Self-efficacy in Cybersecurity Tasks and its Relationship with Cybersecurity Competition and Work-related Outcomes

Jian Ming Colin Wee
University of Illinois at Urbana-Champaign

Masooda Bashir
University of Illinois at Urbana-Champaign

Nasir Memon
New York University Polytechnic School of Engineering

Abstract

Research on cybersecurity competitions is still in its nascent state, and many questions remain unanswered, including how effective these competitions actually are at influencing career decisions and attracting a diverse participant base. The present research aims to address these questions through surveying a sample of ex-cybersecurity competition participants from New York University's Cyber-Security Awareness Week (CSAW). 195 survey respondents reported on their self-esteem, general self-efficacy, and perceived efficacy in cyber-security-related tasks, along with important competition- and career-related variables such as reasons for participating, competition performance, appeal and effectiveness of competitions, job satisfaction, and perceived organizational fit. Correlational analyses showed that confidence in cybersecurity-related tasks was positively related to interest in cybersecurity, performance within the competition, job satisfaction within a cybersecurity job, and perceived organizational fit within cybersecurity organizations. Specific self-efficacy was better at predicting competition performance than general self-efficacy or self-esteem, but was unrelated to participants' positive image of competitions and whether or not the cybersecurity competitions influenced their career decisions. Instead, general self-efficacy was a better predictor of positive competition experience even more-so than performance within the competition. Overall, the results show that participants with self-confidence in their cybersecurity-relevant skills are more likely to do well in the competition and be satisfied when entering a cybersecurity career, but any participant with high general self-efficacy will likely still have a positive experience when participating in competitions.

1. Introduction

With the advent of modern data sharing and networking technologies, the need for cybersecurity professionals to protect information networks from online threats has increased exponentially (NICCS, 2015). One of the main methods to address to increase the cybersecurity workforce is through the sponsorship of cybersecurity competitions. These contests are commonly hosted by educational institutions and are typically targeted towards high school- and college-aged students. Competitions challenge participants to develop innovative strategies to attack o defend computer systems, while raising awareness about online threats and teaching network security practices through live exercises. Thus, competitions are a good method of recruiting the next generation of cybersecurity specialists (Gavas, Memon & Britton, 2012). Unfortunately, research on the effectiveness of cybersecurity competitions is still in its nascent state. We do not know much about how participant personality traits are related to their performance in the competition or in cybersecurity jobs, nor do we know much about the participants' perceptions about how effective the competition is.

A previous exploratory study conducted in 2012 on cybersecurity competition participants assessed participants on several common psychological variables like vocational interests, personality, culture, self-efficacy, attachment style, and problem solving style, with the aim of describing the psychological and demographic profile of cybersecurity competition participants, and identifying potentially interesting individual differences that separated those who would enter the cybersecurity workforce post-competition and those who would not (Bashir et al, 2015). Researchers found self-efficacy to be among the highest individual differences within the sample, suggesting that self-confidence in one's abilities could be especially important to a cybersecurity professional. Self-efficacy is defined as an individual's belief about his or her ability/capability to complete a specific task (Bandura, 1994). Due to the large number of measures administered during this exploratory study, many of the assessments used were broader, abbreviated versions of the validated measure. This was the case for the measure of self-efficacy. In the previous study,

self-efficacy was assessed by a simplistic two-item measure of self-efficacy ("In general, how confident are you about your ability to work in a cybersecurity/information assurance field" and "In general, how comfortable are you with your level of knowledge to work in cybersecurity/information assurance field?"). Furthermore, the exploratory nature of the study also limited the assessment of an important array of dependent variables that could elaborate on the importance of self-efficacy in competition and career outcomes. Thus, there is a need to perform more in-depth research into the role of self-efficacy in determining competition effectiveness and career success.

The present study aimed to extend Bashir et al.'s (2015) research into cybersecurity competition participants by using more comprehensive measures of self-efficacy and similar personality variables to elucidate the role of self-efficacy in broader cybersecurity outcomes. These outcomes included present job satisfaction, perceived organizational fit, as well as perceptions about the overall appeal and effectiveness of competitions at attracting people into the cybersecurity workforce. In 2016, we conducted a follow-up survey in another sample of Capture the Flag competition participants from New York University's Cyber-Security Awareness Week (CSAW). CSAW Capture the Flag is an annual on-site competition with an 11-year history. Capture the flag is a team-based activity where contestants race each other to retrieve a digital key hidden within a host network. Often, one team tries to hack the network to retrieve they key while the opposing team tries to protect it from being stolen. Since its inception, CSAW has developed into to a prestigious international competition which annually recruits over 10,000 participants from around the world. Our online survey of CSAW's capture the flag participants included more detailed assessments of self-esteem, general self-efficacy, and perceived efficacy in cybersecurity-related tasks. We also asked more competition-related questions involving public appeal and gender composition of teams, which had been omitted in the exploratory survey in 2012.

