International Education Studies; Vol. 13, No. 5; 2020
ISSN 1913-9020 E-ISSN 1913-9039
Published by Canadian Center of Science and Education

Student Learning Outcomes (SLOs) and Assessment of Cybersecurity Body of Knowledge (BOK): Evaluation & Challenges

Ala Alluhaidan[1] & Evon M. Abu-Taieh[1,2]

[1] College of Computer & Information Sciences, Princess Noura Bint Abdulrahman University, Saudi Arabia

[2] Computer & Information Sciences, The University of Jordan, Jordan

Correspondence: Evon M. Abu-Taieh, Computer & Information Sciences, The University of Jordan, Aqaba, Jordan.

Received: October 10, 2019 Accepted: January 4, 2020 Online Published: March 21, 2020

doi:10.5539/ies.v13n5p13 URL: https://doi.org/10.5539/ies.v13n5p13

Abstract

The rapid growth of technology and related fields has led to creation in academia to match the expansion demand for IT professionals. One of the current majors that attract attention in industry is cybersecurity. There is a great need for individuals who are skilled in cybersecurity to protect IT infrastructure. Coaching a security-focused workforce has become the target of government agents, industry, and academic institutions.

As research and academic faculties respond to this growing demand, evolving curriculum and methodologies for teaching cybersecurity graduates still need to be formed comprehensively. There have been few researches to define and assess the student outcomes in cybersecurity. This paper presents a step forward by developing Student Learning Outcomes (SLOs) and the desired assessment method to measure those outcomes.

This research contributes to academia and training institution by defining the SLOs and suggests preferable assessment methods in cybersecurity. This initial research is based on a qualitative study of academician evaluation of cybersecurity courses. The paper presents the result of interviews along with discussions of ongoing and future suggestions.

Keywords: cybersecurity, objective, student learning outcomes (SLOs), education

1. Introduction

Today, there is a movement towards exploring the world of cybersecurity in theory and practice. This movement needs a base stand in terms of knowledge base and how to judge this knowledge according to universal standards. Cybersecurity now are taught in undergraduate and graduate levels covering wide range of topics. Multiple certificates are recognized internationally to certify personnel in this domain. Setting and measuring learning outcomes for those who are teaching cybersecurity is becoming a challenging process.

Numbers show that the world of cybersecurity will expand in the following years. The market share of cybersecurity, globally, now is almost $106 billion and is expected to increase to around $639 billion within four years. Job advertisement for cybersecurity majors has increased by 57% since 2016. Educational institutions are now responsible for feeding the market with skilled individuals that are knowledgeable of cybersecurity and its ethics (ACS, 2016). This urgent the need for a more robust standard in evaluating the graduates in this major and prepare them for the job market.

With increased need for training and educating more cybersecurity professionals, there are few researches on informing educators of successful ways to engage and educate cybersecurity students. Fortunately, research has covered the topics that could be included in a graduate level education in cybersecurity. Specifically, in addressing the knowledge gap, this research relies on the research by (Abu-Taieh, 2017) which comprehensively covers the important pillars under the cybersecurity umbrella in IT related fields. Still, for SLOs and assessment methods in evaluating cybersecurity education and training, there is not enough research and evidence on what are more effective and there is a great opportunity to fill this gap and provide effective learning strategies. The findings can inform the development of curricula, training, and exercises.

SLOs are statements that describe the significant and essential learning students should have gained by the end of a class (Lesch, 2012). The ability to demonstrate learning is the key and encompasses a performance of some

kind. This demonstration should be done within a context such as classroom learning settings. Learning outcomes refer to obvious and measurable knowledge, skills, and attitudes (Lesch, 2012).

This research is extending the knowledge body in cybersecurity (Abu-Taieh, Alfaries, & Alotaibi, 2018) and uses this knowledge and topics as guidance for selecting the applicable SLOs. With the pillars listed in this body of knowledge (Abu-Taieh, Alfaries, & Alotaibi, 2018). The researchers recognized an overlap with the topics there and the topics in computer science major. Therefore, the research focused on the programs that run under the computer science and IT-related degrees. Also, decided to focus on the concentration of graduate programs in cybersecurity.

