Spring 5-2020

Faculty Perceptions of Open Educational Resources in Cyber Curriculum: A Pilot Study

Alan Stines

FACULTY PERCEPTIONS OF OPEN EDUCATIONAL RESOURCES IN CYBER CURRICULUM: A PILOT STUDY

A dissertation submitted to Dakota State University in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in

Cyber Operations

May 2020

By

Alan Stines

Dissertation Committee:

Dr. Kyle Cronin
Dr. Wayne Pauli
Dr. Mark Geary
Dr. Alex Koohang
Dr. Kevin Floyd

Dakota State University
Completion of Dissertation Final Defense Form

Student Name: Alan Stines Student ID: [redacted]

Title of Dissertation: Faculty Perceptions of Open Educational Resources in Cyber Curriculum

Location of Final Defense: Online via Zoom
Date and Time of Final Defense: 24 March 2020 (Date) 1:00 (Time)

Semester of Intended Graduation: Spring 2020

The above-named student has:

☒ Satisfactorily passed his/her final defense without revisions to the dissertation

☐ Satisfactorily passed his/her final defense with revisions to the dissertation (page 2)

Revisions due: _____ (date)

☐ Had his/her final defense deferred and will be rescheduled (Please attach letter)

☐ Not satisfactorily completed his/her dissertation defense (Please attach letter)

Kyle Cronin — Signature	Kyle Cronin (co-chairperson)	April 20, 2020 — Date
_____ Signature	(co-chairperson)	Date
Kevin Floyd — Signature	Kevin Floyd (member)	April 20, 2020 — Date
Mark Geary — Signature	Mark Geary (member)	April 20, 2020 — Date
Alex Koohang — Signature	Alex Koohang (member)	April 20, 2020 — Date
_____ Signature	(member)	Date

Completed form will route automatically to:
Dakota State University
Office of Graduate Studies and Research
FAX: 605-256-5093 PHONE: 605-256-5799 E-MAIL: gradoffice@dsu.edu

ACKNOWLEDGMENT

The pathways through life do not always extend in a straight line; only through the guidance of others have I been able to be here with the research presented herein. Brittany, as my wife and best friend, being here would be impossible without your multi-faceted support. Special thanks to my mom, Kathy, for always being available to help proofread my papers and encouraging me to follow my passions in life. To my sister, Amy, thank you for goading me a bit and pushing me to be a better version of myself. To my greater extended family, thank you for all the love, support, and encouragement to be a happy individual.

My committee has been very valuable in providing insights into my research and mentoring me as a growing academic. When I transitioned from industry in 2015 to pursue a career in teaching technology, I very much felt like a fish out of water when it comes to the classroom as an educator. Through your involvement during this process, I have not only produced stronger research but have absorbed and grown my teaching philosophy. Thank you, Dr. Cronin, for agreeing to be my chair and helping me focus on what is important as both a student, educator, and academic. There is a bigger purpose we all fulfill in our paths of life, and I am grateful for the opportunity to be blessed by so many in our paths together.

If I have seen further than others, it is by standing upon the shoulders of giants. ~ Isaac Newton

ABSTRACT

The cyber landscape is growing and evolving at a fast pace. Public and private industries need qualified applicants to protect and defend information systems that drive the digital economy. Currently, there are not enough candidates in the pipeline to fill this need in the workforce. The digital economy is still growing, thus presenting an even greater need for skilled workers in the future. The lack of a strong workforce in cybersecurity presents many challenges to safeguarding U.S. national security and citizens across the world. The William and Flora Hewlett Foundation defines Open Educational 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. OERs weaken barriers to learning by reducing costs, increasing access, and allowing adaptability of educational materials to meet the needs of an instructor in their field. In this study, the research aims to study cyber faculty members from higher educational institutions in the United States to determine their perceptions of using OER for cyberlearning. A survey instrument from the Babson Survey Research Group was adopted and adapted by the researcher for use in statistical analysis. Individuals from cyber professional organizations, an academic conference, and professional development opportunities in the Summer of 2019 completed the survey to help build the sample for data analysis. The research questions in the study aim to look for statistically significant differences in perceptions of cyber faculty by looking at their years of experience and the number of specialty roles faculty fill in their cyber endeavors. Further understanding

of the perceptions of OER by cyber faculty will help understand the roles these educational tools play in tackling the challenges that exist in the cyber landscape.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

Alan Stines

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Background

Executive order 13870 in May 2019 by the president of the United States views the cybersecurity workforce as "a strategic asset that protects the American people, the homeland, and the American way of life." The order calls on federal agencies to grow the capability of the cyber workforce and provide cyberlearning pathways and incentives for cyber professionals. The founding of the President's Cup Cybersecurity Competition will identify untapped cybersecurity potential existing in the United States government workforce with recommendations to extend the competition to non-federal employees. The use and improvement of the NICE framework to develop cyber potential and career pathways are highly encouraged among federal entities according to the executive order (Trump, 2019).

One of the professional organizations associated with promoting cybersecurity, the Aspen Cybersecurity Group, is a cross-sector public-private forum consisting of government officials, industry executives, academia, journalism, and other members from civil society. The role of the group is to bring attention to the challenges in the cybersecurity workforce, promote collaboration between private and public sectors, and work towards strengthening the pipelines in supplying qualified candidates to the workforce through skills development and educational opportunities. The Aspen Cybersecurity Group identifies four major trends contributing to the workforce gap listed below (Aspen Cybersecurity Group, 2018).

1. Demands for skills are outgrowing the supply of qualified workers.

2. Untapped potential for cybersecurity roles exists in the current workforce.
3. More than 50% of candidates are considered unqualified by employer requirements.
4. The general population remains unaware of the potentials in cyber career fields

In testimony before the United States House of Representatives' Committee on Science, Space and Technology's Subcommittee on Research and Technology, Dr. Diana L. Burley recommended in 2017 that post-secondary institutions collaborate to build a comprehensive cybersecurity curriculum and ultimately guide individuals into the cybersecurity workforce and should extend to K-12 education. Raising awareness and broadening participation to women and minorities should also be a key priority in building a more diverse workforce. The testimony recommends that any actions are taken based on the testimony be empirically based, sustainable, and scalable to meet the dynamic landscape of the cybersecurity field (Subcommittee on Research and Technology, 2017).

One partnership between government, academia, and private sector organizations is the National Initiative for Cybersecurity Education (NICE). The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce coordinates NICE. Through cybersecurity training, education, and workforce development opportunities, NICE works to strengthen the posture of the cyber ecosystem. The ultimate vision is empowering a digital economy with knowledgeable and skilled individuals in the cyber workforce. NICE has three major goals to deliver on its missions, through its vision, and upholding the values of the organization. The first goal is to accelerate learning and skills development for individuals to address the shortage of skilled cybersecurity workers. The second goal is to nurture a diverse learning community where individuals can strengthen their education and

opportunities. Guiding career development pathways and adjusting methodologies is NICE's third goal to match the changing needs of the workforce (Beecroft & Edwards, 2016).

In the NIST's special publication 800-181, NICE's Cybersecurity Workforce Framework defines a consistent taxonomy for defining the cyber ecosystem that is not limited to job titles or specific occupational terms. The framework consists of categories, specialty areas, and work roles that classify the Knowledge, Skills, and Abilities (KSAs) that are needed by individuals working in the field. Seven categories make high-level groupings over various Specialty Areas among cybersecurity professionals. Specialty Areas coalesce within each category that defines more specific groupings to Work Roles individuals fill in their career paths. Work Roles consist of various tasks, knowledge, skills, and abilities individuals employ that are applicable in the workforce. The NICE framework describes a rich ecosystem consisting of interrelated components that all work together to improve the security posture in an organization (Newhouse, Keith, Scribner, & Witte, 2017).

The cyber landscape continues to evolve at a fast pace, a yearly report from the European Union Agency for Network and Information Security (ENISA) demonstrates a shifting landscape of a wide variety of topics related to cybersecurity. In 2017 alone, many new emerging attack threats emerged that require constant development and refinement of skills by professionals to identify and respond to these cyber developments (European Union Agency for Network and Information Security, 2018). For all that these topics display the landscape in-breadth, it takes very diverse skillsets, both technical and non-technical, from individuals to make an impact on cyber readiness overall (Jones, Namin, & Armstrong, 2018). Cyber professionals become life-long learners of their trade, constantly following developments in the field to address new, changing, and more sophisticated attacks. The

United States Department of Defense is taking strong initiatives to develop partnerships in industry, academia, and government bodies as a key initiative in its strategic plan (Myauo, 2016). Through collaboration and resource sharing throughout the industry can new individuals begin to develop the skills needed to succeed in the workplace.

Using tools in cyber practices is a big part of performing job duties, but practitioners cannot be reliant on just using tools alone. Technical skills complement analytical skills to build a well-rounded cyber professional. The field requires skills that go deeper into researching how attacks happen and creating mitigations that prevent their success. Performing job duties in cybersecurity often requires problem-solving skills in addition to highly technical skills like programming to create new tools in this shifting environment. Educators should strive to not focus on teaching specific tools for techniques in identifying and preventing cyber threats; but instead try to bestow a more investigative and operational standpoint to learning cyber operations practices (Pauli & Engebretson, 2012). There is a shortage of qualified students to meet the needs of the evolving workforce (Krutz & Richards, 2017). In addition to preventing and mitigating attacks, professionals must create resilient systems and practices for recovering from cyber events (Mailloux & Grimaila, 2018).

Traditional learning methods usually consist of using a textbook and following problems that emphasize memorization or stress fact-based findings in the resource. Proponents of information technology fields are challenging educators to move beyond traditional teaching methods to emphasize a more hands-on learning environment to prepare students for the workforce (Martin & Woodward, 2013). Active learning is an approach used by many educators to emphasize hands-on learning in the development of skills that complement fact-based knowledge. Cyber education requires learning beyond theoretical

concepts and should include giving hands-on experience to students. Cyberlearning materials could mean access to a variety of machines and networks to simulate real-world environments (Topham, Kifayat, Younis, Shi, & Askwith, 2016).

Professional certifications are becoming more common in the hiring decisions for potential candidates in entry computer science roles (Denning & Frailey, 2011). Some certifications, like EC-Council's Certified Ethical Hacker certificate, undergo continuous improvement cycles to include the latest tools, techniques, and procedures relevant in the workforce (EC-Council, 2019). Knapp et al. recommend faculty monitor and maintain personal certifications to make informed decisions as to the direction of their curriculum. They note in the limitations that certifications should not be considered the only important input to maintaining curriculum in a cybersecurity program; educational accreditation entities, local advisory boards, and evolving industry standards (Knapp, Maurer, & Plachkinova, 2017).

The cybersecurity field is increasingly looking for candidates that possess the hands-on skills for performing specific job duties. Traditional classroom learning focuses on theoretical teaching and not necessarily on hands-on learning skills relevant to the workforce. In cybersecurity, there is a challenge to safely offer students the opportunity to work with cyber concepts they will experience in the field while not compromising the security of University systems and software. As more educational opportunities are offered online, not on the traditional on-campus environment, providing a laboratory for cyber activities becomes a challenge. In the landscape of cybersecurity education, many topics may require varying laboratories for hands-on instruction. Some of these topics may include things like cryptography, malware analysis, secure software development, ethics training, security

auditing, digital forensics, and even ethical hacking. Providing an environment for students to engage with hands-on activities with these topics may require many resources, including multiple computers, networks, and infrastructure, to mirror a real-life environment (Martin & Woodward, 2013).

Typically a cyber laboratory should be isolated from real-life technology environments, including University infrastructure and even the students' home network environment. These situations can provide many challenges to cyber faculty wishing to engage in cyber learning opportunities. Several laboratory types have been proposed, including physical labs, simulation labs, virtual machine labs, and even multiple virtual machine labs. Physical laboratories work well in the traditional learning approach at an educational institution but are not flexible enough to apply to online learning models. A simulation laboratory Is often an environment specifically set up to emphasize certain cyberlearning topics. Simulated environments can help students understand the real-life impact have certain cyber concepts. Virtual environments can be either cloud-based or based on desktop virtualization (Topham et al., 2016).

Knowledge of programming structures and logic presents major core literacies in the development of cyber professional skills. Forging new pathways in education to elevate computer literacy through reading, writing, and mathematical literacy is pivotal in preparing individuals in the digital age (Arquilla & Guzdial, 2017). A recent survey from the Organization for Economic Co-operation and Development (OECD) found that individuals with higher literacy and problem-solving skills in technology-rich environments are more employable and tend to have higher wages. Future outlooks on the labor force also show an

increase in demand for individuals to enter the workforce who possess computer skills and problem-solving competencies (OECD, 2016).

Open educational materials provide a unique opportunity for individuals to reduce barriers in educational endeavors. No cost materials, cheap distributions methods, such as the internet, and diversity of available topics is transforming learning for individuals across the globe (Richter & McPherson, 2012). In particular, the availability of open materials on mobile devices is becoming increasingly popular for accessing information (Ally & Samaka, 2013). Individuals seeking to transform the landscape of cybersecurity education can create and find resources to shape the technical, analytical, and problem-solving skills needed for the cyber workforce.

Online learning models can experience many advantages and disadvantages to the learning environment. A major advantage of online learning is the convenience for students to participate in the learning environment. Students are no longer limited by geographic location when engaging in educational opportunities, allowing students the freedom to seek and control their educational destiny. Online learning is typically more cost-effective for both the student and educational institutions as well. However, several barriers are present in online learning models. For example, Computer literacy can create a huge gap since most of the course material may rely on technology to deliver learning. Some students may lack access to the Internet from which many online learning Models rely on for course delivery. Access to technology can present a barrier to those wishing to expand their educational opportunities. Online courses typically involve a little bit more faculty preparation to be effective then there is in traditional face to face courses. Students learn using a variety of methods, but some literature suggests cyberlearning is best via tactile or kinesthetic modality, which can be

difficult to engage students within a course that is purely online. Online learning opportunities can provide many advantages and disadvantages to students in the educational sphere, but faculty should take care to be sure that they meet the needs of the student and the population that 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) may have when dealing with cybersecurity topics.

