Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 27

9-23-2024

How State Universities are addressing the Shortage of Cybersecurity Professionals in the United States

Gary Harris
University of Arkansas at Little Rock, gary@garyharris.com

Recommended Citation
Harris, Gary (2024) "How State Universities are addressing the Shortage of Cybersecurity Professionals in the United States," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 27.
DOI: https://doi.org/10.62915/2472-2707.1194
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/27

How State Universities are addressing the Shortage of Cybersecurity Professionals in the United States

Abstract

Cybersecurity threats have been a serious and growing problem for decades. In addition, a severe shortage of cybersecurity professionals has been proliferating for nearly as long. These problems exist in the United States and globally and are well documented in literature. This study examined what state universities are doing to help address the shortage of cybersecurity professionals since higher education institutions are a primary source to the workforce pipeline. It is suggested that the number of cybersecurity professionals entering the workforce is related to the number of available programs. Thus increasing the number of programs will increase the number of cybersecurity professionals entering the workforce. This study used a qualitative approach to examine the programs offered through a sample of 201 state universities using a document review of online academic catalogs. The research examined the quantities and levels of cybersecurity programs and identified the institutions that used the National Centers of Academic Excellence (CAE) structure to develop their programs. The results showed that an impressive 84.6% of the universities sampled offered a cybersecurity program and of which more than 50% received a CAE designation. Although the results were impressive, there are still unanswered questions requiring further study in regards to having a satisfactory number of programs to generate the needed talent to reduce the shortage. This study generated several important questions and recommendations and highlighted the availability of cybersecurity programs at the state university level at a snapshot in time. The results can be used to help identify any additional academic needs to help address the shortage of cybersecurity professionals.

Keywords

cybersecurity, computer security, higher education, cybersecurity professionals, cybersecurity education, information assurance, cybersecurity workforce shortage

Cover Page Footnote

N/A

How State Universities are addressing the Shortage of Cybersecurity Professionals in the United States

Gary A. Harris
Department of Information Science
University of Arkansas at Little Rock
Little Rock, AR USA
gaharris@ualr.edu
ORCID: https://orcid.org/0009-0003-3749-5086

***Abstract*—Cybersecurity threats have been a serious and growing problem for decades. In addition, a severe shortage of cybersecurity professionals has been proliferating for nearly as long. These problems exist in the United States and globally and are well documented in literature. This study examined what state universities are doing to help address the shortage of cybersecurity professionals since higher education institutions are a primary source to the workforce pipeline. It is suggested that the number of cybersecurity professionals entering the workforce is related to the number of available programs. Thus increasing the number of programs will increase the number of cybersecurity professionals entering the workforce. This study used a qualitative approach to examine the programs offered through a sample of 201 state universities using a document review of online academic catalogs. The research examined the quantities and levels of cybersecurity programs and identified the institutions that used the National Centers of Academic Excellence (CAE) structure to develop their programs. The results showed that an impressive 84.6% of the universities sampled offered a cybersecurity program and of which more than 50% received a CAE designation. Although the results were impressive, there are still unanswered questions requiring further study in regards to having a satisfactory number of programs to generate the needed talent to reduce the shortage. This study generated several important questions and recommendations and highlighted the availability of cybersecurity programs at the state university level at a snapshot in time. The results can be used to help identify any additional academic needs to help address the shortage of cybersecurity professionals.**

Keywords— cybersecurity, computer security, higher education, cybersecurity professionals, cybersecurity education, information assurance, cybersecurity workforce shortage

I. Introduction

Cybersecurity threats to computers and networks have been an issue for decades and are continuing to grow in numbers, severity, sophistication, and cost [1], [40], [42]. In addition, there has been a growing shortage of cybersecurity professionals in the United States and globally to deal with the increased threats. These points are demonstrated and cited in the literature review. Additionally, there are news stories and articles almost daily about cyberattacks [51]. A growing 91 page list of significant cyber incidents can be downloaded from the Center for Strategic & International Studies, Significant Cyber Incidents: Strategic Technologies Program website [21]. It provides a very clear picture of the cybersecurity problem even though the list only includes government and defense entities, high technology companies, and financial crimes over $1 million since 2006. There are numerous resources on the Internet documenting cyberattacks over a long period of time. The main point is that the quantity and severity of cyberattacks are increasing as well as the shortage of cybersecurity professionals.

The results of this study were impressive. The research identified that a majority of the sample universities offered some type of a cybersecurity program and have used a cybersecurity academic framework to develop their programs, such as the National Centers of Academic Excellence (CAE). Although the study provides a sample representation of how universities are helping to address the shortage of cybersecurity professionals, several important questions were identified that require further research.

A. *Purpose and Significance of the Research*

Several studies have suggested that higher education institutions are a primary source of workforce talent and development [8], [23], [56], [62]. In addition, many studies have identified the severe shortage of cybersecurity professionals [9], [38], [45], [46]. It is suggested that increasing the number of available cybersecurity programs can increase the number of cybersecurity professionals into the workforce pipeline and help address the shortage [37].

