Understanding the Personality Characteristics of Cybersecurity Competition Participants to Improve the Effectiveness of Competitions as Recruitment Tools

Colin Wee and Masooda Bashir

Abstract This paper reports on the results of a survey designed to study the psychological characteristics of a sample of cybersecurity competition participants from Cybersecurity Awareness Week (one of the largest cybersecurity competitions in the USA). By comparing the personality, vocational interests, culture, decision-making style and attachment style between participants who reported their intention to enter cybersecurity careers post-competition and those who did not, we evaluated the effectiveness of cybersecurity competitions as a recruitment tool. Overall, most cybersecurity competition participants tended to be high in openness, rational decision-making style, and investigative interests. Conversely, participants scored lower on neuroticism, intuitive decision-making style, and realistic interests. Individuals' scores on investigative interests, openness to experience, rational decision-making, and self-efficacy were good predictors of their intention to enter cybersecurity careers post-competition. To increase the influx of people into cybersecurity careers, cybersecurity competitions can be designed to attract more people with these characteristics.

Keywords Cybersecurity · Cybersecurity competitions · Career choice · Human factors

C. Wee (✉) · M. Bashir
Graduate School of Library and Information Science, University of Illinois at Urbana-Champaign, 501 E. Daniel St., Champaign, IL 61820, USA
e-mail: jwee2@illinois.edu

M. Bashir
e-mail: mnb@illinois.edu

D. Nicholson (ed.), *Advances in Human Factors in Cybersecurity*,
Advances in Intelligent Systems and Computing 501,
DOI 10.1007/978-3-319-41932-9_10

1 Introduction

To address the shortage of skilled cybersecurity professionals in the workforce, the United States government has directed funding to the sponsorship of cybersecurity competitions—high-school and collegiate contests of skills such as hacking and reverse engineering, designed to raise awareness about cybersecurity threats and foster interest in cybersecurity careers. Thus far, no known studies have attempted to validate the effectiveness of competitions as a recruitment tool. Beyond looking at the percentage of competition participants who enter cybersecurity careers in the future, we know little about the nature and types of people that are attracted to these competitions and require evidence that competitions are effective at funneling like-minded people into cybersecurity careers. We thus aimed to evaluate cybersecurity competition participants through a psychological lens to discover if there are certain people with particular personality traits that make them more receptive to the competition recruitment strategy.

Cybersecurity competitions offer many benefits and opportunities to the parties involved. Schools host cybersecurity competitions because they can teach network security practices through live exercises and evaluate their own computer security curricula [1]. Technology and security companies often hold career fairs and professional networking sessions during these competitions to attract future talent [2]. Participants of cybersecurity competitions get to learn about cybersecurity careers and practice dealing with contemporary security threats. The U.S. Department of Homeland Security's National Initiative for Cybersecurity Careers and Studies states that, "cyber competitions foster talent in potential cybersecurity professionals that might otherwise be unidentifiable through traditional academic means" [3]. DefCon, the world's largest hacker convention, also holds its own cybersecurity competitions for hackers to pit their skills against each other. With the current shortage of skilled cybersecurity professionals in the workforce [4], the US Department of Homeland Security and the National Security Agency often sponsor major competitions such as National Collegiate Cyber Defense Competition (NCCDC) and New York University's Cybersecurity Awareness Week (CSAW). The government continues to search for ways to increase the influx of talent into the field of cybersecurity.

There is at present a dearth of psychological studies on cybersecurity competitions and participants of these competitions. The closest primary studies have been conducted in samples of IT professionals, software engineers, and hackers. IT professionals were found to possess high openness to experience and show interest in problem-solving and practical issues. Conversely, non-IT professionals were more social and enterprising [5]. Software engineers were characterized by high levels of introversion and rationality [6]. Hackers, defined as people who infiltrate and compromise the security of computer networks [7], have been found to have

lower levels of self-control and moral-decision-making [8]. While we expect the personality traits of competition participants to be similar to others in the IT field, relating these traits to recruitment outcomes in competitions is a step forward to improving competitions, and will supplement the growing body of research on how to best design competitions to mimic real-world cybersecurity challenges [9].