Problem Statement

There are not enough workers to meet current workforce demand in cybersecurity ("Cybersecurity Supply/Demand Heat Map," n.d.). Also, the cyber industry is growing and will need even more skilled workers to fill cyber roles in the future (Reagin & Gentry, 2018). Building bridges over the Digital Divide to shape a safer digital society in the future is essential for success in society (Rogers, 2016). Educators are increasingly aware of using open learning materials in traditional learning environments to aid course pedagogy (Adams, Liyanagunawardena, Rassool, & Williams, 2013). Though cyber practices exist in computer science disciplines, cyber contexts extend beyond the digital realm across industries, society, and are a vital part of the modern infrastructure (Goodman, 2014).

Using the National Initiative for Cybersecurity Education (NICE) framework as a guide, educators can cultivate the Knowledge, Skills, and Abilities (KSAs) through a variety of sources to help students succeed in cyber-related fields (Jones et al., 2018). These learning experiences can be a way to cultivate cyber awareness among the population and supply a cyber-resilient workforce who protects the digital infrastructure in their future occupations

(Mailloux & Grimaila, 2018). In the context of the NICE framework's cyber specialty areas, there is a broad range of contexts that cyber entails, which are not limited to the technology discipline.

Open Educational Resources (OER) provide no-cost opportunities for helping learners advance academic pursuits (Richter & McPherson, 2012). As awareness of OER is increasing among faculty for potential use in course curricula, there is a growing acceptance of OER throughout higher education (Adams et al., 2013). Gaps in the literature exist when researching the influence of OER in the tumultuous and changing field of cybersecurity. With a broad range of options for delivering a curriculum for students in key cyber study areas; cyber professionals report in one study that the knowledge, skills, and abilities required for their job roles were mostly learned on-the-job or self-taught as opposed to a school setting (Jones et al., 2018). To what extent are OERs being used by instructors in their course pedagogy, do faculty find it effective, and what are the perceptions of the barriers that exist for faculty with OER?

Purpose

The purpose of this study is to frame faculty perceptions of OER in the context of cyber curriculum usage in U.S. higher education environments. According to Creswell (2014), survey design "provides quantitative data or numeric description of trends, attitudes, or opinions of a population by studying a sample of that population" (Creswell, 2014). The study focuses on two independent variables, years of teaching experience and the number of cyber discipline focus areas chosen, to determine if there are significant statistical differences with the dependent variables framed into three constructs: OER awareness, OER perceived

effectiveness, and OER potential barriers. The research measures each independent variable for its significance with each of the three constructs of dependent variables.

Significance

The study will set a foundation to study the awareness, perceptions of OER effectiveness, and perceptions of OER potential barriers to the adoption of OER in cyber curricula. It will paint a big picture of the current perceptions of faculty surrounding OER usage in cyber course pedagogy. Results will lead to further research on the utilization and efficacy of OER in different high-level functions of the cyber discipline and help cyber faculty make informed decisions when deciding content for cyber curriculum instruction.

Nature of Study

The figure below frames the research model of this study. It shows the relationship between years of teaching experience and the number of cyber focus areas chosen as independent variables, and the awareness of OERs perceived OER's effectiveness and perceptions of OER potential barriers in cyber curriculum context as dependent variables. The model adapts from previous research into faculty perceptions of OER with alterations in application to the context of cyber disciplines (Leichte, 2018).

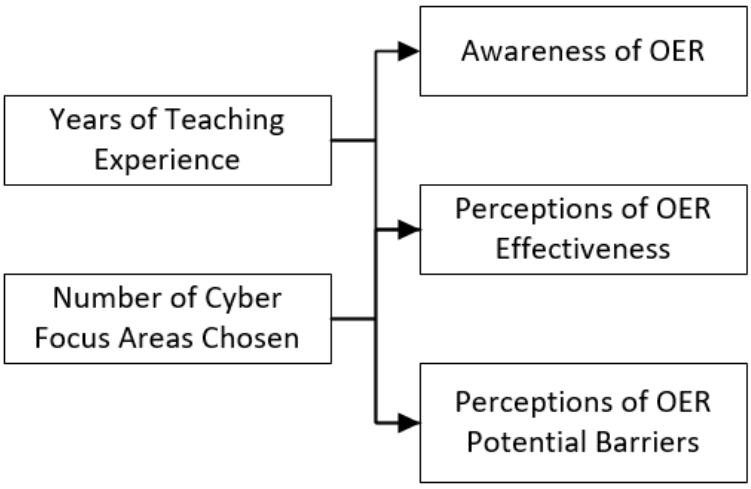

Figure 1. Working Model

Research Questions

This research deals with perceptions of OERs from the perspective of faculty members teaching cybersecurity-related content. The first question illuminates the perceptions of cyber faculty and how they may differ based on faculty experience teaching in academia. The second question sheds light on any perceptions that may exist within cyber faculty grouping based on whether the faculty is a specialist, focusing on fewer aspects of the cyber landscape or a generalist, teaching many different subjects across the NICE framework. The last question looks for differences in perceptions of cyber faculty to determine if there is a significant difference with the amount of time a faculty member has been teaching and whether they are a specialist or generalist according to the NICE framework. The questions

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 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 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?

Conceptual Framework

The Babson Survey Research Group has published multiple reports summarizing faculty perceptions of open educational resources over the years. The most recent was conducted during 2017-2018 and gathered over 4000 responses from faculty and department chairpersons. The report uses descriptive statistics to highlight the perceptions of OER by participants. The survey reports an overall awareness of OER among faculty of about 46%, with faculty awareness increased since the last survey period. Awareness identifies as a possible grouping of related questions to the perceptions of open educational resources by faculty (Seaman & Seaman, 2018). This researcher uses the Babson survey as a basis for instrument creation in this study of faculty perceptions of OER in the cyber curriculum and identifies the first construct of *awareness*.

Hilton identifies twenty studies surrounding perceptions in OER published between 2015 and 2018. In total, these studies included 10,807 students and only 379 faculty. Hilton reports that one of the challenges in studying OER research is that several studies have serious methodological issues (Hilton, 2019). One study, containing a sample size of 127 educators,

frames perspectives of OER in terms of efficacy using descriptive statistics, but the study disseminates through a popular open textbook distributor, OpenStax, which may introduce bias (Pitt, 2015). Though the term *efficacy* and *benefits* exist in the literature, this research into the effects of OER in cyber usage uses the term *benefits* to frame a construct on the positive impacts on course pedagogy.

In 2014, a quantitative study on factors influencing motivations for faculty to share and collaborate on course curriculum identified that several key factors influence successful adoption and usage strategy of OER. Among them are the technological readiness of the institution, the awareness of OER, and the knowledge of how to find high-quality OER. The sample included 754 responses from teachers in primary, secondary, and higher education. Data analysis procedures include factor analysis. The authors of this survey were able to determine five factors contributing specifically to barriers in OER adoption and usage (Pirkkalainen, Jokinen, & Pawlowski, 2014). The researcher forms the third construct, *barriers* that exist within the context of this study on cyber faculty perceptions of OER. It also helps frame methodology using factor analysis to identify subgroups in the data.

Many studies in the literature seem to be using various definitions of contributing factors that exist in OER research. A common theme in the literature is to use descriptive statistics of individual questions to paint a picture of specific aspects OER usage and adoption of OER in results. Using Hilton's warning that methodological flaws exist in published literature (Hilton, 2019), the researcher surmises there is lacking empirical data and results surrounding the factors that affect faculty perceptions of OER. In this research, the researcher proposes a stronger methodology for identifying factors and reporting how OER perceptions

among the cyber faculty population, giving an introspective look to the population of cyber faculty.

Assumptions

The researcher reports the following assumptions and potential bias to limit accidental interference during this research. For the reasons listed below, the researcher has chosen not to be an active participant in the study for concerns of being a potential outlier in the data. The researcher has chosen a methodology and data analysis plan that will focus on the descriptive statistics of the population of the study. Where possible, the researchers aim to reduce the influence of preconceived notions that may skew the results of the study.

The researcher of this study is a full-time faculty member employing OERs in multiple courses at a public state university in the United States. The researcher only teaches courses in computer science and cybersecurity disciplines. The researcher has co-authored OER materials in a statewide initiative to support open textbook transformation grants and adopt OER (Croteau, 2017). The researcher's home institution, as of 2019, has over 35% of its course sections tagged as no- or low-cost for course materials, well above the state average. It is the researcher's philosophy that *access to knowledge* comes with as little impedance as possible. *Proof of knowledge* is the responsibility of certifying agents like formal education programs, certifications, boot-camp programs, and others to verify individuals have the knowledge, skills, and abilities to be successful in the workforce. The researcher believes that it is a fundamental human right to have access to knowledge. Digital OER is a means to that end in the researcher's opinion.

Scope, Limitations, and Delimitations

The scope of the project aims to answer the stated research questions, provide a strengthened methodology for those pursuing OER research, validate the conceptual framework proposed, and gain insights of cyber educators in U.S. higher education that engage in scholarly activities to broaden their knowledge of the cybersecurity landscape. The researcher's goal in this study is to study the population of cyber faculty and their perceptions towards open educational resources in their course instruction. Following other publishers in the field, the researcher aims to provide statistical data that describe the population of cyber faculty and their perceptions towards open course materials.

A significant limitation in the research is obtaining a large enough sample size to describe the actual population adequately. The researcher has limited resources to offer incentives and participate in events for soliciting participation from relevant sources. The study uses online professional organization communication methods and in-person cyber professional development opportunities to build a sample from the relevant cyber faculty population. Using a diverse recruitment strategy, the researcher hopes to improve the sample size to provide adequate coverage of the population (Ponto, 2014).

Though the strength of the data may be a concern due to small sampling, the study will tie together in the field of ever-changing field cybersecurity and OER research. Further research into OER studies with cyber context will have a methodology to begin working their path of inquiry. The researcher intends to draw focus on the potential impacts of OER research to solve a cyber workforce development issue. Descriptive statistics will provide a mechanism to gain familiarity with the field and set a baseline for understanding the OER context in the field of cybersecurity.

Chapter Summary

In this chapter, the researcher provides a frame of reference to the research presented in this study. The needs of the cybersecurity workforce are increasing for qualified candidates. More job opportunities are becoming available, but many positions go unfilled simply due to a lack of qualified candidates. The complexity of the cybersecurity field means public, private, and academic sectors must find creative ways to foster the knowledge, skills, and abilities to build a diverse cyber workforce. Open educational resources (OERs) reduce the barriers needed to gain access to knowledge. With increased acceptance of OERs in traditional learning environments, there is an opportunity to leverage OER to help solve the cyber workforce issue. This study will build upon previous research into OER to set a baseline of faculty perceptions specific to the cyber field.

CHAPTER 2

LITERATURE REVIEW

Needs of Cyber Workforce

A cybersecurity professional group, the International Information System Security Certification Consortium $(ISC)^2$, notes in a 2018 study with cybersecurity professionals that 59% of their respondents view their organization is at extreme or moderate risk due to cybersecurity staff shortage. The top reported job concern was the lack of skilled or experienced cybersecurity personnel, followed by a lack of resources to perform the job effectively. The top three most important qualifications for employment were or relevant cybersecurity work experience, knowledge of cybersecurity concepts, and certifications. For job satisfaction, 68% of respondents reported being very satisfied or somewhat satisfied with their employment. Cyber professionals in the survey reported the most valuable educational methods to be face-to-face instructor-led training and internet-based training. 54% of respondents reported that they were going to pursue a cybersecurity certification within the next year (International Information System Security Certification Consortium, 2018).

Cyber Seek, an organization focused on studying the supply and demand of cybersecurity jobs across the United States, notes that there are almost a million individuals currently employed in the cybersecurity industry. However, the current vacant jobs total over 504,000 at the time of this study ("Cybersecurity Supply/Demand Heat Map," n.d.). Cyber professionals are understaffed in their work environments, with the demand for cyber

professionals still growing. Maximizing diversity and transforming the workforce across multiple disciplines could help educate teachers and students of the possibility of a cyber profession. Maximizing awareness of cyber professions across STEM fields could help to improve the pipeline of qualified candidates to the workforce (Ivy, Lee, Franz, & Crumpton, 2019). Goodman, in 2014, recommends a two-pronged approach for improving the cybersecurity workforce posture. The first is to investigate the workforce itself and identify the knowledge, skills, and abilities that individuals need to possess to succeed. The second is to form partnerships in academia, government, and industry to help grow the workforce in a bottom-up approach (Goodman, 2014).

The Aspen CyberSecurity Group has put forward four recommendations that they believe contribute to the gap in cybersecurity employment. The first trend is that the demand for skills is significantly outpacing the growth and supply of qualified candidates. Inventive ways are needed to educate the populace and train them in the skills needed to participate in the workforce. Another trend contributing to the gap is that large pools of skilled count candidates are left untapped. Unfilled positions could be from a lack of awareness among the population of cybersecurity career pathways or due to individuals with existing skill sets not fitting into the workforce pipeline. A contributing factor limited eligibility is that employers often over-spec the requirements needed for positions. Doing so means that more than 50% of applicants are unqualified for entry-level jobs. Awareness of cybersecurity career paths and how individuals can succeed is also a major contributing factor for building and qualified candidate pipeline. The Aspen CyberSecurity Group encourages employers to review job postings to make sure they're relevant to the jobs in which they are seeking applicants and embrace mentorship, learning, and pathways for allowing individuals to grow their skill sets.

Other factors identified that could help solve this workforce issue include things like not requiring college degrees as a mandatory requirement for employment, simplifying job postings so that they use the NICE framework and avoid industry jargon, and commit to employee development by launching apprenticeship training programs to help individuals grow in their job duties (Aspen Cybersecurity Group, 2018).

