Issues in Information Systems
Volume 25, Issue 2, pp. 418-437, 2024

DOI: https://doi.org/10.48009/2_iis_2024_133

Faculty perceptions of open educational resources in cyber curriculums

Alan Stines, *Middle Georgia State University, alan.stines@mga.edu*

Abstract

The evolving cyber landscape requires a growing number of qualified professionals to protect and defend digital information systems. There is a significant shortage of skilled candidates to meet this demand, posing risks to U.S. national security and global safety. Open Educational Resources (OER) reduce learning barriers by lowering costs, increasing access, and allowing educational materials to be adapted to specific needs. This study examines U.S. cyber faculty perceptions of OER in higher education using an adapted survey from the Babson Survey Research Group. Data from cyber professionals and academic conferences were analyzed to explore differences based on faculty experience and roles. Understanding these perceptions can clarify the role of OER in addressing cyber education challenges.

Keywords: cyber education, OER, open educational resources

Introduction

Executive Order 13870, issued in May 2019, highlights the cybersecurity workforce as a strategic asset for protecting the American people, homeland, and way of life. The order mandates federal agencies to enhance cyber workforce capabilities and provide learning pathways and incentives for cyber professionals. The President's Cup Cybersecurity Competition was established to identify untapped cybersecurity potential within the U.S. government workforce, with recommendations to extend the competition to non-federal employees. Furthermore, the executive order strongly encourages using and improving the NICE framework to develop cyber potential and career pathways among federal entities (Trump, 2019).

The Aspen Cybersecurity Group, a cross-sector public-private forum, addresses the challenges in the cybersecurity workforce by promoting collaboration between private and public sectors. The group emphasizes strengthening the pipeline of qualified candidates through skill development and educational opportunities. The Aspen Cybersecurity Group has identified four significant trends contributing to the workforce gap: the demand for skills is outgrowing the supply of qualified workers, untapped potential for cybersecurity roles exists within the current workforce, more than 50% of candidates are deemed unqualified by employer requirements, and the general population remains largely unaware of the potential of cyber career fields (Aspen Cybersecurity Group, 2018).

In testimony before the U.S. House of Representatives' Committee on Science, Space, and Technology's Subcommittee on Research and Technology, Dr. Diana L. Burley recommended 2017 that post-secondary institutions collaborate to build a comprehensive cybersecurity curriculum. This curriculum should guide individuals into the cybersecurity workforce and extend to K-12 education to raise awareness and broaden participation, particularly for women and minorities. The testimony emphasized that any actions taken

should be empirically based, sustainable, and scalable to meet the dynamic landscape of the cybersecurity field (Subcommittee on Research and Technology, 2017).

A notable partnership between government, academia, and private sector organizations is the National Initiative for Cybersecurity Education (NICE). Coordinated by the National Institute of Standards and Technology (NIST), NICE aims to strengthen the cyber ecosystem through training, education, and workforce development opportunities. NICE's vision is to empower a digital economy with knowledgeable and skilled individuals in the cyber workforce. Its three primary goals are to accelerate learning and skills development, nurture a diverse learning community, and guide career development pathways to match the changing needs of the workforce (Beecroft & Edwards, 2016).

NIST's NICE Cybersecurity Workforce Framework, defined in Special Publication 800-181, provides a consistent taxonomy for describing the cyber ecosystem. It includes categories, specialty areas, and work roles that classify the Knowledge, Skills, and Abilities (KSAs) required by cybersecurity professionals. This framework outlines a comprehensive ecosystem of interrelated components working together to improve an organization's security posture (Newhouse et al., 2017).

The cyber landscape is constantly in flux, demanding that professionals continuously develop and refine their skills. Reports from the European Union Agency for Network and Information Security (ENISA) underscore the emergence of new attack threats, underscoring the need for diverse technical and non-technical skills to maintain cyber readiness (Jones et al., 2018). Cyber professionals must be life-long learners, staying updated on the latest developments to address new and sophisticated attacks. Collaboration between industry, academia, and government is crucial for skill development and the success of the cybersecurity workforce (Myauo, 2016).

Educators should emphasize problem-solving and analytical skills over specific techniques, preparing students for the dynamic nature of cyber threats. Traditional learning methods often focus on memorization, but cybersecurity education requires hands-on learning and active engagement to develop practical skills (Pauli & Engebretson, 2012). Providing environments for students to engage in hands-on activities, such as isolated cyber labs, is essential for effective learning (Martin & Woodward, 2013; Topham et al., 2016).

Professional certifications are increasingly crucial in hiring decisions for entry-level cybersecurity roles (Denning & Frailey, 2011). Certifications like the EC-Council's Certified Ethical Hacker undergo continuous updates to remain relevant to the workforce. Faculty should maintain their certifications and adapt curricula, integrating industry standards and advisory board recommendations (Knapp et al., 2017).

Open educational materials provide unique opportunities to reduce barriers to academic pursuits. These no-cost materials, coupled with the widespread availability of mobile devices, are transforming learning and increasing access to information globally (Richter & McPherson, 2012). Online learning models offer significant advantages in terms of convenience and cost-effectiveness, though they also present challenges such as technology access and computer literacy (Ally & Samaka, 2013).

Faculty should ensure that they meet the needs of the students, and the population universities serve to deliver qualified candidates to the workforce (Fedynich, 2014). This research surveys the literature to discover the awareness, effectiveness, and potential barriers creators and adopters of Open Educational Resources (OER) face when dealing with cybersecurity topics.

