Information & Security

L. Pitman & B. Payne
vol. 54 (2023): 7-24
https://doi.org/10.11610/isij.5403

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

The C-factor in the Cybersecurity Equation: The Importance of Student Cybersecurity Competitions

Lora Pitman [1] (✉), *Brian Payne* [2]

[1] *Department of Intelligence and Security Studies, Coastal Carolina University, Conway SC, United States, https://www.coastal.edu/index.php*

[2] *Old Dominion University, Norfolk VA, United States, https://www.odu.edu*

ABSTRACT:

This study explored the role of cybersecurity competitions for students' knowledge, skills, and future interest in participants in these events. The authors conducted a survey of 41 Virginia students, registered to participate in two cybersecurity competitions in November 2021 and in April 2022. The sample includes high-school and college students, who were asked questions which can be divided in three conceptual categories: 1) experience with prior cybersecurity competitions; 2) experience with the most recently attended one at the time of the survey; 3) interest in taking part in future ones. The results from the survey reveal some intriguing patterns regarding the students' demographics, particularly regarding first-generation students, some benefits from the cybersecurity competitions, skills that such activities help develop, the most appealing aspects of them for students, and the opportunity to interact with people of a different race/ethnicity. A discussion of the results is provided along with recommendations how such competitions can be better organized to serve the needs of the participants and encourage them to pursue a career in the field.

ARTICLE INFO:

RECEIVED: 18 JAN 2023
REVISED: 10 May 2023
ONLINE: 26 MAY 2023

KEYWORDS:

cybersecurity education, cybersecurity competitions, cybersecurity skills

✉ E-mail: lpitman@coastal.edu

Introduction

A report by the International Information System Security Certification Consortium from 2021 shows that the cybersecurity workforce needs to grow by 65% in order to satisfy the demand for skills on the job market.[1] In an article for the Cybercrime Magazine, Steven Morgan [2] forecasts that there will be 3.5 million unfilled cybersecurity jobs in 2035. These statistics are no surprise as the lack of cybersecurity talent has been well-documented and continues to grow. A Pew Research Center survey [3] highlights some of the barriers to supplying the workforce with the much-needed professionals - the top two reasons why students interested in STEM did not pursue a degree/career in the field were time and financial obstacles for students to go/remain in college and lack of interest in the field.[4] The loss of such students is significant as data shows that nearly half of the students who intended to graduate with a STEM-degree switched to another major, with their number even higher in community colleges.[5]

While this study pertains to the students in the U.S., similar agencies tracking the enrollment numbers in U.K. colleges, such as the Higher Education Statistics Agency (HESA) point to the same tendency – computer science was the most abandoned major, followed by business and engineering.[6] In South America, only 15% of the college graduates earn a STEM-degree in Brazil, 14% in Argentina, and 13% in Colombia.[7] However, not all countries have low STEM graduation rates. According to a UNESCO study published by Statista,[8] the top countries producing STEM-degree graduates are Tunisia, Germany, Singapore, India, and Russia. Since this study does not include China, some context needs to be added as well to these results as it is reported to have a high number of STEM-graduates – China awards 77,000 STEM doctoral degrees per year compared to only 40,000 in the U.S.[9] The comparison between the number of STEM-graduates per country needs to be interpreted with caution as differences in the quality of the education itself. In a study from 2021, Loyalka and colleagues [10] juxtapose the skills that STEM students receive during their college time in the U.S., China, India, and Russia. They find that these differences are notable, as students in China, India and Russia do not acquire the same level of critical thinking skills as the students in a four-year STEM-program in the U.S. At the same time, students in India and Russia develop academic skills in STEM in the first two years of their college program, contrary to those in China.

Considering these quantitative and qualitative dimensions of STEM education in general, one goal becomes apparent - to research ways to spark and retain interest in STEM fields, particularly cybersecurity, considering the growing need for talent. The latter could be a challenging task especially when it comes to attracting low-income students who often face financial and time barriers, and minority groups, frequently encountering cultural and other barriers. Moreover, efforts need to be concentrated on how to provide such students with a multifaceted cybersecurity education that will not only help increase the graduation rates but also will distinguish itself with its inclusive and rewarding institutional culture.

To serve this purpose, the current study is centered around cybersecurity competitions as a means to ignite, retain and increase student interest in the field of cybersecurity, while at the same time helping participants develop technical, social and critical-thinking skills that will shape them as accomplished professionals filling the growing cybersecurity talent gap. The main research question we pose is how the experience of cybersecurity competitions can be further improved, be made more efficient and inclusive. We addressed this question though gathering data about the profiles of participants in such competitions, to what extent are cybersecurity competitions helpful to them, and which components are most helpful. The study is based on a Likert-scale survey, of 41 high-school and college students, participating in cybersecurity competitions We derived the results from this study quantitatively through a descriptive analysis of the data. Through this research, we aim to continue to monitor demographic patterns of participants in cybersecurity competitions and to fill a gap in the scholarship about more specific skills that students may value and which they may potentially obtain from their involvement in these events.