Secondary education plays a vital role in the development of individuals for the cyber workforce. Both students and teachers lack awareness of career pathways and the ability to grow within the workforce. Recommendations to help close this gap include professional development opportunities, information sessions, and seeding the possibilities of cyber professionalism outside of their traditional computer science curriculum. Employers may seek highly technical skills, but soft skills such as verbal communication, written communication, the ability to work independently, and work as a member of a team are also important. While STEM fields tend to focus on developing problem-solving abilities, other fields can contribute to the context and critical thinking skills desired in the workforce (Ivy et al., 2019).

GenCyber, a summer camp aiming to engage students from kindergarten to high school, can help raise awareness of cyber careers to individuals at an early age. Students can discover more about the cyber career field, the type of work that professionals use in day-to-day operations, and begin growing skill sets needed for the workforce. The mission of GenCyber is to increase interest in cybersecurity, increase diversity in the cybersecurity workforce, raise awareness, and help improve teaching cybersecurity content in K through 12 curricula. There are three types of summer camps available: camps for students, camps for teachers, and camps featuring a combination of teachers and students. Camps can vary in length between one week and three weeks an is open to the general populace free of charge.

Funding for the camps comes from the National Security Agency (NSA) and the National Science Foundation (NSF). In 2016, the GenCyber program funded over 120 camps nationwide that reached more than 4,000 students and 1,000 teachers. These programs are offered at universities and institutions nationwide and have shown success in generating interest in both teachers and students (Ladabouche & LaFountain, 2016).

The Digital Divide

In President Bill Clinton's 1990 State of the Union address, he unveiled a comprehensive plan to help make computers and the internet more widely available to Americans as a top priority for his administration. The Digital Divide to Digital Opportunity proposal aimed to make the internet and communications technologies commonplace in homes, schools, libraries, and throughout local communities. President Clinton stressed the importance technology would play in the future economic, political, and social life of all Americans. The speech helped define the term *Digital Divide* in the following quote. *"Opportunity for all requires something else today – having access to a computer and knowing how to use it. That means we must close the digital divide between those who've got the tools and those who don't."* The plan included funding and partnerships with technology industries to make computers more ubiquitous in U.S society ("Making a difference in communities across the nation," 2000).

Internet and computing technologies have become commonplace in American society in the almost twenty years since President Clinton's original proposal. In 2018, one report states that over half of the world's population is currently using the internet and that 85.3% of households in developed countries had access to the internet (ITU Publications, 2018).

Research into the digital divide continues to identify gaps in access to technology among many types of groups but extends to include topics such as skill-based competencies. Consumption skills, for example, primarily focus on the abilities of users to consume and use commodity technology; such as reading websites, email, and consuming digital content. Production skills are abilities for users to not just consume technology but to produce new technologies. For example, this may include activities like creating websites, writing code, or producing new content for others to consume through the internet (Rogers, 2016).

In 2016, President Obama signed an executing order creating a commission for enhancing the U.S. national cybersecurity posture. The commission examined the cybersecurity landscape and tasked with working with both private and public entities across industry, academia, and government to provide recommendations to improve U.S. cybersecurity capabilities. The mandate of the commission includes studying and researching actions necessary to improve cybersecurity awareness, risk management, and adoption of best practices throughout the private sector and all levels of government (Obama, 2016).

NICE Framework

The National Cybersecurity Workforce Framework (NCWF) by the National Initiative for Cybersecurity Education (NICE) is an effort to increase cyber awareness for workforce development needs. The framework identifies seven key areas to the cybersecurity field, which does not use jargon or technical language based on different roles cybersecurity professionals may work in the field (Santos, Pereira, & Mendes, 2017). These non-technical descriptions help eliminate language barriers to individuals with low computer skills to understand and interpret concepts into learning about the field. In August 2017, under the

National Institute of Science and Technology (NIST) Special Publication 800-181, conceptualizes the NICE framework (Newhouse et al., 2017).

Table 1. Seven NICE Framework Categories

Code	Category	Description
SP	Securely Provision	Conceptualizes, designs, procures, and/or builds secure information technology systems, with responsibility for aspects of system and/or network development
OM	Operate and Maintain	Provides the support, administration, and maintenance necessary to ensure the effective and efficient information technology (IT) system performance and security.
OV	Oversee and Govern	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
PR	Protect and Defend	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
AN	Analyze	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence
CO	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 (IT) systems, networks, and digital evidence.

Goodman (2014) identified two major viewpoints about building a cybersecurity workforce (Goodman, 2014). The first involves taking an introspective look at the needs-based demand on the cybersecurity field. In a recent survey of cybersecurity professionals, the top ten skills and abilities identified as important to the job, all were learned mostly on-the-job by the individual to fill a required task. Learning the knowledge from a school setting showed the second most important for only three of the most important skills. Individuals reported that most of the top skills required in the cybersecurity knowledge they acquired are either on-the-job or self-taught. Two limitations to this study exist: the concept of self-taught versus school setting might be ambiguous, and the KSAs could be covered in school course curricula but additionally learned from self-learning or on-the-job training. Questions on the survey asked what medium of instruction was most beneficial to their learning; therefore, multiple forms of learning for the same KSA could apply. The KSA associated with programming logic and structures participants rated a school environment as being most beneficial to their learning. A common theme among all respondents is that soft skills were very important to learn in a school setting before joining the workforce (Jones et al., 2018).

Goodman's (2014) second viewpoint identifies the need for colleges and universities to develop pathways to the workforce and partnerships with industry (Goodman, 2014). Working towards a secure digital infrastructure through cybersecurity can be seen as a public good and akin to providing safety for society (Asllani, White, & Ettkin, 2013). Building communities of responsible computer users will rely on extending cyber awareness beyond the computer science curriculum into other disciplines of study and contexts (Santos et al., 2017). Research relating to *digital citizenship* builds upon this notion that users must take some ownership of their role in a digital society (Hollandsworth, Dowdy, & Donovan, 2011).

Raising awareness of the benefits, risks, and consequences of participating in digital interactions is increasingly becoming common in K-12 educational environments (Hollandsworth, Donovan, & Welch, 2017). Institutions that embrace and teach digital citizenry concepts may have an advantage in incorporating deeper cybersecurity-related content into the curriculum.

Educational Theories

Individuals joining the cyber workforce need more than just technical skills to be successful. Science, technology, engineering, and mathematical (STEM) fields play a role in a well-rounded workforce, but a resilient cyber workforce also includes psychology, critical thinking, reasoning skills, and the ability to interact in a team environment socially (Dawson & Thomson, 2018). Secondary education provides an opportunity to help build an interdisciplinary approach to the cyber workforce pipeline by portraying how both technical and non-technical roles can fill the cyber workforce pipeline and raise awareness of cybersecurity issues (Ivy et al., 2019). The educational and awareness in higher education cybersecurity strategies must focus on the needs of the cybersecurity workforce (Goodman, 2014).

John Dewey Is an influential figure in educational and social reform topics. Though Dewey's works are largely from the early to mid 20th century, the influence of his perspectives still influences the educational landscape today in the 21st century. Dewey was an outspoken critic of the traditional "old school" teaching methodologies that emphasized studying the body of knowledge as static and unchanging. Instead, Dewey promoted a child-centered approach to educational reform emphasizing education as a necessity of life, social

change, and reconstruction of individual experience (Achkovska-Leshkovska & Spaseva, 2016).

Dewey saw education as a means of social change and a key pillar upon which a democratic, free, and peaceful world relies. Only educated individuals could fully participate in a free and democratic society. Education, under Dewey, should aim to create individuals who can understand the complexity of social issues and take an active approach to engage in societal concerns. Education should not just consist of telling of facts and body of knowledge, but rather be an active and constructive process that promotes cognitive development and critical thinking skills (Pérez-Ibáñez, 2018).

Dewey viewed education as a continuous process constantly undergoing renewal, reconstruction, and shaping the evolution of society. Educational philosophy is a lens by which individuals can discuss important societal factors, understand them, and reach consensus on the impacts of solutions in the social community. Education, in an iterative development cycle, will influence the direction that society evolves through time (Campbell, 2016).

Bloom's Taxonomy, first introduced in 1956 by Dr. Benjamin Bloom, is a popular classification system for organizing educational objectives. The goal is to describe different levels of learning and how learning objectives can scale to higher levels of thinking. Bloom's Taxonomy exists as a pyramid as a symbol that higher levels of thinking build upon a base of common knowledge. At the bottom of the pyramid, knowing and understanding facts and knowledge is required for a learner to have a solid foundation of the contexts under study. As the learner moves up the pyramid, that can build upon that context into applying and analyzing their usage of topics. At the highest levels of thinking, the learner should be able to

create and evaluate new topics inside a body of knowledge. Bloom's Taxonomy is one of the most imperative elements in designing curriculum, building learning outcomes, and evaluating that students are meeting objectives through the curriculum (Sikandar, 2017).

The use of rubrics in educational settings is a way of ensuring that students are meeting performance expectations in their studies. Rubrics contain concise performance criteria, rating scales, and descriptions that give clear expectations for students to succeed on deliverables (Minnich et al., 2018). Rubrics help educators measure how well students are performing to expectations, promote critical thinking in students to meet those expectations, and facilitate communication between students and instructors for directional learning (de la Rosa Gómez, Meza Cano, & Miranda Díaz, 2019). The use of a rubric in cybersecurity education can help educators make sure that student learning outcomes meet the needs of the cybersecurity industry.

Cyber Curriculum Development

Developing materials for cyber training comes with many challenges. The shifting landscape means that materials must undergo improvement cycles for relevance in real-world scenarios. Individuals cannot expect to come prepared to the field of cyber for every scenario that may occur; instead, educators must focus on bestowing relevant skills needed to excel in the field from both technical and non-technical contexts (Jones et al., 2018).

Further research shows that hands-on exercises and case studies can be very beneficial to improving understanding and retention of cyber training in general. Those in the field of cyber must develop a diverse set of skills to tackle the wide array of topics that exist in real-life scenarios and try to align learning objectives to that of the workforce. An underlying

theme that individuals should keep in mind is that there is little research to show that cyber curricula reflect the needs of the industry (Santos et al., 2017). Integrating Bloom's Taxonomy into cyber curriculum usage could help qualify that individuals are gaining higher levels of thinking while engaging in cybersecurity topics (Harris & Patten, 2015).

Professional certifications may hold the key to shaping cybersecurity curricula. Industry certifications help qualify that individuals possess the knowledge, skills, and abilities for work in the job field as much as one-third of cybersecurity-related jobs require some form of certification. Educators can find value by shaping and refining the curriculum based on certifying organizations and their pursuits to remain relevant in a changing landscape. Maintaining knowledge of industry certifications, and how they evolve to meet the needs of industry, could provide great insight for those wishing to create and refine cyber curricula to meet the needs of the workforce. Educators need to acknowledge that education should not focus on qualifying individuals for certification or test. Instead, educators should focus on learning the skills and abilities needed to enhance learners' knowledge of new techniques and trends (Knapp et al., 2017).

Some curriculum developers suggest that cyber education programs need to extend beyond the traditional classroom environment to entail more extracurricular activities and partnerships with local industries requiring individuals with cyber skills. These partnerships and learning opportunities can help develop new opportunities for learners the practice the skills they need to succeed in the industry (Woodward, Imboden, & Martin, 2013). Expanding beyond computer-related disciplines, proponents of cyber literacy may begin to run into new issues spreading awareness of topics in today's world. The Digital Divide for knowledge of Information and Communications Technologies (ICTs) continues to separate not only those

with the skills and abilities to perform simple computer-related tasks; but for individuals to bridge the barrier between not just being consumers of technology, but those that understand how it works in-depth (Rogers, 2016). The proliferation of technology continues to evolve as more people gain access to the internet; assuming all learners have access to such ICT devices is still premature (Rowsell, Morrell, & Alvermann, 2017). The rise in mobile devices and faster mobile broadband speeds hold high potential as a possible conduit for reaching out to individuals in bridging the digital divide; however, the cost of such devices and access continues to be a limiting factor for many individuals (U.S. Department of Commerce: National Telecommunications and Information Administration, 2014). Capitalizing on OER and mobile device access continues to be an interesting area of study for furthering educational goals for those who did not have access to it before (Ally & Samaka, 2013).

Background of OER

In 2002, The United Nations Educational, Scientific, and Cultural Organization (UNESCO) put forward a report summarizing a forum studying education in developing countries. Participants included members from government, industry, and educational backgrounds. General topics discussed included defining open courseware and the impact it could have on higher education. Additional topics included recommendations, assessing needs, limitations, and other concerns. The forum began with a rough definition of Open Courseware, as defined below.

Open Courseware

1. Provides educational resources for college and university faculties to adapt following their curricular and pedagogical requirements.

2. Includes the technology to support open, meaningful access, and use of the courseware.
3. Includes at a minimum the course description, syllabus, calendar, and at least one of the following:
    - Lecture notes
    - demonstrations, simulations, illustrations, learning objects
    - reading materials
    - assessments projects
4. Does not normally provide direct open learning support for students

Working groups at the forum were organized and tasked with making recommendations concerning the use of open courseware in higher education of developing countries. One goal of the working group was to formalize the name and definition of the concept known as open courseware. The group recommended the term Open Educational Resources with the following definition:

"The open provision of educational resources, enabled by information and communication technologies, for consultation, use, and adaptation by a community of users for non-commercial purposes."

The working group gave other recommendations for open educational resources. Research areas for evaluation, improvement, accessibility, quality, usability, and effectiveness were identified as potential areas to study in OER research (UNESCO, 2002).

