with agreeableness and .25 with conscientiousness. These findings are face valid and reflective of collectivist values of group harmony and cooperation. Conversely, the largest correlation between individualism and personality was for Vertical Individualism and Openness (r = .35). For Self-efficacy, we observed small to moderate significant relationships with extraversion, conscientiousness, neuroticism, and openness. This is similar to past meta-analyses on self-efficacy motivation and the big-five personality traits (Judge & Ilies, 2002).

4.4 Observed Gender Differences

The gender gap in the cybersecurity profession, like other STEM fields, has long been perceived as an issue for recruiting a diverse, well-trained workforce. Even in a competition that prepares for future career in cybersecurity, we observe a huge difference in male and female participants. Of our 492 respondents, just 67 indicated that they were female, resulting in 7.3:1 ratio of male to female participants. Understanding the reasons for this significant disparity is important for determining why women are not attending cybersecurity competitions and not entering the cybersecurity profession. Since we are conducting an exploratory study on the gender, we are not comparing the performance difference between two genders, which may be a future research interest. We are more interested in how gender differences relate to the participants' psychological and culture characteristics and their career interests. The main tool we use here is T-test to compare the mean score of two genders. Before conducting T-tests on 25 different scores, we remove the samples having too many missing variables, which leaves 318 male samples and 49 female samples. Among these twenty-five scores, which comes from different measures, only seven of them are statistically significant different: Neuroticism from the Big Five; Artist, Social, Enterprising, and Conventional from RIASEC; Intuitive from Decision Making; and the efficacy measure. Figure 3 explicitly shows the differences between male group and female group over these seven scores.

Among these seven significant different scores, the means of female samples are generally higher than the means of male samples, except for the efficacy measure. Female participants have higher mean value than male participants on Neuroticism, which indicates that it is easier for the female respondents to experience negative emotions. In the RIASEC measurements, female participants have significantly higher mean values on Artist, Social, Enterprising, and Conventional attributes than male participants. Moreover, female participants have higher scores on intuitive decision-making, indicating that they are more likely to rely on hunches and feelings. Lastly, the only variable that male participants are significantly higher than female participants is self-reported efficacy regarding working in the cybersecurity/information assurance field. It should be noted that this sample is drawing from all participants in the cybersecurity competition, not necessarily those who are determined to go into cybersecurity field or already worked in related area.

Overall, there are not many differences between female and male among the population of competition participants regarding the measures we applied, and the differences we did find lead to ambivalent conclusions. Female participants have higher social scores, potentially allowing them the opportunity to communicate more effectively to work successfully in teams. However, high scores on Neuroticism and Intuitive Decision may make the female participants more prone to more easily experiencing negative emotions. A tendency to make intuitive decisions may not be valued in an environment that emphasizes more logical approaches. However, due to the constraints of our data, we have not been able to

		1	2	3	4	5	6	7	8	9	10
1.	BFI Extraversion										
2.	BFI Agreeableness	**.17**									
3.	BFI Conscientious	**.22**	**.35**								
4.	BFI Neuroticism	**-.35**	**-.37**	**-.39**							
5.	BFI Openness	**.27**	**.19**	**.23**	**-.16**						
6.	Atch. Avoidance	**-.34**	**-.27**	**-.16**	.09	**-.11**					
7.	Atch. Anxiety	**-.10**	-.06	**-.18**	**.39**	-.04	**-.08**				
8.	V. Individualism	**.12**	**.11**	.08	.03	**.35**	**-.12**	**.13**			
9.	H. Individualism	.01	-.02	**.16**	.01	**.40**	**.15**	.07	**.42**		
10.	V. Collectivism	**.18**	**.32**	**.21**	-.07	**-.15**	**-.21**	.01	**.25**	**.17**	
11.	H. Collectivism	**.33**	**.47**	**.25**	**-.15**	**.41**	**-.40**	.03	**.39**	**.19**	**.44**

***Table 3*. Intercorrelations between select variables and personality. Bold font indicates significance, $p < .0$.**

assess differences between women who intend to enter the cybersecurity field and those who actually work in the field. More work should be done to understand the characteristics of the women who do successfully enter the cybersecurity profession.

5. Conclusion & Future Work

The survey results presented in this paper begin to provide the empirical data needed to assess whether competitions are an effective way to encourage students to pursue careers in cybersecurity. The data presented here helps to develop a profile of current and former students who have competed and their characteristics. We are only beginning to understand the data, however, and much work needs to be done to understand whether competitions are effective recruiting tools in this field. There are perhaps other relevant psychological or sociological factors that are relevant. A longitudinal study of competitors from the beginning of their cybersecurity education into their careers would be useful to more fully understand the role competitions play in career choices.