The current workforce demand in cybersecurity far exceeds the supply of qualified workers, and this gap is expected to widen as the cyber industry continues to grow (Reagin & Gentry, 2018). Addressing the Digital

Divide is crucial for shaping a safer digital society (Rogers, 2016). Educators increasingly use open learning materials to enhance course pedagogy (Adams et al., 2013). While cyber practices are rooted in computer science, they span various industries and societal contexts, forming a vital part of modern infrastructure (Goodman, 2014). The NICE framework guides educators in cultivating Knowledge, Skills, and Abilities (KSAs) to help students succeed in cyber-related fields (Jones et al., 2018). These learning experiences promote cyber awareness and a resilient workforce (Mailloux & Grimaila, 2018).

Open Educational Resources (OER) offer no-cost opportunities for academic advancement (Richter & McPherson, 2012). As faculty awareness of OER grows, so does its acceptance in higher education (Adams et al., 2013). However, gaps remain in understanding OER's influence on cybersecurity education. Cyber professionals often learn necessary skills on the job or through self-study rather than in school (Jones et al., 2018).

This study investigates the extent of OER use in course pedagogy, its practicality, and perceived barriers among faculty. This study also examines faculty perceptions of OER in U.S. higher education cyber curricula. Using a survey design, it explores the impact of two independent variables—years of teaching experience and the number of cyber discipline focus areas—on three dependent variables: OER awareness, perceived effectiveness, and potential barriers. This research aims to identify significant statistical differences in these constructs based on the independent variables (Creswell, 2014).

This study provides foundational insights into faculty perceptions of OER, focusing on awareness, perceived effectiveness, and potential barriers to adoption in cyber curricula. The results will inform future research on OER utilization and efficacy in various cyber disciplines by comprehensively depicting current faculty perceptions. The findings will help cyber faculty make informed decisions about curriculum content, ultimately enhancing cyber education.

Based on the purpose of the study, the following research questions are asked:

> **RQ1:** *Are there statistically significant differences in the combined dependent variables (OER awareness, OER perceptions of effectiveness, and perceptions of OER potential barriers) and the independent variable of the number of years of teaching experience held by faculty?*
>
> **RQ2:** *Are there statistically significant differences in the combined dependent variables (OER awareness, OER perceptions of effectiveness, and perceptions of OER potential barriers) and the independent variable of the number of cyber focus areas chosen?*
>
> **RQ3:** *Is there a statistically significant interaction between the independent variables of the number of years of teaching experience held by faculty and the number of cyber focus areas chosen on the combined dependent variables of OER awareness, OER perceptions of effectiveness, and OER potential barriers?*

Literature Review

A 2018 ISC2 study showed that 59% of cybersecurity professionals view their organizations at risk due to staff shortages, with a lack of skilled personnel and resources as top concerns. The most valued qualifications are relevant work experience, knowledge of cybersecurity concepts, and certifications (International Information System Security Certification Consortium, 2018). Cyber Seek reported over 504,000 job vacancies in the U.S. cybersecurity industry (Cybersecurity Supply/Demand Heat Map, n.d.). Addressing this gap involves increasing diversity, promoting awareness in STEM fields, and forming

partnerships between academia, government, and industry to develop the workforce (Ivy et al., 2019; Goodman, 2014).

The Aspen Cybersecurity Group identified four significant trends contributing to the workforce gap: demand for skills exceeding supply, untapped pools of skilled candidates, over-specified job requirements leaving many unqualified for entry-level jobs, and a lack of awareness of cybersecurity career paths. Recommendations include reviewing job postings, embracing mentorship, and launching apprenticeship programs (Aspen Cybersecurity Group, 2018).

Secondary education plays a vital role in developing the cyber workforce. Both students and teachers lack awareness of career pathways. Recommendations include professional development opportunities and integrating cyber professionalism into the curriculum. Employers also seek soft skills such as communication and teamwork, which are critical alongside technical skills (Ivy et al., 2019). GenCyber, a summer camp program funded by the NSA and NSF, aims to raise awareness of cyber careers among K-12 students and teachers. The program offers free camps, reaching thousands of participants nationwide to generate interest in cybersecurity (Ladabouche & LaFountain, 2016).

The Digital Divide

President Clinton's 1990 address highlighted the digital divide, emphasizing access to technology for economic and social life (Making a Difference in Communities across the Nation, 2000). Despite significant advancements, gaps in technology access and skills remain (ITU Publications, 2018; Rogers, 2016). President Obama's 2016 order aimed to enhance U.S. cybersecurity through public and private collaboration (Obama, 2016).

NICE Framework

The NICE Cybersecurity Workforce Framework, outlined in NIST Special Publication 800-181, identifies seven critical areas in cybersecurity. These areas provide a taxonomy to improve workforce development and make cybersecurity concepts accessible to a broader audience (Newhouse et al., 2017).

Table 1: Seven NICE Framework Categories

Code	Category	Description
S.P.	Securely Provision	Conceptualizes, designs, procures, and builds secure information technology systems, with responsibility for aspects of system and network development
O.M	Operate and Maintain	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (I.T.) system performance and security.
O.V.	Oversee and Govern	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
P.R.	Protect and Defend	Identifies, analyzes, and mitigates threats to internal information technology (I.T.) systems and networks.

Code	Category	Description
AN	Analyze	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence
C.O.	Collect and Operate	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
IN	Investigate	Investigates cybersecurity events or crimes related to information technology (I.T.) systems, networks, and digital evidence.