Open Educational Resources

Since its initial finding, the terminology for Open Educational Resources has expanded to include many definitions by various. The William and Flora Hewlett Foundation is one such organization that was present at the first UNESCO forum investigating the use of open of course materials in developing countries. They are partners with UNESCO, Creative Commons, and MIT and share a common goal of promoting worldwide public access to learning materials organizations and tasked with evaluating the usage of OER (William and Flora Hewlett Foundation, 2019). The William and Flora Hewlett Foundation's definition is used to set the context for what OER entails in this study.

Open educational resources are 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 (William and Flora Hewlett Foundation, n.d.).

Open-Source Software

The term "open-source" refers to something people can freely modify and share because the design is publicly accessible. This term developed in the context of software engineering as an approach to creating software programs ("What is open source?," n.d.). Open Source Software (OSS) is the source code from a computer program that anyone can inspect, modify, or enhance to their liking. Programmers in this design approach collaboratively work together to create software programs and freely share code among one another to fix and add features. This approach is different from other approaches in that either the person team or organization who created it maintains exclusive control over the rights. Dictating how people can modify or use the software is known as "proprietary" or "closed-

source" software. Authors of open-source software freely share their code and make it available to others who can use it (Open Source Initiative, 2007).

Just because the software is openly accessible does not mean then it isn't subject to licensing agreements from the authors. These licensing agreements dictate free redistribution, allowing derived works, provide no discrimination against persons or groups, and be non-restrictive with other software. Open-source licensing can affect the way people use, study, modify, distribute, and attribute those that created the software (Open Source Initiative, 2007). Some people may prefer using open-source software over proprietary software because it includes more control, ability to train, security, and stability. Many organizations hire programmers and developers specifically for their knowledge of open source software ("What is open source?," n.d.).

Open-source software has proven beneficial in software development courses. Open-source software can simulate real working environments that develop software. The collaborative environment among members contributing to a team effort and the flexibility for source code modifications teaches students to develop their skills during instruction. Open-source software can help facilitate learning and understanding of version and source control systems and leverage developer documentation as a learning instrument. Open-source software is generally free, helping to reduce the costs of course materials. Students must understand the software development process, how to test, and configure the environment. The use of open-source software can help set the context of a real-life project. In one study, the researchers found that by including open-source software as course material helped increase the confidence of students dealing with complex in real-world projects (Dorodchi & Dehbozorgi, 2016).

Open Textbooks

The costs of traditional textbooks can present a barrier for many students wishing to further educational endeavors. Open textbooks are a type of OER that faculty can choose to replace the traditional textbook. Open textbooks provide faculty and students with low-cost alternatives to traditional textbooks to help make higher education more affordable (Costello, Bolger, Soverino, Brown, & Conole, 2019). The Community College Open Textbook Project (CCOTP), in partnership with Rice University's Connexions program, was created in March 2008 to study and identify sustainable models for promoting the use of open textbooks at community colleges and provide a proof-of-concept for an open textbook. The CCOTP Identified several challenges to the production and adoption open textbooks: 1) faculty members and students expectations of high production quality and inclusion ancillary materials in open textbooks 2) methods for documenting and maintaining control over various versions of open textbooks, and 3) the process of converting existing open content to digital and accessible formats (Baker, Thierstein, Fletcher, Kaur, & Emmons, 2009).

Rice University's Connexion program evolved into today's OpenStax textbook repository. The repository consists of many textbooks that cover various subject areas common in education. Over 1,000 courses internationally use OpenStax textbooks as primary source material (The William and Flora Hewlett Foundation, 2015). One study reports that the use of open textbooks is key to reducing costs for students. The study found that grades given in the courses were comparable regardless of textbook choice between a traditional or open textbook. The withdrawal rate was reduced in the courses using an open-source textbook over a traditional textbook (Clinton, 2018).

OER Landscape

William and Flora Hewlett Foundation in 2019 released a strategic report on the global OER landscape. They surveyed around 150 articles from around the world surrounding OER research. Experts recognize that in North America, the costs, perceptions, open textbooks, and student outcomes tend to be the most prominent topics of study. Of 126 of the studies, higher education studies form about 58% of the OER research body identified in the report. 70% of studies explore multiple topics in OER. Most studies tend to focus on the adoption and discoverability of OER (34%) and teacher practice and pedagogy using OER (34%). Studies of perceptions of OER (27%) and policy design and implementation (25%) are other common areas of focus in the literature. Around 50% of these studies use mixed methodologies and around 31% use opinion/perceptions surveys. Five experts interviewed for the strategic report largely believe that openly licensed textbooks lead to as good or better student learning outcomes than traditional textbooks. Policy advocates recommend more research on the adoption implementation OER in educational settings. These methods can include financing, overcoming administrative challenges, or promoting educator best practices. One expert notes an area for improvement, “I've seen hardly any research that is scientifically rigorous. The vast majority of the research is anecdotal in nature and a lot of it is so small scale that it becomes irrelevant for generalization of findings.” The experts recommend as a priority to see if more rigorous research methods can validate the impacts on student learning outcomes.

Funding for OER research can come from a variety of sources. Though there are some global partners like the Hewlett and flora Hewlett foundation that fund OER projects. Many monetary gains by OER authors more likely will come from institutional or small-scale benefactors. Funders may include state governments, industry partners, or strategic

organizations. One advocate notes OER itself is underfunded, but individuals that can capitalize on OER as a means to solve a problem can find big money available to them in such pursuits. OER practitioners can provide a more versatile learning toolset by adopting OER pedagogy and engage in learning opportunities (William and Flora Hewlett Foundation, 2019). Though OER usage shows cost savings for students over traditional learning materials, developing sustainable financial models to encourage faculty and policy-makers to continue supporting OER is a concern. Barriers to the adoption of OER could be reservations about the quality and the loss of control over intellectual property when adopting OER. A common theme among the literature surrounding the financial sustainability of OER is its inability to generate stable revenue streams and that it may compete for commercially available alternatives. Many forms of monetary compensation may come in the form of grants to faculty for creating or adopting OER. However, most projects do not survive beyond two to three years in practice once start-up funding has been exhausted (Annand, 2015).

The University System of Georgia (USG) consists of 26 post-secondary public institutions of higher learning in the southeastern state of Georgia. The state of Georgia passed a budget proposal in 2014 that includes an initiative for an Affordable Learning Georgia program. This initiative implemented Textbook Transformation Grants that included monetary benefits for encouraging faculty to transform their learning materials into lower-cost options for students (Croteau, 2017). Since its inception, the initiative has saved over 379,000 students an estimated 61.9 million dollars in textbook costs. All 26 of the USG institutions have participated in the initiative, with 334 out of 566 applications funded (“ALG statistics, research, and reports,” n.d.). In 2018, the USG conducted a system-wide faculty perception survey of OER among faculty and professional staff at the institutions. The instrument used

by USG builds upon the same survey instrument used in this study by Seaman and Seaman. In total, 1,719 faculty and staff across 25 of the USG institutions participated in the survey. 84.5% of the respondents were instructional faculty, primarily teaching in a face-to-face setting (Gallant & Lasseter, 2018).

Cyber OER

The Cybersecurity Labs and Resource Knowledge Base (CLARK) is an OER repository consisting of cybersecurity topics. Clark organizes cybersecurity topics into courses, units, modules, micro modules, and nanomodules. CLARK aims to be a cybersecurity digital library that allows faculty teaching cybersecurity to post materials and share their cybersecurity curriculum with other educators (Dark, Kaza, & Taylor, 2018).

CLARK requires submissions to be learning-outcomes based on Bloom's Taxonomy. Submissions also follow classification themes to help searchers find relevant cyber OER easier. For example, a course can be marked with a level indicator to show its relevance towards various K-12 education environments, multiple higher education environments, or job training purposes("CLARK," n.d.).

As of 2018, CLARK contains 116 learning objects entered by 38 different curriculum developers. The systems design is scalable to adjust to emerging topics across the cybersecurity landscape. A National Security Agency grant financially supports CLARK for continued development and support (Dark et al., 2018).

OER Research

Since 2002, the United Nations Educational Scientific and Cultural Organization (UNESCO) and other proponents of OER continue to embrace the creation and adoption of open learning materials to supply and improve learning (UNESCO, 2002). Open Educational Resources (OERs) provide educators with unique opportunities to transform learning for individuals across the world (Richter & McPherson, 2012). Many free resources exist for students and educators to help them improve student engagement. Educators should be encouraged to seek out new sources on materials and develop their content (Johnson, 2014). The creation and adoption of OER resources continue to increase among educators and institutions, wanting to leverage the benefits of embracing OER (Adams et al., 2013). This research will focus on UNESCO's definition of OER described as "teaching, learning, and research materials in any medium, digital or otherwise, that reside in the public domain or available under an open license that permits no-cost access, use, adaptation, and redistribution by others with no or limited restrictions (UNESCO, 2002)."

For what OER can help to improve learning environments, there are limitations and recommendations that adopters should consider when adopting OER (Wiley & Hilton III, 2018). In one report published in the Higher Education Journal, the authors identified three main tensions that exist for educators using a mixed methodology when engaging with OER resources. The barriers include tensions between organizational policies and needs of the individual educator, institutional responsibility to maintain academic integrity, and the balance between cost efficiency and learning objectives for students (Kaatrakoski, Littlejohn, & Hood, 2017). Educators can spend as much or even more time building course materials when using open materials (Bliss, Robinson, Hilton, & Wiley, 2013). Research into

developing sustainable financial and evaluation models for continuous improvement over time eludes many institutions (Annand, 2015). Ultimately the decision to adopt OER must be up to the individual, and institutions should consider its use, but not mandate educators conform to no-cost course resource options (Masterman, 2016).

The RISE (Resource Inspection, Selection, and Enhancement) framework is a useful mechanism for helping educators streamline the process for finding, selecting, and enhancing OER resources by fulfilling learning outcomes using continuous improvement (Bodily, Nyland, & Wiley, 2017). The feedback loops in the model help drive future development as materials evolve, and constant tweaking is applied to improve pedagogy and delivery of materials. This process may help alleviate tensions that OER is not of academic and professional quality. Although this research is not yet complete, it holds great promise to laying a foundational framework for evaluating student performance in OER contexts. Students are also open to using open learning materials for coursework to replace traditional purchased textbooks and exhibit higher engagement rates than with traditional learning materials (Lindshield & Adhikari, 2013). However, students do exhibit barriers when it comes to accessibility with online materials and the quality of the material they learn. Overall, most individuals may consider OER resources as equal quality to traditional textbook usage in a learning environment (Bliss et al., 2013). Research into using OER has drastically increased in recent years with academic and research communities becoming more receptive to incorporating OER (Paragarino, Silveira, & Llamas-Nistal, 2018).

The COUP (cost, outcomes, uses, and perceptions) framework is a common mentality to frame the study of OER (Bliss et al., 2013). Research into the effects of “cost” focus on how much students save in courses that use open textbooks, how much students typically

spend on textbooks, and how the cost of research materials affects students' academics choices. Studies surrounding OER “outcomes” tend to focus on how OER affects grades, learning outcomes, and retention rates. Research studying the “use” of OER focus on how often and how students use learning materials in academic learning include the type of materials and the medium in which they access it. It can also include the types of licensing used and how faculty may transform OER for their purposes. Research in OER perceptions considers how various actors perceive OER in the academic ecosystem. Topics in perceptions research can include the awareness, quality, benefits, and barriers facing OER in the research body by faculty and students (Hendricks, Reinsberg, & Rieger, 2017).

In one case study, researchers found that student and teacher perceptions of the cost of traditional textbooks between $60.00 and $83.00 fairly typical per course. The majority of students spend between $200 and $300 per semester on textbook materials alone. However, with OER materials implemented, students and teachers reported spending less than $20 on course materials per course (Bliss et al., 2013).

OER Perceptions Research

Most of the research encountered in the literature review points to a positive view of OER among faculty and students. In one study in 2015 at Ohio State University, faculty and students across twelve courses were generally pleased with their experience using open and affordable materials in a study using descriptive analysis. The researchers found that the quality and experience of using OER were the most significant factors to their positive views of OER (Jaggars, Folk, & Mullins, 2018).

At Regis College, researchers used an OER in an introductory astronomy course and measured students' academic performance of two groups of students in Fall 2017 and Fall 2018. Each class had 14 students from generally similar backgrounds (non-science majors). The fall 2017 class used a traditional textbook, but the fall 2018 course used an OER. The researchers found that students saved about $200 a semester by using the OER. Descriptive analysis in SPSS found there were no statistical differences in the final course grades between the two groups (Mathew & Kashyap, 2019).

One study in an introductory information systems course covered four different sections; two sections used a traditional textbook and two used an OER textbook. The researcher uses statistical analysis to determine if there were any significant differences between the groups. The researcher found that students across all four sections had nearly the same performance on quizzes and tests. Technical assignments requiring hands-on exercises also saw a near-identical scoring across all sections. The researcher reports that students using the OER can have better performance in discussion topics than those using the traditional textbook. Overall, the researcher claims that students using OER can achieve the same level of student learning compared with students using purchased textbooks (Wang & Wang, 2017).

In 2017, Grewe and Davis focused their research on the impacts and efficacy of using OER and student achievement in an online history course. The study looks at correlations of OER between prior academic achievement and student achievement. The researcher found a moderate positive correlation between OER and Non-OER in regards to student achievement. Overall the researcher found that OER students performed as well or better than students using commercial textbooks. The researcher notes that one limitation in this study is the small

sample size and suggest the model is ready for large-scale investigation (Grewe & Davis, 2017).

Conclusion

There is a strong need for cooperation between governments, industry, and educational institutions to collaborate on developing a workforce that can adapt to the changing needs within the field of cybersecurity. As the field of cyber continues to grow, evolving new topics on critical infrastructures, creating resilient systems, and extending cybersecurity principles to all technology users is of increasing importance to securing society's digital infrastructure. Technical training is not enough to satisfy the needs of the workforce; analytical, problem solving, and communication skills need to complement technical skills so that individuals can adapt to changing environments. OER introduces new possibilities to shape learning environments for many individuals across the globe. Limitations and misconceptions of OER play an important role in adoption and creation, but OER can provide new and engaging opportunities for learners to tackle new topics. Encouraging cyber professionals, industry leaders, and educators to create, contribute, and adopt open learning materials could help produce a more mature and safe digital society.