2 Current Study

Researchers in this study were given the unique opportunity to study cybersecurity competition participants from one of the largest and most well-established competitions in the world to investigate if there are ways to improve these competitions effectiveness at recruiting people into careers in cybersecurity. Funded by a grant from the National Science Foundation, this is the first study to attempt to develop psychological profiles for the target population of cybersecurity competition participants. By understanding which individual differences among cybersecurity competition participants are correlated with their decision-making and entrance into cybersecurity careers, future cybersecurity competitions can leverage these characteristics to increase recruitment rates.

For this study, researchers sent an online survey to a mailing list of all previous participants of Cybersecurity Awareness Week (CSAW). CSAW is an annual on-site competition organized by New York University's Tandon School of Engineering, and has run regularly for more than 11 years. Many different competitions are held during Cybersecurity Awareness Week, ranging from hacking embedded systems to essay-writing competitions. For the purposes of this study, we focused only on participants from CSAW's capture the flag (CTF) contest, because capture the flag is one of the most common types of activities held across competitions, thereby increasing the generalizability of our results. Capture the flag is a team-based activity where contestants race each other through digital mazes to find a unique identifier called a flag. These flags may manifest as a secret password, random string, or unique image [2].

We approached this study with two research questions. Due to the pioneering nature of psychological research in cybersecurity competition participants, we adopted an exploratory approach and assessed participants on a broad range of psychological measures, including measures of personality, adult attachment styles, decision-making styles, and vocational interests. We aimed to study the following:

1. To establish a psychological profile of cybersecurity competition participants.
2. To evaluate competition effectiveness by identifying specific traits that influenced whether or not participants intend to enter cybersecurity careers post-competition.

3 Method

3.1 Participants

588 Participants from the first decade of the Cybersecurity Awareness Week (CSAW) Conference capture the flag competition responded to an online survey about the characteristics of cybersecurity competition participants. The capture the flag competition is open to participants across the world, and the basic premise of the tasks involved in capture-the-flag has not changed over time. An incentive of a $10 Amazon gift card was offered to each participant who completed at least 70 % of the survey. 11.9 % (n = 67) of respondents identified as female. 48.4 % (n = 272) of the overall group identified as white and 32.0 % (n = 180) as Asian. 2.5 % (n = 14) were African-American, 6.4 % (n = 36) were Hispanic/Latin American, and 0.2 % (n = 1) identified as Native American. At the time of the survey, 50.38 % (n = 199) of the sample were undergraduates, 29.4 % (n = 116) were high school students, with the rest having completed graduate and other professional degrees. The mean age of the respondents was 24.26 years old. 37.4 % (n = 161) of the participants were employed full-time, 25.1 % (n = 108) were employed part-time and the remaining 162 were unemployed or still in school. Among the employed workers, 44.5 % (n = 126) were working in a cybersecurity or information-assurance occupation.

3.2 Measures

The survey comprised measures of personality, interest, decision-making style, attachment style, culture, and self-efficacy. The survey also asked about the competition experience, opinions about hacking, and intentions of pursuing a career in cybersecurity. The survey also included 2 quality control items which requested individuals to select specific response options to ensure that they were paying attention.

Personality. Respondents were asked to complete a 44-item Big Five Personality Inventory to assess personality according to the Big Five dimensions of Openness to experience, Conscientiousness, Extraversion, Agreeableness, and Neuroticism [10]. Openness to experience reflects an individual's degree of intellectual curiosity, creativity, and preference for variety of experience. Conscientiousness refers to how organized and dependable the individual is. Extraversion is a measure of how outgoing or reserved an individual is. Agreeableness refers to an individual's tendency to be either friendly and compassionate or analytical and detached. Neuroticism refers to an individual's tendency to experience unpleasant emotions, such as anger, anxiety, or vulnerability, easily. The alpha reliabilities for the five scales ranged from 0.73 to 0.79.