Background

There is a growing body of literature on cybersecurity competitions since 2014 after Tobey, Pusey, and Burley [11] observed that there was a need but also a lack of such research. The most recent scholarship on the issue demonstrates their importance for the professional growth of the participants in them and for the field of cybersecurity itself. Theoretically, the themes that appear in these large- and small-scale quantitative and qualitative studies can be divided into two groups: studies devoted to the characteristics of the competitors and some of the difficulties standing in their way to becoming such, and studies devoted to the effects of the competitions to the development of skills and their application in the cybersecurity field.

Characteristics of Cybersecurity Competitors and Obstacles

Surveying participants from the Cybersecurity Awareness Week competition, a research team, led by Bashir [12] discovered some patterns in the competitors' educational level – 50% of them were undergraduate students, 29% were high-school students, and 17% graduate students. At the same time, only 15% of the participants were women but the authors underline that at the time the percent of women employed in the field was even lower (6%). Other notable conclusion from the same study pertaining to race/ethnicity is that the number of African American, Hispanic, and Latin American students also fell significantly when undergraduate and graduate students were considered. However, the researchers observe that the diversity in the cybersecurity competitions was much higher than the diversity of the field itself. As for meeting the competitors' expectations, most of them confirmed that they participated in such competitions before, they acquired new skills, and would recommend participating to a friend. Lastly, the same study pointed to an interesting tendency – of those who responded that the cybersecurity competition changed their plans or at least to

some extent, 86% declared an increased likelihood of pursuing a career in the field.

Focusing on the same CSAW competition, Bashir, and colleagues [13] found that those who were working efficiently on their own, showed good decision-making and investigative curiosity were also the ones who expressed increased interest in a cybersecurity career. They also link their results to a recommendation for cybersecurity competition organizers to tailor the events in a way to attract more participants with the highlighted characteristics as those would be the ones more likely to pursue a career in the field.

Another group of authors, explores the experience of cybersecurity competitors from a longitudinal lens that concentrated on a smaller number of only 11 undergraduate students.[14] The authors of the study were able to list some intriguing patterns by providing a more detailed account on the question what the barriers were for students who were just beginning to participate in such competitions encounter. Most frequent obstacles cited by students involved anxiety about approaching new challenges for which they felt unprepared, but they also mentioned that consistent training how to use different tools along with peer-mentoring by more experienced competitors helped them overcome this.

The same concerns about the involvement of first-time cybersecurity participants are also expressed by Jelena Mirkovic and her colleagues.[15] They decided to alleviate the problem with a two-folded approach: conducting an in- class Capture-the-Flag exercises (CCTFs) in an introduction-level course and organizing a theoretical Capture-the-Flag event that was supposed to walk the participants through the steps of an actual competition, as some of the elements were brainstormed collectively to increase engagement.

An integral part for the success of the participants in cybersecurity competitions is also the structure of the team. La Fleur, Hoffman, Gibson and Buchler [16] focused on team performance and found empirical support that "factors such as experience-level, exposure to challenge-based cyber simulation training, and skills role composition" are crucial for the outcome of teamwork. These findings shed light on how the cybersecurity field where teamwork is very common can learn from the factors making a cybersecurity competition team successful. At the same time, these insights can be used in an academic setting so that students are better equipped with skills to be highly efficient team-members in such events and in their future careers.

Benefits and Further Improvement of Cybersecurity Competitions

The concerning shortage of qualified cybersecurity professionals has left many researchers to explore ways in which this problem can be fixed. Michael Dunn and Laurence D. Merkle are another group of scholars who seek a solution in cybersecurity competitions. A study by them addresses the question whether such events are capable of increasing the interest in cybersecurity, particularly for women whose numbers in the field are notably low.[17] Their findings demonstrate not only that participation in such competitions increases interest in the

field, but this is especially true for female participants who showed an even higher rate of willingness to join the field than their male counterparts.

Aware of the overall advantages that cybersecurity competitions offer to participants, Manson et al.[18] noticed some inconsistencies across events pertaining to definitions and concepts in various types of competitions, such as "Capture-the-Flag", "Hack-a-ton", "Build-it, Break-it, Fix-it" and others. Their proposed response, part of the more comprehensive initiative of a Cybersecurity Competition Federation, is to adopt a "common lexicon…for the diverse set of activities and events that constitute the current landscape of cybersecurity competitions".[19] They elaborate by detailing the kind of characteristics for which each competition should provide information – level of knowledge, ability and skill needed for the competition, the fields to which the competition is relevant, whether the competition is individual or a team one, and who is eligible to participate in terms of educational and professional level, age, and certifications.

