Initial Steps Towards Assessing Cybersecurity Courses

Scott Bell
sbell@nwmissouri.edu

Northwest Missouri State University

Abstract - The past two decades have witnessed explosive growth of the Internet, cloud-based data storage, and the number of wireless connected mobile devices. This growth has led to a similar rise in cyber-related threats and in response, a dramatic growth in university offerings of cybersecurity related content.

This paper presents the background of, and results from, the third phase in the development of a tool which can be used to assess changes in student interest in, and self-efficacy towards, pursuing jobs or additional education in cybersecurity. This phase involved collection of data over two semesters, providing a larger sample size and initial evidence of useful outcomes.

The results are mixed, but the survey does show interesting initial results. With additional work, it has the potential to allow educators to approach future improvement of pedagogy in cybersecurity courses in a more scientific manner. This work provides a starting point for discussions among those interested in building stronger cybersecurity programs that produce strong graduates in this field.

Categories and Subject Descriptors

K.3.2 [Computers and Education]: *Computer and Information Science Education*

General Terms

Assessment, Security

Keywords

Education, Cybersecurity, Assessment

1 INTRODUCTION

The field of computing is growing at an incredible rate. Faculty are presented with the problem of trying to squeeze an ever-changing (and growing) list of topics into a static number of credit hours while still achieving consistent or improving outcomes. This is true among all of the various 'sub-fields' as well. The work presented here is a first step towards assessing student outcomes within a cybersecurity course. However, the approach used here could potentially be applied in other sub-fields within computing as well.

Over the span of two decades, the Internet and its associated technologies have grown to dominate all facets of daily life. Unfortunately, this rapid growth has led to a variety of problems for those trying to manage the supporting infrastructure. The quantity and magnitude of risks faced daily by users and resources connected to the Internet have grown as rapidly as the network itself. In response to this rising number of threats, industry and government entities have heightened their focus on improving the security measures within their respective domains. Unfortunately, the workforce needed to design, implement and maintain these plans is spread incredibly thin. Those of us managing the pipeline of students entering this field have been struggling to catch up with the growing demand for new, well-trained, cybersecurity professionals.

Faculty are hampered by both the need to teach a large number of highly technical skills and a limited (although growing) number of highly interested students. There has been tremendous innovation in the variety of training approaches available to meet this challenge. We have deployed online learning tools, incorporated new technologies such as virtualization within existing courses, hosted cyber-defense competitions, added entirely new courses to curriculum and even created new degree programs in order to train this new generation of cyber defenders. However, all of this has happened so quickly, and on such a wide and diverse scale, there has not been adequate time to assess the quality of these efforts. We don't have evidence that we are optimizing (or even truly improving) our ability to recruit, retain and graduate students within the area of cybersecurity. This paper presents the next step towards developing a tool capable of providing this critical feedback.

2 BACKGROUND

The field of cybersecurity education is a dynamic and growing environment. Demand for graduates with skills in cybersecurity is growing rapidly, with 91% growth in the number of job postings from 2010 to 2014 according to the 2015 Burning Glass Report [12]. While a few schools have been teaching security content for many years [5, 6], the field is a relatively new focus of study at many universities. As a result, there has been very little opportunity for assessment instrument development in this area.

At the international level, there has been significant effort made towards the development of curriculum and learning objectives within cybersecurity in recent years. The ACM-IEEE Computer Science curriculum committee, and the ACM Special Interest Group for Information Technology Education (SIGITE) committee have placed security at the center of their most recent recommended curriculum for both Computer Science and Information Technology [1, 14]. Cybersecurity topics are integrated throughout the suggested curriculum within both of these documents. These guidelines provide faculty with a relatively stable (though incredibly wide) base from which to develop curriculum for our courses. The next logical step is to begin assessing how well the courses are being received. Given that a primary goal of many of these new courses and programs is to encourage students to pursue jobs or additional education in cybersecurity, this work is a step towards developing a tool capable of measuring if these outcomes are being met.