The purpose of this research is to examine how state universities are helping to address the shortage of cybersecurity professionals as of the time period of this study. This study is significant because it highlights the availability of cybersecurity programs at the state university level at a snapshot in time and can help identify any additional academic needs to address the shortage of cybersecurity professionals. The premise is that the more cybersecurity programs that are available to potential students - the more cybersecurity professionals will be added to the cybersecurity workforce, thus helping to reduce the shortage of cybersecurity professionals. Reducing the shortage of cybersecurity professionals will help deal with the growing cybersecurity threats.

B. *Theoretical Framework*

The theoretical framework that drove this study is the Human Capital Theory. The Human Capital Theory suggests that employees are the human capital of an organization [23], [43]. In addition, the theory suggests that an employee's expertise (specific knowledge and skills, such as cybersecurity) are essential to the successful operation of an organization. Additionally, the theory suggests that an employee's expertise is often gained through college and should be aligned with the needs of industry [8], [23], [56], [62]. The Human Capital Theory suggests that education can improve productivity and the quality of work, but cannot adequately address the gap between organizational needs (such as cybersecurity professionals) and the workforce supply pipeline (higher education) [32].

II. Review of literature

This literature review will examine the literature involving cybersecurity problems and incidents and the long term growing U.S. and global shortage of cybersecurity professionals. It will demonstrate that there have been identified problems with systems security for decades and these problems are continuing to grow. In addition, this literature review will demonstrate that there is and has been a growing shortage of cybersecurity professionals for decades and getting worse. There is a plethora of literature going back decades that identify the cybersecurity problems and shortage of cybersecurity professionals. This literature review provides a broad coverage of the previous work demonstrating the cybersecurity problems and workforce shortages over time. Lastly, this literature review will provide a high-level overview of three common academic cybersecurity frameworks and programs that are designed to be used by higher education to help develop their cybersecurity programs. Some older references have been included in this literature review to provide background and a historical perspective on cybersecurity threats and shortages of cybersecurity professionals.

A. *Cybersecurity Problems and Incidents - Brief Background*

Cyberattacks and data thefts have been identified as a problem for several decades [60]. Reference [60] pointed out that computer networks and threats to computer systems was first identified in the 1960s. For example, data manipulation first appeared in the 1960s which impacted the trust in data integrity. Congress held hearings on these threats in 1966. The first cyber espionage case appeared in 1968 [60]. In addition, terrorists, criminals, and nation states were identified as possible actors in cyberattacks. This belief has since been confirmed in many studies [24], [36], [44], [55].

In the early 1970s, RAND Corporation suggested technology would not be able to solve the cybersecurity problem [60]. However, changes in systems programming to improve computer security started in the 1970's. Additionally, in the 1980s, networks moved into the global arena and new threats started to emerge, such as hacking and computer viruses. Even Hollywood took notice of the problem and released the cyber-hacking movie "War Games" in 1983. The advent and popularity of the Internet in the 1990s and the start of data collection and interactivity on the web in the early 2000s created a new generation of hackers [31].

There are several different types of cybersecurity threats. For example, ransomware has become one of the major cybersecurity threats. Many studies have cited several large and notable ransomware attacks in recent years. For example, in 2021 the largest oil pipeline system, the Colonial Pipeline, was the target of a ransomware attack causing it to shut down resulting in shortages in the Southeast U.S. [29]. One 2020 study estimated the cost at over $20 billion to businesses. In 2023 the FBI reported that the highest number of ransomware attacks was in the healthcare industry [48].

Data breaches are another major threat. The Identity Theft Resource Center (ITRC) gathered statistics showing that there have been over 9000 data breaches in the past 15 years that has affected over 10 billion people [26]. The largest known data breach occurred in January 2024 and compromised over 26 billion records [47]. The data breach was named the Mother of All Breaches (MOAB).

New methods and techniques are continually being devised to exploit system vulnerabilities [4]. In addition, the quantity, severity, cost, and sophistication of cyberattacks have continued to grow for decades [2], [14], [17], [29]. A 2020 U.S. Cybersecurity and Infrastructure Security Agency (CISA) study estimates the annual global cost of cybersecurity incidents ranged from $1.75 Trillion in 2013 to a projected $10.5 Trillion by 2025, which is about $28.8 billion per day [51]. Table I provides a very small sampling of examples of this growing problem.

TABLE I. Examples of the Growing Problem

References	Example
[1]	Highlights a Forbes news headline “Warning As 26 Billion Records Leak” published January 23, 2024.
[3], [52]	Almost 250 million healthcare records targeted from 2005-2019.
[4], [6]	The average data breach clean-up cost is estimated to be $4 million.
[14]	In 2015, there were over 500 million records stolen from mobile devices. Identified 430 million new malware cases in 2016.
[16]	Cybercrimes costs reach $400 billion annually
[20]	The estimated cost rose to $10.1 million for a single healthcare data breach topping all other sectors for the 12th year.
[29]	In 2021, educational institutions experienced over 5.8 million attacks in less than a one-month period.
[30]	Cybercrime losses estimated to reach $6 trillion by 2021.
[35]	In 2015, the estimated average cost was $3.8 million for a single data breach.
[48]	Ransomware attacks in healthcare doubled from 2022 to 2023.
[50], [55]	Identified huge data breaches at Target and NSA in 2013, Sony Pictures, Yahoo, Anthem, and OPM in 2014, RUAG and Carphone Warehouse in 2015, and Equifax and Zomato in 2017
[53]	Noted a drastic increase in cyberattacks after the Sep. 11, 2001 terrorist attacks.
[61]	Cyberattacks increased by 32% from 2017 to 2018.

