Profiling Cybersecurity Competition Participants: Self-Efficacy, Decision-Making and Interests

Predict Effectiveness of Competitions as a Recruitment Tool

Masooda Bashir, Colin Wee, Nasir Memon, Boyi Guo

University of Illinois at Urbana-Champaign

Author note

Masooda Bashir, School of Information Sciences, University of Illinois at Urbana-Champaign; BoyiGuo, Department of Statistics, University of Illinois at Urbana-Champaign; Colin Wee, Department of Psychology, University of Illinois at Urbana-Champaign. Nasir Memon, Computer Science and Engineering, New York University Tandon School of Engineering.

Correspondence concerning this article should be addressed to Dr. Masooda Bashir, School of Information Sciences, University of Illinois at Urbana-Champaign, 501 E. Daniel St., MC-493, Champaign, IL 61820. E-mail: mnb@illinois.edu. Phone: +1(217) 244-1139.

Word count: 8713

Abstract

This paper presents the main results of a large-scale survey on cybersecurity competition participants in the past decade. 588 participants of the Cybersecurity Awareness Week (CSAW) competition were surveyed with measures of personality, interests, culture, decision-making and attachment styles in an exploratory study designed to identify the characteristics of cybersecurity competition participants. Subgroups analyses were performed to examine individual differences between self-proclaimed hackers and non-hackers, males and females, and cybersecurity employees versus students. Regression analyses were used to identify variables that influenced the extent to which cybersecurity competitions were effective at convincing participants to pursue a future career in cybersecurity. Cybersecurity participants who displayed higher self-efficacy, rational decision-making style, and more investigative interests were more likely to declare an interest in a career in cybersecurity after the competition.

Abstract word count: 128

Keywords: Cybersecurity; Information Assurance; Human Factors; Career Choice; Recruitment; Cybersecurity Competitions.

1.Introduction

In the last decade, cybersecurity and information assurance has emerged as a top priority for both governments and industry. Cybersecurity breaches such as Sony Pictures Entertainment's data leak in late 2014 are worst-case scenarios for many organizations. A 2015 global survey indicated that 83% of organizations list cybersecurity attacks as a top three concern (ISACA, 2015). Furthermore, the United States government emphasized the importance of cybersecurity by passing four sweeping bills in 2014, including the Cybersecurity Workforce Assessment Act (Pub.L. 113-246), aimed at developing a plan for increasing the number of trained cybersecurity professionals in the workforce. Still, there is at present a shortage of skilled cybersecurity professionals available for hire (ISACA, 2015), thus current methods of increasing the influx of workers into cybersecurity careers need to be validated and improved upon to meet global demand.

A key method used by both government and industry to attract individuals into cybersecurity careers has been the sponsorship of cybersecurity competitions. The United States Air Force sponsors the CyberPatriot competition and education program to prepare high school and middle-school students for higher education in STEM fields and potential careers in cybersecurity. The Department of Homeland Security and the National Security Agency continue to sponsor major competitions such as the National Collegiate Cyber Defense Competition (NCCDC) and New York University's Cybersecurity Awareness Week (CSAW). These contests are coordinated by educational institutions around the United States and are typically targeted towards high school- and college-aged students. Competitions such as the University of Santa Barbara's International Capture the Flag competition challenge participants to develop innovative strategies to attack or defend computer systems, while both raising

awareness about the various hacker threats and teaching network security practices through live exercises (Vigna et al., 2014). Schools benefit from cybersecurity competitions because they can evaluate their own computer security curricula and foster teamwork and ethical behavior among their students. Conversely, industries benefit from cybersecurity competitions because they are places for professional networking with potential hires (Gavas, Memon & Britton, 2012). Competitions are thus a good method of fostering the next generation of cybersecurity specialists. Cybersecurity competitions are also sometimes held concurrent with hacker conventions. DefCon, the world's largest annual hacker convention, conducts its own capture the flag competition for hackers to test their skills against each other and push the limits of the field of cybersecurity. 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" (NICCS, 2015). While there has been remarkable work done by the cybersecurity education community to develop the "best" competitions, little empirical research has been done to explore the types of people that are attracted to these competitions and whether these competitions really are effective at funneling like-minded people into cybersecurity careers.

This paper aims to develop a psychological profile of participants from one of the longest-running cybersecurity competitions in the world, Cybersecurity Awareness Week (CSAW). CSAW is an annual on-site competition organized by New York University's Tandon School of Engineering. CSAW started 11 years ago as a capture the flag competition. 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 (Gavas, Memon & Britton, 2012). These flags may also be hidden within a host

network, where one attacking team develops exploits and attempt to retrieve it while the defending teams tried to protect it from being stolen. Since its inception, CSAW has since then grown from a small student-run initiative to a prestigious international competition which annually recruits over 10,000 participants from around the world. Over time, CSAW has diversified the types of competitions it offers; now participants ranging from high school students to graduate researchers compete on tasks including a capture-the-flag challenge, a high school forensics challenge, an embedded systems challenge, an AT&T applied security essay competition, a video competition and a department of homeland security quiz tournament. Since many of these competitions target separate audiences, the current paper only develops a psychological profile for capture the flag participants from CSAW as it is the largest and most established population to sample from. The profile we develop can also be compared to workers currently employed in the field of cybersecurity to understand if competitions are attracting people who are similar, or different to the characteristics of the current workforce. Although using only participants from CSAW limits the generalizability of our inferences to other competitions and is subject to range restriction, CSAW is the largest and most established on-site cybersecurity competition and there is a need pioneering preliminary research into the understudied field of cybersecurity competitions. By focusing on the unique characteristics of cybersecurity competition participants and learning about their interests and motivations, we can not only design the best competitions but also effectively attract the most talented students into cybersecurity careers.

As a secondary objective, we also compare and contrast the psychological profiles of subgroups within the competitors, addressing questions such as “Are self-proclaimed hackers different from non-hackers in any individual difference characteristic?” Understanding these

competitors, especially the differences between those who go on to pursue jobs in the cybersecurity field and those who do not, is key to assessing the utility of cybersecurity competitions in attracting like-minded people into cybersecurity careers.

2. Theory and Past Research

2.1 Profiling Cybersecurity Participants

Improving cybersecurity competitions is an important part of solving the workforce deficiency in the field of information assurance. Our research marks an exploratory step into identifying the types of people competitions are attracting and whether or not they are motivated after the competition to enter careers in cybersecurity. We accomplish this by using participants from one of the most established cybersecurity competitions to infer the overall disposition of cybersecurity competition participants in general.

Previous researchers have noted that participants attend competitions for a variety of reasons other than just learning new cybersecurity skills, including because (1) they have the opportunity to apply the skills they have to new challenges, (2) they work in teams to develop socialization skills, and (3) they network with fellow cybersecurity students and with potential employers (Gavas&Memon, 2012). It is imperative that we study more about who these cybersecurity competitors are and what interests they have – and, ultimately, learn how to best direct interested people into cybersecurity careers.