When looking for models to base a cybersecurity assessment tool on, a good first place to look is within the field of Computer Science itself. There have been numerous efforts to assess academic quality within specific areas of Computer Science. Several studies have focused on introductory programming courses [7, 11, 13]. These typically assess student skill levels or comprehension of specific topics in order to measure the effectiveness of the classroom experience. While these efforts provide useful outcomes for their target courses, there are difficulties in adapting skill-based assessment tools to a rapidly changing area of study such as cybersecurity.

The knowledge and skills needed in this field can change significantly in a relatively short period of time and even from course to course, or job to job. This makes knowledge-based assessment impractical. By the time an assessment tool has been created and validated, the content would possibly be outdated and the process would need to start again. Additionally, a course may increase a student's desire to pursue further knowledge or a career within a field of study without achieving mastery in the subject matter. There has been significant work done investigating the factors affecting student self-efficacy and how improved self-efficacy can affect course performance in programming courses [9].

Looking at other options, studies performed in fields such as Chemistry and Physics have shown that self-efficacy based assessments can be used to identify growth in student interest and potential for entry into the field. Further, self-efficacy has been shown to be critical in time on task and persistence within a field of study [2, 8, 10]. The work presented in this paper shows the results from the initial implementation of an assessment tool which is currently under development for a cybersecurity course. This tool is being designed to provide educators with insight into the effects their courses are having on both student self-efficacy in relation to cybersecurity tasks and student interest in pursuing an academic or career path in cybersecurity. The target course for this instrument is an introductory cybersecurity course spanning a broad range of topics.

2.1 The Objective

It should be noted that this tool is not intended to measure course outcomes such as "*A student completing this course will be able to do X.*" This type of assessment can be effective in fields such as Mathematics or even in some of the introductory computer programming courses where the content of a given course is very well defined, and the outcomes are very similar throughout academia. There is little change expected over time within such courses, making topic-based outcome assessment useful. Currently, cybersecurity is taught in a variety of ways to a variety of depths and with a constantly changing list of topics. However, in every case, a consistent goal is to increase student interest and self-efficacy within the field, and thus the selection of these as the target metrics. The tool does include statements about basic topics, but from a different perspective: "*I would be able to do X*" Or "*it would take me a week to figure out how to do Y*". When finalized, the tool is expected to be useful in introductory computer security courses that cover a variety of topics. That being said, this tool might very well prove to be useful in other, more specialized, courses as well.

3 APPROACH

The development of this tool has progressed through multiple stages. The work has been performed at two universities. The first is a large R1 research university, and the second a small regional state university. One hindrance to assessing the courses at both schools has been the relatively low enrollment in individual courses. Some of the graduate level elective courses have enrollments between five and ten students each semester, making statistically significant data difficult to collect.

3.1 Qualitative Study

The first phase of this work was a qualitative study performed in an introductory cybersecurity course with 30 students enrolled. This course has mixed upper-level undergraduate and graduate enrollment. Given the relatively small enrollment numbers, and lack of research in this area, it was determined that this would be the best way to develop a list of topics that could potentially be used for assessing student outcomes within the course. Fifteen students volunteered to participate in the study which consisted of three rounds of interviews at the beginning, middle and end of the semester. Out of the initial volunteers, 12 completed all three rounds of interviews. Students were asked about their perceptions of the course, experiences within the course, motivations for taking the course and how they viewed cybersecurity as a whole. Students were also asked about their future career and academic plans as they related to cybersecurity.

Based on the outcomes of these interviews, it became apparent that examining self-efficacy and student interest in cybersecurity topics had the potential to provide valuable feedback to educators. Several specific topics which influenced student perceptions, participation and interest in cybersecurity were mentioned repeatedly by students during the interviews. A detailed explanation of the qualitative portion of this work can be found in previously published work [3].