The literature demonstrates that there has been an identified problems with systems security for decades. In addition, it has demonstrated that cybersecurity problems are growing and getting worse. The problems are not just increasing in size, severity and sophistication, but also in cost to organizations.

B. *National and Global Shortage of Cybersecurity Professionals*

Similar to the literature dealing with the long and growing problem with cybersecurity, there is a plethora of literature involving the U.S. and global shortage of cybersecurity professionals. There has been a shortage of cybersecurity professionals in the United States for decades. For example, in 2001 the National Science Foundation provided cybersecurity scholarship funding to six universities "in recognition of a shortage of cybersecurity professionals" in the national government [57]. In addition, the Cyber Security Research and Development Act (H.R. 3394) was introduced in 2001 to "help reduce the critical shortage of cybersecurity professionals" [53]. The shortage continues to grow and becoming more critical. For example, from 2015 to 2021 a reported 62% of companies are facing a cybersecurity talent shortage and the number of vacant cybersecurity vacancies has increased by 50% [58].

The shortage of cybersecurity professionals is not just in the U.S., but global. For example, the Information Systems Audit and Control Association conducted a survey of over 3400 members in 129 countries and the results showed that 86% of the survey participants identified a global skills gap of cybersecurity professionals [22]. In addition, the survey showed that 92% of the participants were planning on hiring additional cybersecurity professionals but believe that it will be difficult to find trained professionals.

The National Audit Office (NAO) in the United Kingdom conducted a survey and found that 85% of the respondents are experiencing problems in recruiting cybersecurity professionals because of the shortage of professionals [19]. The NAO believes it will take 20 years to address the problem. In addition, as a result of the shortage, a new Cyber Academy was launched in the UK by the National Skills Academy [41].

The reported numbers of the global shortage of cybersecurity professionals is shocking. For example, in 2018, it was estimated that there were over 1 million global cybersecurity vacancies [16]. The shortage was expected to grow to 1.8 million by 2022 [15], [24]. However, another study estimates the 2018 shortage at 3 million [59]. There are many studies that have provided estimates of cybersecurity professional shortages along with eye opening descriptions of the shortages. Table II provides a small sampling of the descriptions of these shortages.

TABLE II. SAMPLE DESCRIPTIONS OF SHORTAGES IN CYBERSECURITY PROFESSIONALS

References	Description
[5]	"faces continual shortages"
[9]	A 2019 study "predicted approximately 62% short of cybersecurity professionals in the U.S."
[11]	"dearth of well-trained cybersecurity engineers"
[12], [27]	"extreme shortage"; 3.5 million cybersecurity vacancies in 2021
[19]	"a dangerous dearth of skills"; "cybersecurity skills crisis"
[25]	"A major obstacle is the shortage of expertise…"; "We are not producing in this country enough of the security talent…"
[28]	"growing demand for cybersecurity professionals outpaces supply", "main obstacle preventing organizations from achieving cybersecurity resilience"
[33]	"needs surpass our ability to meet them"
[34]	"outpaces the supply"; "national security situation"; "tremendous problem"; "behind by about 2.5 million people"; "lack of personnel"
[37], [49]	"severe shortage of cybersecurity workers"; In 2019 there were over 313,000 cybersecurity vacancies in the U.S. alone. There were 209,000 unfilled positions just four years earlier in 2015.
[38]	"cybersecurity workforce skills gap has grown by 26% year on year", "a profession in dire need", "seems to be little done to address the underlying issues contributing to this skills gap"
[40]	"many entities struggle to fill positions", "due to a significant shortage of skilled professionals"
[45]	Shortage is "well documented" with the workforce gap increasing by 26.2% from 2021 to 2022
[46]	Survey indicated 61% of "cybersecurity teams are understaffed" "in 2025, there will be a predicted 3.5 million unfilled cybersecurity positions worldwide"

The literature has demonstrated that there is a long time and growing severe shortage of cybersecurity professionals. Some organizations and governments have taken notice of this problem and have attempted to help solve the problem, such as providing cybersecurity scholarship funding. However, the problem is continuing to grow.

C. *Academic Cybersecurity Frameworks and Programs*

One approach that some organizations and government entities have taken to help solve the cybersecurity skills shortage is the development of academic cybersecurity frameworks and programs. These frameworks and programs were developed to provide a structure to help guide educators in planning and implementing cybersecurity education programs. Table III provides three of the common frameworks and programs that have been developed.