Resources

The research contained within this proposal sets the stage for the involvement of OER involvement in cyber curricula. Parts of this literature review have been accepted to the 2019 8th International Conference on Language, Medias, and Culture (ICLMC 2019) in Osaka and

have been suggested for publication in journal format under the title *Exploring Open Educational Resources in Cyber Training* by Alan Stines & Houssain Kettani.

CHAPTER 3

RESEARCH METHODOLOGY

The purpose of this study was to frame the awareness, perceived effectiveness, and perceived barriers of Open Educational Resources (OER) for faculty teaching courses with the cyber curriculum. A previous survey by the Babson Survey Research group surrounding faculty perceptions of open educational resources was modified, with permission, to apply to the cyber field and frame three constructs: awareness, effectiveness, and perceived barriers. The study surveyed faculty to determine if there were any significant statistical differences between independent variables of an educator's years of teaching experience and cyber discipline focus area to that of the dependent variables measuring awareness, perceived effectiveness, and potential barriers of using OER in course instruction. The research aims to provide insights into the following research questions.

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 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 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?

Research Methods and Design

The design selected for this study was a cross-sectional descriptive quantitative methodology. Quantitative methods implementing survey design are useful for determining the attitudes, opinions, and trends of a population by studying a sample of that population (Creswell, 2014). Descriptive studies combine both verbal descriptions and descriptive statistics to provide context to research questions (Procheş, 2016). Descriptive studies are useful in trend analysis, population monitoring, and hypothesis generation (Grimes & Schulz, 2002). Cross-sectional studies are carried out over a short period to reflect the characteristics of a population at a given point in time (Levin, 2006).

A cross-sectional study surveys faculty involved in several avenues of cyber professional development. Cross-sectional studies are appropriate when the study is descriptive, in the form of a survey, and the aim is to describe a population or subgroup of a population at one point in time (Levin, 2006). An internet-based survey tool allows the researcher to standardize and provide ease of use for participants and the researcher among the many data collection points. A third-party vendor, SurveyMonkey, was chosen to facilitate the research.

The design exhibited some limitations that must be into consideration with the presented research. A common mistake when using descriptive studies is overstepping the

data, introducing bias, and drawing inferences that do not exist in the data (Grimes & Schulz, 2002). The researcher proposes research questions to study to explore data surrounding the area of study. Using empirical research methods, the researcher aims to study and report evidence of the relationship between faculty perceptions of using OER in cyber contexts. Evidence includes factor groupings, selected terminology, or complete coverage of the issues at study.

Population

The target population for the survey consisted of faculty pursuing professional development opportunities focusing on cyber-related topics. Faculty professional development includes many activities designed to help improve teacher performance and better learning outcomes for students (Steinert et al., 2006). Faculty consists of individuals teaching in institutions of higher education. The Carnegie Classification System defines six different types of institutions of higher education: doctoral universities, master's colleges, and universities, baccalaureate colleges, associate's colleges, special focus institutions, and tribal colleges (Carnegie Commission, 2018). Cyber refers to subject areas defined under the National Initiative for Cybersecurity Education (NICE) framework describing the cybersecurity workforce needs in the industry (Newhouse et al., 2017). Cyber faculty are individuals from institutions of higher education, seeking to deepen their cyber knowledge and teaching practices through faculty professional development initiatives.

Sampling

Purposive sampling, also known as judgmental sampling, is used when the researcher wants to study a small subset of a larger population, which are identifiable, but an enumeration of all of them is nearly impossible (Babbie, 2001). Operating under the assumption that "motivating faculty is like herding cats" (Hoadley & Mento, 2010), a multi-prong approach to soliciting feedback from cyber venues build the sampling. Participants were solicited for in email newsletters with professional organizations, online forum postings with professional organizations, and at in-person professional development events.

During survey collection, several individuals expressed a desire to share the research with colleagues and solicit additional responses on the researcher's behalf. Snowball sampling is appropriate when members of a special population are difficult to find, and the researcher may ask individuals representative of a group to seek out other participants on the researcher's behalf (Babbie, 2001). The researcher did not actively ask participants to perform snowball sampling in fear of demotivating responses. However, if the participant volunteered or asked about the confines of the sampling, it was encouraged to help build responses for data analysis. Discussion of the population intent was also shared to give influential members of the group guidance with whom to solicit responses from if they carried out snowball sampling.

Informed Consent

This research involves human subjects as participants and falls under the purview of the Institutional Review Board (IRB). IRB ruled the project exempt from review for falling outside the definitions of Human-Subject Research, as noted under federal regulation 45 Code

of Federal Regulations Part 46.102(e)(1) under the protection of human subjects. An addendum submitted after original approval to the IRB for approval with slight modifications to the instrument and approval of advertising materials. IRB reviews occurred before any data collection started. The front page of the survey served as informed consent in written format.

There were no foreseen risks for participating in the survey. Participants were informed their participation was purely voluntary, and they could quit the survey at any time. Clear definitions for what the study was about and what the researcher was asking participants to perform were displayed. The researcher informed participants that their answers are confidential and to be kept private during research and publishing. Survey Monkey was configured to prevent logging of Internet Protocol (IP) addresses to help preserve anonymity and privacy as well. Only participants older than 18 could complete the survey.

The informed consent included information on the approval by IRB and provided contact information to follow up with questions. Volunteers needed to agree to the statement of consent to continue completing the survey.

Data Collection Procedures

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, only offers abilities to “buy responses” based on general demographics and does not support an incentives ability directly. Cyber faculty, being a niche population as defined above, 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 have a significant effect on participation in survey research but are best when incentives are allocated fairly for the participants (Singer, Groves, & Corning, 1999).

Instrument

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, Pitt, Hendricks, Key, & Lalonde, 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 identifying 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, number of years teaching at the collegiate level, the number of years teaching in the cyber discipline, who typically has control over selection of resources for courses, and identifying primary focus of cyber teaching through the NICE framework. There are seven questions that 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 two survey faculty perceptions of Oh ER effectiveness. These questions include topics of weather OER leads to an improvement in students' performance, improvements in student satisfaction, that 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 3rd construct aims to assess 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.

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 each, have been published

since 2014 by the group. The later studies use similar instrumentation to 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, Is an organization focusing on empirical research related to the perceptions and efficacy in a higher education environment open educational resources and academia. This group uses the Maps and research surveys as a road map for compiling various research across the OER spectrum (Hilton III & Mason, n.d.). The survey used in this study bases its design upon the 2014 instrument used to study perceptions of open educational resources in academia.

Factor analysis is useful for finding correlated variables that form together to create a latent variable consisting of multiple parts. This statistical method will be useful 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 related to the concepts of awareness, potential benefits, and potential barriers facing the cyber OER landscape. Cronbach Alpha is a measure of 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).

Data Analysis

Collected data was 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 to one another. 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 procedure requires the quality of the data to pass certain tests to give a valid result during the analysis. In total, nine assumptions dictate the quality of the reported data. However, there is some flexibility to massage the data during analysis to account for assumptions violating the tests. The list below describes MANOVA assumptions and how they relate to the study for using SPSS for data analysis ("One-way MANOVA in SPSS Statistics," n.d.).

- Assumption #1: Two or more dependent variables use interval-based values. There are three dependent variables in this study. They are the average values of 3 constructs defined as OER of awareness, OER perceptions of benefits, and OER perceptions of barriers of cyber faculty.
- Assumption #2: Independent variables should consist of two or more independent groups. In this study, the dependent variables consist of the number of years teaching experience held by faculty and the number of roles that faculty fill according to the NICE framework.
- Assumption #3: No participant should be in more than one group. In the two dependent variables for this study, the participants reporting the number of years teaching and the number of NICE roles filled by faculty are independent of one another and do not exist in more than one group.
- Assumption #4: MANOVA provides higher reliability with larger sample sizes. An adequate size is to have more responses than the number of dependents variables in the analysis. With a dual-pronged approach to seeking participants online and in-person events, the researcher will provide an adequate dataset for analysis.

- Assumption #5: There are no outliers in the data. Steps will be taken during data and analysis to eliminate any potential outliers.
- Assumption #6: There is normality in the multivariate data. The Shapiro-Wilk test of normality can test each of the dependent variables, but the researcher has to decide whether multivariate normality exists in the sample.
- Assumption #7: There is a linear relationship between each pair of dependent variables for each of the groups representing the independent variables. In this study, all three dependent variables use 7 Likert-scale instruments from 'Strongly Disagree' to 'Strongly Agree' and using the same linear relationship.
- Assumption #8: There is homogeneity of the variance-covariances matrices. Box's M test of equality of covariance is useful to determine if data violates this assumption.
- Assumption #9: There is no multicollinearity in the sample. While it is ideal to have dependent variables that relate to one another, if the correlation is too high (greater than 0.9), it could become an issue during the MANOVA procedure.

MANOVA requires all assumptions to be met for appropriateness of its usage. Assumptions 1, 2, 3, and 7 were fulfilled for MANOVA by the survey instrument design before soliciting participants for the study. During data analysis in the next chapter, assumptions 4, 5, 6, 8, and 9 are addressed for the appropriateness of using MANOVA.

Chapter Summary

The study set out to determine if there are any significant differences in faculty perceptions of OER awareness, OER effectiveness, and OER potential barriers to the independent variables (numbers of years teaching and the number of NICE roles filled) using

a cross-sectional descriptive quantitative methodology. The findings will describe the characteristics of the usage of OER by faculty in current cyber curriculum instruction. Results faculty perceptions of OER effectiveness and potential OER implementation barriers could help educators in the field of cybersecurity.

CHAPTER 4

RESULTS AND DISCUSSION

The research aims to provide insights into cyber faculty perceptions of Open Educational Resources (OER) in cyber curriculum usage of U.S. higher education environments focusing on cyber education. It illustrates the landscape that OER is playing in these educational environments seeking to increase awareness and strengthen pipelines for new candidates entering the cyber workforce. The participants were asked to measure their perceptions of OER in their cyber curriculum. From this information, this research intended to answer the following questions.

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 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 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?

The research employs a quantitative methodology using survey design. The survey used in this study was adapted from a previous survey instrument developed by the Babson Survey Research Group. The previous instrument was used in three large-scale nation-wide surveys across the United States (E. Allen & Seaman, 2016; I. E. Allen & Seaman, 2014; Seaman & Seaman, 2018). The original instrument is also widely used in the literature for studying faculty and their perceptions of OER (Hilton III & Mason, n.d.).

The survey instrument in this research solicited faculty participants from multiple venues across the United States involved in cybersecurity initiatives in higher education in the summer of 2019. Centers of Academic Excellence (CAE) are cybersecurity programs in higher education that gain certification by the National Security Agency (NSA) and Department of Homeland Security (DHS) for documenting where their curriculum meets the knowledge, skills, and abilities (KSAs) of graduates in their programs meet the needs of the cybersecurity workforce as defined in the National Initiative for Cybersecurity Education (NICE) framework. The solicitation for participants occurred in two monthly CAE email newsletters and through the CAE online discussion board. The researcher also solicited participants from two faculty professional development workshops hosted for faculty of CAE institutions in Minnesota and Nevada in face-to-face interaction. The researcher also sought out respondents by attending and promoting the research at the Community College Cyber Summit (3CS) in Bossier City, Lousiana.

The participants 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 collected 80 survey responses in total. Ten of the 80 responses were eliminated due to incomplete data leaving 70 complete responses for analysis. General demographic information in the table below shows results from the survey.

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 Universities	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

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

69% of respondents identified as Male. Females comprised 30% of the sample. One respondent (1.4%) identified as Other. The figure below shows the demographic breakout of gender among cyber faculty in the sample.

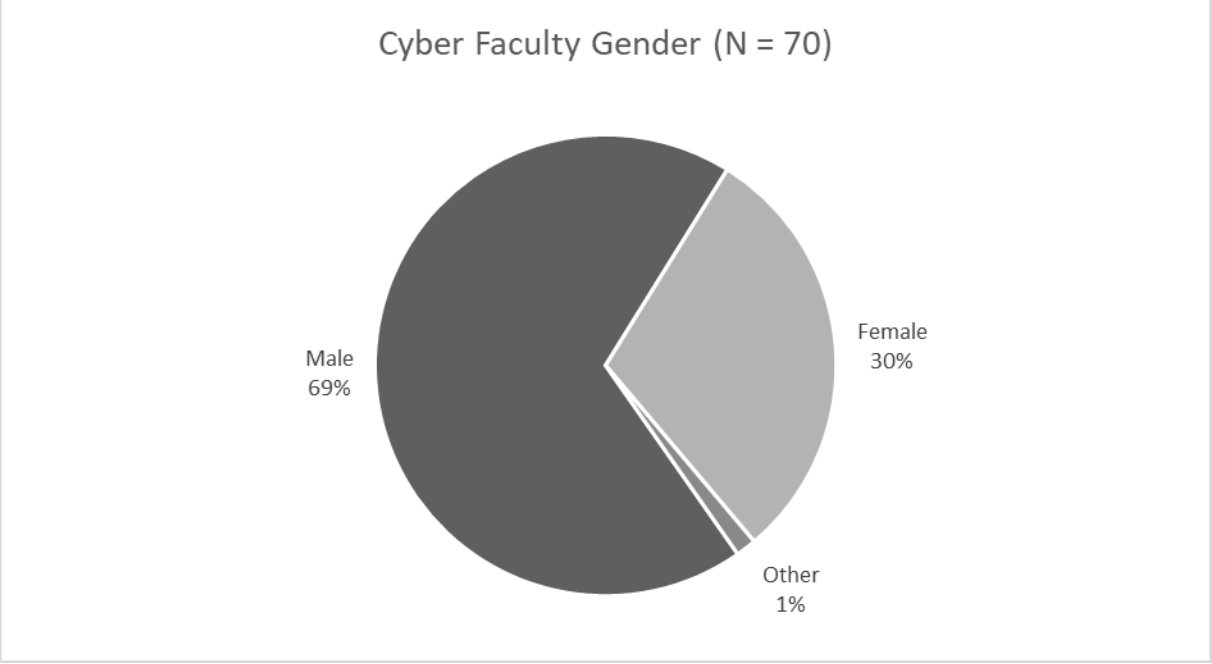

Figure 1. Cyber Faculty Gender Demographic

Participants from associates colleges make up 34% of the sample. Doctorate-granting Universities comprised 32.9% of the sample. There were no participants from tribal colleges. The figure below shows the demographic breakout of the sample by institutional type.