3.2 Preliminary Survey Results

The second phase of this project involved the development and delivery of an initial pre / post survey. A set of 22 statements related to either a career or academic pursuit in cybersecurity was developed from the interview records collected during the initial qualitative study. The list of statements is shown in Table 1.

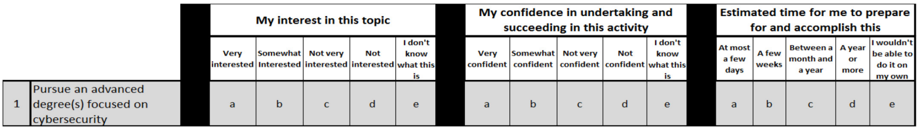
Q1	Pursue an advanced degree(s) focused on cybersecurity
Q2	Find ways to exploit vulnerabilities in existing software
Q3	Perform research focused on cybersecurity
Q4	Learn how to crack users' passwords
Q5	Take additional courses focused on cybersecurity

Q6	Discover ways to protect personal data on the Internet
Q7	Write software that is safe from buffer overflow attacks
Q8	Manage security for a Fortune 500 company
Q9	Implement a protocol to allow data to be sent securely over a network
Q10	Perform network penetration tests for companies
Q11	Learn how to use SSL certificates
Q12	Find a job which involves cybersecurity
Q13	Learn how to intercept and read network traffic
Q14	Write an algorithm that uses asymmetric encryption to authenticate a user
Q15	Work for an organization that researches ways to make computing more secure
Q16	Learn how to verify a digital signature
Q17	Have cybersecurity concepts incorporated into other courses that I take
Q18	Remove detected threats from a home computer
Q19	Read articles / web posts about cybersecurity on your own
Q20	Install and run malware checking software on a home computer

Q21	Learn how to detect cyber attacks
Q22	Find a job which is specifically oriented towards cybersecurity

Table 1: Statements included in survey

For each statement, participants are asked to rate their interest in the topic, confidence in succeeding at the task, and to provide an estimated time they felt they would need to prepare for and perform the task. Each of these ratings were measured on a four-point Likert scale, with a fifth option being included to allow participants to indicate they didn't know what the topic was or that they would not be able to complete the task. Figure 1 shows a sample question with the scales used from the survey.