TABLE III. THREE COMMON ACADEMIC CYBERSECURITY FRAMEWORKS AND PROGRAMS

References	Framework or Program	Description
[17], [33], [54], [59]	National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework	Established by U.S. Department of Homeland Security and the National Institute of Standards and Technology to create a common cybersecurity lexicon and identify the skills needed by cybersecurity professionals. Published in 2012.
[6], [15]	Cybersecurity Curricula 2017 (CSEC2017)	Established by the IEEE Computer Society, Association for Computing Machinery, Association for Information Systems Special Interest Group on Information Security and Privacy, and the International Federation for Information Processing Technical Committee on Information

		Security Education to provide higher education institutions with cybersecurity guidance and link academic programs to industry needs. Published in 2017.
[54]	National Centers of Academic Excellence (CAE)	Established by the National Security Agency to create academic cybersecurity criteria for higher education institutions. Schools that met the criteria were awarded the designation. Launched in 1999.

This literature review has demonstrated that there has been a growing cybersecurity problem for decades. In addition, it has demonstrated a long and growing national and global shortage of cybersecurity professionals. The authors of the cited studies have described the growing shortage using terms such as dangerous, extreme, crisis, and severe. This literature review has demonstrated that this is a problem that needs to be mitigated before it gets out of control. Additionally, this literature review presented three common academic cybersecurity frameworks and programs developed to help with cyber threats and the shortage of cybersecurity professionals.

III. Methodology

A qualitative approach was used in this study to examine how state universities are helping to address the shortage of cybersecurity professionals in the United States. Qualitative research methods have been used in studies involving privacy and security because they can help answer the "what" and "how" research questions [10]. In addition, this approach was selected over a quantitative approach because it can address unique aspects of the phenomenon being studied.

Reference [7] used a qualitative study methodology to explore the challenges and opportunities organizations confront when addressing the skills and competencies employers need from their employees and future employees. As part of the study, organizational documents were collected and analyzed as part of the research. Document reviews are a common data collection method in the qualitative approach [13]. This study used a document review for the data collection and analysis.

A. *Scope and Delimitations of the Research*

The scope of the research was limited in focus to provide effective and useful results due to the time constraint of collecting the data for a specific time period and to complete the study within the set time frame and available resources. The scope of this study focused on cybersecurity programs that are offered at state universities in the United States. The study involved reviewing a sampling of 201 state universities across all 50 states to see what cybersecurity programs are being offered. The research takes a snapshot in time of the available cybersecurity programs in the sample universities.

This study specifically examined the quantities of cybersecurity programs available, levels of the programs (certificate, undergraduate, and graduate programs), and institutions that used an academic framework to develop their program. The frameworks establish standards to foster the quality of the programs. It was not possible to determine if a university used the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce or Cybersecurity Curricula 2017 (CSEC2017) academic frameworks because they were not mentioned in their online catalogs. However, it is easy to determine if a university used the National Centers of Academic Excellence (CAE) structure.

The CAE designation is not an accreditation. It is a recognition that identifies institutions with cybersecurity programs that have met specific rigorous requirements established by the National Security Agency (NSA) and other sponsors of the program [39]. In addition, there are three types of designations that an institution can pursue: Cyber Defense (CAE-CD), Cyber Research (CAE-R), and Cyber Operations (CAE-CO). A university can achieve one or more of the designations based on the academic direction of the school. For example, a research university can pursue the Cyber Research designation to foster their cybersecurity research programs. The goal of the program is to establish academic excellence to produce qualified cybersecurity professionals needed by the United States. For this reason, institutions that received a CAE designation were identified in this study to provide a perspective on the adoption of cybersecurity standards in academia to meet the workforce needs.

B. *Data Source and Collection*

To examine how state universities are helping to address the shortage of cybersecurity professionals in the United States a document review was conducted. Online academic catalogs of state universities were reviewed to identify what types of cybersecurity programs are being offered. There are nearly 2000 public universities in the United States. The sample size of state university online academic catalogs was 202 randomly selected universities in this study, which is approximately 10% of the number of public universities. The selection was made from a list of over 2000 universities ordered by state. The researcher went down the list in sequence by state and selected the next state university in the list until four universities were selected for the state. Each state was processed in the same manner to avoid bias. At least one sample university was selected from each of the 50 states. An equal number of samples from each state were attempted with the goal of selecting four universities from each state for a total of 200. However, some small states had less than four state universities. Universities were selected from larger states to make up for the smaller states with few state universities by going back to a previous state and selecting the next state university in line. The researcher selected the state universities in the order of the list provided and did not pick and choose by choice to avoid bias. Two additional universities were selected in case of deletions for a total of 202 institutions. One record was deleted due to an inconsistency leaving 201 records to be analyzed. The data was collected during the month of January 2024.

Different search terms were used to identify the cybersecurity programs. These include computer security, information systems security, information security, information assurance, and computer or digital forensics. The researcher watched for other terms that may have been appropriate.

The data collected from the online academic catalogs examined the different levels of cybersecurity programs being offered. The identified levels of programs include certificate programs (non-credit, undergraduate, and graduate), associate degrees, bachelor degrees, master degrees, and doctorate degrees. In addition, it identified the cybersecurity topic as a major, minor, or concentration. A minor is a secondary area of study in addition to a major. A concentration is when the degree major is in a related field, such as Information Technology, but has a concentration of courses in Cybersecurity.

A second data source was used to determine if the sample universities have received the Center of Academic Excellence (CAE) designation due to the difficulty in finding a CAE designation on the university websites. The National Security Agency's CAE in Cybersecurity website [18] was reviewed to identify if a sample university received the CAE designation. In addition, the type of designation was identified, such as Cyber Defense (CAE-CD), Cyber Research (CAE-R), and Cyber Operations (CAE-CO).