Based off the results of the previous study, as well as meta-analytic findings in organizational research, we developed several hypotheses regarding self-efficacy and the outcome variables of competition success (operationalized by within-competition performance and effectiveness at recruiting cybersecurity professionals) and career success (operationalized by job satisfaction and job fit). Based on Robert Lent's (2005) Social Cognitive Careers theory, self-efficacy in specific domains (such as cybersecurity) should direct participants to prefer activities and careers that reinforce their beliefs. Tracey (2010) found that self-efficacy and interests were associated with career choice, specifically the congruence of one's interest to his or her occupation was related to his or her self-efficacy in career decision making. Thus, we predicted that self-efficacy in cybersecurity should have a positive relationship with interest in cybersecurity. Self-efficacious participants should also report that they found cybersecurity competitions as an effective means of recruiting into the cybersecurity workforce. We also predicted that self-efficacy should be related to job satisfaction, perceived job fit, as well as performance score in the competition. This prediction is derived from past meta-analyses which have shown that self-efficacy has a strong positive relationship with work performance (Stajkovic & Luthans, 1998) and job satisfaction (Judge & Bono, 2001). We further explore the different type of self-efficacy (generalized and specific) as well as self-esteem and their relationships with these outcome variables. To summarize, we made the following hypotheses regarding self-efficacy and competition or career outcomes.

H1. Self-efficacy in cybersecurity would be positively related with interest in cybersecurity activities.

H2. Self-efficacy in cybersecurity would be positively related to performance and satisfaction within the cybersecurity competition.

H3. Self-efficacy in cybersecurity would be related to how effective the competitions are at recruiting individuals into the cybersecurity workforce.

H4. Self-efficacy in cybersecurity would be positively related to job satisfaction in cybersecurity.

H5. Self-efficacy in cybersecurity would be positively related to perceived fit within cybersecurity organizations.

Knowledge of these relationships will help to verify the importance of efficacy as an indicator variable for competition success and career success.

2. Related Work

There has been barely any research into the effectiveness of competitions at attracting students into the cybersecurity workforce. Cheung et al (2012) studied interests and skills in participants to a cybersecurity workshop and found that prior knowledge was a major factor in determining if competitions could attract students to cybersecurity careers. Tobey, Pusey and Burley (2014) studied participants from the National Cyber League competition and found that competitions increased the interests of people already skilled in cybersecurity tasks. Most recently, Bashir et al. (2015) exam-

ined the psychological profiles of 588 past participants from Cybersecurity Awareness Week (CSAW). Cybersecurity participants showed a profile of having high openness to experience, investigative interests, rational decision making styles, and self-efficacy. Participants who displayed higher self-efficacy and investigative interests were also found to be more likely to declare a career in cybersecurity post-competition (Bashir, Wee, Memon & Guo, 2016, under review). The present study contributes to the sparse literature on cybersecurity competitions by measuring some important work and competition-related outcome variables and investigating their relationship with the individual difference variables of self-efficacy and specific interest in cybersecurity.

3. Methodology

This study was reviewed and monitored by the University of Illinois' Institutional Review Board to ensure all ethical guidelines were adhered to. We contacted participants from New York University's Cybersecurity Awareness Week (CSAW) Capture-the-Flag competition and invited them to take an online survey about their opinions about cybersecurity competitions and their own perceived confidence and interests in the field of cybersecurity. The survey was completely voluntary and participants' identities were kept confidential. An incentive of a $10 Amazon gift card was offered to each participant who completed at least 80% of the survey. A total of 402 people from the mailing list clicked on the survey link, and 205 consented to complete the survey for monetary compensation (Response rate of 51%). After filtering out the insufficient effort responders who failed two quality control items (e.g. Please select the 'strongly disagree' option), 195 participants provided useable data.