Goodman (2014) emphasized two viewpoints for building a cybersecurity workforce: investigating workforce needs and forming partnerships in academia, government, and industry (Goodman, 2014). Surveys show that the top skills needed are often self-taught or learned on the job, with soft skills fundamental to early education (Jones et al., 2018).

Educational Theories

John Dewey's educational theories emphasize experiential learning, critical thinking, and social skills, which are crucial for cybersecurity education. Dewey advocated for education as a means of social change and personal development (Achkovska-Leshkovska & Spaseva, 2016; Pérez-Ibáñez, 2018). Bloom's Taxonomy, introduced in 1956, classifies educational objectives and promotes higher levels of thinking (Sikandar, 2017). Using rubrics in education helps measure performance and promote critical thinking, ensuring student learning outcomes meet industry needs (Minnich et al., 2018).

Cyber Curriculum Development

Developing cyber training materials is a dynamic process that requires addressing the evolving landscape (Jones et al., 2018). Hands-on exercises, case studies, and professional certifications are crucial elements that align educational objectives with industry needs (Knapp et al., 2017). However, partnerships with local industries and extracurricular activities enhance learning opportunities, providing real-world context and practical experience (Woodward et al., 2013).

Open Educational Resources (OER) provide low-cost alternatives to traditional textbooks and enhance learning experiences. Open-source software and open textbooks are vital components of OER, offering flexibility and reducing costs (UNESCO, 2002; William and Flora Hewlett Foundation, n.d.).

OER Landscape and Research

Open Educational Resources (OER) have been increasingly recognized for their potential to reduce educational costs and improve access to learning materials. The William and Flora Hewlett Foundation's strategic report on the global OER landscape surveyed around 150 articles, highlighting critical areas of research: adoption and discoverability of OER, teacher practice and pedagogy, perceptions of OER, and policy design and implementation. North America's most prominent study topics include costs, perceptions, open textbooks, and student outcomes. Studies show that openly licensed textbooks can lead to equal or better student learning outcomes than traditional textbooks (William and Flora Hewlett Foundation, 2019).

While the potential of OER is promising, the road to its widespread adoption is not without its challenges. Funding for OER projects often comes from organizations like the Hewlett Foundation, state governments, and industry partners. However, sustaining financial models for OER remains a challenge. Many projects struggle to survive beyond initial funding phases due to the lack of stable revenue streams and competition with commercially available alternatives. Barriers to OER adoption include concerns about quality, loss of intellectual property control, and the need for ongoing support and development. These challenges underscore the urgency of addressing these issues to fully realize the potential of OER in transforming education.

The University System of Georgia (USG) has set a shining example of the potential impact of OER with its successful implementation of the Affordable Learning Georgia program in 2014. The program provides Textbook Transformation Grants to encourage faculty to adopt low-cost learning materials. Since its inception, the initiative has saved over 379,000 students an estimated $61.9 million in textbook costs. A 2018 system-wide survey of USG faculty and professional staff revealed that 84.5% of respondents were instructional faculty, primarily teaching face-to-face, and highly satisfied with OER usage. This success story serves as an inspiration for the transformative power of OER in education (Croteau, 2017; Gallant & Lasseter, 2018).

The Cybersecurity Labs and Resource Knowledge Base (CLARK) is an OER repository focused on cybersecurity topics. CLARK organizes resources into courses, units, micro modules, and nanomodules, and submissions are based on Bloom's Taxonomy to ensure learning outcomes are met. Funded by the National Security Agency (NSA), CLARK aims to be a scalable digital library supporting cybersecurity curricula' ongoing development and dissemination (Dark et al., 2018).

OER Perceptions Research

Research on OER perceptions indicates a positive view among faculty and students. At Ohio State University, a 2015 study across twelve courses found that faculty and students were pleased with the quality and experience of using open and affordable materials. The study highlighted that the most significant factors influencing positive views were the quality and accessibility of the OER materials (Jaggars et al., 2018).

In an introductory astronomy course at Regis College, researchers compared the academic performance of two groups of students over two semesters. The Fall 2017 class used a traditional textbook, while the Fall 2018 class used an OER. The study found no significant differences in final course grades between the two groups, with students saving approximately $200 per semester using OER materials (Mathew & Kashyap, 2019).

An introductory information systems course study covered four sections, two using a traditional textbook and two using an OER textbook. Statistical analysis revealed no significant differences in performance on quizzes and tests. However, students using OER performed better in discussion topics, suggesting that OER can support equal or better learning outcomes compared to purchased textbooks (Wang & Wang, 2017).

In a 2017 study by Grewe and Davis, the impacts of OER on student achievement in an online history course were examined. The study found a moderate positive correlation between the use of OER and student achievement, with OER students performing better than those using commercial textbooks. Although the study had a small sample size, it suggested that OER could positively impact student learning outcomes, warranting further large-scale investigation (Grewe & Davis, 2017).

Methodology

The instrument for this study derives from previous instruments surveying faculty perceptions of educational resources (I. E. Allen & Seaman, 2014; Bliss et al., 2013; Jhangiani et al., 2016). All three previous instruments employ Creative Commons licensing, allowing freedom to share and adapt the material with source attribution (Creative Commons, n.d.). The adapted instrument includes four parts: Part 1: General Questions, Part 2: Cyber Faculty Perceptions of OER Awareness construct, Part 3: Cyber Faculty Perceptions of OER Effectiveness construct, and Part 4: Cyber Faculty Perceptions of OER Barriers construct.