Efforts to make the cybersecurity competition structure a more well-organized one date back to 2005 and even prior to this, as the National Science Foundation (NSF) sponsored a workshop called Cyber Security Exercise Workshop with the clear goal for "educators, students, and government and industry representatives… [to assess] the feasibility and desirability of establishing regular cybersecurity exercised for postsecondary-level students".[20]

Over time, the value of cybersecurity competitions for students has been further established. In a study from 2012, Efstratios Gavas, Nasir Memon and Douglas Britton [21] emphasize not only the technical expertise from which participants benefit, but also the interpersonal and other social skills that they develop such as professional networking, teamwork, and cooperation. At the same time, such events help educators bridge the gap between theory and practice as "cybersecurity challenges are multifaceted, they allow for extra-curricular explore to topics not discussed in the classroom owing to time or resource constraints".[22] In addition to this, the authors argue that cybersecurity competitions also provide a safe environment in which participants can practice their skills. However, Chris Eagle [23] underscores that the mere participation in cybersecurity competitions is not a recipe for success by itself as "rarely do teams receive a detailed critique of their performance, which is essential in addressing weaknesses exhibited during the competition".[24] Eagle's warning should be used by competitions' designers to increase the educational value not only for the winning teams, but also for the ones who did not finish among the top-participants/teams. Peng et al.[25] propose another method to work toward the same goal – through visualization of cybersecurity competitions for spectators. This way, they claim, viewers will have the opportunity to get educated and those who are new to the field can get interested in it and choose to pursue a cybersecurity-related education and subsequent career in the same sector.

To bring some more helpful insights for how to preserve the interest of students in the field of cybersecurity, a research team, led by Bertrand [26] analyzes cybersecurity competition participants' experiences in such events through social media. They found that online communities, such as Reddit, can be a safe

space for people to ask and receive advice, exchange expertise, and increase involvement in cybersecurity competitions. The authors discovered that participants very frequently inquired about the career path they are considering and sought information for it online. Therefore, they suggest that larger events should include not only competitions and training sessions, but also seminars pertaining to the topics of interest to the participants. Another recommendation that they make is to increase the awareness of cybersecurity competitions nationwide, as attention to such events is still mostly generated from the metropolitan areas. Moreover, special attention needs to be paid to attracting first-generation students and other underrepresented groups. Pusey, Gondree, and Peterson [27] also remind academics and practitioners the need for inclusion of underprivileged groups of participants and meeting their needs, as "competitors tend to be male, Caucasian, third-generation Americans with a high socio-economic status".

In light of these patterns, the present study seeks to explore whether the demographics of the participants in cybersecurity competitions have changed, and whether the results from the survey of participants in a relatively small, regional cybersecurity competition overlap with the ones from other studies which were mostly derived from surveying participants in CSAW. Further details about the methods the authors employed can be found in the following section.

Methods

This study is based on survey of students who competed at two Capture the Flag (CTF) events - a hybrid one in November 2021 with 13 teams, including virtual and in-person participants, mostly from Virginia, and an in-person one in April 2022 with 23 teams, including participants exclusively from Virginia. The 41 respondents are students from high-schools, community and 4-year colleges in Virginia. Students had the opportunity to decide who wants to be on their team, but they were able to join one, in case they were alone or just work on their own. Teams had no more than four students and were given 5-6 hours to solve cybersecurity challenges related to different topics. The top 3 teams who solved most challenges received recognition and prizes.

The surveyed students, who participated in the two events were asked about their previous participation in cybersecurity competitions, the most appealing aspects of such competitions, their feedback for the one they most recently attended at the time of the survey in terms of preparation, assistance from professors, skills needed, benefits from the competition, interest in taking part in future ones and whether they think all students should be required to participate in competitions. In addition, they were also asked about their interaction during the competition with employers/businesses, people of other races and ethnicities, and people from different fields/majors. While the sample size is relatively small, allowing primarily for a descriptive analysis of the results, the variety of questions in the survey, the details about the events themselves, and the diversity of participants in terms of gender, race, institution, and experience allowed the authors to draw some important conclusions.

Results

Demographics of the Participants

The survey results pertaining to the participants' demographics, listed in Table 1 below, reveal patterns consistent with those for the field of cybersecurity in general when it comes to gender and race. The majority of the participants (78%) are male and only 22% of them are female; they are also mostly white (46.3%), as the percent of Black/African American (17.1%) and Asian (19.5%) is almost identical. Participants from other races/ethnicities accounted for 7.2% of all students who took part in the competition.

A very interesting finding is denoted by the percent of participants who are first-generation students. Almost half of them (46.3%) indicate that they do not have any parent who has a college degree and 12.2% that they have only one of their parents possessing a college degree. To put these results in a context, the percent of participants with both parents being college graduates is 36.6%. This is an important finding that highlights the importance of cybersecurity competitions as they appear to attract first-generation students, also from families where neither parent has a profession very close to the field of cybersecurity. The latter can suggest that such activities can serve to retain the interest in the field of first-generation students' and such not coming from families where one or both parents are occupied in cybersecurity or a related area. Further analysis of this part of the results will be provided in the discussion section.