The survey asked for a range of information about the participants, including (1) the gender composition of their competition groups, (2) their performance and satisfaction regarding the most recent competition, (3) their reasons for participating in the competitions, (4) their perception of how effective cybersecurity competitions are, and (5) their interest and confidence in performing several cybersecurity tasks. We also included established measures of psychological constructs such as self-esteem and generalized self-efficacy.

Our previous research on cybersecurity competition participants highlighted the importance of self-efficacy in cybersecurity fields and its relation to the effectiveness of competitions as a recruitment tool and the intention to pursue a cybersecurity career. However, one of the criticisms we received was that our measure of self-efficacy only included two un-validated, self-constructed items. To explore deeper how self-efficacy is related to competition effectiveness and career intent, we administered several established measures of psychological constructs that were similar to the concept of self-efficacy. More specifically, is overall self-esteem, and generalized self-efficacy (not limited to just cybersecurity tasks), related to how effective the competition was at influencing the participant's decision to enter a cybersecurity career?

We included Rosenberg's (1965) self-esteem scale as a measure for the participants' self-esteem, defined as stable feelings of overall self-worth. This was a 10-item scale with items such as "On the whole, I am satisfied with myself" and reversed scored items such as "I certainly feel useless at times". The scale response was on a 4-point scale of 'Strongly Disagree' to 'Strongly Agree'. Cronbach's Alpha reliability for the scale was .89.

We included Chen, Gully & Eden's (2001) New General Self-Efficacy (NGSE) Scale as a measure of general self-efficacy, defined as "beliefs in one's own abilities to meet situational demands" (Wood & Bandura, 1996). The scale comprised 8 items on a 5-point scale from 'Strongly Disagree' to 'Strongly Agree'. Sample items include 'When facing difficult tasks, I am certain that I will accomplish them'. We were interested if confidence in one's own abilities was related to performance in the competition and subsequent interest in a cybersecurity career. The Cronbach's Alpha reliability of the NGSE was .90.

To measure specific self-efficacy in cybersecurity tasks, we created a detailed 20-item measure listing various cybersecurity-tasks recommended by a panel of cybersecurity experts. The measure was pre-tested in a sample of university students and the best-performing items were selected. On a five point scale of "No Confidence at all" to "Completely Confident", Participants would rate their confidence in completing tasks such as "Erect firewalls to protect against intrusion" and "Perform reverse engineering". The full list of items is displayed in Table 1 on the next page. A principal components analysis was conducted to establish factorial validity of the self-created scale. All items loaded positively (>.45) on the first factor, which explained 37.48% of the total variance, while the next best factor only explained 9.78%. Together, this provides evidence that the scale is measuring a single construct of specific self-efficacy. Cronbach's Alpha reliability for the measure was .91.

Encrypt data transmissions to conceal confidential information	Identify and address information security threats in an organization

Educate clients about computer security threats	Remove malware from computer systems
Erect firewalls to protect against intrusion	Monitor current reports of computer viruses and update virus protection systems
Perform reverse engineering	Harden network embedded devices
Work with different operating systems	Perform penetration tests to verify network security
Back up data in a computer	Counter denial of service attacks.
Spoof MAC addresses	Develop proof of concept exploits of vulnerabilities
Modify user account permissions	Install and upgrade network hardware
Decode encrypted data	Set up a virtual private network (VPN)
Interpret and resolve exploits	Write secure network protocols

Table 1. Activities used to assess cybersecurity self-efficacy.

Interests are defined as trait-like preferences for activities or environments associated with these activities (Rounds & Su, 2014). To measure specific interests within the field of cybersecurity, we used the same tasks described by the panel of cybersecurity experts and asked participants to rate them on a 5-point scale of "Strongly Dislike" to "Strongly Like". The Cronbach's Alpha reliability of the measure was .86.

We measured two organizational outcome variables that contribute to career success. To limit our inferences to the field of cybersecurity, we only asked competition participants holding cybersecurity jobs to complete the organizational outcome portion of the survey. The first measure was of job satisfaction, defined as cognitive and affective evaluations of the favorability of one's job (Judge, Hulin & Dalal, 2009). Job satisfaction was measured with the 8-item Job In General Scale (Ironson et al., 1989; Smith et al., 1987) which asks participants to respond to job descriptors such as "Enjoyable" or "Disagreeable" on a 3-point scale. Cronbach's Alpha reliability of the measure was .85. The second measure was of perceived organizational fit, defined as the judgments of congruence between an employee's personal values and the organizational culture (Cable & Derue, 2002). Perceived organizational fit was assessed with Cable and Derue's nine items on a 5-point scale of "Strongly Disagree" to "Strongly Agree". Sample items include "My abilities and training are a good fit with the requirements of my job" and "The things that I value in life are very similar to the things that my organization values". The Alpha reliability for the scale was .89.