Several recent studies have focused on the personality traits of IT professionals (Ash et al., 2006A, 2006B; Cruz, DaSilva&Capretz, 2015; Lounsbury et al., 2007; Lounsbury et al., 2009; Rosenbloom et al., 2008; Warren, Young, & Williams, 2012). Ash et al. compared the personality traits and vocational interests of IT professionals to those of working professionals from other fields. In the first of two studies, the researchers used the NEO-FFI (a well-

established “big five” personality measure) to show that IT professionals score higher on the openness to experience scale and lower on the conscientiousness scale (Ash et al., 2006A). In their second study, the researchers used the Strong Interest Inventory (a psychometric tool used extensively by vocational counselors and occupational researchers) to show that IT professionals are more likely to prefer realistic and investigative occupational themes. Non-IT professionals, on the other hand, scored higher on the social and enterprising job themes (Ash et al., 2006B). Cruz, DaSilva&Capretz (2015) reviewed 90 studies in software engineering and summarized that studies using personality measures most often used the Myers-Briggs Type Indicator and reported higher levels of introversion, sensation, thinking, judging and rational temperaments in their samples. Overall, the above studies show that IT professionals have distinct personality traits and occupational preferences compared to professionals in other industries. While cybersecurity is a component of Information Technology, it is a rather unique field within the industry. The job duties of cyber security professionals are distinct from those jobs subsumed under Ash et al.’s definition of IT professionals (application developers, programmers, web administrators, and software engineers). While IT professionals focus on building and configuring software architecture, security professionals have to investigate how such systems could fail and enact contingencies to defend against intrusion. Thus, there is still much to learn about the individual differences of cybersecurity professionals. We therefore developed the following research aim.

Research Aim 1: To establish an individual difference profile of cybersecurity participants and compare between groups (eg. gender, enter cybersecurity jobs vs. did not enter cybersecurity jobs)

Since this was an exploratory study, the choice of the specific individual difference variables to compare participants on was based on the broad themes of personality, interests, culture, attachment style, and decision-making style. We hypothesized that cybersecurity competition participants would have similar profiles as other IT professionals. More specifically, they should be characterized as being high in openness and possess realistic and investigative interests.

2.2 Competition Effectiveness

Even though there have been many cybersecurity competitions over the last decade, it is still not clear whether competitors are interested in careers in cybersecurity. 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. They concluded 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 attract students to cybersecurity careers. Both of these papers are good steps towards understanding the effectiveness of competitions and determining which students are best suited for competitions. As both papers acknowledge, much more work needs to be done to determine if cybersecurity competitions are effective at attracting talent to the profession.

There is also a growing body of research into how to best develop cybersecurity competitions and how to use competitions to further cybersecurity education (Cheung, et al., 2011; Conklin, 2005; Werther, et al., 2011). This body of literature focuses on the design of the competitive exercises and how to integrate skills into scenarios that closely mimic real-world

cybersecurity challenges. These researchers envision competitions as opportunities to teach particular skills; the hope is that this will lead to more skilled cybersecurity professionals.

This paper evaluates the effectiveness of cybersecurity competitions in several ways. Beyond looking at the quantity or proportion of participants who plan to pursue a career in cybersecurity after the competition, this study also uses participants' individual difference scores to predict whether or not they end up in cybersecurity careers after the competition. This way, we will know if cybersecurity competitions are particularly effective in convincing a specific demographic of people based on a specific personality trait or interest. Future competitions can then be designed to either broaden the appeal to other demographics or narrow down and focus on attracting more of the specific demographic.

Research Aim 2: To evaluate competition effectiveness and identify specific individual differences that influenced whether or not they would enter cybersecurity careers post-competition.

2.3. Hacker types

Hackers have existed since the invention of the telephone in 1878, and the definition of what a hacker is has evolved over time (Devitt, 2001). Generally, a 'hack' is a clever technical solution to a problem arrived at through non-obvious methods, and early hackers' lives revolved around making and improving computers and software (Levy, 1984; Turkle, 2005).

Contemporarily, hackers are defined as individuals who apply their knowledge of computers to infiltrate and compromise the security of other networks (Coleman, 2012). The term hacker is often worn as a badge of honor among hackers, but the media commonly attribute negative connotations to the word. To this day, technologists have not reached a consensus on the boundaries of what a 'hacker' is. Some hackers try to separate the definition from those who

perform illicit actions to circumvent computer security, while others are fine with clumping malicious and non-malicious computer activity together (Coleman, 2013).

There is a growing body of research studying the psychological characteristics of hackers and how they differ from non-hackers. Bossler & Burruss (2011) applied self-control theory (Gottfredson & Hirschi, 1990) to explain deviant online activity and found that lower levels of self-control were positively related to hacking behavior. Deviant peer associations were later shown to be a stronger predictor of hacking behavior than low self-control (Holt, Bossler, & May, 2012). Bachmann (2010) studied the cognitive styles of participants of a hacker convention and found that the hackers preferred complex problems over simple ones, and used rational thinking styles more than intuitive approaches. Similarly, Schell and Melnychuk (2010) examined the characteristics of 133 attendees of various hacker conferences from 2005 to 2007. The researchers found that the majority of respondents hacked for non-malicious reasons, with 31% reporting that they hack to solve interesting puzzles and challenges, and 22% reporting that they hack to advance network, software, and computer capabilities. In the same study, Schell & Melnychuk also discovered that 66.9% of the sample scored in the intermediate range of the Autism Quotient (AQ) Spectrum, which is consistent with prior research on the AQ scores of math, computer science, and physical science students (Baron-Cohen, 2001; as cited in Schell & Melnychuk, 2010). Sociologist Bernadette Shell (2000) surveyed 216 hackers at a security convention on creativity, depression, and lifestyles and found that they were generally highly creative and had excellent stress management and multi-tasking skills. Two studies assessed college-aged hackers on the Big-Five personality dimensions and came up with conflicting results. Rogers, Seigfried and Tidke (2006) studied American collegiate hackers and found that self-reported hackers tend to be more extraverted, which goes against common stereotypes of a

reclusive hacker. Rogers, Smoak & Liu (2006) categorized a sample of Canadian students as computer deviants or non-deviants based on their self-reported hacking and virus writing behavior. They found no significant association between the Big-Five personality traits and whether or not individuals were classified as deviants, but found that deviants scored lower on a moral decision-making scale. More research needs to be done using a broader array of psychological measures to determine if there are indeed psychological differences between hackers and non-hackers. Hacker samples are usually difficult to come by, thus researchers often resort to conducting surveys about hackers during hacker conventions and cybersecurity competitions. Since we were already measuring an array of psychological variables to address Research Aim 1, we decided to compare self-admitted hackers versus non-hackers along the same lines. We also included additional measures of self-control, entitlement, and self-efficacy in cybersecurity based on previous literature on hacking, which suggested that low self-control (Bossler & Burruss, 2011) and higher self-entitlement (Shaw et al., 1998) was related to greater deviant tendency. Due to the divisiveness in the definition of what a hacker is, it may be the case that not everybody who participates in cybersecurity competitions is willing to consider themselves a hacker, and there could be an underlying individual difference that drives this perspective. Thus, we developed the following research aim.

Research Aim 3a. Compare individual differences between self-reported hackers and non-hackers.