The general question section consists of seven questions that identify the demographic information of the population. General questions include the gender of the participant, whether the participant is a full-time or part-time educator, what type of university the participant comes from, the number of years teaching at the collegiate level, the number of years teaching in the cyber discipline, who typically has control over the selection of resources for courses and identifying the primary focus of cyber teaching through the NICE framework.

Seven questions frame awareness of open educational resources in the cyber faculty population based on a seven-point Likert scale. This section asks participants to rate on a scale from strongly disagree to strongly agree their ability to recognize if a selected resource is in the public domain, whether I selected resources subject to copyright, comfort factor in using Creative Commons licensing for academic material, license agreements used in software, identifying current teaching practices that use OER, and comfort level using open educational resources as both primary and supplemental resources.

The effectiveness construct also includes 7 Likert scale questions to survey faculty perceptions of Oh ER effectiveness. These questions include topics of whether OER leads to an improvement in students' performance, improvements in student satisfaction, whether OER usage is different from traditional learning methods, whether open educational materials lead to more equitable access to education than traditional learning models, improving retention for at-risk students, whether there are financial benefits at an institutional level for adoption of OER, and whether OER helps educators improve their practice in the classroom.

The third construct assesses the faculty perceptions of barriers facing OER adoption. 12 Likert scale questions cover topics relating to difficulty in using OERs in course pedagogy, difficulty in finding OERs to use, whether they are up to date, relevant to teaching context, abilities to find useful OER, permission to use or adapt OER, institutional support for using OER, integration of OER into course materials, and propensity to using OER in the future (See Appendix A).

Reliability and Validity

The Babson Survey Research Group is at the forefront of survey research revolving around faculty perceptions of open educational resources. Three publications, each supporting thousands of responses from faculty and Department chairpersons, have been published since 2014 by the group. The later studies used instruments like the 2014 study, with only minor differences. In the latest 2018 study, the survey group has found that awareness of OER has increased, with approximately 46% of faculty reporting awareness of OER as opposed to 34% in the 2014 study (E. Allen & Seaman, 2016; I. E. Allen & Seaman, 2014; Seaman & Seaman, 2018). The open education group, led by John Hilton III, focuses on empirical research related to the perceptions and efficacy in a higher education environment, open educational resources, and academia. This group uses maps and research surveys as a road map for compiling various research studies

across the OER spectrum (Hilton III & Mason, n.d.). The survey used in this study is based on the 2014 instrument used to study perceptions of open educational resources in academia.

Factor analysis helps find correlated variables that form together to create a latent variable of multiple parts. This statistical method will be helpful in this study to determine which questions relate to the stated constructs in the research questions. The formed constructs in data analysis will compose questions closely associated with awareness, potential benefits, and potential barriers facing the cyber OER landscape. Cronbach Alpha measures how closely related a set of items are as a group. The score determined in data analysis will indicate a scale of reliability to the constructs formed during factor analysis (Field, 2019).

Subjects

The subjects for this study (N=70) were faculty participating in cyber professional development activities in the United States during the survey period. The survey period was open from May 2019 to October 2019. Sampling occurred through participation in professional organizations, faculty training workshops, and an academic cybersecurity conference. An internet survey service, SurveyMonkey™, was used to deliver and collect response data from participants. SurveyMonkey reports that, on average, the survey took five minutes to complete. The study gathered 80 survey responses in total. Ten of the 80 responses were eliminated due to incomplete data, leaving 70 complete responses for analysis. The general demographic information in Table 2 below shows the survey results.

Table 2: General Survey Demographic Information

Demographic	Value	N=70	%
Gender			
	Male	48	68.6
	Female	21	30
	Other	1	1.4
Institution Type			
	Doctorate-Granting Institutions	23	32.9
	Master's Colleges and Universities	14	20
	Baccalaureate Colleges	7	10
	Associates Colleges	24	34.3
	Special Focus Institutions	2	2.9
Teaching Status			
	Part-Time	13	18.6
	Full-Time	51	72.9
	Other	6	8.6

Demographic	Value	N=70	%
Primary Resource Selection Role			
	Me	52	74.3
	Another faculty member	3	4.3
	A faculty committee	5	7.1
	Department, program, or division	7	10
	Administration	1	1.4
	Other	2	2.9

Data Collection Procedures

Upon approval from the institution's Institutional Review Board (IRB), where this study took place in online formats, the researcher welcomed participants, provided a brief overview of the research, and invited them to participate in the survey located online. No incentives were offered for online participants. This is partly due to the survey tool selected, Survey Monkey, which only provides the ability to "buy responses" based on general demographics and does not directly support an incentive ability. As a niche population defined above, cyber faculty was not an option in the Survey Monkey interface as a targetable demographic. Another option would have been to collect personally identifiable information with the survey instrument since there is a third-party tool involved that stores the collected data in the cloud; the researcher did not want to disclose that information to a third party and not be in complete control of it. The researcher did consider other methods to provide incentives like monetary rewards at face-to-face engagements. Research shows that an incentive of $5 can significantly affect participation in survey research but is best when incentives are allocated relatively to the participants (Singer, Groves, & Corning, 1999).

Data Analysis

Collected data were analyzed through Multivariate Analysis of Variance (MANOVA) to answer given research questions. MANOVA procedure tests the significance of group differences for multiple dependent variables if they are related. One purpose of using a MANOVA is to determine if the response variables alter the observer's manipulation of the independent variables (Salkind, 2014). MANOVA requires the data quality to pass specific tests to give a valid result during the analysis. ("One-way MANOVA in SPSS Statistics," n.d.).