We assessed two competition-related outcome variables. The first was the self-reported score of the participant in the competition. Since the survey was taken anonymously, participants were requested to refer to the online scoreboard for their respective CSAW CTF competition and report their scores anonymously. Another crude measure of competition performance used was whether participants reached the qualifying rounds or finals. Participants were also asked the extent to which they were satisfied with their past performance in cybersecurity competitions on a 5-point scale.

To identify the primary reasons for participating in cybersecurity competitions, participants were asked to complete the sentence "I participate in cybersecurity competitions because I want to..." Several reasons such as "learn about cybersecurity careers'" and "hone cybersecurity-related skills" were provided and participants were to rate their agreement on a 5-point scale of "Strongly Disagree" to "Strongly Agree".

To evaluate the effectiveness of competitions as recruiting tools, we asked several single-item questions regarding the participants' opinions on cybersecurity competitions. Responses to these questions were on a 5-point scale of "Strongly Disagree" to "Strongly Agree". Table 2 shows the list of questions that were used to assess effectiveness of competitions at attracting and recruiting cybersecurity talent.

Cybersecurity competitions are effective at recruiting people into careers in the field.
Cybersecurity competitions increase the appeal of the field to the general public.
My experience in cybersecurity competitions was a major factor in influencing my career decisions.
The skills I learned from cybersecurity competitions were useful

Table 2. Questions regarding cybersecurity competition effectiveness.

For each of the measures of career success, competition performance, and questions on perceived cybersecurity competition effectiveness, we examined whether there was a significant correlation with interests and/or self-efficacy.

4. Results & Discussion

4.1 Demographics

Of the 195 participants who passed the quality control checks, 5% were female (n = 11). The average age of the sample was 24.28. 58.9% of the sample was White, while 30.2% was Asian. These demographics were similar to the previous study conducted within the same population of CSAW participants. Within the sample, 45% (n = 88) people

were currently employed within cybersecurity jobs. The sample was evenly split between people who participated in CSAW for the first time (33.6%), for two times (33.6%), for three times (25.1%), and more than three times (7.6%). Team composition was varied within the sample, ranging from individuals participating alone and teams of 43. The average team size was 5 people. 71% of the sample (n = 145) reported working in all-male teams, 23% (n = 47) reported teams with a minority of females, while only 4.4% (n = 9) of participants reported working in majority female or all female teams. 16.7% (n = 34) of the participant sample reported reaching the finals of CSAW while 83.3% (n = 169) reported reaching the qualifying rounds before being eliminated.

4.2 Reasons for Participating

We found significant differences in the participants' primary reasons for participating in cybersecurity competitions (Figure 1). On average, most of the participants strongly agreed that they participated to "challenge myself with solving problems" and "hone cybersecurity-related skills". These reasons were endorsed to a significantly greater extent over the other options of "socialize with like-minded peers", "compete against others" and "learn about cybersecurity careers". From the data, participants prioritized mastery goals (improving one's skills) over social goals (competing and socializing) and finally career goals were the least prioritized.

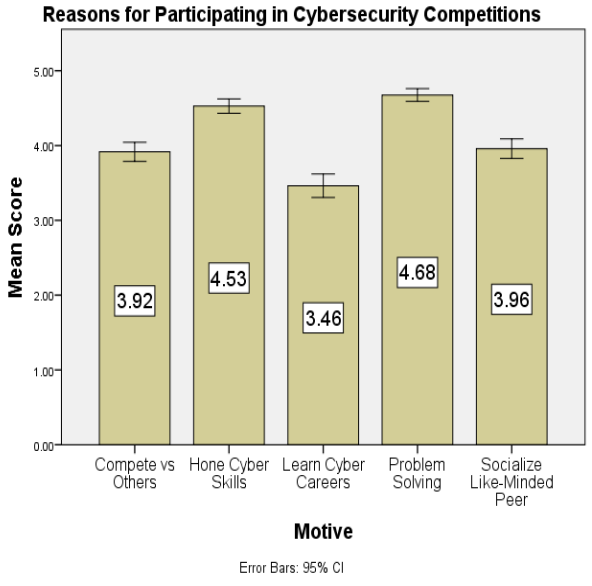

Figure 1. Graph showing participant endorsement of reasons for participating in cybersecurity competitions. Error bars indicate 95% confidence intervals.