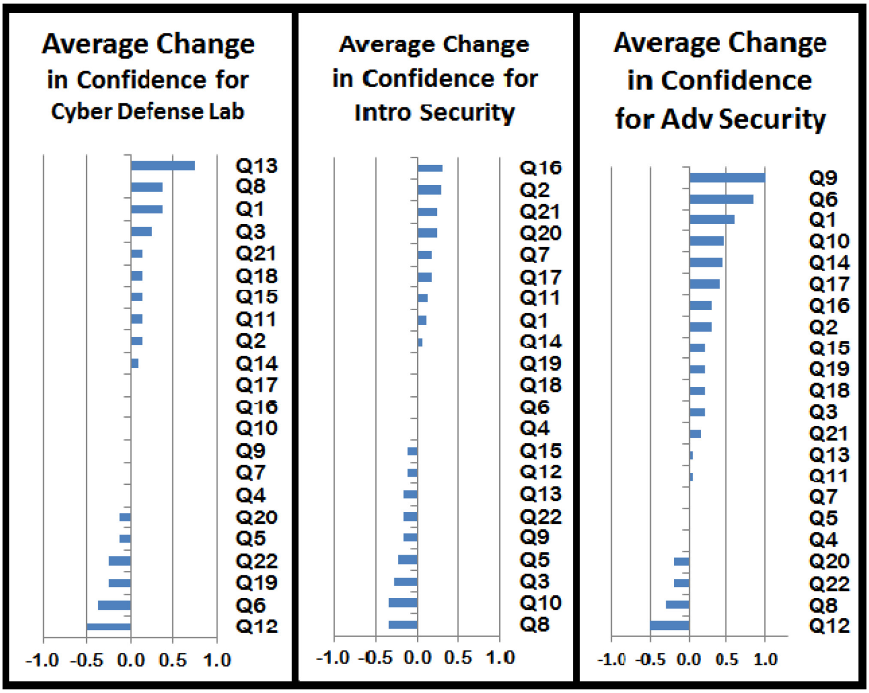


		My interest in this topic					My confidence in undertaking and succeeding in this activity					Estimated time for me to prepare for and accomplish this				
		Very interested	Somewhat Interested	Not very interested	Not interested	I don't know what this is	Very confident	Somewhat confident	Not very confident	Not confident	I don't know what this is	At most a few days	A few weeks	Between a month and a year	A year or more	I wouldn't be able to do it on my own
1	Pursue an advanced degree(s) focused on cybersecurity	a	b	c	d	e	a	b	c	d	e	a	b	c	d	e

Figure 1: Example of question format and options.

At the research university, students in three different cybersecurity courses with very limited enrollment and in a CS1 course with a much larger enrollment participated in the survey. The cybersecurity courses included one undergraduate course, one graduate course, and a cyber defense lab course which is designed for students wanting to participate in cyber-defense competitions. Several of the questions showed significant results, but given the very small sample sizes, it could not be said for sure that the results were valid. However, these initial outcomes did show that the approach may have merit. Additionally, it appeared that some of the questions likely needed to be modified in order to measure effect sizes more precisely. Comparing the results from students enrolled in the different courses also provided some insight into how students view cybersecurity at various points within their academic career.

Overall, this phase showed potential in helping faculty identify pedagogical components which increase student self-efficacy and interest in this subject. Figure 2 shows the average change in student confidence and self-efficacy by course for the cybersecurity courses. Further details of this initial trial can be found in previously published work [4].



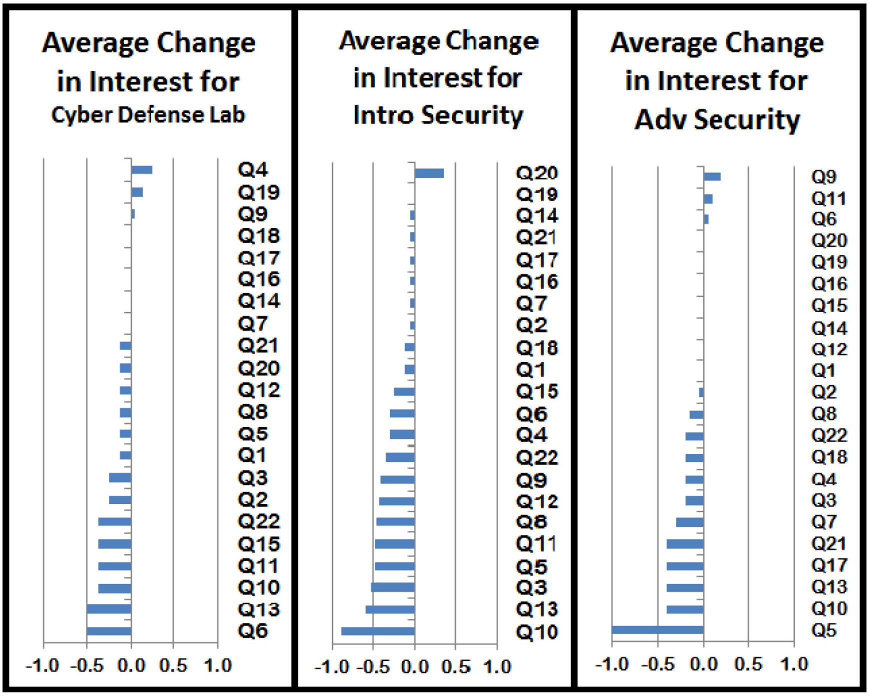


Figure 2: Average change in confidence and interest at research university

3.3 Initial Longitudinal Trial

Given the limited sample size of the preliminary trial, modifications were limited to slight rewording and reformatting of a few statements prior to the next set of surveys being performed. Additional data has now been collected in three sections of an introductory cybersecurity course at a regional state university. All three sections used the same reading and lecture materials, exams, hands-on laboratory assignments and online simulation assignments. Data from these surveys is shown in Figure 3. Enrollment in these courses was between 45 and 123 students per section. Two of the sections were taught by the same instructor (Spring 2015 Section 1 and the Spring 2016 section) while the third section (Spring 2015 Section 2) was taught by a different instructor.