C. Data Aggregation

After the data was collected from the online academic catalogs, a detailed review was conducted to eliminate any errors or anomalies. One record was deleted due to showing a potential incorrect entry. The second data source was then used to identify the sample universities that received a CAE designation and the type of designation. This was added to the collected online academic catalog data.

The next step aggregated the data based on the number and types of cybersecurity programs being offered by the sample universities. The aggregation included, program levels, CAE designations, and topic implementation, such as being a major, minor, or concentration. Tables IV through X provide the aggregated data of cybersecurity programs for the sample state universities. Table IV presents overall counts of the sample state universities that have or don't have cybersecurity programs. The percentage calculations in Table IV are based on the total number of sample universities, 201.

TABLE IV. OVERALL AGGREGATED DATA - CYBERSECURITY PROGRAMS

Aggregated Item	Quantity	Percentage
Total number of state universities in the sample	201	100%
Universities with cybersecurity programs	170	84.6%
Universities with no cybersecurity programs	31	15.4%

Table V displays the counts of universities that have a cybersecurity program and have or don't have a CAE designation. These counts came from the NSA's CAE in Cybersecurity website [18]. The percentage calculations in Table V are based on the total number of sample universities that have a cybersecurity program, 170.

TABLE V. UNIVERSITIES WITH A CAE DESIGNATION

Aggregated Item	Quantity	Percentage
Universities with CAE designation	86	50.6%
Universities with no CAE designation	84	49.4%

Table VI presents the aggregated data of the 86 state universities with cybersecurity programs that have the CAE designation. The data shows the distribution of the type of CAE designation awarded to the universities. The data includes the universities that may have been awarded more than one type of designation. The percentage calculations in Table VI are based on the 86 state universities with the CAE designation.

TABLE VI. UNIVERSITIES WITH CAE DESIGNATION BY TYPE

Aggregated Item	Quantity	Percentage
Universities with Cyber Defense (CAE-CD)	67	77.9%
Universities with Cyber Operations (CAE-CO)	8	9.3%
Universities with Cyber Research (CAE-R)	38	44.2%

Table VII presents the counts of the state universities that have a cybersecurity certificate program. The data shows the level of the certificate program, such as non-credit professional, undergraduate, and graduate. The percentage calculations in Table VII are based on the total number of sample universities, 201.

TABLE VII. UNIVERSITIES WITH CYBERSECURITY CERTIFICATE PROGRAMS

Aggregated Item	Quantity	Percentage
Universities with non-credit professional certificate programs	7	3.5%
Universities with undergraduate certificate programs	49	24.4%
Universities with graduate certificate programs	78	38.8%

Table VIII presents the counts of the state universities that have an undergraduate cybersecurity program. The data shows the level of the program, such as associate or bachelor degree programs. In addition, it shows if cybersecurity is a major, minor, or concentration of a degree program. The percentage calculations in Table VIII are based on the total number of sample universities, 201.

TABLE VIII. UNIVERSITIES WITH CYBERSECURITY UNDERGRADUATE PROGRAMS

Aggregated Item	Quantity	Percentage
Universities with undergraduate degree programs	123	61.2%
Universities with undergraduate degree programs and/or a minor	149	74.1%
Universities with associate degree programs (major)	10	5%
Universities with associate degree programs (concentration)	1	<1%
Universities with bachelor degree programs (major)	65	32.3%
Universities with bachelor degree programs (concentration)	56	27.9%
Universities that offer a cybersecurity minor	57	28.4%

Table IX presents the counts of the state universities that have a graduate cybersecurity program. The data shows the level of the program, such as a master or doctorate degree program. In addition, it shows if cybersecurity is a major, minor, or concentration of a degree program. The percentage calculations in Table IX are based on the total number of sample universities, 201.

TABLE IX. UNIVERSITIES WITH CYBERSECURITY GRADUATE PROGRAMS

Aggregated Item	Quantity	Percentage
Universities with graduate degree programs	95	47.3%
Universities with master degree programs (major)	57	28.4%
Universities with master degree programs (concentration)	36	17.9%
Universities with master degree programs (minor)	1	<1%
Universities with doctorate degree programs (major)	2	<1%
Universities with doctorate degree programs (concentration)	8	4%
Universities with doctorate degree programs (minor)	2	<1%

Table X presents the counts of state universities that offer a higher level program but not a lower level program. In addition, it shows programs that offer a lower level program but not a higher level program. The data shows the level of the program, such as certificate, bachelor, graduate, or doctorate. The percentage calculations are based on the total number of sample universities for different counts as shown in the table note.