There have been several attempts by researchers and the media to classify hackers into subgroups. Rogers (2006) proposed a detailed taxonomy of 9 different hacker subgroups, ranging from novices to professional criminals, organized within a circumplex model based on skill level and motivation. He concluded that hackers have four main motivations for hacking: Curiosity,

Notoriety, Financial, and Revenge. Chiesa, Ducci & Ciappi (2009) identified very similar hacking motives in their study, and also proposed additional motives including boredom, love of technology, and ensuring the safety of computers and data. A contemporary taxonomy of hackers adopted by popular media divides the demographic into ‘black-hat hackers’ (those who infiltrate systems to cause damage or gain access to classified information), ‘white-hat hackers’ (those who hack to locate and diagnose vulnerabilities in order to bolster existing security measures), and ‘grey-hat hackers’ (those who do not hack for personal gain but still perform technically illegal activities; Moore, 2010). When designing our exploratory study on cybersecurity competition participants, we expected that competition participants would comprise a diverse sample of hackers with different motivations, thus we decided to investigate if there were psychological profile differences between the three different subgroups of ‘white-hat hackers’, ‘black-hat hackers’ and ‘grey-hat hackers’.

Research Aim 3b. Compare individual differences between white-hat hackers, black-hat hackers and grey-hat hackers.

3. Material and Methods

3.1. Participants

Participants from the first decade of the Cybersecurity Awareness Week (CSAW) Conference capture the flag competition were invited to take an online survey about the characteristics of cybersecurity competition participants. The capture the flag competition has always been open to participants across the world, and the basic premise of the tasks involved in capture-the-flag has not changed over time. Thus, it is possible, although not optimal, to combine participants over the years to form the population of CTF participants from which to sample from.

An email from the CSAW organizers with a link to the survey was sent to approximately 8,000 past competition participants. An incentive of a \$10 Amazon gift card was offered to each participant who completed at least 70% of the survey. The email list included competitors from all ten years of the competition, so some respondents had competed very recently, while others had not been to the competition in almost a decade. This provided us with data about both current students (those who competed recently) and those who had moved on from school to careers.

Data collection was halted after the first 588 people responded to the survey. The amount of gift cards budgeted for paying subjects had been reached and the sample size was adequately large, thus the decision was made to call off further data collection. It took about a month for 588 responses to be collected, so the time period was not too short such that the sample would comprise only of early responders. 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. Only 2.5% ($n = 14$) were African-American, 6.4% ($n = 36$) were Hispanic/Latin American, and 0.2% ($n = 1$) identified as Native American. The 2.9% ($n = 16$) selected “other” for this question, 7.65% ($n = 43$) preferred not to answer, and eight failed to provide any response. 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 a total of 229 items, containing measures of personality, interest, decision-making style, attachment style, culture, efficacy, and entitlement. The survey also asked about the competition experience, opinions about hacking, and intentions of pursuing a career in cybersecurity. The survey included 2 quality control items which requested individuals to select specific response options to ensure that they were paying attention. Measures of the individual difference constructs assessed in this survey are detailed below.

Personality. Personality dimensions were assessed according to the Big Five Personality Dimensions (Costa & McCrae, 1990). Respondents were asked to complete a 44-item Big Five Personality Inventory (Goldberg, 1990). This measure provides a personality profile across five factors: openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism. This five-factor model is used to describe broad personality dimensions, with particular related qualities slotted within each dimension.

The Openness to experience dimension reflects an individual's degree of intellectual curiosity, creativity, and preference for variety of experience. Those who score low on this dimension can be characterized as more down-to-earth and conforming and preferring routines to novelty. Those who score high are typically creative, imaginative, and curious. Openness was assessed with 10 items that had a scale reliability of .73.

Conscientiousness refers to how organized and dependable the individual is. High scorers on this dimension tend to be organized, hard-working, and dependable, preferring planned behavior to spontaneity. Low scorers can be negligent or disorganized and are not as goal-oriented as their higher-scoring counterparts. Conscientiousness was assessed with 9 items that had a scale reliability of $\alpha = .78$.

Extraversion is a measure of how outgoing or reserved an individual is. Those who score highly on the extraversion dimension tend to seek stimulation in the company of others and can be assertive and talkative. Low scorers tend to be loners who often take more passive roles. Extraversion was assessed. Extraversion was assessed with 8 items that had a scale reliability of $\alpha = .79$.

The Agreeableness dimension refers to an individual's tendency to be either friendly and compassionate or analytical and detached. Those who score high on the "agreeableness" dimension tend to be more trusting and good-natured, while low scorers can be suspicious of others, irritable, and often critical. Individuals who score low on agreeableness may be characterized as ruthless by others who are more agreeable. Agreeableness was assessed with 9 items that had a scale reliability of $\alpha = .74$.

Neuroticism refers to an individual's tendency to be either nervous or confident. Sometimes referred to as emotional stability, this dimension assesses an individual's tendency to experience unpleasant emotions, such as anger, anxiety, or vulnerability, easily. Those who score high on "neuroticism" tend to be self-conscious and worried, while low scorers are calmer and less emotional. Unlike the other four dimensions, low scorers on neuroticism tend to be considered more socially healthy. Neuroticism was measured with 8 items that had a scale reliability of $\alpha = .79$. Together, these five traits describe an individual's personality. There were 460 cybersecurity competition participants who completed the 44-item Big Five section of our survey.

Vocational Interests. To assess vocational interests, respondents were asked to complete a truncated 30-item version of the O*Net Interest Profiler (Lewis & Rivkin, 1999). This measure used Holland's (1997) 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**. There are also six work environments that can be characterized in the same way. The best fit or congruence for workers and workplace occurs when the three-letter code matches. Using a standard measure, people can be assigned a three-letter code that identifies the three areas in which they score the highest. Workplaces can be assessed by determining the most common personality type in that workplace.

Each of the six types describes personality characteristics that manifest in “an increasing differentiation of preferred activities, interests, competencies, and values” (Holland, 1997). A brief rundown of Holland’s typology and our measure of interests is on the next page:

- (1) Realistic – a preference for activities that include the explicit, ordered, or systematic manipulation of object, tools, and machines (5 items, $\alpha = .82$);
- (2) Investigative – a preference for activities that include the observational, symbolic, systematics, and creative investigation of physical, biological, and cultural phenomena (5 items, $\alpha = .84$);
- (3) Artistic – a preference for unsystematized activities that include the manipulation of physical, verbal, or human materials to create art forms or products (5 items, $\alpha = .79$);
- (4) Social – a preference for activities that include the leading or manipulation of others to inform, train, develop, cure, or enlighten (5 items, $\alpha = .80$);
- (5) Enterprising – a preference for activities that include the manipulation of others to attain organizational goals or economic gain (5 items, $\alpha = .82$);
- (6) Conventional – a preference for activities that include the explicit, ordered, and systematic manipulation of data (5 items, $\alpha = .82$).

Other researchers have found that Holland's RIASEC model is stable across ethnic groups and gender (Low, et al., 2005; Day, Rounds, and Swaney, 1998; Day and Rounds, 1998) and that it is useful for students as young as middle school age (Osborn, 2002).