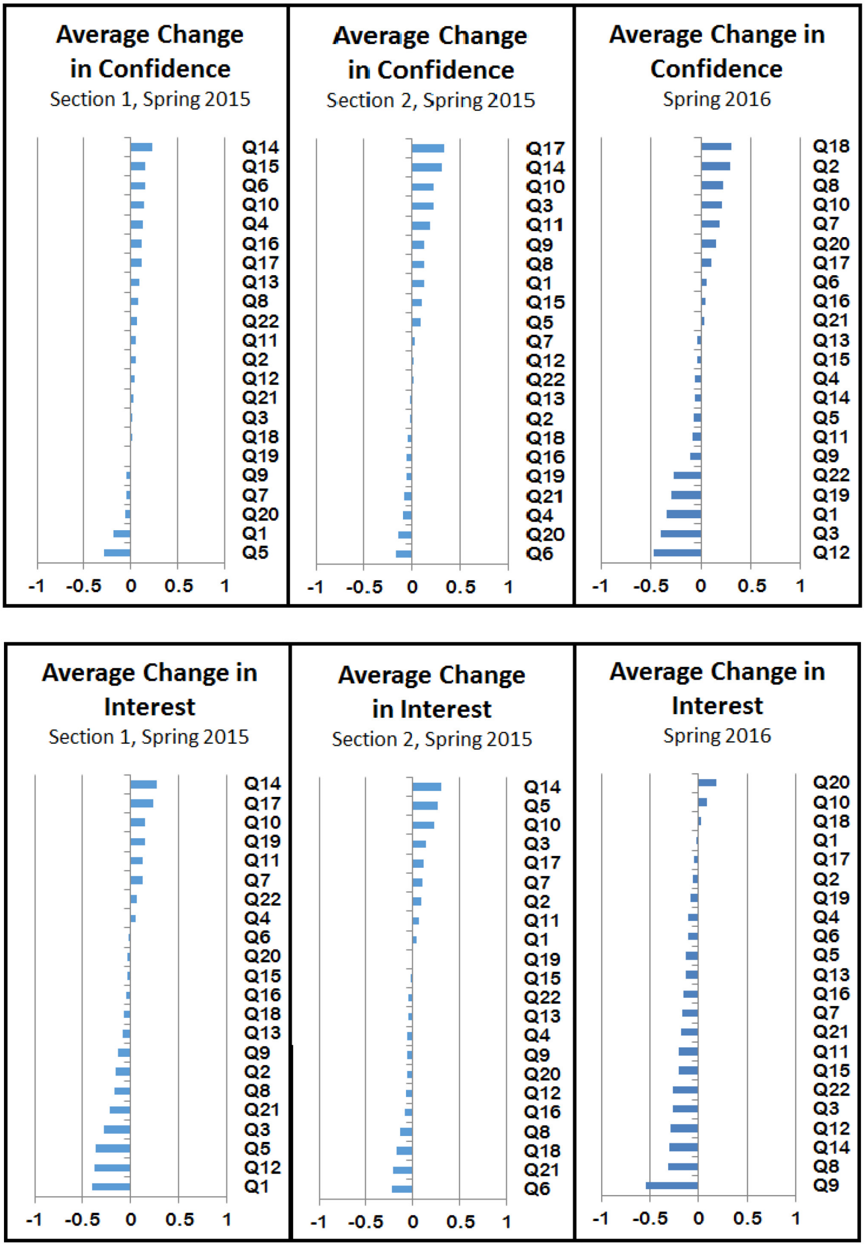


Figure 3: Average change in confidence and interest at regional university

This is a broad, survey type course which covers a large percentage of the topics included in the Security+ certification exam. The course is required for students enrolled in a master of applied computer science degree and satisfies an upper-division elective requirement for undergraduate students in a traditional computer science program. A course in networking is the only prerequisite, although the majority of undergraduate students enrolling in the course have had at least two semesters of programming prior to enrolling.