As for the educational entity from which the students came, the majority of them came from the institution where the competition took place and where it was most advertised. While not very high, but still notable is the presence of high-school students (12.2%) in the competition, which is another indicator that cybersecurity competitions have the power to attract and retain students' interest in the cybersecurity field.

Respondents' Previous Experience with Cybersecurity Competitions

The results related to the students' previous experience with cybersecurity competitions further testifies about their potential to be a powerful tool for retaining their interest in the cybersecurity field and even attracting new ones. Combined, the percent of students who already participated in cybersecurity competitions prior to the one after which the survey was conducted is 80.4%. For 12.2% of all participants, this was the first time they take part in such competition. The majority of the respondents ranked in the top 3 teams in the two cybersecurity competitions (34.5%), a smaller percent in the top 5 teams (18.4%) and 31.6% outside of the top 5 teams. Additional numbers, shown in Table 2 indicate the percent of participants who did not know their ranking at the time the survey was conducted or did not have the opportunity to participate actively or at all due to unforeseen circumstances.

Table 1: Demographics.

Gender	
Male	78% (N=32)
Female	22% (N=9)
Race	
White	46.3% (N=19)
Asian	19.5% (N=8)
Black/African American	17.1% (N=7)
American Indian/Alaskan Native	2.4% (N=1)
Mexican	2.4% (N=1)
Egyptian	2.4% (N=1)
First Generation Students	
Students with no parents who have a college degree	46.3% (N=19)
Students with both parents who have a college degree	36.6% (N=15)
Students with a mother who has a college degree	9.8% (N=4)
Students with a father who has a college degree	2.4% (N=1)
Students not knowing if either parent has a college degree	4.9% (N=2)
Mother's Occupation	
Homemaker	26.8% (N=11)
Business manager/accountant/teacher/nurse/engineer	22% (N=9)
Administrative personnel/small business owner/reporter	12.2% (N=5)
Clerical worker/salesperson/technician	7.3% (N=3)
Machine operator/truck driver/service worker/waitress	4.9% (N=2)
Skilled manual employee/electrician/farmer/police officer	2.4% (N=1)
Disabled/Retired	2.4% (N=1)
Not applicable	19.5% (N=8)
Father's Occupation	
Skilled manual employee/electrician/farmer/police officer	24.4% (N=10)
Business manager/accountant/teacher/nurse/engineer	17.1% (N=7)
Machine operator/truck driver/service worker/waiter	14.6% (N=6)
Commissioned/non-commissioned officer/enlisted personnel	9.8% (N=4)
Administrative personnel/small business owner/reporter	4.9% (N=2)
Disabled/Retired	4.9% (N=2)
Not applicable	22% (N=9)
Educational Institution	
ODU	73.2% (N=30)
High school	12.2% (N=5)
TNCC	2.4% (N=1)
ECPI	2.4% (N=1)
Christopher Newport University	2.4% (N=1)
Attending evening classes	2.4% (N=1)
Prefer not to answer	2.4% (N=1)

Table 2. Participation in Cybersecurity Competitions.

Number of cybersecurity competitions in which the student participated	
Participated in 1-5 cybersecurity competitions	65.8% (N=27)
Participated in 6 or more cybersecurity competitions	14.6% (N=6)
Have not participated yet	12.2% (N=5)
Question was not applicable	2.4% (N=1)
Success in participants' most recent cybersecurity competition	
Top 3 teams	34.2% (N=13)
Top 5 teams	18.4% (N=7)
Outside of Top 5 teams	31.6% (N=12)
Did not participate at all or actively in the cybersecurity competition	7.9% (N=3)
Do not know their ranking yet	7.9% (N=3)

Respondents' Most Recent Experience with Cybersecurity Competitions

This section of the results, illustrated in Table 3a adds to understanding the students' most recent experience with cybersecurity competitions and includes data about questions related to the level of their preparation for the competition, level of interaction with people from different races/ethnicities, different majors, and employers, the level to which they find various aspects of the cybersecurity competitions more or less appealing, and level to which they find various skillsets developed by such competitions. Regarding the students' preparation for the events, the majority of respondents strongly agreed and agreed (65.9%) that they were adequately prepared for the competition. However, less students felt that their teachers/professors provided assistance to help them prepare for the competitions – only 9.8% strongly agreed and 41.5% agreed with this statement, as opposed to 48.8% who disagreed and strongly disagreed with the same statement. As for the competition itself, all respondents agreed and strongly agreed that it required them to use a variety of skills and knowledge, that by participating they learned something new about cybersecurity, that the competition provided real-world examples of problems outside of the classroom setting, and that they would participate in a similar competition again in the future. More nuanced are the responses to the question whether all students should be required to participate in competitions. Slightly more than half of the students agreed and strongly agreed with this statement (62.5%) and 37.5% of them disagreed and strongly disagreed.