Results

Satisfying the assumptions needed to perform MANOVA, the researcher calculates the mean for all the factors in their respective groupings for each respondent. These dependent variables test the significance level with the independent variables of years of teaching experience and the number of roles cyber faculty fill in teaching under the NICE framework. Recall the three research questions—one for each independent variable and one that looks for a combination of the two independent variables.

RQ1: *Are there statistically significant differences in the combined dependent variables (OER awareness, OER perceptions of effectiveness, and perceptions of OER potential barriers) and the independent variable of the number of years of teaching experience held by faculty?*

There are no statistically significant differences in the perceptions of OER based on the number of years of teaching experience held by faculty, F (18, 173.019) = 1.272, p > .05; Wilk's Λ = .704, partial η2 = .111.

RQ2: *Are there statistically significant differences in the combined dependent variables (OER awareness, OER perceptions of effectiveness, and perceptions of OER potential barriers) and the independent variable of the number of cyber focus areas chosen?*

There are no statistically significant differences in the perceptions of OER based on the number of NICE roles chosen by faculty, F (18, 173.019) = 1.099, p >.05, Wilk's Λ = .736, partial η2 = .097.

RQ3: *Is there a statistically significant interaction between the independent variables of the number of years of teaching experience held by faculty and the number of cyber focus areas chosen on the combined dependent variables of OER awareness, OER perceptions of effectiveness, and perceptions of OER potential barriers?*

There are no statistically significant differences in the perceptions of OER based on the number of years of teaching experience and the number of NICE faculty roles chosen, F (63, 102.332) = .807, p >.05, Wilk's Λ = .3, partial η2 = .331.

Discussion and Conclusion

In the study, the researcher sought to determine if there were statistically significant differences in the perceptions of Open Educational Resources (OER) in cyber-focused curricula. The cyber workforce is experiencing a shortage of qualified workers. As the industry continues to grow, insufficient qualified workers will weaken the security posture of the public and private sectors in years to come. Further understanding of the cybersecurity educational landscape will help drive innovations and pathways for student development to fill vital employment needs in the future.

During data analysis, the assumptions for MANOVA were satisfied well enough to provide reliability for a pilot study. The sample consisted of seventy faculty members in higher education across the United States seeking professional development opportunities in cybersecurity. Statistical analysis through the MANOVA determined there were no statistically significant differences between the two independent variables (years of teaching experience, number of NICE roles chosen) and the combination of the two variables (years of teaching experience + number of NICE roles chosen) with p-values greater than 0.05 of significance. The findings indicate that among cyber faculty pursuing professional development, there are no statistical differences in their perceptions of Open Educational Resources (OER) used in cyber curricula.

Several research considerations must be considered while interpreting the research findings presented in this work. First, the survey instrument utilized self-reporting, which is subject to bias on behalf of the participants. The sampling size of only 70 participants also presents a study limitation. MANOVA results are more reliable when they include larger sample sizes than smaller ones. A sample size of around one hundred and fifty would have achieved a more statistically reliable result. Still, the sample in this study could only muster slightly less than half of a robust sample size. The combined dependent variables (awareness, benefits, and barriers) may also not fully represent all the perceptions held by faculty towards OER. During factor analysis, two other factors were identified, with solid loading factors removed from the analysis to fit the stated research questions surrounding awareness, potential benefits, and potential drawbacks.

With a substantial pilot study implemented to further the reliability and validity of the research, there is still room to further the research presented in this study. Based on the literature, the research identified three areas of interest (awareness, potential benefits, and potential barriers) to help frame the three dependent variables presented in the research questions. Two additional groupings emerged during factor analysis with strong loading values that were removed to contain the scope of the research to the instrument. Further investigation through the literature is needed to determine what these additional groupings represent, with additional modifications to the instrument for group-related questions.

Further investigation is required to assess these factors' influence on cyber faculty perceptions of OER, taxonomy, and relevance in the literature. Usability and adaptability are good terminology for these constructs, but more research is needed. Other independent variables collected with the survey instrument could provide other exciting aspects to discovering significant differences in the perceptions of OER. The researcher is interested in further research investigating the type of institution faculty come from, teaching status, and who controls course material selection. Further investigation into these areas may help identify trends in the population and where OER might be most effective.

This research contributes to the body of knowledge in understanding the role that OER can play as educators, industry leaders, and government officials work to build cybersecurity awareness in the general population and open opportunities to those wishing to pursue a career in the cybersecurity workforce.

References

Achkovska-Leshkovska, E., & Spaseva, M. (2016). John Dewey's educational theory and educational implications of Howard Gardner's multiple intelligences theory. *International Journal of Cognitive Research in Science, Engineering and Education*, *4*(2), 57–66. https://doi.org/10.5937/IJCRSEE1602057A

Adams, A., Liyanagunawardena, T., Rassool, N., & Williams, S. (2013). Use of open educational resources in higher education. *British Journal of Educational Technology*, *44*(5), E149–E150. https://doi.org/10.1111/bjet.12014

Allen, E., & Seaman, J. (2016). Opening the textbook: educational resources in U.S. higher education. Retrieved from http://www.onlinelearningsurvey.com/reports/openingthetextbook2016.pdf

Allen, I. E., & Seaman, J. (2014). Opening the curriculum: open educational resources in U.S. higher education, 2014. *Babson Survey Research Group*, *52*. Retrieved from https://eric.ed.gov/?id=ED572730

Ally, M., & Samaka, M. (2013). Open education resources and mobile technology to narrow the learning divide. *The International Review of Research in Open and Distributed Learning*, *14*(2), 14. https://doi.org/10.19173/irrodl.v14i2.1530

Aspen Cybersecurity Group. (2018). Principles for growing and sustaining the nation's cybersecurity workforce, (November).