Further analysis of the motivations for participating suggests that the primary motivation for participation changes with the number of times a participant attends CSAW. Participants who attended CSAW for the first time were motivated to learn about cybersecurity careers much more than participants who were returning for the third time or more (3.81 vs 3.17, $t = 3.13$, $p < .01$). This suggests that career fairs and recruitment efforts might be best directed at first-time attendees of cybersecurity competitions. Although the difference did not reach statistical significance, there was a trend where socializing with peers became increasingly important as a reason for participating in subsequent cybersecurity competitions. This could be due to friendships formed and maintained during the first time at the competition.

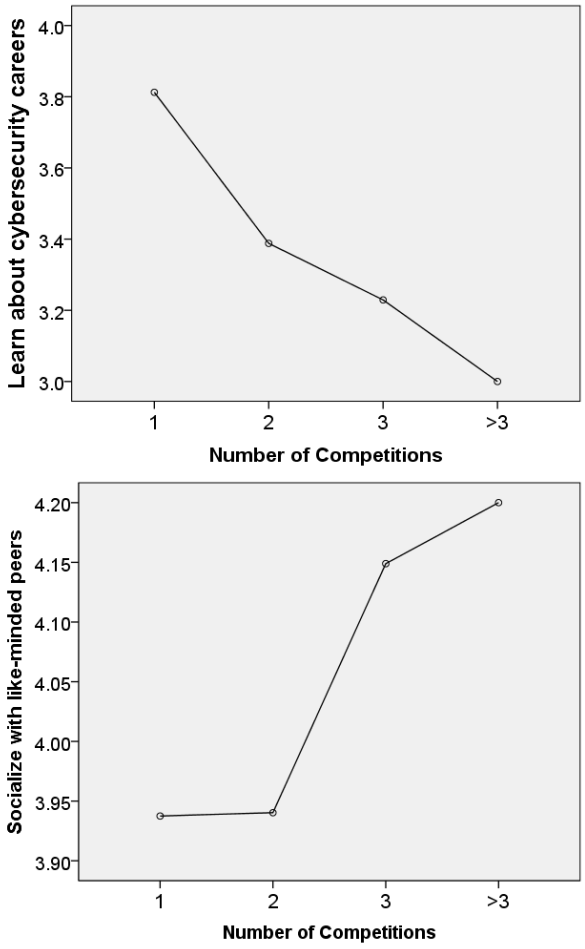

Figure 2. Graphs of mean motivation for participation against number of competitions for Career and Socialization motives.

4.3 Self Efficacy and Self-Esteem

Table 3 shows the means, standard deviations, and correlations between self-esteem, generalized self-efficacy, specific self-efficacy in cybersecurity tasks, and specific interests in cybersecurity tasks. Our measure of specific self-efficacy was highly correlated with general self-efficacy, and less correlated with self-esteem, establishing convergent and discriminant validity. In agreement with Hypothesis 1, specific efficacy in cybersecurity tasks was significantly related to interests in cybersecurity (r = .16) but the relationship was only a small one. Nevertheless, the significant correlation agrees with Tracey's (2010) reported relationship between career self-efficacy and interest congruence.

	N	M	SD	1	2	3	4
1. Self-Esteem	190	3.0	.57	*.89*			
2. GSE	192	4.1	.59	**.55**	*.90*		
3. Spec. Interest	195	3.7	.56	**.16**	**.30**	*.86*	
4. Spec. SE	193	3.4	.63	**.29**	**.47**	**.16**	*.91*

Table 3. Correlations between self-efficacy, self-esteem and interest measures.