Table 3a: Feedback on the cybersecurity competition and preparation of the students.

Statement	Strongly Agree	Agree	Disagree	Strongly Disagree
"I felt adequately prepared to participate in the cybersecurity competition."	29.3% (N=12)	36.6% (N=15)	31.7% (N=13)	2.4% (N=1)
"My teachers/professors provided assistance to help prepare me for the cybersecurity competition."	9.8% (N=4)	41.5% (N=17)	39% (N=16)	9.8% (N=4)
"The competition required me to use a variety of skills and knowledge."	80.5% (N=33)	19.5% (N=8)	0%	0%
"By participating in the competition, I learned something new about cybersecurity."	65.9% (N=27)	34.1% (N=14)	0%	0%
"The competition provided real-world examples of problems outside of the classroom setting."	51.2% (N=21)	48.8% (N=20)	0%	0%
"I would participate in a similar competition again in the future."	87.8% (N=36)	12.2% (N=5)	0%	0%
"All students should be required to participate in competitions."	27.5% (N=11)	35% (N=14)	30% (N=12)	7.5% (N=4)

The participating students were also asked some additional questions about the competition (shown in Table 3b), mainly focusing on their interaction with different people. The majority of the respondents (63.4%) assessed the extent to which they had the opportunity to interact with employers/businesses during the competition as "a great deal" and "somewhat". An even higher percent of

the students (87.8%) agreed that the competition provided an opportunity for them to interact with people from other races/ethnicities. Despite the lower number of respondents who characterized the extent to which they had an opportunity to interact with people with different fields or majors as "a great deal", a similar percent of them (80.5%) indicated that the competition still provided the opportunity to do so, even if only to some extent.

Table 3b: Additional feedback about interaction.

To what extent did you have the opportunity to interact with:	"A great deal"	"Somewhat"	"Not much"	"Not at all"
"Employers/businesses during the competition"	17.1% (N=7)	46.3% (N=19)	14.6% (N=6)	22% (N=9)
"People of a different race or ethnicity other than your own"	53.7% (N=22)	34.1% (N=14)	7.3% (N=3)	4.9% (N=2)
"People with different fields or majors"	24.4% (N=10)	56.1% (N=23)	7.3% (N=3)	12.2% (N=5)

Table 4 shows the respondents' opinion about the most appealing aspects of the cybersecurity competitions. According to the results, the most appreciated aspect, that enjoyed support from 90.2% of the students is the mental challenge that the cybersecurity competitions represent, followed by the help they provide to students to be better prepared in the future (70.7%), followed by the opportunity to showcase their skills (61%), the opportunity to work with teammembers (56.1%), the opportunity to meet with other competitors (51.2%) and to put their participation on their resume (48.8%). The lowest support among students generated the interest in playing computer games as a motivation to participate in the event (17.1%) and interest in the physical feeling of competition (14.6%).

The last set of results from the survey pertain to the skills/qualities that cybersecurity competitions help students develop. All respondents agreed that such events help students develop their computer skills "a great deal" or at least "somewhat". Among the other top 5 choices are also "problem-solving", "technical skills", being "detail-oriented" and the "ability to work in a team". While the other proposed options, shown in Table 5, also enjoyed a solid amount of support, there were less participants who rated their role as being "a great deal" or "somewhat".

Table 4: Most appealing aspects of the cybersecurity competitions.

Cybersecurity competitions aspect:	Percent of students sharing the view*
"The mental challenge"	90.2% (N=37)
"Help with being better prepared in the future"	70.7% (N=29)
"Showcasing skills"	61% (N=25)
"The opportunity to work with team-members"	56.1% (N=23)
"The opportunity to meet with other competitors"	51.2% (N=21)
"The opportunity to put on resume"	48.8% (N=20)
"Interest in playing computer games"	17.1% (N=7)
"Interest in the physical feeling of competition"	14.6% (N=6)

*Rated by respondents 4 and below on a scale from 1, being most appealing aspect to 8, being the least appealing.

Table 5: Students' ranking of skills that cybersecurity competitions develop.