This paper, present current state of SLOs that are used in cybersecurity curricula in master programs, inherit and develop SLOs and assessment methods for each pillar in the BOK (Abu-Taieh, Alfaries, & Alotaibi, 2018), and discuss challenges that may face instructors with suggested solutions. Within research and academic institutions, the access to and handling of knowledge needs to be guided by concrete cybersecurity principles in order to prepare the right personnel and have a reliable measure for learning outcomes (CPHC, 2015).

Our approach relies on searching for the SLOs of graduate programs in cybersecurity, identifying the major areas that are focused on, suggesting and develop SLOs and assessment methods. Following, the paper explains the challenges in teaching cybersecurity with suggested ways to overcome those challenges. As the world now move to more knowledgeable individuals in the world of cybersecurity, the learning outcomes should be well defined and measured.

This research is organized as follows, the literature review in the cybersecurity SLOs, next is the methodology, followed by results, contribution, discussion, and conclusion.

2. Literature Review

In this section four axiom are examined and discussed. First, the benefits of implanting SLOs. Second, challenges in implementing SLOs. Third, assessment methods to measure student performance are utilized in academia. Fourth, cybersecurity training methods.

2.1 Benefits of Implementing SLOs

Experts in educations identified the need for establishing Student Learning Outcomes (SLOs) in order to unify knowledge standards and give equal opportunity for student coming from different backgrounds. Student learning outcomes are brought into effect in order to have fair and comparable measures for learning. Benefits and challenges of implementing (SLO) and their use in the education system vary depending on subject.

SLOs help evaluators to judge student results and ultimately improve teaching practice and student learning. SLOs to be effective, they should be adaptable by incorporating different data sources whether assessment is customized or general and demonstrate student's learning outcome. SLOs flexibility is judged when they are adjusted to changes in curriculum and evaluation criteria. Further, SLOs make instructors focus more on objectives that are applicable for their student population (Lachlan-Haché, Cushing, & Bivona, 2012).

Moreover, incorporating SLOs will enhance educator knowledge and skills by emphasizing teacher knowledge of curriculum, assessments, school context, and student records. Research approved that evaluation systems that rely on SLOs allows teachers to benefit from SLOs in taking authorship over the performance. Moreover, SLOs inspire collaboration and exchange best practice among instructors. By helping in setting subject-level, grade-level, or team-based SLOs, instructors can agree on common learning targets for their students and work cooperatively to improve student learning outcomes (Lachlan-Haché, Cushing, & Bivona, 2012).

2.2 Challenges in Implementing SLOs

To form an SLO, there are multiple criteria to be met. In other words, SLOs need to meet certain condition to be applicable in academia. They must be thorough, equivalent, and conform to state guidance. This imposes a certain challenge in finding a measurable SLO that meets those conditions. Finding an SLO that is rigor and assuring its comparability across different levels (classrooms, schools, and regions) is challenging given the diverse contexts, assessments, and growth measures. To condense, the most prominent challenges in creating an SLOs are: 1) identifying high-quality assessments for all grades and subjects, 2) creating applicable growth targets for levels that include students with dissimilar achievement levels, 3) setting aspiring and attainable goals and the size of an objective (broad content versus specific skills), 4) addressing the school and district culture change that will result from implementing SLOs, and 5) continuous improvement of the SLO process (Lachlan-Haché, Cushing, & Bivona, 2012).

2.3 Assessment Methods

Different assessment methods to measure student performance are utilized in academia. Assessment method can be direct or indirect and they are defined as 'strategies, techniques, tools and instruments for collecting information to determine the extent to which students demonstrate desired learning outcomes' (WSSU, 2018). Those methods range from direct assessment such as quiz, exam, presentation, project, and lab exercise to indirect methods such as interviews and surveys. Each of those evaluation methods is designed to measure one or more SLO. Of course, depending on the material and the goal to be measured, a certain method may perform better in measuring the outcome over another. Notably, the most common assessment tools in cybersecurity courses are laboratory-based exercises, experiential learning materials, tests, and challenge-based courses. More advanced classes use organized attack and defend scenarios that allow students to have hands-on experience (Vasserman, Bell, & Sayre, 2015).