Interests. Respondents were requested to complete a short 30-item version of the O*Net Interest Profiler [11]. This measure used John Holland's RIASEC interest classification to assign vocational personality types. This model assumes six vocational personality types and work environments—Realistic, Investigative, Artistic, Social, Enterprising, and Conventional [12]. Realistic types show preference for activities that include the explicit, ordered, or systematic manipulation of tools and machines. Investigative types like activities that involve systematic observation and creative investigation. Artistic types prefer the creation of art and products. Social types like helping and interacting with others. Enterprising types enjoy positions of power and the pursuit of economic gain. Conventional types prefer activities that involve the systematic manipulation of data. The six scales had alpha reliabilities ranging from 0.79 to 0.84.

Culture. Another measure included in the survey was a 16-item measure of Individualism–Collectivism [13], 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. Those who score highly on vertical collectivism (VC) see themselves as a part of broader group and are willing to accept hierarchy and inequality within that group. In contrast, those who score highly on horizontal collectivism (HC) also see themselves as part of a larger group, but they perceive all members of the group as being equal. Those who score highly on individualism perceive themselves as autonomous beings, not part of a group. Vertical individualism (VI) assesses the extent to which individuals strive to be distinct and desire special status, while horizontal individualism (HI) denies that individuals should seek special status as they strive to be individual. The scales had alpha reliabilities of (VI: 0.55 HI: 74, VC: 0.68 HC: 0.66.).

Decision-Making Style. To assess decision-making style, respondents were also given the General Decision Making Style Scale [14]. An individual's decision-making style is not a personality trait, but rather a habit-based propensity to react in particular ways in a decision context. The rational decision-making style is characterized by thoroughness and a logical evaluation of alternatives. Dependent decision makers search for the advice and direction of others, whereas avoidant decision makers shun decision making responsibility. The spontaneous decision-making style is characterized by a sense of immediacy and a desire to get through the decision-making process as quickly as possible. The decision-making style scales have alpha reliabilities ranging from 0.73 to 0.89.

Attachment Style. Also included were 9 attachment-related questions adapted from the Experiences in Close Relationships Scale (ECR-RS) [15]. ECR-RS can be dichotomized into avoidant attachment and anxious attachment subscales. Individuals who score highly on both avoidance and anxiety are fearful and avoidant of relationships, which those who score low on both are secure in their relationships. Low avoidance, high anxiety individuals are preoccupied with their relationships, while high avoidance, low anxiety individuals are dismissive of relationships and tend to avoid them. Avoidant attachment was assessed with 6

items with a scale reliability of α = 0.76. Anxious attachment was assessed with 3 items with an alpha of 0.89.

Self-Efficacy. Respondents were also asked two questions to assess their perception of their own self-efficacy towards cybersecurity tasks. The items were "In general, how confident are you about your ability to work in cybersecurity/information assurance field?" and "In general, how comfortable are you with your level of knowledge to work in cybersecurity/information assurance field?" If an individual's self-efficacy is much lower than their ability, they may fail to challenge themselves and set goals that are too low. Conversely, if an individual's abilities are much lower than their self-efficacy, they may set impossible goals and possibly quit when they fail to meet those goals. The self-efficacy scale had a reliability of 0.91.

Career. Finally, to determine the influence of competitions on participants, we asked the following questions: "Do you plan on pursuing a career in the cybersecurity/information assurance field?", and "Did participating in the competition cause you to change any plans for your future career or academic path". Individuals who answered "Yes" to both questions were sorted into a 'success' group where competitions successfully influenced participants' intention into a cybersecurity career.

4 Results

Preliminary analyses were first conducted in the entire competition sample (N = 588). 95.5 % of participants had competed in at least one cybersecurity competition within the past two years. 52 % reported that the main motivation for participating in competitions was for fun and enjoyment, while 27 % joined in order to learn new skills. The sex distribution in the sample was heavily skewed towards men (M = 521 vs. F = 67) but this sex disparity is reflective of many cybersecurity samples [16]. Women generally scored higher than males in all measures except self-reported efficacy in cybersecurity tasks.