Skill/quality:	Percent of students sharing the view (rated "a great deal" or "somewhat")
"Computer skills"	100% (N=38)
"Problem-solving skills"	97.5% (N=40)
"Technical skills"	94.7% (N=36)
"Being detail-oriented"	92.1% (N=35)
"Ability to work in a team"	90.3% (N=37)
"Creativity"	86.9% (N=33)
"Initiative"	81.6% (N=31)
"Flexibility/adaptability"	81.1% (N=30)
"Verbal communication skills"	78.9% (N=30)
"Strategic Planning skills"	78.9% (N=30)
"Work ethic"	78% (N=32)
"Interpersonal skills"	73.7% (N=28)
"Organization ability"	73.7% (N=28)
"Tactfulness"	68.4% (N=26)
"Written communication skills"	63.2% (N=24)
"Leadership skills"	57.9% (N=22)

Discussion

The following sections summarize the answer to our research question in this study – how cybersecurity competitions can be improved through an increased effectiveness and increased inclusiveness. Regarding demographics, the first part of the results corresponds with some general patterns in the field of cybersecurity and previous studies. While there are still more male participants in cybersecurity competitions than female (22%), the latter is commensurate with the overall estimates of women employed in the field of cybersecurity in the U.S. – 21.5%[28]. However, these numbers do not mean that continuous efforts to attract and retain more women in the field should cease. Other minority groups from the surveyed population, however, are more represented in this study's sample than in the workforce. For instance, the field has 72.6% of white employees, as opposed to only 46.3% in the two cybersecurity competitions where this survey was conducted; 8% of Black/African American employees vs. 17.1% in the cybersecurity competitions; 7.3% of Asian employees vs. 19.5% in the cybersecurity competitions[29]. These results show that cybersecurity competitions or this regional one, in particular, attracted more diverse talent than the workforce. This is also possible as the area itself has a more diverse population, but this makes it even more important that areas with diverse population develop cybersecurity talent and encourage students from minority groups to pursue careers in the field. Further studies need to be conducted to establish why people from minority groups, once interested in cybersecurity, decided not to pursue a career in the field.

The next set of results presents a very intriguing and positive tendency – a very high number of first-generation students who participated in the two cybersecurity competitions. Their number would be even higher if students with only one of their parents being a college graduate are considered. Moreover, a significant number of participants do not necessarily come from a family where one or both parents have a cybersecurity-related occupation (e.g., engineers, IT-specialists, etc.) These insights further bolster the assumption that cybersecurity competitions have the ability to offer an inclusive environment in which not only students from families where both parents have a college degree, specifically in STEM, are thriving.

As for the educational institution from which respondents are coming, regional competitions should provide the necessary conditions for participants from as more institutions as possible to be involved. In particular, such events need to be advertised ahead of time, and if possible, affordable accommodations should be offered to students who may need them and may not be able to afford them in case the event is an in-person one.

Another positive sign for cybersecurity competitions' ability to attract and retain talent is the number of respondents who have participated in more than one cybersecurity competitions previously (80.4%), but also those for whom the event was the first one of this kind (12.2%). Organizers of cybersecurity compe-

titions need to make sure that the needs of both first-time and returning competitors are met and every other competition that they attend enriches their professional preparation.

Regarding effectiveness of the cybersecurity competitions, while there is broad agreement among respondents that they felt prepared for the competition and that it provided real-world examples of problems outside of the classroom, more needs to be done by professors to prepare participants for such competitions. It is true that the majority of the respondents still agreed that professors and teachers assisted them in their preparation for the event, but the number can further improve in this category so that the percent of students who strongly agreed with this statement can outweigh the percent of those who just agreed. This assistance can be implemented either in class or through an additional workshop for students interested in joining such competitions.

Cybersecurity competitions should aim to provide students with the opportunity to interact with other participants from different fields/majors and from different races/ethnicities. To this extent, the two cybersecurity competitions satisfied this necessity, but when it comes to interactions with employers and businesses during the competition, there is room for improvement. Cybersecurity competition organizers should ensure that all of the elements of the cybersecurity talent pipeline are present in some form and the possibility of communicating with future employers is crucial.

A very interesting question from the survey inquired about the participants' most beloved aspect of the competition. Organizers of cybersecurity competitions need to focus on these most appealing features and discover ways to expand them to attract even more participants. Among them are the mental challenge, the opportunity to be better prepared in the future, to showcase skills, the opportunity for teamwork and to meet with other competitors. From another perspective, these components can be summarized in two groups – the chance to acquire/practice technical skills and the chance to acquire/practice social skills, as both groups were highlighted as very important, gaining more than 50% support among participants.

Lastly, respondents were asked about the skills/qualities that the cybersecurity competitions help them develop the most as they had to rank 16 skills/qualities important for a career in the field. The results from this question demonstrate areas in which cybersecurity competitions should aim to provide more to participants. In particular, along with the top 8 choices that respondents agreed that competitions help develop, organizers should aim to design the competitions in a manner that encourages more the enhancement of verbal communication skills, strategic planning skills, work ethic, interpersonal skills, organizational ability, tactfulness, written communication skills and leadership skills.