2.4 Cybersecurity Training Methods

Cyber Defense Exercises (CDXs) proved its utility in improving student performance. More details, 'The learning measurements are performed at two CDXs: Locked Shields and Crossed Swords. First one is the largest unclassified live-fire CDX in the world with nearly 900 participants (with Blue teams as main training audience). Second one is a small-scale exercise designed to train Red teams' (Maennel, Ottis, & Maennel, 2017). These kinds of exercise are very comprehensive and complicated which requires more thorough process of measurement scale. Therefore, the study (Maennel, Ottis, & Maennel, 2017) proposes a scalable measurement approach called '5-timestamp methodology' to include feedback (benchmarks) and learning measurement. With a timestamp, feedback can be collected at different stages. This work contributes to knowledge by providing recommendations for improvement in learning experience in CDXs. Crossed Swords measurement is more about providing instant feedback to support effective learning. Learning evaluation in these exercise includes, as suggested by the article, the followings: cyber legal aspects, time management and periodization, crisis communication, reporting, ability to convey big picture, cooperation and information sharing, teamwork: delegation, dividing and assigning roles, conduction forensic investigation, handling cyber incidents, monitoring networks, detecting and responding to attacks, system administration and prevention of attacks, and finally learning the network (Maennel, Ottis, & Maennel, 2017).

Another paper (Jalali, 2017) describes the effectiveness of Challenge Based Learning (CBL) methodology in cybersecurity education. Evaluation shows improvement in students' skills and how they possess passion in learning more and pass their knowledge to others. Furthermore, student work towards publishing their research findings and presenting their accomplished to fellow classmates. The study (Jalali, 2017) analyzed 1,479 simulations and compared the performances of experienced professionals with inexperienced group in cybersecurity domain. Experienced group was better in proactive decision-making. In summary, findings point to the importance of training in decision-making focusing on systems thinking skills (Jalali, 2017). Particularly, 'decision-making for the development of cybersecurity capabilities, has not received adequate attention' (Jalali, 2017).

The research (Knapp, Maurer, & Plachkinova, 2017) refers to the necessity of guidance on how to maintain and improve the relevancy of curricula to real life cybersecurity issues. Cybersecurity professionals need continually to keep up with cybersecurity programs and new threats. More important, schools and university should focus on their graduates' knowledge within this domain using professional certifications in cybersecurity industry which help in maintaining an updated curriculum. Specifically, (Knapp, Maurer, & Plachkinova, 2017) covers the evolving changes in professional certifications and how they can be reflected in a cybersecurity curriculum. Using a case study of undergraduate classes and how their content are reflected in professional certificates, the study made suggestions on how to maintain a curriculum through certification (Knapp, Maurer, & Plachkinova, 2017).

Vasserman, Bell, and Sayre (2015) developed a survey assessment tool for cybersecurity courses. The assessment was designed to measure interest and confidence. Findings show that there is a difference between the freshmen students and the advanced students. Also, students in cybersecurity major have more self-confidence and interest than students in general IT related major. Yet, students appear to become less interested as the semester goes. The survey consisted of statements that ask students if they are interested in pursuing a degree in cybersecurity, writing a cyber algorithm, reading external material about cybersecurity, and understanding network traffic (Vasserman, Bell, & Sayre, 2015).

In order to understand students' comprehension of cybersecurity topics, researchers reviewed a study (Scheponik et al., 2016) that relies on interviews with cybersecurity students to study how students feel about core cybersecurity concepts. Those interviews are intended to illicit students understanding of security scenarios

particularly provocative thinking. Student opinions were analyzed using structured qualitative method with thematic analysis in order to record misunderstandings and challenging reasoning. The aim is to utilize that information in developing effective cybersecurity assessment tools. This is still a working in progress project.

One of the effective ways in creating learning environment in cybersecurity is cyberworlds (Scheponik et al., 2016). An interactive virtual environment combines web-based VR platform and 3D cyberworld platform. Those cyberworlds help in understanding technologies such as video games. Students in this experience started to have a new perspective that is deeper vision of the VR. Indeed, their self-confidence is increased as they acquired new technical skills. Experiment proved that virtual environment is excellent way to teach cybersecurity concepts (Scheponik et al., 2016).