The primary goals of this phase of the project were to determine if the survey was capable of providing useful outcomes for instructors, and see how consistent the results would be between sections taught by the same instructor or two different instructors covering the same material. The surveys were administered by paper during the first and next to last weeks of the semester.

4 OUTCOMES

The results from the longitudinal trial were analyzed on a per-course basis in two ways. The first analysis was performed by calculating the average change for each item from the pre to post survey. This allows us to identify how student responses for each topic are changing over the duration of the semester within a specific course. For example, ’Perform network penetration tests for companies’ (Q10) showed a positive change for both interest and confidence in all three sections. Conversely, ’Find a job which involves cybersecurity’ (Q12) showed a negative change for both interest and confidence in all three sections. Using these outcomes, faculty can identify ways in which content and / or pedagogical methods for a given course are working and also determine where the course might be altered to produce better outcomes. The second analysis involved determining if the outcomes from these surveys were statistically significant. This will help identify outcomes which are actually showing real changes in student perspective versus those which are the result of random changes in student responses.

4.1 Average Chance

There are several interesting trends within the data that has been collected thus far, although few of them display consistent patterns between sections at this point. Here are several examples:

- Q14 had strong positive changes in both confidence and the Spring, 2015 sections but decreases for both in the Spring, 2016 section.
- Q10, and Q17 were in the top third in all three sections for change in both interest and confidence.
- Q8 rates in the bottom third for change in interest, but in or near the top third for change in confidence for all sections.
- Q19 rates in the top half for change in interest but the bottom third for change in confidence for all sections.
- Q15 rates in the top half for change in interest and confidence except for interest in spring 2016 (just below the midpoint).
- Q20 rates in the bottom half for change in interest and confidence for 2015 and the top third for 2016.
- Q13 rates in the middle third for change in both interest and confidence for all sections.
- Q12 rates in the bottom half for change in both interest and confidence for all sections.

Each of these outcomes leads to questions such as "What did we do right / wrong to cause that outcome and how can we maintain / fix these outcomes in future offerings of this course?" As an example of how this data might be used, student interest and confidence in finding a job in cybersecurity appears to be decreasing over the duration of this course in all sections. In an attempt to minimize or even reverse this negative impact, the instructor could invite a guest speaker who is able to discuss job opportunities in the field and help students understand how job searches and placement in this field are similar to and / or different from job searches for other fields.

4.2 Statistical Analysis

In order to identify statements that are providing statistically significant outcomes, or those that may need to be removed / altered to generate more consistent results, data from each of the three sections was analyzed using the Wilcoxon Signed Rank test. Those providing significant results ($p < 0.01$) from this analysis are shown in Table 2. As was mentioned above, the graduate courses sampled at the research university had enrollment numbers between five and ten students and thus were not analyzed in this way.

The results show that the survey is capable of detecting statistically significant changes for at least some of the items being sampled. An example of an interesting outcome from this analysis can be seen within the Spring 2016 results. Several statements displayed a significant positive change in the time value. A hypothesis from this outcome is that through their experiences in this course, students realize these tasks are not as time consuming / difficult as they perceived them to be at the beginning of the semester. Similarly, during the same semester, there were only 2 values related to student interest which showed a significant change, and both of these were decreases.