The results from the present survey reveal some important and positive patterns for the meaning of cybersecurity competitions but they need to be interpreted with caution due to the small sample size. More studies are needed to compare national and international cybersecurity competitions with regional

ones. Specifically, it needs to be compared whether participants feel less prepared at bigger competitions and more comfortable at smaller ones, whether high-school students, potentially prepared at a lower level in this stage of their life tend to participate less in bigger competitions, and whether the upwards tendency of increased participation by first-generation and by students potentially coming from lower-income families, showed in this study, will be preserved when bigger, national and international competitions are considered. For a more comprehensive analysis of the data, further large-scale quantitative studies need to be pursued, preferably in a non-US, international setting, so that results can be compared in cross-cultural context. In addition, qualitative analysis should also be incorporated, including focus groups and interviews.

Conclusion

The importance of the cybersecurity competition, as a concept, has been confirmed by various studies over the years. However, this does not mean that further efforts to maintain and even increase the value of such events should not be made. Furthermore, as the number of cybersecurity competitions organized across the U.S. and worldwide continues to grow, it is essential that research continues to compare the profile of the participants, their satisfaction, the skills that these competitions help develop, and what aspects should be enhanced so that the cybersecurity workforce does not lose talent at a time at which there is a serious shortage of cybersecurity professionals, but the need of such is only increasing.

The study in this paper aimed to contribute to this goal and to encourage other scholars to document the results of cybersecurity competitions at their institutions so that a comprehensive monitoring system can be eventually developed. The latter could help the public and the private sector significantly in terms of designing cybersecurity competitions that have clear guidelines and requirements, are inclusive and last but not least – bolstering participants' academic and professional preparation and their interest in joining or remaining in the field.

In addition to regular monitoring of cybersecurity competition aspects, researchers need to also focus on recommendations focusing on the stage before students decide to join cybersecurity competitions and after they started participating in such. In particular, how participants can be best prepared for them, and how their participation in such events can make them more capable and confident when they enter the job market. Special attention needs to be given to minority groups (first-generation, low-income students, women, people of color, and others), as studies, such as present one, show that cybersecurity competitions have the ability to attract them. Regardless, it is the cybersecurity community's responsibility to keep them in the field and make sure their career expectations are fulfilled and the profession gives them the opportunity to continue to grow through different initiatives, including cybersecurity competitions - the "C-factor" in the cybersecurity equation.

Acknowledgements

This research is supported in part by the National Science Foundation under grant DGE-1914613.

References

1 "International Information System Security Certification Consortium," (*ISC)2 Cybersecurity Workforce Study*, 2021, https://www.isc2.org//-/media/ISC2/ Research/ 2021/ ISC2-Cybersecurity-Workforce-Study-2021.ashx.

2 Steven Morgan, "Cybersecurity Jobs Report: 3.5 Million Openings In 2025," *Cybercrime Magazine*, November 9, 2021, https://cybersecurityventures.com/jobs/.

3 Brian Kennedy, Meg Hefferon, and Cary Funk, "Half of Americans think young people don't pursue STEM because it is too hard," Pew Research Center, 2018, https://www.pewresearch.org/fact-tank/2018/01/17/half-of-americans-think-young- people-dont-pursue-stem-because-it-is-too-hard/.

4 Kennedy, Hefferon, and Funk, "Half of Americans think young people don't pursue STEM because it is too hard."

5 Steve Olson and Jay B. Labov, *Community colleges in the evolving STEM education landscape: Summary of a summit* (National Academies Press, 2012).

6 Karl Flinders, "Computer science undergraduates most likely to drop out," *ComputerWeekly.com*, August 1, 2019, https://www.computerweekly.com/news/ 252467745/Computer-science-undergraduates-most-likely-to-drop-out.

7 "Organisation for Economic Co-operation and Development (OECD)," *Education at a Glance 2017: OECD Indicators*, 2017, https://download.inep.gov.br/acoes_ internacionais/estatisticas_educacionais/ocde/education_at_a_glance/CN_Brazil_OECD_2017.pdf.

8 Katharina Buchholz, "Infographic: Where Most Students Choose STEM Degrees," *Statista Infographics*, 2020, https://www.statista.com/chart/22927/share-and-total-number-of-stem-graduates-by-country/.

9 Remco Zwetsloot, Jack Corrigan, Emily Weinstein, Dahlia Peterson, Diana Gehlhaus, and Ryan Fedasiuk, "China is Fast Outpacing U.S. STEM PhD Growth," (CSET Data Brief), Center for Security and Emerging Technology, 2021, https://cset.georgetown.edu/publication/china-is-fast-outpacing-u-s-stem-phd-growth/.

10 Prashant Loyalka, Ou Lydia Liu, Guirong Li, Elena Kardanova, Igor Chirikov, Shangfeng Hu, Ningning Yu et al., "Skill levels and gains in university STEM education in China, India, Russia and the United States," *Nature human behaviour* 5, no. 7 (2021): 892-904. https://doi.org/10.1038/s41562-021-01062-3.

11 David H. Tobey, Portia Pusey, and Diana L. Burley, "Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league," *ACM Inroads* 5, no. 1 (2014): 53-56, https://doi.org/10.1145/2568195.2568213.