Culture: Individualism-Collectivism. Another measure included in the survey was a 16-item version of Triandis' 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.

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. This section of the survey was completed by 417 competitors and was scored on a 5-point scale. The scales had alpha reliabilities of (VI: .55 HI: .74, VC: .68 HC: .66.).

Decision-Making Style. Respondents were also administered the General Decision-Making Style Scale (GDMS, Scott & Bruce, 1995) to assess their decision-making style. 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. There are five decision styles: (1) rational (5 items, $\alpha = .82$), (2) intuitive (5 items, $\alpha = .73$), (3) dependent (5 items, $\alpha = .76$), (4) avoidant (5 items, α

= .89), and (5) spontaneous (5 items, $\alpha = .84$). It is important to educators and competition creators to understand how participants actually go about solving the problems presented, and this measure tries to assess that.

The rational decision-making style is characterized by thoroughness and a logical evaluation of alternatives. Those who score higher on the intuitive style tend to rely more on hunches or gut feelings. Dependent decisionmakers search for the advice and direction of others, whereas avoidant decisionmakers 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. This section of the survey was completed by 374 participants on a 5-point scale.

Attachment Dimensions. Also included were 9 attachment-related questions adapted from the Experiences in Close Relationships Scale (Fraley, Waller & Brennan, 2000). 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 $\alpha = .76$. Anxious attachment was assessed with 3 items with an alpha of .89. Items were responded to on a 7-point scale of strongly disagree to strongly agree.

Entitlement. The survey used Campbell et al.'s (2004) Psychological Entitlement Scale to assess competitors' entitlement, which can be defined as an individual's "stable and pervasive sense that one deserves more and is entitled to more than others" (p. 31). Psychological

entitlement is an individual characteristic that is not context dependent and thus is not related to whether the individual deserves the reward in any particular context. Entitlement was mainly included for study between hacker types. A sense of entitlement often correlates with narcissism and high self-esteem and has been found to correlate with a tendency toward deviant behavior (Grijalva & Newman, 2015; Miller, 2015). Entitlement was on a 7-point scale and had an alpha-reliability of .63.

Self-Control. We included the 20-item Self-Control Scale from Grasmick et al. (1993) to measure competitors' self-control—the ability to evaluate alternative actions rather than respond to immediate impulses. Individuals with better self-control can better manage their lives, and a higher measure of self-control is often associated with greater success in a number of personal and professional activities, including better grades, lower rates of criminality and pathology, and better overall adjustment. Self-control was mainly included for comparison between hacker types. The self-control scale had an alpha-reliability of .87.

Self-Efficacy. 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). 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. Self-efficacy was

mainly included for comparison between hacker types. Self-efficacy questions were on a scale of 1-7, with 7 representing high efficacy. Self-efficacy had a reliability of .91.

Hacker vs. Non-hacker. To facilitate our study of Research Aim 3, we asked individuals to self-report if they identified themselves as a computer hacker (Y/N). If participants answered yes, they would be asked if they considered themselves a white-hat, black-hat, grey-hat hacker, or if they were unsure about the classification. Participants were also asked if they hacked for malicious, non-malicious, or mixed reasons.

3.3. Analyses

The main aim of this project was to create a psychological profile of cybersecurity competitors to better understand their motivations for joining competitions. Publicity and design of future competitions can hedge on any unique motivations and subgroup differences found, in order to attract a larger participant pool who may go on to be employed in information assurance. To create a psychological profile of participants, the mean scores on the exploratory set of various individual difference measures were calculated. The importance of each individual difference variable was assessed by its correlation with whether or not a participant was currently in or would go into the field of cyber security.

We also examined if competitions were more successful at attracting a specific demographic of people to join the cybersecurity field. We divided the sample into “will enter” and “won’t enter” categories, where ‘will enter’ meant that the respondent was likely to pursue a cybersecurity career, and ‘won’t enter’ indicated that the competition definitely did not convince the participant. Ambivalent participants were excluded from these analyses. Three questions, described in Table 1, were used to determine whether the participants’ career plans had been

affected by their competition experience. Those who responded “Yes, probably” and “Yes, certainly” to Question 1 were allocated to the “will enter” group, as were those who responded “Yes” or “Sort of” to the second question and indicated that they were “More likely to pursue a career in cybersecurity.” The ‘won’t enter’ group consisted of those who responded negatively to the first question, as well as those who indicated they were less likely to pursue a career in cybersecurity. We deleted the double-counted people in each group. There were 359 respondents in the ‘will enter’ group and 72 people in the ‘won’t enter’ group. Regression analyses were performed to determine if the effectiveness of the competition could be predicted by any individual difference variables (Personality, Interests, Individualism-Collectivism, Attachment Styles, Decision-making Styles, Self-Control & Entitlement).

We compared individual differences between hackers and non-hackers, white-hat hackers with black-hat hackers using independent samples t-tests.

4. Results and Discussion

Preliminary analyses were first conducted in the entire competition sample ($n = 588$) to determine the general motivation for participating in cybersecurity competitions. 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% claimed to join 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 (Tobey, Pusey & Burley, 2014). Women generally scored higher than males in all measures except self-reported efficacy in cybersecurity tasks. Gender comparisons between subgroups (hackers vs. non-hackers, ‘will enter’ group vs. ‘won’t

enter' group) were deemed untenable as the number of females was too small, reducing the validity of any comparison made.

4.1 Aim 1: To establish an individual difference profile of cybersecurity participants and compare between groups.

Few researchers have studied cybersecurity participants on a wide array of individual difference variables. This study contributes to the field by identifying general psychological traits that cybersecurity competition participants can be grouped by. While employers demand certain knowledge, skills and abilities from their cybersecurity employees, knowing the typical personalities of cybersecurity competition participants is a more nuanced matter that employers may be undecided upon. Competitions can capitalize on the general demeanor of cybersecurity competition participants in order to attract more applicants who will in turn increase the recruitment to these companies. Means and standard deviations between variables for the entire sample are reported in Table A1 of the Appendix. Table 2 below gives a brief summary of the personality, interest, and decision-making profile for the entire sample ($n = 588$) of cybersecurity competition participants.

Overall, cybersecurity participants have the highest scores in openness, investigative interests, and rational decision-making style. This is in agreement with Ash et al.'s (2006A) findings on IT professionals in general. While Ash's sample did not include people from the discipline of cybersecurity, it is safe to say that cybersecurity competition participants are similar to most people in information technology. One difference from Ash's findings is that cybersecurity competition participants score lowest in realistic interests, while conscientiousness ranks higher in the profile. This could be because cybersecurity competitions demand a lot of time and effort over a short period, and the activities involved place less emphasis on physically

building and repairing computers, thus they attract more conscientious and less realistic people. Cybersecurity competition participants are also predominantly rational decision-makers, which is sensible considering that logic is planned action is required for competitions.