4.1 Aim 1: To Establish a Psychological Profile of Cybersecurity Competition Participants

Few researchers have studied cybersecurity participants on a wide array of individual difference variables. This study contributes to the field by identifying what traits participants score highest in so that competitions can be designed to optimize their appeal to people with these kinds of traits. Means and standard deviations between variables for the entire sample are reported in Appendix A. Table 1 gives a brief summary of the personality, interest, and decision-making profile for the entire sample (n = 588) of cybersecurity competition participants.

Table 1 Mean scores for personality, interests, decision-making, and attachment styles and other measured variables

Personality	Mean (SD)	Interests	Mean (SD)
Openness	3.67 (0.55)	Investigative	3.33 (0.94)
Agreeableness	3.61 (0.60)	Social	2.90 (0.94)
Conscientiousness	3.54 (0.64)	Artistic	2.87 (0.96)
Extraversion	3.14 (0.70)	Conventional	2.80 (0.87)
Neuroticism	2.62 (0.70)	Enterprising	2.56 (0.92)
		Realistic	2.53 (0.90)
Decision-making	Mean (SD)	Other	Mean (SD)
Rational	3.95 (0.70)	Avoidant attachment	3.76 (1.11)
Intuitive	3.38 (0.69)	Anxious attachment	3.81 (1.68)
Dependent	3.38 (0.75)	Individualism	3.65 (0.73)
Avoidant	2.72 (0.94)	Collectivism	3.65 (0.77)
Intuitive	2.70 (0.69)	Self-efficacy	4.96 (1.55)

Overall, cybersecurity participants have the highest scores in openness, investigative interests, and rational decision-making style. This is in agreement with findings on IT professionals in general [5]. Within the sample of cybersecurity competition participants, there were 126 individuals holding jobs in information assurance at the time of survey completion. These individuals were compared on all the measured individual difference dimensions with other individuals who reported that competitions had convinced them to consider cybersecurity careers. The comparison group comprised 241 individuals who were not employed in cybersecurity. Results of this comparison showed that cybersecurity employees and those interested in cybersecurity were highly similar, with current cybersecurity employees only showing higher trait-scores on investigative interests (3.60 vs. 3.25, $t(243) = 2.80$, $p < 0.01$), while scoring lower on agreeableness (3.55 vs. 3.71, $t(303) = -2.18$, $p = 0.03$) and perceived self-efficacy at cybersecurity tasks (5.24 vs. 5.89, $t(361) = 4.83$, $p < 0.01$). This finding suggests that within competition participants, those highest in investigative interests and confidence in their own cybersecurity skills have a higher probability to end up in cybersecurity careers post-competition.

4.2 Aim 2: To Evaluate Competition Effectiveness by Identifying Specific Traits that Influenced Whether or Not Participants Intend to Enter Cybersecurity Careers Post-competition

Competition effectiveness can be operationalized as the percentage of the total number of participants who reported that the competition persuaded them to enter

the field of cybersecurity. 61 % of the participants surveyed reported that they were more persuaded to enter a career in cybersecurity after the competition. About a third of these participants were already within cybersecurity jobs at the time of the survey, suggesting that they managed to find a cybersecurity job in the time between them participating in cybersecurity competitions as a student and the date of the survey.

To identify the important individual difference variables for predicting entrance into cybersecurity careers, we correlated each participant's scores with whether competitions were 'successful' in influencing their career decision to enter the field of cybersecurity (See Table 2). Participants' self-efficacy had the greatest predictive correlation with the competition's influence on the participant ($r = 0.504$, $p < 0.01$). Participants with higher self-efficacy in cybersecurity tasks would more likely admit that the competition made them want to pursue a career in cybersecurity. This finding is in accordance to Robert Lent's Social Cognitive Careers theory [17], which states that self-efficacy in specific domains (in this case, cybersecurity), directs participants to select activities and careers that reinforce their beliefs. Competition designers can capitalize on this strong relationship between self-efficacy and competition influence if they wish to increase future recruitment into cybersecurity careers. One way to do this could be to increase the positive reinforcement, encouragement, or reward whenever participants accomplish tasks during different stages of the competition. Participants will consequentially feel like their actions are leading to significant progress, thereby boosting their confidence in cybersecurity tasks.