Given these outcomes, instructors can focus more on introducing ways these students could help solve these problems, and the benefits to society of doing so (and thus, hopefully, improving student interest). Such outcomes allow instructors to adjust content and teaching methods in an attempt to systematically improve student interest and confidence across the majority of these topics. Using this assessment tool, a long-term goal for such a course would be to minimize the number of topics which show significant decreases and maximize the number of topics which show significant increases.

item	**p value**	**effect size**
Spring 2016 (n = 46)		
Q2 confidence	< 0.05	0.310
Q3 confidence	< 0.05	-0.358
Q4 time	< 0.05	0.350
Q6 time	< 0.05	0.295
Q7 time	< 0.05	0.362
Q8 interest	< 0.05	-0.328
Q9 interest	< 0.01	-0.394
Q10 time	< 0.05	0.337
Q11 confidence	< 0.05	0.303
Q11 time	< 0.05	0.381
Q12 confidence	< 0.05	-0.370
Q14 time	< 0.05	0.351
Q16 time	< 0.01	0.406
Q19 confidence	< 0.05	-0.300
Spring 2015 Section 1 (n = 45)		
Q1 interest	< 0.05	-0.412

item	**p value**	**effect size**
Q5 interest	< 0.05	-0.359
Q5 confidence	< 0.05	-0.368
Q11 time	< 0.05	-0.361
Spring 2015 Section 2 (n = 123)		
Q3 time	< 0.05	0.208
Q5 interest	< 0.05	0.201
Q5 time	< 0.05	0.213
Q6 interest	< 0.01	-0.264
Q6 confidence	< 0.05	-0.184
Q8 time	< 0.05	0.181
Q9 time	< 0.05	0.218
Q10 interest	< 0.01	0.243
Q10 confidence	< 0.005	0.264
Q10 time	< 0.05	0.203
Q14 interest	< 0.005	0.316
Q14 confidence	< 0.005	0.317
Q17 confidence	< 0.005	0.282

item	p value	effect size
Q18 interest	< 0.05	-0.226
Q21 interest	< 0.01	-0.240
Q22 time	< 0.01	0.254

Table 2: Wilcoxin Signed Rank Results

5 FUTURE PLANS

Future efforts will be focused on adjusting survey statements to improve the ability to provide useful significant outcomes. Additional plans include testing pedagogical changes within target courses to see if student outcomes will reflect these changes.

Data will continue to be collected at both participating institutions. A new version of the survey is currently being developed. This new version will incorporate several changes based on observations and data from the initial phases. For example, due to the number of incomplete surveys, topics which are providing little to no significant outcomes and those providing duplicate outcomes, will be removed in an attempt to reduce the size of the survey. This was expected when the survey was initially designed as a broad range of topics was chosen in order to ensure that a wide range of factors were captured. An online version of the survey will also be used in the future, providing a more user-friendly interface.

While the survey shows evidence of interesting effects, additional data needs to be collected to provide better validation of these outcomes. In order to do this, use of this survey will be expanded to include other institutions offering similar courses. This should increase the evidence of the success or failure of topics and also help identify strengths / weaknesses in the instrument. As the survey matures, faculty will be able to share identified best-practices and subsequently measure outcomes to see if this transfer of pedagogy results in a similar transfer of student outcomes (which is our ultimate goal).

6 SUMMARY

Interest and self-efficacy in a given task have been shown to be instrumental in student development and in building a desire to pursue a given career in other fields. In order to more effectively identify course components and pedagogical practices that help build these outcomes within cybersecurity courses, we have developed a prototype survey based on results from both a longitudinal qualitative study and an initial trial application of the instrument. This paper presents results from a second set of applications of this survey showing changes in student interest and self-efficacy in relation to several topics from cybersecurity courses.

The survey has been used in three cybersecurity courses at a large research university and in three sections of a network security course at a regional state university. The results from these implementations of the survey demonstrate it's ability to identify some statistically significant changes in student interest and self-efficacy in relation to cybersecurity. It has also shown differences in student perspectives at various levels of academic maturity. With additional tuning and larger sample sizes, there is hope that this survey can become a tool for improving pedagogical methods within cybersecurity courses.