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, $t(243) = 2.80$, $p < .01$), while scoring lower on agreeableness (3.55 vs. 3.71, $t(303) = -2.18$, $p = .03$) and perceived self-efficacy at cybersecurity tasks (5.24 vs. 5.89, $t(361) = 4.83$, $p < .01$). 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. That those who hold cybersecurity jobs are less agreeable may reflect cybersecurity competitions being more appealing to agreeable people due to the team-based nature of the tasks, but real-life cybersecurity job tasks may not always be so collaborative. Due to the cross-sectional design of this study, we are unable to verify if these trait differences within people were the same before and after participating in the competition. However, literature speaks to the stability of vocational interest and personality traits over time (Low, Yoon, Roberts & Rounds, 2006; Roberts, Walton & Viechtbauer, 2006) thus examining the predictive ability of interests and

personality on career choice post-competition is still a viable strategy as these traits would not be expected to change much during the competition.

It is also worth noting that although mean-level scores in investigative interests differed, rank-order interests between cybersecurity employees and other competition participants were the same. In other words, both groups were most interested in investigative tasks, and least interested in realistic tasks. This similarity in interest pattern is a sign of interest congruence, which has positive implications with job performance (Nye, Su, Rounds & Drasgow, 2012). Based on evidence that there were no significant differences between cybersecurity employees and participants encouraged by competitions to consider a cybersecurity career on 22 out of 25 individual difference variables from a variety of measures, we can infer that cybersecurity competitions are effective in attracting like-minded people into the field of information assurance.

4.2 Aim 2: To evaluate competition effectiveness and identify specific individual differences that influenced whether or not they would 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. The effectiveness of competitions as a tool to teach participants different skills was also assessed as a secondary question. We asked participants to report on the types of cybersecurity skills that they learned during the competition. Of the 587 people who answered this question, 66.3% reported having learned skills applicable to life in cybersecurity. Whether or

not they learned skills in the competition was positively related to whether they were likely to pursue a cybersecurity career ($\rho = .14, p < .01$). We also classified participant responses to a follow-up open-ended question asking about the types of skills learned in the competition. A cybersecurity expert assigned each response one or more labels indicating types of skills in the field of cybersecurity. Of the 223 who responded to the question, 22.42% reported having gained experience in reverse engineering. 15.25% of participants reported gaining experience with security tools and operating systems (e.g. Linux, Wireshark, Metasploit etc.). 14.8% reported improving their analytic skills, 13% reported an increase in network and web security skills, 11.66% gained experience with forensics, 11.21% learned cryptography skills, 8.52% gained experience in exploitation, 7.62% gained experience with hacking/penetration testing, 6.28% gained teamwork experience and 5.38% gained experience in steganography.

To identify the important individual difference variables for predicting entrance into cybersecurity careers, we correlated the participant scores with whether they ‘will enter’ or ‘won’t enter’ cybersecurity post-competition. Complete means and standard deviations for the ‘will enter’ and ‘won’t enter’ groups are shown in in Table A2 of the Appendix. Figure 1 shows the significant correlations between entrance into cybersecurity careers and each individual difference measure independently. These multiple R correlations were calculated by entering all the subscale variables into a discriminant function (i.e. Enter/Do not enter = $O+C+E+A+N$, and Enter/Do not enter = $R+I+A+S+E+C$, where OCEAN are the big 5 personality subscales and RIASEC are the six vocational interest types). Entitlement and Self-control were completely unrelated to the competition’s influence on the participant’s career choice, and were disregarded from the multiple regression analysis. Participants’ self-efficacy had the greatest predictive validity over the competition’s influence on the participant ($R = .50, p < .01$). Participants with

higher self-efficacy 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 (2005) Social Cognitive Careers theory, which states that self-efficacy in specific domains (in this case, cybersecurity), directs participants to select activities and careers that reinforce their beliefs. One limitation to this inference was that domain-specific self-efficacy was only assessed with two items, thus future replication with a better measure of general self-efficacy as well as domain-specific self-efficacy is needed.

Figure 2 shows the significant correlations with career choice for specific scales within these measures. Personality, Interests, Decision-making styles, and Attachment styles had significant predictive validity on the competition's influence on the participant. Specifically for personality ($R = .30$), when the five NEO-FFI dimensions were regressed on entrance into cybersecurity careers, Conscientiousness ($r = .22, p < .01$) and Openness ($r = .24, p < .01$) exhibited significant regression coefficients. High levels of conscientious and open-mindedness were the main personality traits responsible for the competition's influence on participants' career choice.

Interests had a multiple correlation of .24 with entrance into cybersecurity careers. Multiple regressions using the six RIASEC dimensions showed that Investigative interests played the largest role in predicting whether or not the participant entered cybersecurity careers. More investigative people would tend to report that the competition had influenced their decision to go into cybersecurity ($r = .15, p < .01$).

Decision-making style had a multiple correlation of .33 with entrance into cybersecurity. More in-depth regression analysis of specific decision-making styles showed that the rational

decision-making styles was the main predictor of the effectiveness of competitions ($r = .28$, $p < .01$).

Culture of the individuals on the individualism-collectivism dimensions showed a multiple correlation of .27 with entrance into cybersecurity careers. More specifically, Horizontal collectivism was the main significant predictor of successful competition influence, with more collectivistic people tending to report that the competition had swayed their career decision ($r = .24$, $p < .01$).

Attachment styles had a multiple correlation of .19 with successful entrance into cybersecurity. Less avoidant people tended to report that they were interested in pursuing a career in cybersecurity because of the competition ($r = -.18$, $p < .01$). Since self-efficacy was by far the best predictor of entrance into cybersecurity careers, we wished to know if measuring the other individual difference variables provided any added value or incremental validity. Thus, each variable was entered into a multiple regression equation with self-efficacy predicting success/failure, and the change in R^2 was assessed for each individual variable. The change in R^2 when a variable is introduced into a regression equation indicates the amount of incremental unique variance explained by that measure. When used in a scenario with a dichotomous outcome of 'will enter' (1) and 'won't enter' (0), a high R^2 indicates that the individual difference variable can explain the competition's influence on the participant's career decision. Measuring that variable in participants would therefore be useful for predicting if the competition would be effective or not. There was no added value in measuring personality with self-efficacy in predicting 'will enter'/'won't enter', because the inclusion of the big five measures did not lead to a significant increase in variance explained (ΔR^2). One reason for the great self-efficacy and personality overlap in variance explained could be because the self-

efficacy measure indirectly assessed major aspects of personality. A regression analysis using the big five dimensions to explain self-efficacy showed that openness to experience and agreeableness were significant predictors of self-efficacy, sharing 25% of the total variance in self-efficacy scores. However, measuring interests with efficacy, individualism-collectivism with efficacy, or decision-making style with efficacy showed significant incremental predictive validity. Together interests, culture, and decision-making with self-efficacy only accounts for 32.3% of the explained variance in career choice, an improvement of 6.9% from using efficacy alone.

In sum, efficacy, interest, and decision-making style measures provide valuable information to predicting whether a competition was effective at convincing participants to enter cybersecurity careers. Competitions as a recruitment tool are more likely to work on individuals high in investigative interests and rational decision-making. These individual differences might be useful for career counselors to identify whether an individual might want to consider cybersecurity careers. Horizontal collectivism might also offer an unorthodox means to predict competition influence, but the inclusion of cultural over other more widely accepted measures for career prediction is not worth the potential skepticism and backlash.