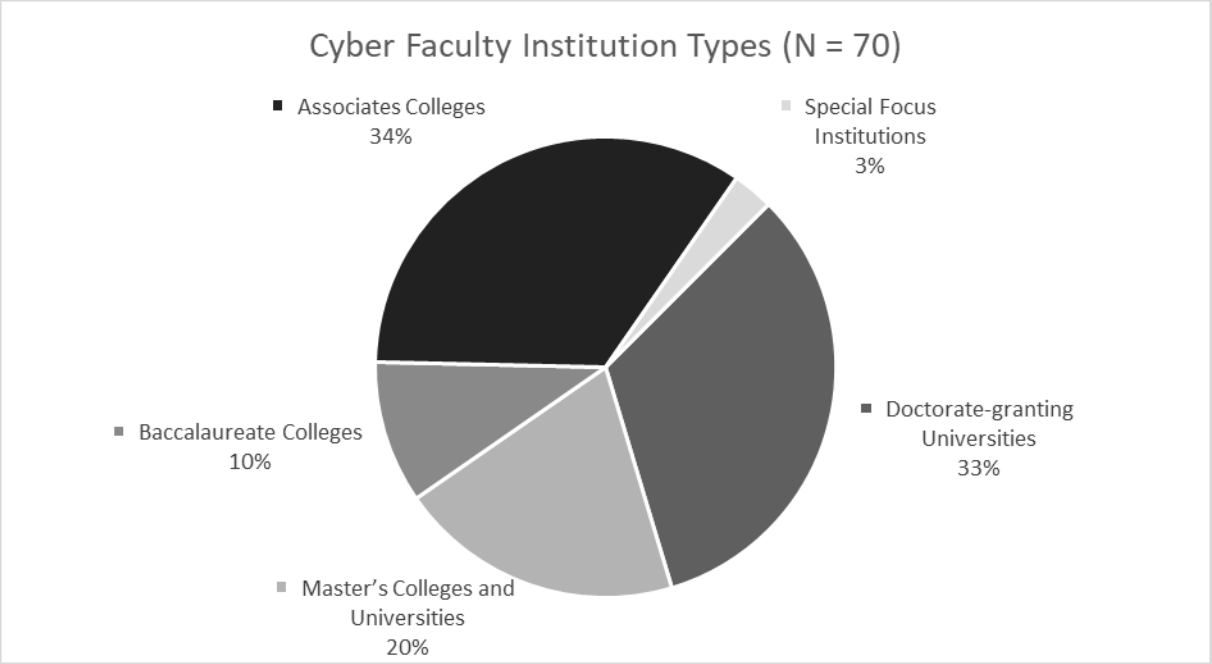

Figure 2. Cyber Faculty Institution Type Demographic

72.9% of participants identified as full-time faculty. Part-time faculty comprised 18.6% of the sample. 8.6% of the respondents selected "other" as their teaching status. The figure below displays the demographic breakout of the teaching status of cyber faculty in the sample.

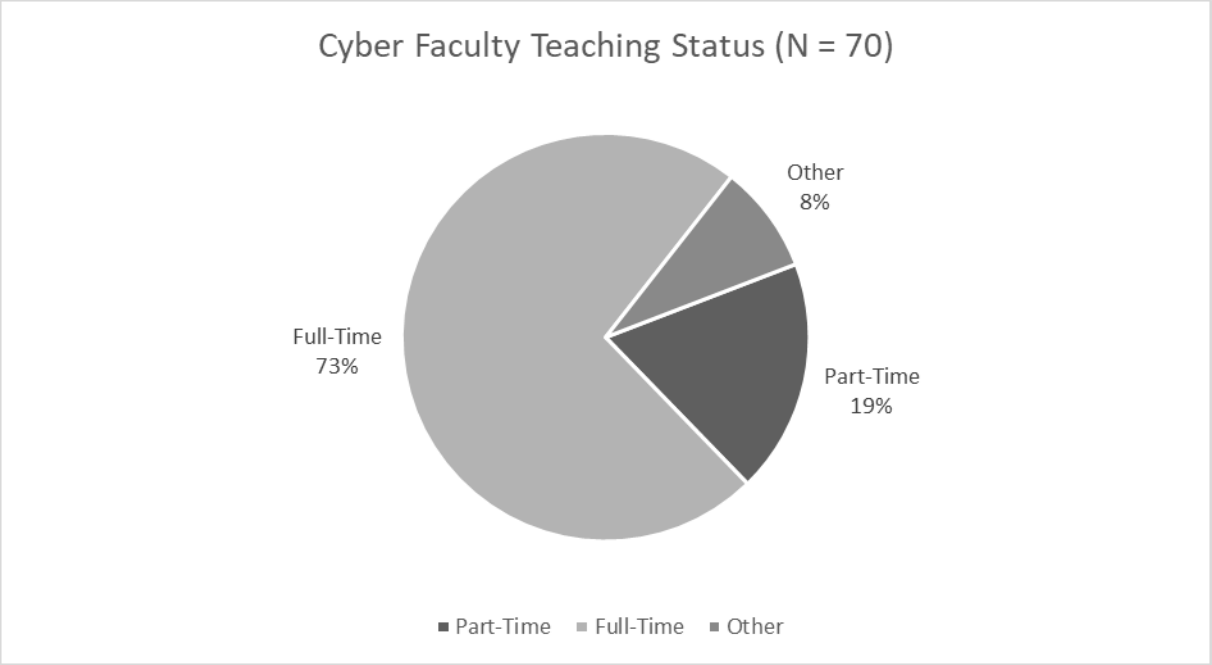

Figure 3. Cyber Faculty Teaching Status Demographic

The majority (74.3%) of cyber faculty surveyed identified themselves as having the primary role in the selection of which educational resources to use in the courses they teach. In 10.0% of the sample, the respondents identified the department, program, or division as having the primary role selection of educational resources. In the figure below, the demographic data shows who has the primary role in selecting educational resources.

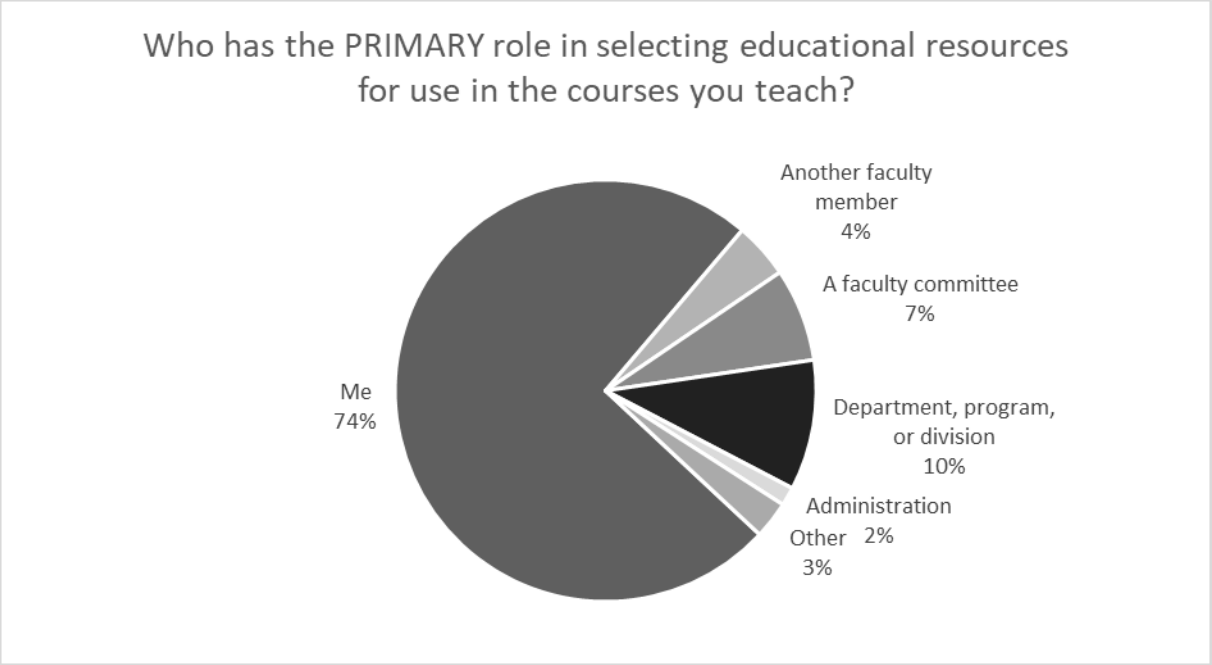

Figure 4. Cyber Faculty Roles in Educational Resource Selection

Independent variables in the study include years of teaching experience and membership to seven job roles in the cyber workforce, as defined by the NICE framework. The teaching experience variable was divided into a 7-point response scale for faculty to identify the amount of time they have spent teaching at a collegiate level. Seven job roles are identified in the NICE framework (Newhouse et al., 2017). Participants could choose multiple NICE framework job roles to indicate fields of study in cyber in which their expertise was focused. An option for "Other" allowed participants to indicate if they performed a cyber role not contained in the NICE framework. The table below displays the demographic results among the independent variables.

Table 3. Demographic Information for Independent Variables

Demographic	Value	N=70	%
Years of Teaching Experience			
	Less than one year	3	4.3
	1 to 3 years	9	12.9
	4 to 5 years	7	10
	6 to 9 years	16	22.9
	10 to 15 years	18	25.7
	16 to 20 years	11	15.7
	More than 20 years	6	8.6
NICE Workforce Role - Analyze			
	False	34	48.6
	True	36	51.4
NICE Workforce Role – Collect and Operate			
	False	41	58.6
	True	29	41.4
NICE Workforce Role – Investigate			
	False	33	47.1
	True	37	52.9

Demographic	Value	N=70	%
NICE Workforce Role – Operate and Maintain			
	False	23	32.9
	True	47	67.1
NICE Workforce Role – Oversee and Govern			
	False	44	62.9
	True	26	37.1
NICE Workforce Role – Protect and Defend			
	False	24	34.3
	True	46	65.7
NICE Workforce Role – Securely Provision			
	False	40	57.1
	True	30	42.9
NICE Workforce Role – Other			
	False	65	92.9
	True	5	7.1

Half (50%) of the respondents have less than ten years of experience teaching at the collegiate level. Educators with 10 to 15 years of teaching experience make up the largest demographic at 25.7%. The figure below represents the years of teaching demographic information.

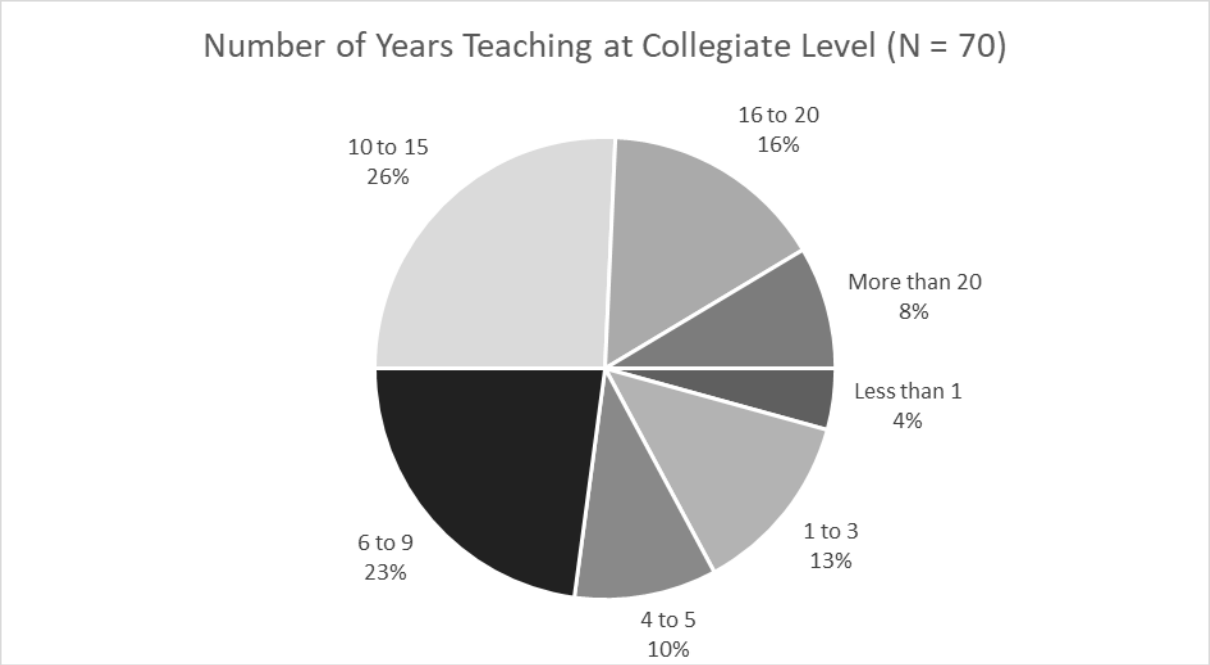

Figure 5. Number of Years Teaching at Collegiate Level

Cyber faculty were allowed multiple selections for various job roles under the NICE framework. An "Other" option was also provided. *Operate and Maintain* and *Protect and Defend* were the most reported workforce framework roles at 47 and 46 times, respectively. *Oversee and Govern* was the least reported NICE framework role. The figure below shows the number of times each job role was selected in the sample.