Few years ago, lack of cybersecurity skills were a problem. With the growing threat of cybercrime and national security issues, increasing the number of skilled cybersecurity professionals has become nationally crucial. As new technologies, unknown threats, and rising vulnerability in ever changing environment increased, there is an urgent need to innovative, effective, and efficient solutions within cybersecurity education. One of those solutions is discussed in (Gallagher, 2016). A six-month course was conducted by Department of Defense is the Cyber Operations Academy Course (COAC) in Washington D.C to 20 mostly military (Gallagher, 2016). The course content and education approach varied from problem-based learning, lecture, defensive/offensive operations, programming, to social engineering. The course was facilitated by teams: facilitators, coaches, and domain experts. Findings show that student have gained cyber knowledge in tools, detected and responded to threats and attack's, and used social engineering for targeting (Gallagher, 2016). Still, there was not a reference research on student learning outcomes in cybersecurity.

This paper presents a collection of SLOs for cybersecurity BOK as well as suggested assessment methods. This work can be a reliable source for any educator in cybersecurity. It gives suggestions and ways to improve the education system output.

3. Methodology

This paper is an extension to the work done in (Abu-Taieh, 2017) and (Abu-Taieh, Alfaries, & Alotaibi, 2018) which lay down cybersecurity BOK. At first stage the research starts with the topics that are suggested in the BOK (Abu-Taieh, 2017) and (Abu-Taieh, Alfaries, & Alotaibi, 2018) and look for the current state of art in SLOs within the master program of cybersecurity. The researchers found a directory (Morgan, 2018) of master programs in cybersecurity around the USA that the research utilizes in finding current SLOs of such a program. Also search manually for cybersecurity program around the world and list their SLOs. After gathering the SLOs, the two authors revise the list as well as each of the pillars in (Abu-Taieh, 2017). SLOs identified for each topic and the suitable assessment method based on the course description in (Abu-Taieh, Alfaries, & Alotaibi, 2018) and the knowledge of SLOs that are listed under the description of the programs around the world. After this session of revision and brainstorming, inherit some of the SLOs of those programs and develop SLOs that fits the BOK referenced here. The SLOs were edited to fit the objective and the goal of this paper. A second review was conducted by the authors independently to evaluate those preliminary SLOs in terms of their relatedness and fitness.

Once the list was finalized by the authors and combined, a qualitative approach is used to elicit more information of the applicability of the SLOs and assessment methods suggested. Three interviews are conducted with experts and professors in the field of cybersecurity. The interview is aimed to consult the relatedness of each SLOs, suitable assessment, and applicability based on expertise (Appendix A). Questions were asked and CV of respondents is used to validate background and teaching courses. After that SLOs were given to be evaluated by the interviewee. Comments were recorded as well. Interviews were transcribed within 24 hours so that no critical information will be missed.

Table 1. Descriptive statistics of interviewees

#	Name	Education	Country	Expertise Level	Classes Taught	Assessment Methods
1	ML	BSC in Public Relations Master in MIS. Master in in Criminology PhD in IST Certificates in: CISSP.	USA	Expert Teaching Experience: 4 years	Cybersecurity Capstone IT & Cloud Structure Intro. to Information Security Principles Risk Management Standards Compliance Statistics E-commerce	Multiple choice Student essay Individual /group project and presentation Poster Group assignment (risk assessment, recovery plan, critical thinking)
2	AV	Bsc Double Major Business Management & Information Systems, Master in IS, PhD in IST	USA	Medium Level Teaching Experience: 3 years	Foundation in IT Introduction in IS DBMS (GIS) Programming in Python.	Exams Project Presentation Report Assignment (individual)
3	RS	Bsc, Msc, PhD in Mathematics.	USA	Expert Teaching Experience: 20 years	Statistics, Probability, Programming in C, C++, and Java	Quizzes, Exams, Presentation, Report Assignment (individual).

The interviewees were two males and one female with medium to expert level in cybersecurity. The summary of their information and their input is in table 1. After this phase of interviews, the researchers conducted a session to revise the input and evaluate each suggestion before incorporating the feedback into the final list of SLOs and assessment methods.