4.3. Aim 3a & 3b. Compare individual differences between self-reported hackers and non-hackers and hacker subgroups (white/black/grey-hat).

Among all participants, 47.1% ($n = 263$) identified themselves as computer hackers, while 52.9% ($n = 295$) identified themselves as non-hackers. More than half ($n = 137$) of the “hacker” subsample reported themselves to be “white-hats”, while only 7 reported to be ‘black-hats’ and 73 reported to be grey hats, and 41 reported to be none of the above/ not sure. In addition, most participants (73.9%) reported that their primary motives for hacking were non-malicious. 89.1%

of the white-hats hacked for non-malicious reasons such as testing security systems. Within the small sample of black-hats, only one admitted to hacking for purely malicious reasons while 3 others admitted to hacking for mixed reasons. 30.1% of the grey-hat hackers hacked for mixed reasons and 61.6% hacked for non-malicious reasons.

From the small sample of self-reported black-hat hackers and the indistinct distribution of hacker motives among white-, grey-, and black- hat hackers, we concluded that our attempt to separate the hacker sample into clearly defined subgroups was heavily influenced by social desirability bias. True black-hat hackers who hack for malicious reasons would be unlikely to admit their status on a self-report assessment due to the risk of negative consequences and stigma associated with malicious hacking. Thus, they may incorrectly report themselves as either white-hat or grey-hat. Consequently, this would render inaccurate any comparison between white-hat and grey-hat hackers because any effect would be confounded by the presence of black-hat hackers. Therefore, we decided to drop Research aim 3b and only focus on Research aim 3a—to compare individual differences between hackers and non-hackers. A separate study focusing only on a sample of hackers from a concentrated environment like a hacker convention would have been more suitable to assess differences in black-hat versus white-hat hackers. Future studies will need a more stringent and subtle method of segregating hackers into subgroups that is not affected by social desirability bias. One more subtle possibility would be to ask for frequencies of specific behaviors like what Rogers et al., 2006a; 2006b) did in his two studies, or specifically sample from known communities of black-hat hackers.

Our exploratory comparisons between hackers and non-hackers on the various psychological variables revealed several significant correlations, summarized in Figure 3. Hackers scored significantly higher than non-hackers on efficacy (5.61 vs. 3.68, $t(545) = 10.17$,

$p < .01$) extraversion (3.22 vs. 3.07, $t(446) = 10.17, p = .02$), conscientiousness (3.61 vs. 3.49, $t(447) = 2.11, p = .04$), and openness (3.82 vs. 3.57, $t(445) = 5.19, p < .01$). Hackers scored significantly higher than non-hackers on the rational decision-making style (4.08 vs. 3.88, $t(349) = 3.06, p < .01$), and lower on the avoidant decision-making style (2.60 vs. 2.83, $t(342) = -2.32, p = .02$). The hacker group, however, did demonstrate a significant difference than the non-hacker group on the two individualism measures – (3.74 vs. 3.53, $t(394) = 3.31, p < .01$) on vertical individualism and (3.97 vs. 3.68, $t(405) = 4.07, p < .01$) on horizontal individualism. This indicates that those who identify as hackers are more individualistic compared to those who do not. Interestingly, the hacker group scored higher (3.51 vs. 3.39, $t(356) = 2.01, p = .04$) than non-hackers on the self-control measure. This is counter to the idea that self-control is an indicator of deviant behavior, or that hacking is deviant behavior. Hackers in our sample actually exhibited a greater sense of self-control than the non-hackers.

In addition to the comparison of means, we performed discriminant function analyses to find out which individual difference variable is most important in predicting hackers from non-hackers. Efficacy had the highest standardized beta-coefficient ($\beta = -.38$), followed by vertical individualism ($\beta = -.11$) and self-control ($\beta = -.10$). Thus measures of these three variables would best be able to predict if someone claims to be a hacker or not.

5. Conclusion

5.1 Summary of Results

The current study investigated three different research questions using a large sample of cybersecurity competition participants. We present a comprehensive profile of cybersecurity participants, showing that they tend to be high in openness, investigative interests, and rational decision-making styles. Individuals high in perceived self-efficacy in cybersecurity tasks, rational

decision-making style, and investigative interests were also more likely to enter cybersecurity careers post-competition. Competition designers should thus target this demographic when trying to attract participants. They can do this by including more logic-based tasks that call for research, investigation, and deduction. They can also provide greater reinforcement or rewards for participants who make even minor strides, which can indirectly boost their sense of competency in cybersecurity-related tasks. By balancing the competition rewards and the types of tasks accomplished, we believe cybersecurity competitions can become a more enjoyable experience not just for the winners, thereby raising the overall appeal to the general public. Our secondary study of hackers showed that self-proclaimed hackers tend to show higher self-efficacy, more self-control, and more individualism. 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.

5.2 Limitations & Future Directions

One major limitation for this exploratory study on cybersecurity competitions was its reliance on retrospective self-report data for participants of different CSAW capture the flag competitions within the past decade. Their reports on individual differences and their perceived self-efficacy could have been vastly different at the age when they actually took part in the competition. We had to settle for retrospective self-report data because it is difficult to acquire a large sample of cybersecurity specialists and hackers. This sampling issue was due to the limited access to competition data from outside of CSAW, as well as the general inaccessibility of the hacker population. Future studies can adopt a longitudinal framework to examine the influence of cybersecurity competitions on participants. Data collected before the competition and immediately after the competition would provide a stronger argument for the effectiveness of

competitions in influencing cybersecurity career choice. 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 (Low et al., 2005; Roberts et al., 2006), so their predictive power on cybersecurity career choice is much more credible.

Another limitation to our current methodology was that we did not collect data the year in which each participant competed, nor their performance within the competition (e.g. prizes awarded or points scored); these variables would have been useful for studying potential cohort effects and other moderators to the relationship between individual differences and career choice. Also, the participant pool for CSAW comprises students already showing an interest in computer science, thus we were unable to study the psychological profiles of cybersecurity employees who chose to enter cybersecurity careers due to other reasons. A comparison of cybersecurity employees who have never attended competitions with those who did will inform researchers about the other kinds of people that current competitions are not effectively targeting. Discussions with industry recruiters can also serve to confirm if our general psychological profile of cybersecurity competition participants extends to cybersecurity employees.

Replication is especially essential to reinforce findings from young field such as cybersecurity research. Conducting pre- and post-competition surveys in other samples drawn from a different cybersecurity competition would be ideal to investigate if the psychological profiles of cybersecurity competition participants generalize across competitions. Interviewing competition participants can also be an alternative method to garner more information on how to improve competitions as a recruitment tool. Even with these limitations in mind, we believe this study to be an important first step in profiling the still understudied population of cybersecurity competition participants. The results also provide some preliminary insight into improving

cybersecurity competitions as a recruitment tool and stimulate an influx of employees into cybersecurity careers.

6. Acknowledgements

This material is based upon work supported by the National Science Foundation. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. We are thankful towards April Lambert & Karen Lamb for their assistance on the project.