[12] Masooda Bashir, April Lambert, Boyi Guo, Nasir Memon, and Tzipora Halevi, "Cybersecurity competitions: The human angle," *IEEE Security & Privacy* 13, no. 5 (2015): 74-79, https://doi: 10.1109/MSP.2015.100.

[13] Masooda Bashir, Colin Wee, Nasir Memon, and Boyi Guo, "Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool," *Computers & Security* 65 (2017): 153-165, https://doi.org/10.1016/j.cose.2016.10.007.

[14] Lindsey J. Thomas, Moises Balders, Zach Countney, Chen Zhong, Jun Yao, and Chunxia Xu, "Cybersecurity Education: From beginners to advanced players in cybersecurity competitions," *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, IEEE, 2019, pp. 149-151, https://doi: 10.1109/ISI.2019.8823310.

[15] Jelena Mirkovic, Aimee Tabor, Simon Woo, and Portia Pusey, "Engaging novices in cybersecurity competitions: A vision and lessons learned at ACM Tapia 2015," *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)* 2015, https://www.usenix.org/system/files/conference/3gse15/3gse15-mirkovic.pdf.

[16] Claire La Fleur, Blaine Hoffman, C. Benjamin Gibson, and Norbou Buchler, "Team performance in a series of regional and national US cybersecurity defense competitions: Generalizable effects of training and functional role specialization," *Computers & Security* 104 (2021): 10.

[17] Michael H. Dunn and Laurence D. Merkle, "Assessing the impact of a national cybersecurity competition on students' career interests," In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 2018, pp. 62-67, https://doi.org/10.1145/3159450.3159462.

[18] Daniel Manson, Portia Pusey, Mark J. Hufe, James Jones, Daniel Likarish, Jason Pittman, and David Tobey, "The cybersecurity competition federation," In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, 2015, pp. 109-112, https://doi.org/10.1145/2751957.2751980.

[19] Manson et al., "The cybersecurity competition federation," 111.

[20] Lance J. Hoffman, Timothy Rosenberg, Ronald Dodge, and Daniel Ragsdale, "Exploring a national cybersecurity exercise for universities," *IEEE Security & Privacy* 3, no. 5 (2005): 27-33, https://doi.org/10.1109/MSP.2005.120.

[21] Efstratios Gavas, Nasir Memon, and Douglas Britton, "Winning cybersecurity one challenge at a time," *IEEE Security & Privacy* 10, no. 4 (2012): 75-79, https://doi.org/10.1109/MSP.2012.112.

[22] Gavas, Memon, and Britton, "Winning cybersecurity one challenge at a time," 77.

[23] Chris Eagle, "Computer security competitions: Expanding educational outcomes," *IEEE Security & Privacy* 11, no. 4 (2013): 69-71, https://doi.org/10.1109/MSP.2013.83.

[24] Eagle, "Computer security competitions: Expanding educational outcomes," 71.

[25] Chao Peng, David Schwartz, Daryl Johnson, Bill Stackpole, Chad Weeden, Jacob Marcovecchio, Drake Richards, Chris Fogle, Christopher Brown, and Victoria Walrond, "Visualization for spectators in cybersecurity competitions," In *2020 IEEE Symposium on Visualization for Cyber Security (VizSec)*, IEEE, 2020, pp. 21-24, https://doi.org/10.1109/VizSec51108.2020.00009.

[26] Joshua Ian Bertrand, Alex Martakis, Hong Liu, Chen Zhong, and Jun Yao, "Exploring Participants' Views of Cybersecurity Competitions through the Lens of Social Media," In *2020 IEEE conference on cognitive and computational Aspects of Situation Management (CogSIMA)*, IEEE, 2020, pp. 155-162, https://doi.org/10.1109/CogSIMA49017.2020.9216073.

[27] Portia Pusey, Mark Gondree, and Zachary Peterson, "The outcomes of cybersecurity competitions and implications for underrepresented populations," *IEEE Security & Privacy* 14, no. 6 (2016): 90-95, https://doi.org/10.1109/MSP.2016.119.

[28] "Cyber Security Specialist Demographics and Statistics [2022]: Number Of Cyber Security Specialists In The US," *Zippia*, 2022, https://www.zippia.com/cyber-security-specialist-jobs/demographics/.

[29] "Cyber Security Specialist Demographics and Statistics [2022]".

About the Authors

Lora Pitman is an Assistant Professor in the Department of Intelligence and Security Studies at Coastal Carolina University. She holds a Ph.D. in International Studies, a Master's degree in Humanities and a Master's degree in Law. She has published multiple peer-reviewed articles, book-chapters, and reports with a focus on international security and cybersecurity.

Brian K. Payne is the vice provost for academic affairs at Old Dominion University, where he is tenured in the Department of Sociology and Criminal Justice. He is the author or co-author of more than 160 journal articles and seven books. He is also the founding Chair of the Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance (HRCyber).