TABLE X. UNIVERSITIES THAT OFFER ONE LEVEL OF A PROGRAM BUT NOT ANOTHER LEVEL PROGRAM

Aggregated Item	Quantity	Percentage
Universities that offer a cybersecurity bachelor degree program but not an associate degree or undergraduate certificate	85	70.2% [(a)]
Universities that offer a cybersecurity graduate degree program but not a graduate certificate	37	38.9% [(b)]
Universities that offer a cybersecurity graduate degree program but not an undergraduate program	18	18.9% [(b)]
Universities that offer a cybersecurity doctorate degree program but not a master degree	1	8.3% [(c)]
Universities that offer a cybersecurity undergraduate certificate or associate degree but not a bachelor degree	16	30.8% [(d)]
Universities that offer a cybersecurity bachelor degree but not a graduate program	43	35.5% [(a)]
Universities that offer a cybersecurity graduate certificate but not a graduate program	20	25.6% [(e)]

Note. Percentage calculations are based on different totals in the following specific notes:
a Percentage calculations are based on the total number of sample universities that offer a bachelor degree program, 121.
b Percentage calculations are based on the total number of sample universities that offer a graduate degree program, 95.
c Percentage calculations are based on the total number of sample universities that offer a doctorate degree program, 12.
d Percentage calculations are based on the total number of sample universities that offer an undergraduate certificate or associate degree, 52.
e Percentage calculations are based on the total number of sample universities that offer a graduate certificate program, 78.

IV. RESULTS AND DISCUSSION

The analysis of the aggregated data shows that 170 (84.6%) of the 201 sample universities offer a cybersecurity program. Only 31 (15.4%) universities did not offer a cybersecurity program at the time of the data collection. Of the 201 sample universities, there are 149 universities (74.1%) that offer an undergraduate minor, certificate, or degree program. There are 115 universities (57.2%) that offer a graduate minor, certificate, or degree program. These results show that a majority of the state universities offer a cybersecurity program. There are valid reasons why some universities do not offer a cybersecurity program. For example, liberal arts institutions, medical schools, and law schools most likely will not offer a cybersecurity program.

At the undergraduate level, of the 123 universities that offer a cybersecurity bachelor degree program, 70.2 % do not offer an associate degree or undergraduate certificate. At the graduate level, of the 95 universities that offer a cybersecurity graduate degree program, 38.9% do not offer a graduate certificate and 18.9% do not offer an undergraduate program. Of the 12 universities that offer a cybersecurity doctorate degree program, only one university does not offer a master degree. In most cases the courses required for a lower level program are included in a higher level program. For example, the courses for an undergraduate certificate are usually included in an associate degree and the courses required for an associate degree are usually included in a bachelor degree. This would suggest that if an institution offers a bachelor degree in cybersecurity, the institution would already have the course offerings available for a certificate or associate degree program and may not need to develop additional courses. These additional lower level programs may provide additional options for potential students and help in reduce the shortage of cybersecurity professionals.

There were 25% to 35% of the sample universities that offered a lower level program but not a higher level program. For example, 16 universities offered an undergraduate certificate or associate degree, but did not offer a bachelor degree. Adding these higher level programs would provide more options for students, but may require additional courses to be developed.

There were 86 (50.6%) of the 170 sample universities with cybersecurity programs that have earned a CAE designation. The largest CAE designation earned by the sample universities is the Cyber Defense (CAE-CD) CAE designation; There were 67 universities (77.9%) that earned the CAE-CD designation. The Cyber Research (CAE-R) designation is the second highest earned with 38 universities (44.2%) earning the designation. Only 8 universities (9.3%) earned the Cyber Operations (CAE-CO) designation. As previously described, the CAE designation is not an accreditation. It is an academic recognition that an institution has met rigorous academic cybersecurity requirements established by the NSA. An institution that does not have a CAE designation does not indicate that their programs are deficient or substandard. The institution may have used another academic framework or may be in the process of submitting the application for the CAE designation at the time of the data collection.

The data aggregation results of this study address the purpose of the research and show how state universities are helping to address the shortage of cybersecurity professionals as of the period of this study. Overall, the results demonstrate that a majority of the state universities are offering some type of a cybersecurity program at this snapshot in time. This may be a good indication that state universities are taking seriously the shortage of cybersecurity professionals. Only a small percentage of the sample universities do not offer a cybersecurity program. In addition, more than half of the universities that offer a cybersecurity program have received the CAE designation.

A. *Limitations*

The major limitation of this study was the differences in the online academic catalogs for the sample universities. Each of the online academic catalogs for the sample universities was very different in structure, format, content, and terminology. For this reason, each catalog was reviewed manually by the researcher to extract the data needed for the research. However, the manual review added some insight to the research from researcher observations that are noted in the study.

Another limitation is that it is not known of any information that may be pertinent to the research that is not included in the online catalogs. For example, the use of specific academic frameworks to develop their cybersecurity programs may have been excluded such as the NICE or CSEC2017 frameworks. This could have shown that industry cybersecurity standards are included in the instruction.

B. *Proposed Recommendations*

Based on the results of the data aggregation three recommendations are proposed to address the premise of the study that the more cybersecurity programs that are available will produce more cybersecurity professionals. The proposed recommendations may help to increase the number and quality of cybersecurity programs to produce more cybersecurity professionals. In addition, they could provide potential students with additional options and may influence their decision to pursue a program.