Several other psychological measures were included in the survey, though we have not yet analyzed this data. Participants were asked questions about their perceptions of entitlement, which measures narcissistic personality traits (Campbell et al., 2004). Also collected was data about decision-making styles, using Scott & Bruce's (1995) General Decision Making Style (GDMS) measure. The GDMS assesses how individuals approach "decision situations" and distinguishes between five decision styles: (1) rational, (2) avoidant, (3) dependent, (4) intuitive, and (5) spontaneous. A third measure used in the survey but not reported on in this paper is a measure of self-control (Grasmick et al., 1993). This measure is based upon the idea that those with low self-control are less capable of foreseeing the long-range consequences of their actions. The data form these three measures will be analyzed and explored in future papers and will provide even more empirical data for understanding cybersecurity competition participants. We are beginning to fill in the empirical lacuna in this area, but much work remains to be done.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. 1342090. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

Campbell, W.K., Bonacci, A.M., Shelton, J., Exline, J.J. & Bushman, B.J. (2004). Psychological entitlement: Interpersonal consequences and validation of a self-report measure. *Journal of Personality Assessment, 83*(1), 29-45.

Capalbo, N., Reed, T. & Arpaia, M., (2011). RTFn: Enabling Cybersecurity Education through a Mobile Capture the Flag Client. *Proc. SAM, 11*, 500-506.

Cheung, R., Cohen, J., Lo, H., Elia, F. & Carillo-Marquez, V. (2012, July). Effectiveness of Cybersecurity Competitions. *Proc. Int'l Conference on Security & Management*.

Cheung, R.S., Cohen, J.P., Lo, H.Z. & Elia, F. (2011). Challenge Based Learning in Cybersecurity Education. *Prof. of the 2011 Int'l Conference on Security & Management, 1*.

Conklin, A. (2005). The Use of a Collegiate Cyber Defense Competition in Information Security Education. *Proc. of the 2nd Annual Conference on In-*

formation Security Curriculum Development. ACM,16-18.

Fraley, R.C., Waller, N.G. & Brennan, K.A. (2000). An iten-response theory analysis of self-report measures of adult attachment. *Journal of Personality and Social Pyschology, 78*, 350-365.

Goldberg, L. R. (1990). An alternative "description of personality": the big-five factor structure. *Journal of personality and social psychology*, *59*(6), 1216.

Grasmick, H.G., Tittle, C.R., Bursik, R.J. & Arneklev, B.J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *Journal of Research in Crime and Delinquency, 30*, 5-29.

Judge, T. A., & Ilies, R. (2002). Relationship of personality to performance motivation: A meta-analytic review. *Journal of Applied Psychology, 87*(4), 797-807. doi:http://dx.doi.org/10.1037/0021-9010.87.4.797

Larson, L. M., Rottinghaus, P. J., & Borgen, F. H. (2002). Meta-analyses of big six interests and big five personality factors. *Journal of Vocational Behavior, 61*(2), 217-239. doi:http://dx.doi.org/10.1006/jvbe.2001.1854

Mount, M. K., Barrick, M. R., Scullen, S. M., & Rounds, J. (2005). Higher-order dimensions of the big five personality traits and the big six vocational interest types. *Personnel Psychology, 58*(2), 447-478. doi:http://dx.doi.org/10.1111/j.1744-6570.2005.00468.x

NICCS Cyber Competitions, available at niccs.us-cert.gov/education/cyber-competitions.

Noftle, E. E., & Shaver, P. R. (2006). Attachment dimensions and the big five personality traits: Associations and comparative ability to predict relationship quality. *Journal of Research in Personality, 40*(2), 179-208.

Patriciu, V.V. & Fortuna, A.C. (2009). Guide for Designing Cyber Security Exercises. *Proc. of the 8th WSEAS Int'l Conference on E-Activities and Information Security and Privacy*, 172-177.

Rottinghaus, P. J., Larson, L. M., & Borgen, F. H. (2003). The relation of self-efficacy and interests: A meta-analysis of 60 samples. *Journal of Vocational Behavior, 62*(2), 221-236. doi:http://dx.doi.org/10.1016/S0001-8791(02)00039-8

Scott, S.G. & Bruce, R.A. (1995). Decision-making style: The development and assessment of a new measure. *Educational and Psychological Measurement, 55*(5), 818*831. Doi: 10.1177/0013164495055005017.

Tobey, D.H., Pusey, P. & Burley, D.L. (2014). Engaging Learning on Cybersecurity Careers: Lessons from the Launch of the National Cyber League. *ACM Inroads, 5*(1), 53-56.

Triandis, H. C. (2001). Individualism-collectivism and personality. *Journal of Personality, 69*, 907–924.

Turner, G.E., Deemer, E.D., Tims, H.E., Corbett, K., and Mhire, J. (2014). Cyber value and interest development: Assessment of a STEM career intervention for high school students. *Electronic Journal of Science Education*, 18:1. Available at http://ejse.southwestern.edu/article/view/11946/0

Werther, J., Zhivich, M., Leeks, T. & Zeldovich, N. (2011). Experiences in Cyber Security Education: The MIT Lincoln Laboratory Capture-the-Flag Exercise. *Proc. of the 4th Conference on Cyber Security Experimentation and Test (CSET)*, USENIX, 12.