4. Results

The interviews revealed great feedback and highlighted some areas that would greatly impact the cybersecurity stakeholders in education. The interview with ML, an expert in cybersecurity for four years, revealed that the number of SLOs for each topic should not exceed three to four SLOs to make it feasible to implement. Also, she mentioned that measuring one SLO should be done with multiple assessment methods. Regarding the common assessment method, she uses multiple exams within the semester to allow students to focus on different chunks of information. A major challenge in implementing the SLOs is not the process of forming the SLOs but more on how to measure those SLOs comprehensively considering different factors. Those factors are the size of class, the level of students, lab spaces, and resources. Another challenge includes the level of proficiency in each skill for each student; some students do great in exams while others are more comfortable in presentations and group projects. One of the suggestions that she mentioned, to overcome this challenge while unifying the measuring process of SLOs, is to include questions from a standardized test in student evaluation. For example, in her case, 20 questions are selected from CISSP (Certified Information Systems Security Professional) certificate to be included in evaluation. Referring to discussion as an assessment method, ML mentioned that is not effective in large classes. Selecting a measure over another is usually a subjective choice depending on the professor recommendation which she recommend having a set of questions set by the course coordinator and implemented on all classes to measure the students' outcomes fairly. Her evaluation of each of our suggested SLOs is documented in the Appendix B.

Interview with AV revealed that tests are usually the best indication of student learning outcome. This is because students usually tend to do project at the last minute or let one take on all the work. He also emphasizes the individual assignments for measuring skills learned. For preparing students for future work, he uses group projects and presentations to familiarize students with real-life work environment. AV sees multiple exams within a semester can help students overcome the anxiety of exams and allow multiple milestone evaluations. He also recommends using items from standardized tests to maintain equity in student outcomes and advocates that SLO assessment method should reflect the complexity of an SLO and time/resources available while maintaining curriculum coverage. Regarding challenges in SLOs and assessment, AV confirms the overload of employing different evaluations in measuring a single SLO.

AV praises the need to include, in cybersecurity BOK, system wide cybersecurity policy and comprehensive protection techniques. Cloud computing and ability to secure data from siphoning should also be taught as it is now the most common approach for processing and storing data. Additionally, awareness of compliance and regulations with this type of service should be included under the pillar 'Laws & Ethics' while understanding the

type of an attack under 'Viruses & Hacking'. The interviewee indicates that operating system SLOs pillar should be simplified more. Moreover, AV suggests excluding physical infrastructure knowledge as indicated under the network pillar. His view is that cybersecurity is more about virtual world.

RS, who is an expert in mathematics and teach math classes for cybersecurity majors, sees quizzes and exams are more indication of knowledge. His assessment methods are more individual based. Also, he recommends for improving student knowledge to set multiple measurement milestones and different assessment tools within the semester to help students instill information as short chunks. For SLOs, he sees that suggested SLOs works for the proposed BOK. He also mentioned that his expertise in Math side of cybersecurity and the assessment methods works for that type of knowledge. The challenge is in the size of class and the students' backgrounds.

In summary, these interviews informed the adapted approach, and the suggestions have greatly improved our results (Appendix B). In table 2, the final refined list of SLOs and assessment tools are listed for each of the cybersecurity pillars. In the next section, more details on how final list of BOK SLOs and assessment methods were developed.

5. Contribution

The contributions of this paper are as follows: 1) suggested SLO for the Cyber Security BOK suggested by (Abu-Taieh, 2017) and (Abu-Taieh, Alfaries, & Alotaibi, 2018). Furthermore, the paper suggested *Assessment Methods* and *Training Methods.* The paper utilized the work and ideas of published work, experts from the field, and the work of academic institutions. To summarize the contribution in Cybersecurity BOK pillars, SLOs, and Assessment tools as shown in table 2. This paper may well be a springboard for academicians, academic institutes, and experts, and practitioners in developing master's program or training courses in the Cybersecurity arena.