The results in Table X show that several universities that offer a bachelor’s degree in cybersecurity often do not offer an undergraduate certificate or associate degree in cybersecurity. The same was also noted for institutions that offer a graduate degree program, but not a lower level program. The first proposed recommendation would be to consider adding lower level programs in cybersecurity when a higher level program is offered. For example, an institution that offers a bachelor degree program could add an undergraduate certificate or associate degree program. In addition, an institution that offers a master’s degree program could add a graduate certificate program. The courses needed for these lower level programs are usually already offered in the higher level programs and may not need to be developed. This could increase the number of available cybersecurity program options for potential students.

Of the 201 sample universities, there are more undergraduate programs than graduate programs. This is typical with most degree subjects. The results in Table X show that several institutions that offer a lower level cybersecurity program do not offer a higher level program in cybersecurity. However, the researcher noted that several of these institutions do offer higher level programs in other subjects. Another proposed recommendation is to consider adding a higher level program in cybersecurity in addition to the lower level programs that are currently offered. Although this recommendation could be a major project in the development of new courses, it may increase the number of available cybersecurity program options for potential students.

Quality instruction is an important aspect of a cybersecurity program. The researcher did not see any use of the NICE or CSEC2017 academic cybersecurity frameworks mentioned in the academic online catalogs. The results in Table V show that about half of the universities (50.6%) that had a cybersecurity program and received a CAE designation. If academic cybersecurity frameworks were not used or a CAE designation was not received, another proposed recommendation would be to add and incorporate an academic cybersecurity framework into the programs currently being offered or in development. In addition, the academic framework used in developing the cybersecurity programs should be prominently highlighted in the online catalogs. This would show potential students that the programs meet established cybersecurity standards and may influence their decision to pursue the program.

C. *Future Research*

The scope and delimitations of the study generate the need for further research. For example, this study examined a sampling of state universities in the United States. Future research could include larger sample sizes and include demographic statistics to determine relationships with programs and graduating cybersecurity professionals. In addition, future research could focus on specific types of cybersecurity programs, such as cryptography, digital forensics, secure software engineering, and cybersecurity operations and management to determine shortages in specific cybersecurity areas.

Higher education institutions are a prime source for the cybersecurity workforce pipeline. However, they are not the only source of cybersecurity professionals. Further research can investigate these other sources, such as private universities, community colleges, technical schools, boot camps, and organizational courses, to evaluate their contribution to the workforce of cybersecurity professionals. Additionally, further research could also be expanded to international institutions since the shortage of cybersecurity professionals is global.

This research study inspired several questions that could be answered with future research. For example, why do universities that offer a bachelor degree program in cybersecurity but not offer an associate degree or undergraduate certificate? The same question would apply to universities that offer a graduate degree in cybersecurity but not a graduate certificate. Future research could investigate the benefits of adding these lower level programs when a higher level program is offered and the impact the new programs would have on the cybersecurity workforce.

Of the universities that did not have a CAE designation, did they use another academic framework to develop their cybersecurity programs, such as the NICE or CSEC2017 frameworks? Future research could address university strategies for cybersecurity program development and effectiveness of program delivery or the effectiveness of the academic cybersecurity frameworks. Of the institutions that have a Cyber Research (CAE-R) designation, are they performing research to increase cybersecurity capabilities that reduce the quantity of cybersecurity professionals needed to mitigate threats? Future research could identify and explore the areas where cybersecurity research is needed.

This study collected the data in a snapshot of time. Future studies could involve reworking this study as a longitudinal study by collecting new data in different snapshots of time, such as in one year intervals. The results of the different studies can be compared to determine if the number and types of cybersecurity programs are increasing or decreasing. Literature reviews conducted during the new snapshots in time can show if progress is being made regarding the shortages of cybersecurity professionals and cybersecurity attacks.

This study has generated questions that cannot be answered with just one research project and will require further research. For example, are there enough programs available to reduce or even eliminate the shortage of cybersecurity professionals? If not, how many is needed? As new cybersecurity programs become available, will the shortage start going down? If the shortage is being reduced, is it having an impact on the number and severity of cybersecurity incidents? If not, how can higher education institutions address that situation? Being able to answer these questions with further research can have a positive impact on the shortage of cybersecurity professionals.

V. Conclusion

Cybersecurity threats have been a serious and growing problem for decades. In addition, several studies have shown that there is a severe shortage of cybersecurity professionals in the United States and globally. Many studies have demonstrated that higher education institutions are a primary source of the talent pipeline to the workforce. This study examined what state universities are doing to help address the shortage of cybersecurity professionals in regards to the availability of cybersecurity programs. This study and other studies suggests that the number of available programs is related to the number of cybersecurity professionals entering the workforce. Thus increasing the number of available programs could add more cybersecurity professionals to the workforce and have an impact on reducing the shortage.

The results of this study show that a majority of the sample state universities are providing cybersecurity programs. In addition, of the institutions that offer a cybersecurity program over half of them have received a National Centers of Academic Excellence (CAE) designation showing their programs meet established cybersecurity standards. Although these findings are impressive, they do not answer the big question "is it enough?" without further research.

It is important to point out that a workforce shortage is a large complex problem and one research study will not solve the problem. This study addresses one small part of the problem. It has proposed recommendations that could increase the number of cybersecurity programs. In addition, this research has generated new questions and suggested future research that may help address the problem. One may consider that this and future research could provide some insight into workforce shortages in other fields.