Bliss, T., Robinson, T. J., Hilton, J., & Wiley, D. A. (2013). An OER COUP: college teacher and student perceptions of open educational resources. *Journal of Interactive Media in Education*, *2013*(1), 4. https://doi.org/10.5334/2013-04

Creswell, J. (2014). *Research design: qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks: SAGE Publications, Inc.

Croteau, E. (2017). Measures of student success with textbook transformations: the Affordable Learning Georgia Initiative. *Open Praxis*, *9*(1), 93. https://doi.org/10.5944/openpraxis.9.1.505

Cybersecurity Supply/Demand Heat Map. (n.d.). Retrieved from https://www.cyberseek.org/heatmap.html

Dark, M., Kaza, S., & Taylor, B. (2018). CLARK – The cybersecurity labs and resource knowledge-base – a living digital library. *27th USENIX Security Symposium, USENIX Security 18*, 66, 37–39. Retrieved from https://www.usenix.org/conference/ase18/presentation/dark

Denning, P. J., & Frailey, D. J. (2011). Who are we---now? *Communications of the ACM*, *54*(6), 25. https://doi.org/10.1145/1953122.1953133

Fedynich, L. V. (2014). Teaching beyond the classroom walls: The pros and cons of cyber learning. *Journal of Instructional Pedagogies*, *13*, 1–7. Retrieved from http://aabri.comwww.aabri.com/manuscripts/131701.pdf

Field, A. (2019). *Discovering statistics using IBM SPSS Statistics* (4th ed.). Thousand Oaks: SAGE Publications, Inc.

Gallant, J., & Lasseter, M. (2018). *2018 USG survey report on open educational resources*.

Goodman, S. E. (2014). Building the nation's cyber security workforce. *ACM Transactions on Management Information Systems*, *5*(2), 1–9. https://doi.org/10.1145/2629636

Grewe, K., & Davis, W. P. (2017). The impact of enrollment in an OER course on student learning outcomes. *The International Review of Research in Open and Distributed Learning*, *18*(4), 231–238. https://doi.org/10.19173/irrodl.v18i4.2986

Hilton III, J. L., & Mason, S. (n.d.). The Review Project.

International Information System Security Certification Consortium. (2018). *Cybersecurity professionals focus on developing new skills as workforce gap widens*. Cybersecurity Workforce Study.

ITU Publications. (2018). Measuring the information society report. *International Telecommunication Union* (Vol. 1). Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf

Ivy, J., Lee, S. B., Franz, D., & Crumpton, J. (2019). Seeding cybersecurity workforce pathways with secondary education. *Computer*, *52*(3), 67–75. https://doi.org/10.1109/MC.2018.2884671

Jaggars, S. S., Folk, A. L., & Mullins, D. (2018). Understanding students' satisfaction with OERs as course materials. *Performance Measurement and Metrics*, *19*(1), 66–74. https://doi.org/10.1108/PMM-12-2017-0059

Jhangiani, R., Pitt, R., Hendricks, C., Key, J., & Lalonde, C. (2016). *Exploring faculty use of open educational resources at British Columbia post-secondary institutions*. BCampus. Victoria, BC. Retrieved from http://oro.open.ac.uk/45178/1/BCFacultyUseOfOER_final.pdf

Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: results from interviews with cybersecurity professionals. *ACM Transactions on Computing Education*, *18*(3), 1–12. https://doi.org/10.1145/3152893

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a cybersecurity curriculum: professional certifications as valuable guidance. *Journal of Information Systems Education*, *28*(2), 101–113. Retrieved from http://jise.org/Volume28/n2/JISEv28n2p101.html

Ladabouche, T., & LaFountain, S. (2016). GenCyber: inspiring the next generation of cyber stars. *IEEE Security & Privacy*, *14*(5), 84–86. https://doi.org/10.1109/MSP.2016.107

Mailloux, L. O., & Grimaila, M. (2018). Advancing cybersecurity: the growing need for a cyber-resiliency workforce. *I.T. Professional*, *20*(3), 23–30. https://doi.org/10.1109/MITP.2018.032501745

Making a difference in communities across the nation. (2000). Retrieved December 1, 2019, from https://clintonwhitehouse4.archives.gov/WH/New/digitaldivide/digital5.html

Martin, N., & Woodward, B. (2013). Building a cybersecurity workforce with remote labs. *Information Systems Education Journal*, *11*(2), 57–62.

Mathew, S., & Kashyap, U. (2019). Impact of OER materials on students' academic performance in an undergraduate astronomy course. *Journal of STEM Education*, *20*(1), 46–50.