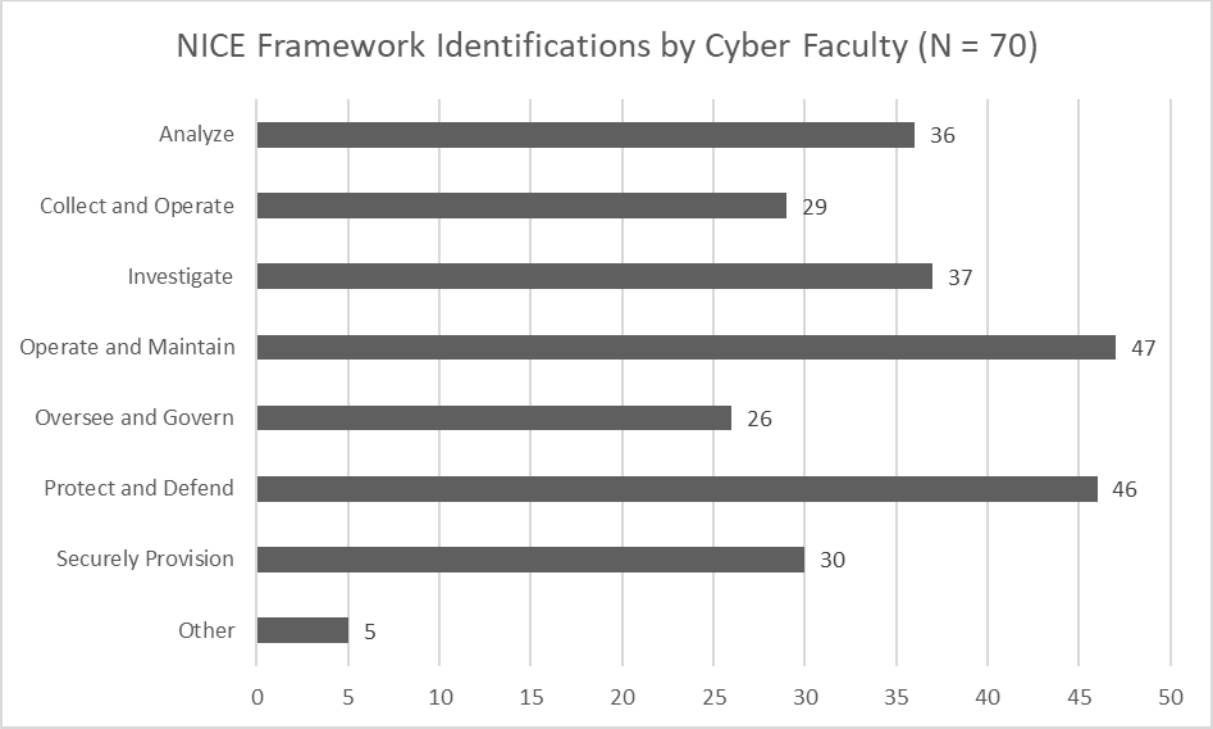

Figure 6. NICE Framework Identifications by Cyber Faculty

Of the 70 completed surveys, 52 faculty indicated they belonged to more than one of the NICE framework roles (74.2%). Thirty-six participants (51.4%) indicated they belonged to four or more NICE framework job roles in their respective fields of study. Fourteen participants (20%) reported focusing on all seven disciplines of the study identified by the NICE framework. Five participants (7.1%) selected the "Other" option. Three participants (4.2%) reported a cyber discipline focus area of "Other" without another NICE framework role selected. The figure below represents the number of cyber discipline areas selected by participants in the study.

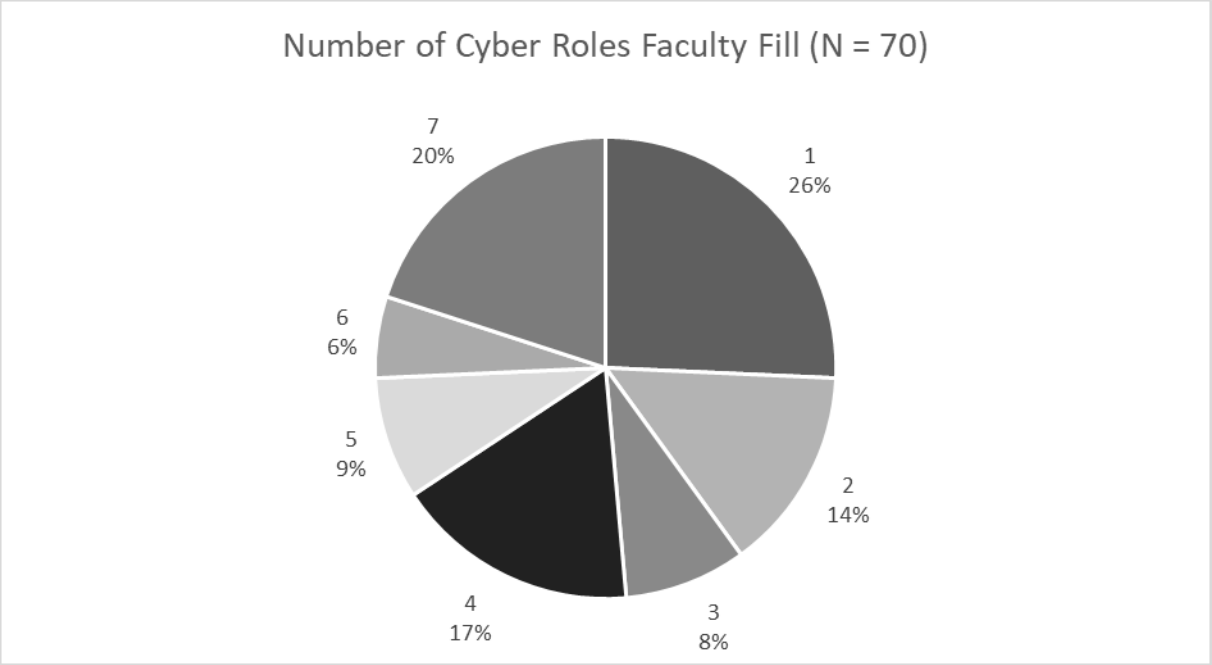

Figure 6. Number of Cyber Roles Faculty Fill

Data Analyses

Factor analysis is useful when determining statistical groups in the data (Field, 2019, pp. 666–667). The study introduces three groupings (OER awareness, OER perceptions of effectiveness, and OER perceptions of potential barriers) as dependent variables. The researcher took some liberty in classifying survey questions into these three constructs when creating the derived instrument, basing it upon literature and the instrument itself. Exploratory factor analysis allows the researcher to confirm grouping within the dependent variable constructs. Analysis began by using component analysis for extraction and a rotational method of varimax with Kaiser Normalization in SPSS with Eigenvalues greater than one (de Vaus, 2002, pp. 188–190). Eliminating communalities of less than 0.4 and rerunning factor analysis identifies five groupings with communalities greater than 0.4 and Cronbach's Alpha scores greater than 0.7. Eliminating low-loading factors helps justify assumption #5 for

potential outliers in the data. Since the research questions focus on three groupings, the researcher took some liberty to identify which three of the five groupings most clearly represent the themes of the research questions and remove the two groupings not associated with the current study. With factor analysis, questions not related to the groups are removed, and only closely related questions contributing to the factors are used, helping to resolve assumption #9 required by MANOVA.

Descriptive Analysis

Three constructs in the data exhibit a cumulative coverage of 66.025% with a Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy of 0.755. The closer the KMO score is to 1.0 indicates that the data is useful and, generally, scores less than 0.5 are not useful, so the research exhibits adequate sampling and satisfies assumption #4 for MANOVA in needing adequate sample size (Field, 2019, pp. 684–685). Using Bartlett's Test of Sphericity, the data reports an approximate Chi-Square of 582.550, 105 degrees of freedom, and a significance level of 0.00. Significance levels less than 0.05 indicate that factor analysis is useful with the data (Field, 2019, pp. 685–686). This finding in factor analysis satisfies assumption #8 for MANOVA in that the variance-covariance matrices are homogeneous.

The awareness component consists of three questions exhibiting a Cronbach's Alpha score of 0.815. Cronbach's Alpha is a measure of the internal consistency of the group composing of its factors and how related they are. A reliability coefficient of 0.70 or greater is considered socially acceptable in most research (de Vaus, 2002). Below is a list of the prompts cyber faculty gave responses to using Likert-based scoring with levels of agreement.

- I feel comfortable in identifying if a select resource exists in the public domain

- I feel comfortable in identifying if a selected resource is subject to copyright
- I feel comfortable in interpreting the license agreements of software that I use in course instruction

The component representing perceptions of perceived benefits of OER resources exhibits a Cronbach's Alpha score of 0.868, above the acceptable cutoff of 0.70. The benefits construct consists of six responses to the survey. Below is a list of the prompts cyber faculty gave responses to using Likert-based scoring with levels of agreement.

- Use of OER leads to improvement in student performance
- Use of OER leads to improvement in student satisfaction
- The open aspect of OER creates different usage and adoption patterns than other online resources
- Use of OER is an effective method for improving retention for at-risk students
- OER adoption at an institutional level leads to financial benefits for students and/or the institution
- Use of OCR leads to critical reflection by educators, with evidence of improvements in their practice

The construct representing perceptions of perceived barriers to OER adoption exhibits a Cronbach's Alpha score of 0.868, above the required cut off of 0.70. The barrier's construct consists of 6 questions to the survey. Below is a list of the prompts cyber faculty gave responses to using Likert-based scoring with levels of agreement.

- It is hard to find OERs to use an course instruction
- There are not enough OER resources for my subject matter
- Existing OER materials are not high quality

- OERs are not current or up-to-date
- OERs are not relevant to my local teaching context
- There is no comprehensive catalog of resources from my subject area

Acceptable Cronbach's Alpha scores for all three constructs help satisfy assumptions #5 for outliers in data. After ensuring all the assumptions that MANOVA requires for analysis are met, the procedure is ready to run and begin answering the research questions. The researcher calculates the mean for all the factors in their respective groupings for each respondent. Nine questions of the original 26 in the survey were removed from data analysis for exhibiting low loading values during factor analysis or not fitting the constructs at study. These questions are listed below.

- I feel comfortable using a selected resource that employs Creative Commons licensing
- I can identify current teaching practices I use that employ OER
- I feel comfortable teaching a course using OER as a primary resource
- I feel comfortable teaching a course using OER for supplemental resources
- Open educational models lead to more equitable access to education, serving a broader base of learners than traditional education
- OERs are difficult to use in course pedagogy
- I do not know if I have permission to use or change OER materials I find
- I lack support from my institution to implement OERs into course curriculum
- OERs are too difficult to change or edit

Research Question Findings

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 level of significance with the independent variables of the number of years of teaching experience and the number of roles cyber faculty fill teaching under the NICE framework. There are three research questions. One for each of the independent variables 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 teaching experience held by faculty?

There are no statistically significant differences in the perceptions of OER based on the number of years teaching experience held by faculty, $F(18, 173.019) = 1.272$, $p > .05$; Wilk's $\Lambda = .704$, partial $\eta^2 = .111$.

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 $\Lambda = .736$, partial $\eta^2 = .097$.

RQ3: Is there a statistically significant interaction between the independent variables of the number of years 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 $\Lambda = .3$, partial $\eta^2 = .331$.

Conclusion

In this chapter, data analysis was performed on the survey data to answer the stated research questions. After reporting general demographic information, factor analysis grouped dependent variables into three constructs: OER awareness, OER potential benefits, and OER potential barriers. Measures for each participant for each construct were combined to form a mean score for each factor. Reliability analysis confirms that each factor loading is enough to continue analysis using the MANOVA procedure. MANOVA procedure found no significant differences between the combined dependent variables and the number of years of teaching experience, the number of faculty NICE roles chosen, or the combined independent variables of years teaching experience held by faculty and the number of NICE roles chosen.

CHAPTER 5

CONCLUSIONS

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, the insufficient supply of qualified workers will weaken the security posture of the public and private sector 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.

Methods

This study used a survey methodology to build a sample of cybersecurity teaching educators seeking professional development opportunities in the United States in the summer of 2019. The survey instrument derived from a validated instrument used by the Babson Survey Research Group to survey thousands of faculty nationwide in multiple studies. Participants for this survey consisted of cybersecurity educators associated with professional organizations and faculty professional development opportunities that appeal to cybersecurity educators. Data collection occurred face-to-face at two Centers of Academic Excellence (CAE) faculty development workshops hosted in St.Paul, Minnesota, and Las Vegas, Nevada hosted by Dakota State University, the National Security Agency (NSA), and Department of

Homeland Security (DHS). A third face-to-face participant solicitation occurred at Community College Cybersecurity Summer (3CS) conference in Bossier City, Lousiana. Online solicitation occurred through professional organizations conduits associated with faculty in the nationwide CAE community. The survey was advertised in two monthly newsletters and posted to the CAE forums asking for participants.

Data collection with the survey instrument yielded a sample size of 70 respondents (N=70). Factor analysis found three groupings in the dependent variables representing the dependent variable constructs (awareness, benefits, and barriers). Other questions were eliminated from the results for having low scoring during factor analysis. Results from the survey were analyzed using Multivariate Analysis of Variance (MANOVA) to determine if there were any statistically significant differences between the independent variables and three grouping constructs representing OER awareness, perceptions of OER potential benefits, and perceptions of OER potential barriers. Independent variables used in this analysis were the number of years teaching that participants held and the number of National Initiative for Cybersecurity Education (NICE) frameworks roles selected. The number of NICE roles chosen represents whether the participant was a specialist in one field or generalist encompassing many fields across the cybersecurity landscape. The two variables were tested independently for statistical significance and then for any statistical difference in the combined effect of the two variables.