Correlations between other personality measures and CSAW's 'success' at increasing participants' intent to enter cybersecurity careers showed that apart from self-efficacy, rational decision-making, openness to experience, and horizontal collectivism, conscientiousness, and investigative interests were all significantly related to increased intent to enter cybersecurity careers. Some, but not all of these individual differences might be useful for competition designers and career counselors to identify if an individual might want to consider cybersecurity careers. For example, competitions can be designed with more logic-based, problem solving tasks to appeal to the rational decision-makers with investigative interests, since this demographic tends to show increased intent to join cybersecurity careers after such competitions. Participants who were more open to new experiences and more

Table 2 Significant correlations of individual difference scores and success of competitions at recruiting participants, $p < 0.05$

Measured variable	*R*
Self-efficacy	0.50
Rational decision-making	0.33
Openness to experience	0.24
Horizontal collectivism	0.24
Conscientiousness	0.22
Avoidant attachment	−0.18
Investigative interests	0.15

conscientious also tended to show greater intent to enter cybersecurity careers post-competition. With knowledge about this target demographic, recruiters can optimize advertisements and marketing during the career fairs that are commonly coupled with cybersecurity competitions.

Although they showed significant correlations, some of the other measures might not be practical for competitions to ask from their participants in normal contest scenarios. While questions about interests and personality are commonly asked in many normal situations (e.g., recruitment, networking), asking participants about their avoidant attachment styles and their culture might be too intrusive for the tiny amount of predictive power they provide.

5 Discussion

The current study investigated two different research questions using a large sample of cybersecurity competition participants. We present a novel, comprehensive psychological profile of cybersecurity participants, showing that they tend to be high in openness to experience, investigative interests, and rational decision-making styles. Individual high in perceived self-efficacy in cybersecurity tasks, rational-decision making style, openness to experience, and investigative interests were also more likely to enter cybersecurity careers post-competition. By designing cybersecurity competitions that attract and cater to these demographics of people, we believe competitions can become a more enjoyable experience for these individuals, and this experience might influence their future career decision-making. These findings may potentially facilitate the development of better competitions that serve to generate more high-quality cybersecurity employees to address the current manpower shortage in the field.

There are several limitations to this study. Since our sample was limited to participants from Cybersecurity Awareness Week, we require further evidence to show that other cybersecurity competitions attract similar types of people for our findings to be generalizable. Replications of this study should be conducted in samples from other cybersecurity competitions such as the National Collegiate Cyber Defense Competition and DefCon. Another limitation of this exploratory study was its reliance on retrospective self-report data for participants of different years of capture-the-flag competitions within the past decade. Although we focused on only capture the flag participants to maximize the similarity of tasks performed by participants, the nature of the competition would not be identical each year. Participants from some years might have faced particularly challenging problems that left an intimidating negative impression about cybersecurity careers while others might have had a particularly extravagant career fair that left a positive impression. Participants from the past years also may not remember clearly, what the competition was like. One redeeming factor for this study's retrospective design is that most of the measures used in this study, such as vocational interests and personality, are known to be highly stable across time [18, 19].

Future studies should measure psychological profiles of cybersecurity employees from different organizations, and compare between those who were recruited from competitions and those who were recruited through other means. This would shed light on possible differences between competition participants and other types of cybersecurity employees. Time-series data collected throughout the different stages of the competition would provide a stronger argument for the effectiveness of competitions in influencing career choice, and allow organizers to pinpoint the specific events in the competition that left a positive influence on participant decision-making. Future research can also measure other competition-related variables such as performance and team size to see if they have any moderating influence on the relationship between personality characteristics and career intent. Interviewing competition participants can also be an alternative method to garner more information on how to improve competitions as a recruitment tool.