6. Discussion and Conclusion

With more comprehensive SLOs, there will be more chance to produce more qualified skilled trainees. This research identifies a gap in literature of cybersecurity regarding the student outcomes and SLOs were developed for the existence BOK in cybersecurity. After the interviews, it was apparent that SLOs for cybersecurity will help in improving the education system within cybersecurity. Assessment methods were also evaluated by interviewees. Challenges in implementing and measuring those SLOs were also discussed and practical solutions were presented.

Table 2. The cybersecurity BOK pillars, suggested SLOs and suggested assessment tools

Pillar	SLO
Cyber Security Assurance (CSAUR)	CSAUR1: Develop and implement information assurance security policies, and emergency management policy. CSAUR2: Develop and ensure quality control in information assurance and security management. CSAUR3: Use of Software Assurance Framework (SAF) CSAUR4: Assess risk in systems across the lifecycle and supply chain.
*Assessment Tools	(1), Organized Attack and Defend Scenarios, (3) (4) (5)
Cyber Security Assessment (CSASS)	CSASS1: Identify the risks an organization faces due to cyber. CSASS2: Describe how cyber-attacks against an organization can be monitored and investigated. CSASS3: Present complex ideas about cybersecurity risks to specialist/non-specialist audiences. CSASS4: Use complex problem-solving techniques to critically review, audit, assess and develop effective management strategies to manage cybersecurity risks.
*Assessment Tools	(1), (3) (4) (5)
Ciphering (CI)	CI1: Understand details of specific protocols, algorithms, and standards currently used in cryptography and how to implement them. CI2: Explain how symmetric and asymmetric encryption and authentication systems safeguard data and recommend encryption and authentication systems. CI3: Identify common flaws in cryptographic regimes.
*Assessment Tools	(1), (2)
Algorithms (Alg)	Alg1: Describe the divide-and-conquer paradigm, dynamic-programming paradigm, greedy paradigm, major graph algorithms. Alg2: Explain the different ways to analyze randomized algorithms. Recite algorithms that employ randomization. Alg3: Explain what an approximation algorithm is, and the benefit of using approximation algorithms. Alg4: Appraise complex information using critical and analytical thinking and judgement.
*Assessment Tools	(1), (2), (3)
Networks (NT)	NT1: Demonstrate an understanding of the physical properties and performance characteristics of communication media; specifically, copper cable, fiber optics and wireless networks. NT2: Demonstrate an understanding and appreciation of the importance of communication standards. NT3: Design software and networks that resist and mitigate cyberattacks. NT4: Describe the challenges of securing networked infrastructure and data.
*Assessment Tools	(1), (2)
Digital Logic and Microprocessors Design (DLMD)	DLMD1: Understand the logical behavior of digital circuits. DLMD2: Understand digital hardware and the advantages and disadvantages of programmable logic devices. DLMD3: Understand how a basic microprocessor can be built from standard building blocks.
*Assessment Tools	(1), (2), (5)
Operating Systems (OS)	OS1: Understanding the types of information to be stored and how that is used by the OS can be used to identify and express requirements. OS2: Describe the concepts of threats and attacks and cybersecurity architecture for operating systems. OS3: Exemplify and explain how the kernel of an OS is designed. OS4: Demonstrate knowledge and understanding concurrency, thread abstraction, synchronizing, shared objects, resources and scheduling, memory management.
Assessment Tools	(1), (2)
Database (DB)	DB1: Understand how structure and transactions are processed in a database. DB2: Describe threats and attacks as well as cybersecurity architecture and operations for possible attacks on databases and the potential cybersecurity controls implemented to mitigate attacks. DB3: Understanding the types of information to be used by software and their classification, and then build and test secure designs to meet those requirements (CPHC, 2015).
*Assessment Tools	(1), (2), (4)
Cyber Law & Ethics (CLE)	CLE1: Demonstrate sensitivity to and sound judgment on ethical issues as they arise in IS. CLE2: Locate and apply case law and common law to current legal dilemmas in the technology. CLE3: Distinguish enforceable contracts from non-enforceable contracts.
*Assessment Tools	(1), (3), (5)