Findings

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.

Limitations

Several considerations of the research must be taken into account while interpreting the findings of the research 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 limitation of the study. MANOVA results are more reliable when it includes larger sample sizes compared to smaller sample sizes. A sample size of around one hundred and fifty would have achieved a more statistically reliable result, but the sample in this study was only able to 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 strong loading factors that were removed from the analysis to fit the stated research questions surrounding awareness, potential benefits, and potential drawbacks.

Discussion

The purpose of this study was to determine if there were any statistically significant differences between perceptions of OER awareness, potential benefits, and potential barriers in the population of cyber faculty pursuing professional development initiatives based on the number of years of teaching experience and the number of NICE framework roles the faculty members associate themselves within their profession. There were three research questions in this study, with one for each independent variable and a third research question looking for statistical differences in the combination of both independent variables. MANOVA was selected to provide answers to these questions. Statistically, there was no significance found in the three research questions, with each having p-values greater than 0.05.

The research also aimed to demonstrate a stronger methodology used for the study of a population than many other bodies of work in the literature surrounding OER research. Though the study did encounter some limitations, such as the data sampling size, the researcher hopes that future investigators will begin to approach OER research using statistical methods rather than just demographic reporting and non-statistical interpretations.

Future Work

With a strong pilot study implemented to further the reliability and validity of the research, there is still more room to further the research presented in this study. The research identified three areas of interest (awareness, potential benefits, and potential barriers) based on the literature 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 to group related questions. The first construct consists of two questions from the original awareness construct.

- I feel comfortable teaching a course using OER as a primary resource.
- I feel comfortable teaching a course using OER for supplemental resources.

The second construct consists of three questions from the original barriers construct.

- I lack support from my institution to implement OERs into the course curriculum.
- OERs are too difficult to change or edit.
- OERs are too difficult to integrate into the technology my students and I use.

Further investigation is needed to determine the influence of these factors on cyber faculty perceptions of OER, taxonomy, and relevance in the literature. Usability and adaptability seem to be good terminology to associate with these constructs, but more research is needed.

Other independent variables collected with the survey instrument could provide other interesting aspects to discovering significant differences in the perceptions of OER. The researcher is interested in pursuing further research investigating the type of institution faculty come from, teaching status, and who controls course material selection at the institution. Further investigation into these areas may help identify trends in the population and where OER might be most effective.

Conclusion

In this study, the researcher aimed to frame perceptions of awareness, potential benefits, and potential barriers in the usage of open educational resources in cyber curricula of faculty members in U.S. higher education pursuing scholarly activities to further their cyber

knowledge. America's cybersecurity workforce is a strategic asset that protects the American people, the homeland, and the American way of life (Trump, 2019). Currently, there are not enough qualified applicants to fill the current cybersecurity job market. Also, the cybersecurity industry is still growing, so without action to help strengthen pipelines into the cyber workforce, there will be even more a shortage of qualified workers in the future (Aspen Cybersecurity Group, 2018). This research contributes to the body of knowledge in understanding the role that OER can play as educators, industry leaders, and government officials work towards building cybersecurity awareness in the general population and opens 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

ALG statistics, research, and reports. (n.d.). Retrieved from https://www.affordablelearninggeorgia.org/about/reports

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

Annand, D. (2015). Developing a sustainable financial model in higher education for open educational resources. *The International Review of Research in Open and Distributed*

Learning, *16*(5), 1–15. https://doi.org/10.19173/irrodl.v16i5.2133

Arquilla, J., & Guzdial, M. (2017). Crafting a national cyberdefense, and preparing to support computational literacy. *Communications of the ACM*, *60*(4), 10–11. https://doi.org/10.1145/3048379

Asllani, A., White, C. S., & Ettkin, L. (2013). Viewing cybersecurity as a public good: the role of governments, businesses, and individuals. *Journal of Legal, Ethical and Regulatory Issues*, *16*(1), 7–14.

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

Babbie, E. (2001). *The practice of social research*. Belmount, CA: Wadsworth/Thomson Learning.

Baker, J., Thierstein, J., Fletcher, K., Kaur, M., & Emmons, J. (2009). Open textbook proof-of-concept via Connexions. *The International Review of Research in Open and Distributed Learning*, *10*(5). https://doi.org/10.19173/irrodl.v10i5.633

Beecroft, K., & Edwards, S. (2016). *Strategic plan*. *National Initiative for Cybersecurity Education*. Cambridge University Press. https://doi.org/10.29085/9781783300792.002

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

Bodily, R., Nyland, R., & Wiley, D. (2017). The RISE framework: using learning analytics to automatically identify open educational resources for continuous improvement. *The International Review of Research in Open and Distributed Learning*, *18*(2), 103–122.

https://doi.org/10.19173/irrodl.v18i2.2952

Campbell, J. (2016). Democracy and education: reconstruction of and through education. *Educational Theory*, *66*(1–2), 39–53. https://doi.org/10.1111/edth.12151

Carnegie Commission. (2018). Basic classification description. Retrieved August 9, 2019, from http://carnegieclassifications.iu.edu/classification_descriptions/basic.php

CLARK. (n.d.). Retrieved November 2, 2020, from https://clark.center/home

Clinton, V. (2018). Savings without sacrifice: a case report on open-source textbook adoption. *Open Learning: The Journal of Open, Distance and e-Learning*, *33*(3), 177–189. https://doi.org/10.1080/02680513.2018.1486184

Costello, E., Bolger, R., Soverino, T., Brown, M., & Conole, G. (2019). Opening the book on the price of student reading lists. In *EdMedia + Innovate Learning* (pp. 1877–1881).

Creative Commons. (n.d.). Attribution 4.0 International (CC BY 4.0). Retrieved from https://creativecommons.org/licenses/by/4.0/

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.).

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

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, *9*(JUN), 1–12. https://doi.org/10.3389/fpsyg.2018.00744

de la Rosa Gómez, A., Meza Cano, J. M., & Miranda Díaz, G. A. (2019). Validation of a rubric to evaluate Open Educational Resources for learning. *Behavioral Sciences*, *9*(12), 126. https://doi.org/10.3390/bs9120126

de Vaus, D. (2002). *Surveys in social research* (5th ed.). Abingdon: Routledge.

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

Dorodchi, M., & Dehbozorgi, N. (2016). Utilizing open source software in teaching practice-based software engineering courses. In *2016 IEEE Frontiers in Education Conference (FIE)* (Vol. 2016-Novem, pp. 1–5). IEEE. https://doi.org/10.1109/FIE.2016.7757683

EC-Council. (2019). Certified Ethical Hacker v10 (CEH). Retrieved February 10, 2019, from https://iclass.eccouncil.org/our-courses/certified-ethical-hacker-ceh/

European Union Agency for Network and Information Security. (2018). *ENISA threat landscape report 2017: 15 top cyber-threats and trends.* Heraklion: ENISA. https://doi.org/10.2824/967192

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

Grimes, D. A., & Schulz, K. F. (2002). Descriptive studies: what they can and cannot do. *The Lancet*, *359*(9301), 145–149. https://doi.org/10.1016/S0140-6736(02)07373-7

Harris, M. A., & Patten, K. P. (2015). Using Bloom's and Webb's taxonomies to integrate emerging cybersecurity topics into a computing curriculum. *Journal of Information Systems Education*, *26*(3), 219–234.

Hendricks, C., Reinsberg, S. A., & Rieger, G. W. (2017). The adoption of an ppen textbook in a large physics course: an analysis of cost, outcomes, use, and perceptions. *The International Review of Research in Open and Distributed Learning*, *18*(4), 78–99. https://doi.org/10.19173/irrodl.v18i4.3006

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

Hilton, J. (2019). Open educational resources, student efficacy, and user perceptions: a synthesis of research published between 2015 and 2018. *Educational Technology Research and Development*, (0123456789). https://doi.org/10.1007/s11423-019-09700-4

Hoadley, E. D., & Mento, A. J. (2010). Integrating The Executive MBA Curriculum: Tales Of The Cat Herder. *American Journal of Business Education (AJBE)*, *3*(4), 91–98.

https://doi.org/10.19030/ajbe.v3i4.419

Hollandsworth, R., Donovan, J., & Welch, M. (2017). Digital citizenship: you can't go home again. *TechTrends*, *61*(6), 524–530. https://doi.org/10.1007/s11528-017-0190-4

Hollandsworth, R., Dowdy, L., & Donovan, J. (2011). Digital citizenship in K-12: it takes a village. *TechTrends*, *55*(4), 37–47. https://doi.org/10.1007/s11528-011-0510-z

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

Johnson, D. (2014). Open educational resources: on the web and free. *Educational*

Leadership, *71*(6), 85–87.

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

Kaatrakoski, H., Littlejohn, A., & Hood, N. (2017). Learning challenges in higher education: an analysis of contradictions within open educational practice. *Higher Education*, *74*(4), 599–615. https://doi.org/10.1007/s10734-016-0067-z

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

Krutz, D. E., & Richards, T. (2017). Cyber security education: why don't we do anything about it? *ACM Inroads*, *8*(4), 5–5. https://doi.org/10.1145/3132217

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

Leichte, C. A. (2018). *A quantitative study of faculty perceptions of open educational resources (OERs) at a community college in western North Carolina*. Wilmington University.

Levin, K. A. (2006). Study design III: cross-sectional studies. *Evidence-Based Dentistry*, *7*(1), 24–25. https://doi.org/10.1038/sj.ebd.6400375

Lindshield, B. L., & Adhikari, K. (2013). Online and campus college students like using an

open educational resource instead of a traditional textbook. *MERLOT Journal of Online Learning and Teaching*, *9*(1), 26–38.

Mailloux, L. O., & Grimaila, M. (2018). Advancing cybersecurity: the growing need for a cyber-resiliency workforce. *IT 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.

Masterman, E. (2016). Bringing open educational practice to a research-intensive university: Prospects and challenges. *Electronic Journal of E-Learning*, *14*(1), 31–42.

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

OECD. (2016). *Skills matter: further results from the survey of adult skills*. OECD Publishing. https://doi.org/10.1787/9789264307353-en

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

Open Source Initiative. (2007). The Open Source Definition. Retrieved from https://opensource.org/osd

Paragarino, V. R., Silveira, I. F., & Llamas-Nistal, M. (2018). Open educational resources: a brief vision from IEEE topics. In *2018 IEEE Global Engineering Education Conference (EDUCON)* (Vol. 2018-April, pp. 2076–2081). IEEE. https://doi.org/10.1109/EDUCON.2018.8363495

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.

Pirkkalainen, H., Jokinen, J. P. P., & Pawlowski, J. M. (2014). Understanding social OER environments—a quantitative study on factors influencing the motivation to share and collaborate. *IEEE Transactions on Learning Technologies*, *7*(4), 388–400.

https://doi.org/10.1109/TLT.2014.2323970

Pitt, R. (2015). Mainstreaming open textbooks: educator perspectives on the impact of OpenStax college open textbooks. *The International Review of Research in Open and Distributed Learning*, *16*(4), 133–155. https://doi.org/10.19173/irrodl.v16i4.2381

Ponto, J. (2014). Understanding and evaluating survey research. *Journal of the Advanced Practitioner in Oncology*, *6*(2), 168–171. Retrieved from http://journals.sagepub.com/doi/10.1177/1477878513517337

Procheş, Ş. (2016). Descriptive statistics in research and teaching: are we losing the middle ground? *Quality & Quantity*, *50*(5), 2165–2174. https://doi.org/10.1007/s11135-015-0256-3

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

Rowsell, J., Morrell, E., & Alvermann, D. E. (2017). Confronting the Digital Divide: debunking brave new world discourses. *The Reading Teacher*, *71*(2), 157–165. https://doi.org/10.1002/trtr.1603

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

Santos, H., Pereira, T., & Mendes, I. (2017). Challenges and reflections in designing cyber

security curriculum. In *2017 IEEE World Engineering Education Conference (EDUNINE)* (pp. 47–51). IEEE. https://doi.org/10.1109/EDUNINE.2017.7918179

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

Steinert, Y., Mann, K., Centeno, A., Dolmans, D., Spencer, J., Gelula, M., & Prideaux, D. (2006). A systematic review of faculty development initiatives designed to improve teaching effectiveness in medical education: BEME Guide No. 8. *Medical Teacher*, *28*(6), 497–526. https://doi.org/10.1080/01421590600902976

Subcommittee on Research and Technology. (2017). *Strengthening U.S. cybersecurity capabilities*. Washington, D.C.: U.S. Goverment 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*, *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/

U.S. Department of Commerce: National Telecommunications and Information Administration. (2014). Exploring the digital nation: embracing the mobile internet. *Journal Of Current Issues In Media & Telecommunications*, *6*(4), 417–461. Retrieved from https://www.ntia.doc.gov/report/2014/exploring-digital-nation-embracing-mobile-internet

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

What is open source? (n.d.). Retrieved from https://opensource.com/resources/what-open-source

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 and 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: SURVEY INSTRUMENT

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.

If you have questions, please contact Alan Stines.

Email: alan.stines@trojans.dsu.edu

Advisor: Dr. Kyle Cronin, kyle.cronin@dsu.edu

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.

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 (IT) systems, networks, and digital evidence.

○ Operate and Maintain - Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) 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 (IT) systems and/or networks.

○ Securely Provision – Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.

○ Other

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".

Part 2: Cyber Faculty Perceptions of OER Awareness

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	7	6	5	4	3	2	1

	Commons licensing.							
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	7	6	5	4	3	2	1

	more equitable access to education, serving a broader base of learners than traditional education.							
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