6 Conclusion

From this study, we paint a psychological profile of cybersecurity competition participants so that organizers can know the type and mindset of people that they are attracting to participate. Participants with higher openness to experience, confidence in cybersecurity skills and interest in logic-based activities are more likely to pursue cybersecurity careers post-competition. This is the first step in research on cybersecurity competitions, and further replication in other competition samples outside of Cybersecurity Awareness Week is encouraged. With enough knowledge about the participants that are receptive to the cybersecurity competition recruitment strategy, competition and career-fair organizers can increase the appeal and positive impression left on the participants, such that more of them choose cybersecurity careers in the future.

References

1. Vigna, G., Borgolte, K., Corbetta, J., Doupe, A., Fratantonio, Y., Invernizzi, L., Kirat, D., Shoshitaishvili, Y.: 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 (2014)
2. Gavas, E., Memon, N., Britton, D.: Winning cybersecurity one challege at a time. IEEE Secur. Priv. **10**, 75–79 (2012)
3. National Initiative for Cybersecurity Careers and Studies. https://niccs.us-cert.gov/training/tc/search/cmp/new
4. Information Systems and Audit Control Association. http://www.isaca.org/pages/cybersecurity-global-status-report.aspx
5. Ash, R.A., Rosenbloom, J.L., Coder, L., Dupont, B.: Personality Characteristics of Established IT Professionals, Encyclopedia of Gender and Information Technology, pp. 983–989. Idea Group Publishing, Philadelphia (2006)

6. Cruz, S., DaSilva, F.Q., Capretz, L.F.: Forty years of research on personality in software engineering: a mapping study. Comput. Hum. Behav. **46**, 94–113 (2015)
7. Coleman, G.E.: Coding Freedom: The Ethics and Aesthetics of Hacking. Princeton University Press, New Jersey (2012)
8. Bossler, A.M., Burruss, G.W.: The general theory of crime and computer hacking: low self-control hackers? In: Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications, pp. 38–67 (2011)
9. Cheung, R., Cohen, J., Lo, H., Elia, F., Veronica, C.M.: Effectiveness of cybersecurity competitions. In: Proceedings of the International Conference on Security & Management. Las Vegas, Nevada (2011)
10. Goldberg, L.R.: An alternative "description of personality": the big-five factors. J. Pers. Soc. Psychol. **59**, 1216–1230 (1990)
11. Lewis, P., Rivkin, D.: Development of the O*NET Interest Profiler. National Center for O*Net Development, Raleigh, North Carolina (1999)
12. Holland, J.L.: Making Vocational CHOICES: A Theory of Vocational Personalities and Work Environments. Psychological Assessment Resources, Odessa (1997)
13. Triandis, H.C.: Individualism-collectivism and personality. J. Pers. **69**, 907–924 (2001)
14. Scott, S.G., Bruce, R.A.: Decision-making style: the development and assessment of a new measure. Educ. Psychol. Measur. **55**, 818–831 (1995)
15. Fraley, R.C., Waller, N.G., Brennan, K.A.: An item-response theory analysis of self-report measures of adult attachment. J. Pers. Soc. Psychol. **78**, 350–365 (2000)
16. Tobey, D.H., Pusey, P., Burley, D.L.: Engaging learning on cybersecurity careers: lessons from the launch of the national cyber league. ACM Inroads **5**, 53–56 (2014)
17. Lent, R.W.: A social cognitive view of career development and counseling. Wiley, Hoboken (2005)
18. Low, K.S.D., Yoon, M., Roberts, B.W., Rounds, J.: The stability of interests from early adolescence to middle adulthood: a quantitative review of longitudinal studies. Psychol. Bull. **131**, 713–737 (2005)
19. Roberts, B.W., Walton, K.E., Viechtbauer, W.: Patterns of mean-level change in personality traits across the life course: a meta-analysis of longitudinal studies. Psychol. Bull. **132**, 1–25 (2006)