Viruses & Hacking (VH)	VH1: Develop advanced knowledge of the type of an attack and the mindsets and motivations of cyber-criminals. VH2: Describe the concepts of threats and attacks and cybersecurity architecture. VH3: Analyze and assess the impact of cybercrime on government, businesses, individuals and society.
*Assessment Tools	(1), (2), (5)
Software Tools & Technique (STT)	STT1: Specify tools and architectures to help secure information systems both proactively and reactively. STT2: Use common performance profiling tools, tools for measuring dynamic code coverage, and tools for automatic testing.
*Assessment Tools	(1) (2), (6)
Software Auditing & Software Engineering (SASE)	SASE1: Describe the key features of Computer Assisted Audit Techniques. SASE2: Use some of the Generalized Audit Software for data extraction and analysis. SASE3: Understanding tools, techniques and methods of software engineering and auditing.
*Assessment Tools	(1), (2), (3), (6)
(1) Exams, Quizzes, and Tests (2) Laboratory-exercises. (3) Case study. (4) Group Project. (5) Discussion. (6) Challenge based Problems.	

For cybersecurity assurance, the interviewee MP suggests including 'Assess risk in systems across the lifecycle and supply chain' in this pillar. Her justification is that it is essential in any organization to include security threats in every stage and in every extension and how it will impact the overall organization. The algorithm pillar was raising concerns as it conveys advance knowledge in algorithm; our justification is that it is essential for cybersecurity to be knowledgeable of different techniques to solve a problem through algorithms. The network pillar SLOs are comprehensive and only needed to merge the similar ones and remove reliability and quality of service as it is not directly related to security according to interviewees' feedback. The SLOs for digital logic and microprocessors design were merged to comprehend the higher concept and avoid redundancy. Also, removed digital technologies and information sources as it is not directly related to the pillar. Operating Systems SLOs for memory and kernel were merged. The database pillar SLOs were kept the same while adding 'Understanding the types of information to be used as suggested by MP and AV. The viruses & hacking, software tools & technique, and software auditing & software engineering pillar and their SLOs were confirmed by the interviews and were not changed.

This research will lay down a road map for educators in cybersecurity and help in equal evaluation for student performance. This certainly will impact the development of curricula, training, exercises, and other educational materials and policies. The depth and dimensions of skills and knowledge expectations are well defined in this paper. With insightful objective measures and interviewee knowledge, one can improve the outcomes of graduates.

Future work can run a larger quantitative approach to evaluate the student outcomes. Also, a longitude study of the effect of incorporating standardized tests in evaluation process of graduates can tremendously help in validating this approach especially in cybersecurity.

References

Abu-Taieh, E. (2017). *Cyber Security Body of Knowledge, IEEE SC2-2017*. The 7th IEEE International Symposium on Cloud and Service Computing. Kanazawa, Japan, November 22-25, 2017. https://doi.org/10.1109/SC2.2017.23

Abu-Taieh, E., Alfaries, A. A., & Alotaibi, S. T. (2018). *Cyber Security Body of Knowledge and Curricula Development. Reimagining New Approaches in Teacher Professional Development*. Book edited by: Vimbi Mahlangu. Intech, London, UK. https://doi.org/10.5772/intechopen.77975

ACS. (2016). *Cybersecurity: Threats, Challenges, Opportunities.* Retrieved from https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

CPHC. (2015). *Cybersecurity Principles and Learning Outcomes For Computer Science And It-Related Degrees*. Retrieved from http://www.eqanie.eu/media/cybersecurity-principles-learning-outcomes-whitepaper.pdf

Gallagher, P. S. (2016). *Assessing Performance in an Innovative Cybersecurity Pilot Course*.

Jalali, M. S. (2017). *Decision-Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment*. ArXiv: 1707.01031 [Cs, Math, Stat]. https://doi.org/10.2139/ssrn.3022626

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. *Journal of Information Systems Education, 28*(2), 101.