4.4 Self Efficacy and Competition Outcomes

Table 4 shows the means, standard deviations, and correlations between self-esteem and self-efficacy variables with measures of competition success and positive experience. Hypothesis 2 predicted that self-efficacy would be a good indicator of competition performance and positive perceptions regarding competition effectiveness and appeal. By and large, this hypothesis was supported. For both metrics of competition performance, participants with higher specific self-efficacy in cybersecurity, but not general self-efficacy or self-esteem, were more likely to pass the qualifying rounds (r = .17, p = .02) and report higher competition scores (r = .24, p = .01). Participants with high self-esteem and self-efficacy (both specific and general) were more likely to be satisfied with their performance in the competition. Hypothesis 3 predicted that self-efficacy would be a good indicator of participant perceptions of competition effectiveness. This hypothesis was also supported. Participants with higher general self-efficacy and self-esteem were more likely to report that the competition was effective at recruitment (r = .26, p < .01) and increased the appeal of cybersecurity to the public (r = .27, p < .01). This relationship was absent for specific self-efficacy in cybersecurity tasks. Contrary to Socio-Cognitive Theory (Lent, 2005), participants with higher self-efficacy were not more likely to report that the competition was a major factor in influencing their career choice. This could be due to the phrasing of the question on career influence—"Competitions were a *major factor* in influencing your career decision". The phrase "major factor" might have occluded the true relationship between career influence and self-efficacy because it forces consideration of relative importance of other factors.

	M	SD	Self Esteem	GSE	Spec. SE
Qualifying vs. Final Round	1.17	.37	.10	.13	**.17**
Competition Score	1746.20	1455.68	-.12	-.05	**.24**
Recruitment effectiveness	3.88	.95	**.27**	**.26**	.09
Public appeal	3.73	1.01	**.18**	**.27**	.12
Career influence	3.59	1.17	.09	.07	-.03
Useful skills learned	4.30	.82	**.23**	**.30**	**.16**
Satisfaction with competition performance	3.25	1.03	**.34**	**.30**	**.24**

Table 4. Correlations between self-esteem, self-efficacy and competition outcomes.

The results here suggest that participants with higher confidence in performing cybersecurity tasks would most likely do well and be satisfied with their performance in cybersecurity competitions. Participants' performance on the competition would not necessarily mean that they found the competition effective or influential on their career decisions. In fact, there was no significant relationship between competition score and the extent to which participants felt the competition was effective or appealing. However, participants who reached the final rounds were more likely to report that the competition was a major factor influencing their career decisions (r = .20, p < .01) and that competitions were an effective tool for recruitment (r = .16, p = .03). Overall, specific self-efficacy was more related to competition performance than general self-efficacy, but general self-efficacy was related to post-competition perceptions such as public appeal, skills learned, and recruitment effectiveness.

4.5 Self Efficacy and Work Outcomes

Hypothesis 4 predicted a significant positive relationship between self-efficacy and self-esteem variables with job satisfaction, while Hypothesis 5 predicted a similar positive relationship with perceived organizational fit. Both these hypotheses were supported within the context of cybersecurity jobs. There was a positive relationship of similar magnitude between both specific and general self-efficacy and job satisfaction ($r = .32$, $p < .01$) and perceived organizational fit ($r = .37$, $p < .01$). Only self-esteem was not significantly related to perceived organizational fit.

	N	M	SD	Self Esteem	GSE	Spec. SE
Job Sat.	88	.72	.40	**.29**	**.33**	**.32**
Perceived Fit	87	3.77	.65	.18	**.37**	**.37**

Table 5. Correlation between self-esteem and efficacy variables with Job Satisfaction and Perceived Organizational Fit.

The establishment of the efficacy relationship with important work outcomes in cybersecurity organizations is an important step to highlight the value of cybersecurity self-efficacy as a predictor variable for these outcomes. Specific self-efficacy in cybersecurity is both related to competition performance outcomes and useful job outcomes. Researchers and employers alike would thus benefit from further exploring the utility of this individual difference in cybersecurity contexts.

5. Limitations & Future Work

One of the limitations of this study is that there was selection bias within the population of competition participants. Since the survey relied on self-report and was voluntary, participants who felt detached or had negative experiences in the competition would more likely not participate at all rather than provide us with their data. This could have resulted in an inflated relationship in the evaluation of competition effectiveness. Participant responses were also retrospective in nature, thus their memory of the competition could have differed from their initial impressions while competing. Future studies can utilize interviews during the competition itself to gather more qualitative data on the benefits of participations in the competition.