Minnich, M., Kirkpatrick, A. J., Goodman, J. T., Whittaker, A., Stanton Chapple, H., Schoening, A. M., & Khanna, M. M. (2018). Writing across the curriculum: reliability testing of a standardized rubric. *Journal of Nursing Education*, *57*(6), 366–370. https://doi.org/10.3928/01484834-20180522-08

Myauo, M. (2016). The U.S. Department of Defense cyber strategy: a call to action for partnership. *Georgetown Journal of International Affairs*, *17*(3), 21–29. https://doi.org/10.1353/gia.2016.0033

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework*. Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-181

Obama, B. (2016). Executive Order -- commission on enhancing national cybersecurity. Retrieved May 11, 2019, from https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity

One-way MANOVA in SPSS Statistics. (n.d.). Retrieved from https://statistics.laerd.com/spss-tutorials/one-way-manova-using-spss-statistics.php

Pauli, J., & Engebretson, P. (2012). Filling your cyber operations training toolbox. *IEEE Security & Privacy*, *10*(5), 71–74. https://doi.org/10.1109/MSP.2012.117

Pérez-Ibáñez, I. (2018). Dewey's thought on education and social change. *Journal of Thought*, *52*(3/), 19–31.

Reagin, M. J., & Gentry, M. V. (2018). Enterprise cybersecurity. *Frontiers of Health Services Management*, *35*(1), 13–22. https://doi.org/10.1097/HAP.0000000000000037

Richter, T., & McPherson, M. (2012). Open educational resources: Education for the world? *Distance Education*, *33*(2), 201–219. https://doi.org/10.1080/01587919.2012.692068

Rogers, S. E. (2016). Bridging the 21st century digital divide. *TechTrends*, *60*(3), 197–199. https://doi.org/10.1007/s11528-016-0057-0

Salkind, N. J. (2014). *Statistics for people who (think they) hate statistics* (5th ed.). Los Angeles: SAGE Publications, Inc.

Seaman, J. E., & Seaman, J. (2018). *Freeing the textbook: educational resources in U.S. higher education.* Retrieved from https://www.onlinelearningsurvey.com/reports/freeingthetextbook2018.pdf

Sikandar, A. (2017). Bloom's Taxonomy (cognitive domain) in higher education settings: reflection brief. *Journal of Education and Educational Development*, *4*(1), 32–47.

Singer, E., Groves, R. M., & Corning, A. (1999). Differential incentives: beliefs about practices, perceptions of equity, and effects on survey participation. *Public Opinion Quarterly*, *63*(2), 251–260. https://doi.org/10.1086/297714

Subcommittee on Research and Technology. (2017). *Strengthening U.S. cybersecurity capabilities*. Washington, D.C.: U.S. Government Publishing Office. Retrieved from https://www.govinfo.gov/content/pkg/CHRG-115hhrg24667/pdf/CHRG-115hhrg24667.pdf

The William and Flora Hewlett Foundation. (2015). Advancing widespread adoption to improve instruction and learning. *Open Educational Resources*, (December). Retrieved from http://www.hewlett.org/wp-content/uploads/2017/02/OER-strategy-memo.pdf

Topham, L., Kifayat, K., Younis, Y., Shi, Q., & Askwith, B. (2016). Cyber security teaching and learning laboratories: a survey. *Information & Security: An International Journal*, pp. *35*, 51–80. https://doi.org/10.11610/isij.3503

Trump, D. J. (2019). Executive Order on America's cybersecurity workforce. Retrieved from https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/

UNESCO. (2002). *Forum on the impact of open courseware for higher education in developing countries*. Final Report, 2002(July), 30.

Wang, S., & Wang, H. (2017). Adoption of open educational resources (OER) textbook for an introductory information systems course. *Open Learning: The Journal of Open, Distance and e-Learning*, *32*(3), 224–235. https://doi.org/10.1080/02680513.2017.1354762

Wiley, D., & Hilton III, J. L. (2018). Defining OER-enabled pedagogy. *The International Review of Research in Open and Distributed Learning*, *19*(4), 133–147. https://doi.org/10.19173/irrodl.v19i4.3601

William & Flora Hewlett Foundation. (2019). *Understanding the global OER landscape*. Retrieved from https://hewlett.org/wp-content/uploads/2019/04/Understanding-the-global-OER-landscape.pdf

Woodward, B., Imboden, T., & Martin, N. L. (2013). An undergraduate information security program: more than a curriculum. *Journal of Information Systems Education*, *24*(1), 63–70.

Appendices

Appendix A: Informed Consent

Informed Consent
Faculty Perceptions of Open Educational Resources in Cyber Curriculum

What this study is about:
The purpose of this survey is to gather information about faculty perceptions of Open Educational Resources (OER) in the context of cyber curriculum usage. It will paint a big picture of the current perceptions surrounding OER usage in cyber course pedagogy.

What I will ask you do:
If you agree to be in the study, you will complete a survey, which consists of four sections. They are:
Part 1: General Questions
Part 2: Cyber Faculty Perceptions of OER Awareness
Part 3: Cyber Faculty Perceptions of OER Effectiveness
Part 4: Cyber Faculty Perceptions of OER Barriers

Risks and Benefits:
There are no foreseen risks to you participating in this study. The participation is completely voluntary, and you can stop at any time.

Your answers will be confidential. The records and data of this study will be kept private. In any sort of report the researcher makes public, he will not include any information that will make it possible to identify you.

This research has been reviewed and approved by Dakota State University's Institutional Review Board for exempt status.

Taking part is voluntary:
Taking part in this study is completely voluntary. You may stop at any time. You must be at least 18-years or older to complete this survey.

Statement of Consent
I have read the above information and have received answers to any questions I have asked. I am 18-years or older. I consent to take part in the study.

By clicking Next, you consent to take part in this study.