7. References

- Ash, R. A., Rosenbloom, J. L., Coder, L. & Dupont, B. (2006A). Personality characteristics of established IT professionals: Big five personality characteristics. In: *Encyclopedia of Gender and Information Technology*, 983-989. Hershey, PA: Idea Group Publishing.
- Ash, R. A., Rosenbloom, J. L., Coder, L. & Dupont, B. (2006B). Personality characteristics of established IT professionals: Occupational personality characteristics. In: *Encyclopedia of Gender and Information Technology*, 990-998. Hershey, PA: Idea Group Publishing.
- Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *The International Journal of Cyber Criminology*, 4, 643-656.
- Bashir, M., Lambert, A.D., Wee, J.M.C., Guo, B., and Memon, N. (2015). Exploring the Vocational Interests of Cybersecurity Competition Participants, 19th Colloquium for Information Security Education (CISSE), June 15-17, Las Vegas, NV (forthcoming).
- Bossler, A. M., & Burruss, G. W. (2011). The General Theory of Crime and Computer Hacking: Low Self-Control Hackers? In T. Holt, & B. Schell (Eds.) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 38-67). Hershey, PA: Information Science Reference. doi:10.4018/978-1-61692-805-6.ch003
- 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.
- Cheung, R., Cohen, J., Lo, H. & Elia, F. (2011). "Challenge Based Learning in Cybersecurity Education," Proc. Of the 2011 International Conference on Security & Management, v. 1.
- Cheung, R., Cohen, J. Lo, H., Elia, F. & Veronica C.M. (2012). "Effectiveness of Cybersecurity Competitions," Proc. International Conference on Security and Management, Las Vegas, Nevada.
- Chiesa, R., Ducci, S., & Ciappi, S. (2009). *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. Boca Raton, FL: Auerbach Publications.
- Conklin, A. (2005). "The Use of a Collegiate Cyber Defense Competition in Information Security Education," Proc. Of the 2nd Annual Conference on Information Security Curriculum Development, ACM, pp. 16-18.
- Coleman, G. E. (2012). *Coding freedom: The ethics and aesthetics of hacking*. Princeton University Press.

- Coleman, G. E. (2013). *Hacker*. In The Johns Hopkins Encyclopedia of Digital Textuality, 2014. Retrieved from <http://gabriellacoleman.org/wp-content/uploads/2013/04/Coleman-Hacker-John-Hopkins-2013-Final.pdf>
- Costa Jr, P. T., & McCrae, R. R. (1990). Personality disorders and the five-factor model of personality. *Journal of Personality Disorders*, 4(4), 362-371.
- Cruz, S., da Silva, F. Q., & Capretz, L. F. (2015). Forty years of research on personality in software engineering: A mapping study. *Computers in Human Behavior*, 46, 94-113.
- Day, S.X., Rounds, J., and Swaney, K. (1998). The structure of vocational interests for diverse racial-ethnic groups. *Psychological Science*, 9(1): 40-44.
- Day, S.X. and Rounds, J. (1998). The universality of vocational interest structure among racial/ethnic minorities. *American Psychologist*, 53: 728-736.
- Devitt, M. (2001). *A brief history of computer hacking*. Retrieved from <http://www.dynamicchiropractic.com/mpacms/dc/article.php?id=18078>
- Fraley, R.C., Waller, N.G. & Brennan, K.A. (2000). An item-response theory analysis of self-report measures of adult attachment. *Journal of Personality and Social Psychology*, 78, 350-365.
- Fraley, R.C. (2010). A Brief Overview of Adult Attachment Theory and Research. Available at <https://internal.psychology.illinois.edu/~rcfraley/attachment.htm>.
- Gavas, E. and Memon, N. (2012). Winning cybersecurity one challenge at a time. *IEEE Security & Privacy*, vol. 10(4), 75-79.
- Goldberg, L. R. (1990). An alternative "description of personality": the big-five factor structure. *Journal of personality and social psychology*, 59(6), 1216.
- Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.
- 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.
- Grijalva, E., & Newman, D. A. (2015). Narcissism and counterproductive work behavior (CWB): Meta-analysis and consideration of collectivist culture, big five personality, and narcissism's facet structure. *Applied Psychology: An International Review*, 64(1), 93-126.

- Haliburton, W., Thweatt, M., and Wahl, N.J. 1998. Gender difference in personality components of computer science students: A test of Holland's congruence hypothesis. *ACM*, 30(1):77-81.
- ISACA, "2015 Global Cybersecurity Status Report," available at <http://www.isaca.org/pages/cybersecurity-global-status-report.aspx>.
- Holland, J.L. (1997). *Making vocational choices: A theory of vocational personalities and work environments* (3d. ed.). Odessa, FL" Psychological Assessment Resources.
- Holt, T. J., Bossler, A. M., & May, D. C. (2012). Low self-control, deviant peer associations and juvenile cyberdeviance. *American Journal of Criminal Justice*, 37(3), 378-395.
- Lent, R. W. (2005). *A social cognitive view of career development and counseling* John Wiley & Sons Inc, Hoboken, NJ. Retrieved from <http://search.proquest.com/docview/620575970?accountid=14553>
- Levy, S. (1984). *Hackers, heroes of the computer revolution*. Delta, New York, NY.
- Lewis, P. & Rivkin, D. (1999). *Development of the O*NET interest profiler*. National Center for O*Net Development, Raleigh, NC.
- Lounsbury, J. W., Moffitt, L., Gibson, L. W., Drost, A. W., & Stevens, M. (2007). An investigation of personality traits in relation to job and career satisfaction of information technology professionals. *Journal of Information Technology*, 22(2), 174-183.
- Lounsbury, J. W., Studham, R. S., Steel, R. P., Gibson, L. W., & Drost, A. W. (2009). Holland's vocational theory and personality traits of information technology professionals. *Handbook of Research on Contemporary Theoretical Models in Information Systems*, 529-543. Hershey, PA: IGI Global.
- Low, K.S.D., Yoon, M., Roberts, B.W., & Rounds, J. (2005). The stability of interests from early adolescence to middle adulthood: A quantitative review of longitudinal studies. *Psychological Bulletin*, 131, 713-737.
- Miller, B. K. (2015). Entitlement and conscientiousness in the prediction of organizational deviance. *Personality and Individual Differences*, 82, 114-119.
- Moore, R. (2010). *Cybercrime: Investigating high-technology computer crime*. Routledge.