Lachlan-Haché, L., Cushing, E., & Bivona, L. (2012). *Student Learning Objectives Benefits, Challenges, and Solutions*. In Performance Management Advantage. Retrieved from https://files.eric.ed.gov/fulltext/ED565846.pdf

Lesch, S. (2012). *Learning Outcomes Learning Achieved by The End of A Course Or Program Knowledge, Skills, Attitudes*. In George Brown College. Retrieved from https://www.georgebrown.ca/policies/assessment-of-student-learning-policy.pdf

Maennel, K., Ottis, R., & Maennel, O. (2017). *Improving and Measuring Learning Effectiveness at Cyber Defense Exercises*. NordSec. https://doi.org/10.1007/978-3-319-70290-2_8

Morgan, S. (2018). *Directory of M.S. in Cybersecurity Programs at Universities in The U.S.* CyberCrime Magazine. Retrieved from https://cybersecurityventures.com/cybersecurity-university-masters-degree-programs/

Scheponik, T., Sherman, A. T., DeLatte, D., Phatak, D., Oliva, L., Thompson, J., & Herman, G. L. (2016). *How students reason about Cybersecurity concepts*. In Frontiers in Education Conference (FIE), 2016 IEEE (pp. 1-5). https://doi.org/10.1109/FIE.2016.7757363

Vasserman, E. Y., Bell, R. S. & Sayre, E. C. (2015). Developing and Piloting a Quantitative Assessment Tool for Cybersecurity Courses (Vol. 16). In *Proceeding of 122nd American Society for Engineering Education Annual Conference and Exposition 2015*. Seattle, Washington, USA 14-17 June 2015.

WSSU. (2018). *In Winston-Salem State University.* Retrieved from https://www.wssu.edu/about/assessment-and-research/niloa/_files/documents/assessmentmethods.pdf

Appendix A

Interview Questions

Q1: What is your education background?

Q2: How long you have been teaching?

Q3: What classes you have taught?

Q4: What are the common assessment methods you used in those classes?

Q5: Reviewing the table above, have you measured any of the SLOs listed with assessment method suggested? Explain more.

Q6: What are the challenges from your perspective in measuring SLOs? Finding a text book?

Q7: What are the most indication of assessment tools in student learning outcome in your opinion?

Appendix B

Summary Evaluation of Suggested SLOs and Assessment Methods

#	Pillar	SLO	MP		AV		RS		Comments	Assessment
			Related							
			Y	N	Y	N	Y	N		
1	CSAUR	CSAUR1	X		X		X			Tests
		CSAUR2	X		X		X			Organized Attack and Defend Scenarios
		CSAUR3	X		X		X			Discussion
		CSAUR4	X		X		X		Can be merged	Case Studies Group Project
2	CSASS	CSASS1	X		X		X			Tests
		CSASS2	X		X		X			Discussion
		CSASS3	X		X		X			Case Studies
		CSASS4	X		X		X			Group Project
3	CI	CI1	X		X		X			Laboratory-
		CI2	X		X		X			exercises
		CI3		X	X		X		Add pros & cons	Tests
4	Alg	Alg1	X		X		X		More general SLOs	Tests
		Alg2	X		X		X			Laboratory
		Alg3	X		X		X			Exercises
		Alg4	X		X		X			Case study
5	NT	NT1	X			X	X			Standardized Tests
		NT2	X		X		X			Laboratory
		NT3	X		X		X			Exercises
		NT4	X		X		X			
6	DLMD	DLMD1	X		X		X			Tests
		DLMD2	X		X		X			Experiential Learning
		DLMD3	X		X		X			Discussion
7	OS	OS1	X		X		X		Can be condensed	Tests
		OS2	X		X		X			Laboratory
		OS3	X		X		X			Exercises
		OS4	X		X		X			
8	DB	DB1	X		X		X			Tests
		DB2	X		X		X			Laboratory-
		DB3	X		X		X			exercises Group Project
9	CLE	CLE1	X		X		X			Tests
		CLE2	X		X		X			Discussion
		CLE3	X		X		X			Case study
10	VH	VH1	X		X		X			Tests
		VH2	X		X		X			Laboratory-
		VH3	X		X		X			exercises Discussion
11	STT	STT1	X		X		X			Tests
		STT2	X		X		X			Challenge based Problems Laboratory- exercises
12	SASE	SASE1	X		X		X			Tests
		SASE2	X		X		X			Case Studies
		SASE3	X		X		X			Challenge based Problems Lab. exercises