Appendix B: Part 1: General Questions

Please provide answers to the following questions:

1. Gender

Radio Buttons:

- ○ Male
- ○ Female
- ○ Other

2. Teaching Status

Radio Buttons

- ○ Part-Time
- ○ Full-Time
- ○ Other

3. Institution Type

Radio Buttons:

- ○ Doctorate-granting Universities
- ○ Master's Colleges and Universities
- ○ Baccalaureate Colleges
- ○ Associates Colleges
- ○ Special Focus Institutions
- ○ Tribal Colleges
- ○ Other

4. Number of Years Teaching at Collegiate Level

Radio Buttons:

Less than 1
1 to 3
4 to 5
6 to 9
10 to 15
16 to 20
More than 20

5. Number of Years Teaching in Cyber Discipline

Radio Buttons:

Less than 1
1 to 3
4 to 5
6 to 9
10 to 15
16 to 20
More than 20

6. Who has the PRIMARY role in selecting educational resources for use in the courses you teach?

Radio Buttons

- ○ Me
- ○ Another faculty member
- ○ A faculty committee
- ○ Department, program, or division
- ○ Instructional design group
- ○ Administration
- ○ Other

7. The NICE Framework provides seven categories for high-level grouping of common cybersecurity functions in the workforce. Which of the options below relates to your disciplines of study in the field of cybersecurity?

CheckBox List: (Multiple Allowed)

- ○ **Analyze** – Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
- ○ **Collect and Operate** – Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
- ○ **Investigate** – Investigates cybersecurity events or crimes related to information technology (I.T.) systems, networks, and digital evidence.
- ○ **Operate and Maintain** - Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (I.T.) system performance and security.
- ○ **Oversee and Govern** – Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
- ○ **Protect and Defend** -Identifies, analyzes, and mitigates threats to internal information technology (I.T.) systems and/or networks.
- ○ **b – Conceptualizes, designs, procures, and/or builds secure information technology (I.T.) systems**, with responsibility for aspects of system and/or network development.
- ○ **Other**

Appendix C: Part 2: Cyber Faculty Perceptions of OER Awareness

The William and Flora Hewlett Foundation defines Open Education Resources (OER) as "teaching, learning, and research materials in any medium – digital or otherwise – that reside in the public domain or have been released under an open license that permits no-cost access, use, adaptation, and redistribution by others with no or limited restrictions".
For each statement, please indicate your level of agreement.

		Strongly Agree	Agree	Somewhat Agree	Neutral	Somewhat Disagree	Disagree	Strongly Disagree
1.	I feel comfortable in identifying if a selected resource exists in the public domain.	7	6	5	4	3	2	1
2.	I feel comfortable in identifying if a selected resource is subject to copyright.	7	6	5	4	3	2	1
3.	I feel comfortable using a selected resource that employs Creative Commons licensing.	7	6	5	4	3	2	1
4.	I feel comfortable in interpreting the license agreements of software that I use in course instruction.	7	6	5	4	3	2	1
5.	I can identify current teaching practices I use that employ OER.	7	6	5	4	3	2	1
6.	I feel comfortable teaching a course using OER as a primary resource.	7	6	5	4	3	2	1
7.	I feel comfortable teaching a course using OER for supplemental resources.	7	6	5	4	3	2	1

Part 3: Cyber Faculty Perceptions of OER Effectiveness
For each statement, please indicate your level of agreement.

		Strongly Agree	Agree	Somewhat Agree	Neutral	Somewhat Disagree	Disagree	Strongly Disagree
1.	Use of OER leads to improvement in student performance.	7	6	5	4	3	2	1
2.	Use of OER leads to improvement in student satisfaction.	7	6	5	4	3	2	1
3.	The open aspect of OER creates different usage and adoption patterns than other online resources.	7	6	5	4	3	2	1
4.	Open educational models lead to more equitable access to education, serving a broader base of learners than traditional education.	7	6	5	4	3	2	1

5.	Use of OER is an effective method for improving retention for at-risk students.	7	6	5	4	3	2	1
6.	OER adoption at an institutional level leads to financial benefits for students and/or institutions.	7	6	5	4	3	2	1
7.	Use of OER leads to critical reflection by educators, with evidence of improvements in their practice.	7	6	5	4	3	2	1

Part 4: Cyber Faculty Perceptions of OER Barriers

For each statement, please indicate your level of agreement.

		Strongly Agree	Agree	Somewhat Agree	Neutral	Somewhat Disagree	Disagree	Strongly Disagree
1.	OERs are difficult to use in course pedagogy.	7	6	5	4	3	2	1
2.	It is hard to find OERs to use in course instruction.	7	6	5	4	3	2	1
3.	There are not enough OER resources for my subject matter.	7	6	5	4	3	2	1
4.	Existing OER materials are not high-quality.	7	6	5	4	3	2	1
5.	OERs are not current or up-to-date.	7	6	5	4	3	2	1
6.	OERs are not relevant to my local teaching context.	7	6	5	4	3	2	1
7.	There is no comprehensive catalog of resources for my subject area.	7	6	5	4	3	2	1
8.	I do not know if I have permission to use or change OER materials I find.	7	6	5	4	3	2	1
9.	I lack support from my institution to implement OERs into course curriculum.	7	6	5	4	3	2	1
10.	OERs are too difficult to change or edit.	7	6	5	4	3	2	1
11.	OERs are too difficult to integrate into the technology my students and I use.	7	6	5	4	3	2	1
12.	I do not think I will be using or continue using OER resources in the next three years.	7	6	5	4	3	2	1