Survey instrument development will continue moving forward based on the outcomes presented here. The long-term objective of this work is to more precisely identify those topics which provide consistent and useful feedback concerning student outcomes from these courses. More consistent outcomes are expected from the survey instrument through broader sampling and minor adjustments to develop a more focused survey.

7 ACKNOWLEDGEMENTS

Thank you to the National Science Foundation and Department of Homeland Security for supporting part of this research through the CyberCorps Scholarship for Service program. Additionally, thank you to faculty members who allowed me to survey their courses:

- Dr. Eugene Vasserman, Kansas State University
- Dr. Xinming (Simon) Ou, University of South Florida
- Dr. Alexandru Bardas, University of Kansas
- Dr. Na Li, Prairie View A&M University

REFERENCES

[1] ACM-SIGITE. IT2008 model curriculum, 2013. Retrieved from http://www.sigite.org/.

[2] W. K. Adams, K. K. Perkins, N. Podolefsky, M. Dubson, N. Finkelstein, and C. E. Wieman. A new instrument for measuring student beliefs about physics and learning physics: The colorado learning attitudes about science survey. *Physical Review Special Topics-Physics Education Research*, 2:01–14, 2006.

[3] Bell, R.S., Vasserman, E. Y., and Sayre, E. C. (2014). A longitudinal study of students in an introductory cybersecurity course. *Proceedings of the 121st Annual ASEE Conference and Exposition*. 2014.

[4] Vasserman, E. Y., Bell, R. S., and Sayre, E. C. (2015). Developing and Piloting a Quantitative Assessment Tool for Cybersecurity Courses. *Proceedings of the 122nd Annual ASEE Conference and Exposition*. 2015.

[5] M. Bishop. Teaching computer security. In *Proceedings of the 9th IFIP International Symposium on Computer Security (IFIP/ SEC)*, pages 65–74, 1993.

[6] S. Cooper, C. Nickell, V. Piotrowski, B. Oldfield, A. Abdallah, M. Bishop, B. Caelli, M. Dark, E. K. Hawthorne, L. Hoffman, et al. An exploration of the current state of information assurance education. *ACM SIGCSE Bulletin*, 41(4):109–125, 2010.

[7] B. Dorn and A. Elliott Tew. Becoming experts: measuring attitude development in introductory computer science. In *Proceeding of the 44th ACM technical symposium on Computer science education*, pages 183–188. ACM, 2013.

[8] H. Fencl and K. Scheel. Engaging students: An examination of the effects of teaching strategies on self-efficacy and course climate in a nonmajors physics course. *Journal of College Science Teaching*, 35(1):20, 2005.

[9] V. Ramalingam, D. LaBelle, and S. Wiedenbeck. Self-efficacy and mental models in learning to program. In *ACM SIGCSE Bulletin*, volume 36, pages 171–175. ACM, 2004.

[10] K. Singh, M. Granville, and S. Dika. Mathematics and science achievement: Effects of motivation, interest, and academic engagement. *The Journal of Educational Research*, 95(6):323–332, 2002.

[11] C. W. Starr, B. Manaris, and R. H. Stalvey. Bloom's taxonomy revisited: Specifying assessable learning objectives in computer science. In *Proceedings of the 39th SIGCSE Technical Symposium on Computer Science Education*, pages 1–10. ACM, 2008.

[12] B. G. Technologies. Job market intelligence: Report on the growth of cybersecurity jobs. http://www.burning-glass.com, 2015.

[13] A. E. Tew. *Assessing Fundamental Introductory Computing Concept Knowledge in a Language Independent Manner*. PhD thesis, Georgia Institute of Technology, Atlanta, GA, USA, 2010. AAI3451304.

[14] The Joint Task Force on Computing Curricula Association for Computing Machinery (ACM) IEEE Computer Society. Computer science curricula 2013, 2013. Retrieved from http://ai.stanford.edu/users/sahami/CS2013//final-draft/CS2013-final-report.pdf.