Another limitation of this study is that we are unable to establish temporal precedence between self-efficacy traits and competition or work outcomes. This prevents us from concluding that boosting self-efficacy in cybersecurity can directly cause better performance and satisfaction within cybersecurity competitions and cybersecurity workforce. It is thus important that longitudinal field experiments be conducted with behavioral interventions that are designed to temporarily raise an individual's general self-esteem or self-confidence, as well as specific efficacy in cybersecurity tasks. Measuring work and performance outcomes after these interventions can provide even stronger evidence for the importance of self-efficacy in cybersecurity competitions and cybersecurity work. Convincing participants that they are capable of handling difficult cybersecurity challenges may be one way to enhance the appeal and recruitment rate of new cybersecurity employees from cybersecurity competitions.

6. Conclusion

This paper presents empirical findings on the differential relationships between generalized self-efficacy and a more specific form of self-efficacy for cybersecurity tasks. Specific self-efficacy was better at predicting competition performance than general self-efficacy or self-esteem, but was unrelated to participants' positive image of competitions and whether or not the cybersecurity competitions influenced their career decisions. Instead, general self-efficacy was a better predictor of positive competition experience. Participants with higher general self-efficacy were more likely to judge the competition favorably, rating it as an effective recruitment tool that teaches useful skills and portrays the field in a positive light. When preparing their students for competitions, educators should pay greater attention to the confidence levels and interest of their students and take steps to keep students involved and interested. Competition organizers may wish to design activities that can enhance individuals' self-confidence in general and they will likely be able to attract more people and cause more people to consider cybersecurity careers post-competition.

This paper also shows that participant motivations for joining cybersecurity competitions primarily revolve around honing skills and problem solving, and that learning about cybersecurity careers may be a salient motive for first-time participants of competitions but this reason becomes less important for those attendees of higher frequencies.

References

A. Bandura, A. (1994). Self-efficacy. In V. S. Ramachaudran, Ed., *Encyclopedia of Human Behavior*, Vol. 4, 71–81. New York: Academic Press.

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

C. Bashir, M., Wee, J. M. C., and Memon, N. (2016). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Under review at Computers and Security*.

D. Cable, D. M., & DeRue, D. S. (2002). The convergent and discriminant validity of subjective fit perceptions. *Journal of Applied Psychology*, *87*(5), 875-884.

E. Chen, G., Gully, S. M., & Eden, D. (2004). General self-efficacy and self-esteem: Toward theoretical and empirical distinction between correlated self-evaluations. *Journal of Organizational Behavior*, *25*(3), 375-395.

F. Gavas, E. and Memon, N. (2012). Winning cybersecurity one challenge at a time. *IEEE Security and Privacy*, *10*(4), 75-79.

G. Ironson, G. H., Smith, P. C., Brannick, M. T., Gibson, W. M. & Paul, K. B. (1989). Construction of a job in general scale: A comparison of global, composite and specific measures. *Journal of Applied Psychology*, *74*, 1-8.

H. Judge, T. A., & Bono, J. E. (2001). Relationship of core self-evaluations traits—self-esteem, generalized self-efficacy, locus of control, and emotional stability—with job satisfaction and job performance: A meta-analysis. *Journal of Applied Psychology*, *86*(1), 80.

I. Judge, T. A., Hulin, C. L. & Dalal, R. S. (2009). Job satisfaction and job affect. In S. W. J. Kozlowski, Ed., *The Oxford Handbook of Industrial and Organizational Psychology*, Vol. 1, 496–526. New York: Oxford University Press.

J. Lent, R. W. (2005). *A social cognitive view of career development and counseling.* John Wiley & Sons Inc. Hoboken, NJ.

K. NICCS: National Institute for Cybersecurity Carers and Studies. (2015). Cybersecurity Competitions. Retrieved online September 11, 2015 from https://niccs.us-ert.gov/training/tc/search/cmp/new.

L. Rosenberg, M. (1965). *Society and the adolescent self-image.* Princeton, NJ: Princeton University Press

M. Rounds, J. & Su, R. (2014). The nature and power of interests. *Current Directions in Psychological Science*, *23*(2), 98-103.

N. Smith, P. C., Balzer, W. K., Brannick, M., Chia, W., Eggleston, S., Gibson, W., et al. (1987). The revised JDI: A facelift for an old friend. *The Industrial-Organizational Psychologist, 24*, 31–33.

O. Stajkovic, S.G. & Luthans, R.A. (1998). Self-efficacy and work-related performance: A Meta-Analysis. *Psychological Bulletin*, *124*(2), 240-261.

P. 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.

Q. Tracey, T. J. G. (2010). Relation of interest and self-efficacy occupational congruence and career choice certainty. *Journal of Vocational Behavior*, *76*, 441-447.