- 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.
- National Initiative for Cybersecurity Careers and Studies.(2015). *Cyber Competitions*.Retrieved online September 11 2015 from <https://niccs.us-cert.gov/training/tc/search/cmp/new>.
- Osborn, D.S. (2002).Using the self-directed search career explorer with middle school students: The practicality of Holland's RIASEC theory.ERIC No. ED465915. Available at <http://eric.ed.gov/?id=ED465915>
- Patriciu, V.V., &Furtuna, A. C. (2009). "Guide for Designing Cybersecurity Exercises," Proc. Of the 8th WSEAS International Conference on E-Activities and Information Security and Privacy, World Scientific and Engineering Academy and Society, pp. 172-177.
- Roberts, B. W., Walton, K. E., &Viechtbauer, W. (2006). Patterns of mean-level change in personality traits across the life course: a meta-analysis of longitudinal studies. *Psychological Bulletin*, 132(1), 1-25.
- Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital investigation*, 3(2), 97-102.
- Rogers, M. K., Seigfried, K., &Tidke, K. (2006). Self-reported computer criminal behavior: A psychological analysis. *Digital Investigation*, 35, 116-120.
- Rogers, M. K., Smoak, N. D., & Liu, J. (2006). Self-reported deviant computer behavior: A big-5, moral choice, and manipulative exploitive behavior analysis. *Deviant Behavior*, 27(3), 245-268.
- Rosenbloom, J. L., Ash, R. A., Dupont, B., & Coder, L. (2008). Why are there so few women in information technology? Assessing the role of personality in career choices. *Journal of Economic Psychology*, 29(4), 543-554.
- 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.
- Schell, B. H., &Melnychuk, J. (2010). Female and male hacker conferences attendees: Their Autism-Spectrum Quotient (AQ) scores and self-reported adulthood experiences. *Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications*, T. J. Holt & B. H. Schell (Eds.), 144-169. Hershey, PA: Information Science Reference.

- 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.
- Shaw, E., Ruby, K., & Post, J. (1998). The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin*, 2(98), 1-10.
- Shell, B. (2000). *Hacker Psychology*. Retrieved from <http://www.happyhacker.org/gtmhh/bank5.shtml>
- 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.
- Turkle, S. (2005). *The second self: Computers and the human spirit*. MIT Press, Cambridge.
- Vigna, G., Borgolte, K., Corbetta, J., Doupe, A., Fratantonio, Y., Invernizzi, L., Kirat, D. & Shoshitaishvili, Y. (2014). Ten Years of iCTF: The Good, The Bad, and The Ugly. *Proceedings of the USENIX Summit on Gaming, Games and Gamification in Security Education (3GSE)*, San Diego, CA.
- Warren, J., Young, D., & Williams, K. (2012). Personality, gender and careers in information technology. *Proceedings of the Americas Conference on Information Systems (AMCIS)*, paper 12.
- Werther, J., Zhivich, M., Leek, T., & Zeldovich N. (2011). "Experiences in Cybersecurity Education: The MIT Lincoln Laboratory Capture-the-Flag Exercise," Proc. Of the 4th Conference on Cybersecurity Experimentation and Test (CSET), USENIX, p. 12.

Table 1.

Questions to determine 'will enter'/'won't enter' Groups

Question	Response options
1. Do you plan on pursuing a career in the cyber security/information assurance field?	"No, certainly not" , "No, probably not", "Maybe", "Yes, probably" and "Yes, certainly"
2. Did participating in the competition cause you to change any plans for your future career or academic path?	"Yes", "Sort of", "No"
3. Which of the following best describes how your plans have changed?	"More likely to pursue a career in IA", "Less likely to pursue a career in IA", "Other"

Table 2.

Brief Profile of Cybersecurity Competition Participants

Personality	Mean(SD)	Interests	Mean(SD)
Openness	3.67 (.55)	Investigative	3.33 (.94)
Agreeableness	3.61 (.60)	Social	2.90 (.94)
Conscientiousness	3.54 (.64)	Artistic	2.87 (.96)
Extraversion	3.14 (.70)	Conventional	2.80 (.87)
Neuroticism	2.62 (.70)	Enterprising	2.56 (.92)
		Realistic	2.53 (.90)
Decision-making	Mean(SD)	Other	Mean(SD)
Rational	3.95 (.70)	Avoidant Attachment	3.76 (1.11)
Intuitive	3.38 (.69)	Anxious Attachment	3.81 (1.68)
Dependent	3.38 (.75)	Individualism	3.65 (.73)
Avoidant	2.72 (.94)	Collectivism	3.65 (.77)
Intuitive	2.70 (.69)	Self-Efficacy	4.96 (1.55)

Note. Attachment and efficacy were on 7-point scales while other measures were on 5-point scales.

Figure 1. Multiple regression predictive validity estimates for entire measures. *There is major overlap in variance explained by personality and efficacy measures, so using a personality measure together with an efficacy measure is not incrementally useful in predicting ‘will enter’-won’t enter’.

Figure 2. Significant correlations of specific individual differences and success of competitions at recruiting participants into the field of cybersecurity.

Figure 3. Significant differences between hackers and non-hackers.

Appendix

Table A1.

Full Profile for Cybersecurity Competition Participants:

Means and Standard Deviations of Study Variables

Variable	N	Mean	SD
Personality			
Extraversion	460	3.14	.70
Agreeableness	460	3.61	.60
Conscientiousness	460	3.54	.64
Neuroticism	460	2.62	.70
Openness	458	3.67	.55
Interests			
Realistic	372	2.53	.90
Investigative	372	3.33	.94
Artistic	372	2.87	.96
Social	374	2.90	.93
Enterprising	372	2.56	.92
Conventional	373	2.80	.87
Attachment Style			
Avoidance	432	3.76	1.11
Anxiety	433	3.81	1.68
Culture			
V_Individualism	416	3.61	.68
H_individualism	417	3.79	.77
V_Collectivism	417	3.54	.83
H_Collectivism	417	3.75	.70
Decision-Making Style			
Rational	374	3.95	.70
Avoidant	375	2.72	.94
Dependent	375	3.38	.75
Intuitive	374	3.38	.69
Spontaneous	374	2.70	.81
Other			
Entitlement	442	3.78	.83
Self-Efficacy inCybersecurity	560	4.96	1.55
Self-Control	383	3.44	.60

Table A2.

Means and Standard Deviations of Individual Differences between ‘Will Enter Cybersecurity’ (N = 359) and ‘Won’t Enter Cybersecurity’ (N = 72) Groups

	‘Will Enter Cybersecurity’		‘Won’t Enter Cybersecurity’	
	Mean	SD	Mean	SD
Personality				
Extraversion	3.20	.69	2.94	.62
Agreeableness	3.65	.59	3.52	.57
Conscientiousness	3.64	.64	3.26	.63
Neuroticism	2.56	.69	2.77	.68
Openness	3.73	.49	3.37	.78
Interests				
Realistic	2.58	.93	2.31	.84
Investigative	3.37	.94	2.98	1.05
Artistic	2.84	.95	2.89	1.11
Social	2.96	.93	2.69	.94
Enterprising	2.53	.93	2.54	.99
Conventional	2.81	.92	2.65	.81
Culture				
V_Individualism	3.68	.66	3.33	.82
H_Individualism	3.85	.73	3.50	.95
V_Collectivism	3.61	.80	3.36	.94
H_Collectivism	3.84	.67	3.38	.86
Attachment Style				
Avoidance	3.69	1.09	4.22	1.19
Anxiety	3.72	1.79	4.02	1.50
Decision-Making Style				
Rational	4.05	.65	3.52	.91
Avoidant	2.60	.94	2.86	.92
Dependent	3.42	.70	3.09	.86
Intuitive	3.39	.67	3.22	.84
Spontaneous	2.67	.81	2.57	.88
Other				
Entitlement	3.76	.85	3.65	.83
Self-Efficacy in Cybersecurity	5.46	1.26	3.40	1.60
Self-Control	3.49	.60	3.42	.63