References

[1] K. Abukari, S. Dutta, C. Li, S. Tang, and P. Zhu, “Corporate communication and likelihood of data breaches,” International Review of Economics & Finance, 94, 103433-, 2024, https://doi.org/10.1016/j.iref.2024.103433

[2] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, and K.-K. R. Choo, “The role of national cybersecurity strategies on the improvement of cybersecurity education,” Computers & Security, 119, 102754–, 2022, https://doi.org/10.1016/j.cose.2022.102754

[3] A. M. Algarni, V. Thayananthan, and Y. K. Malaiya, “Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems,” Applied Sciences, 11(8), 3678, 2021, https://doi.org/10.3390/app11083678

[4] K. Amorosa and B. Yankson, “Human error - A critical contributing factor to the rise in data breaches: A case study of higher education,” Holistica Journal of Business and Public Administration, 14(1), 110–132, 2023, https://doi.org/10.2478/hjbpa-2023-0007

[5] T. Andel and J. McDonald, “A systems approach to cyber assurance education,” Proceedings of the 2013 on InfoSecCD ’13: Information Security Curriculum Development Conference, 13–19, 2013, https://doi.org/10.1145/2528908.2528920

[6] M. E. Armstrong, K. S. Jones, A. S. Namin and D. C. Newton, “Knowledge, skills, and abilities for specialized curricula in cyber defense: Results from interviews with cyber professionals,” ACM Transactions on Computing Education, 20(4), 1–25, 2020, https://doi.org/10.1145/3421254

[7] N. Arthur-Mensah, “Bridging the industry–iducation skills gap for human resource development,” Industrial and Commercial Training, 52(2), 93-103, 2020, http://dx.doi.org/10.1108/ICT-11-2019-0105

[8] A. M. Baird and S. Parayitam, “Employers’ ratings of importance of skills and competencies college graduates need to get hired: Evidence from the New England region of USA,” Education & Training, 61(5), 622-634, 2019, http://dx.doi.org/10.1108/ET-12-2018-0250

[9] T. Balon and I. Baggili, “Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education,” Education and Information Technologies, 28(9), 11759-11791, 2023, https://doi.org/10.1007/s10639-022-11451-4

[10] A. G. Bello, D. Murray, and J. Armarego, “A systematic approach to investigating how information security and privacy can be achieved in BYOD environments,” Information & Computer Security, 25(4), 475–492, 2017, https://doi.org/10.1108/ics-03-2016-0025

[11] J. Bhuyan, F. Wu, C. Thomas, K. Koong, J. W. Hur, and C. Wang, “Aerial drone: An effective tool to teach information technology and cybersecurity through Project Based Learning to minority high school students in the U.S.,” TechTrends 64, 899–910, 2020, https://doi.org/10.1007/s11528-020-00502-7

[12] B. J. Blazic, “The cybersecurity labour shortage in Europe: Moving to a new concept for education and training,” Technology in Society, 67, 101769-, 2021, https://doi.org/10.1016/j.techsoc.2021.101769

[13] L. D. Bloomberg and M. Volpe, Completing your Qualitative Dissertation: A Road Map from Beginning to End. Thousand Oaks, CA: SAGE Publications Inc., 2019.

[14] N. G. Brooks, T. H. Greer, and S. A. Morris, “Information systems security job advertisement analysis: Skills review and implications for information systems curriculum,” Journal of Education for Business, 93(5), 213–221, 2018, https://doi.org/10.1080/08832323.2018.1446893

[15] D. L. Burley and A. H. Lewis, “Cybersecurity Curricula 2017 and Boeing: Linking curricular guidance to professional practice,” Computer, 52(3), 29–37, 2019, https://doi.org/10.1109/MC.2018.2883567

[16] D. N. Burrell, “An exploration of the cybersecurity workforce shortage,” International Journal of Hyperconnectivity and the Internet of Things, 2(1), 29–41, 2018, https://doi.org/10.4018/IJHIoT.2018010103

[17] K. Cabaj, D. Domingos, Z. Kotulski, and A. Redpicio, "Cybersecurity education: Evolution of the discipline and analysis of masters programs," Computer Security, 75, 24-35, 2018, https://doi.org/10.1016/j.cose.2018.01.015

[18] CAE In Cybersecurity Community, "CAE Institution Map," n.d., CAE Community. [Online] Available: https://www.caecommunity.org/cae-map

[19] T. Caldwell, "Plugging the cyber-security skills gap," Computer Fraud & Security, 2013(7), 5–10, 2013, https://doi.org/10.1016/S1361-3723(13)70062-9

[20] S. J. Choi, M. Chen, and X. Tan, "Assessing the impact of health information exchange on hospital data breach risk," International Journal of Medical Informatics, 177, 105149–105149, 2023, https://doi.org/10.1016/j.ijmedinf.2023.105149

[21] Center for Strategic & International Studies. "Significant Cyber Incidents", 2024, Strategic Technologies Program. [Online] Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[22] J. Chow, E. Crutchlow, and J. Cain, "Industry cybersecurity workforce development," Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, 19–19, 2015, https://doi.org/10.1145/2751957.2756528

[23] N. Chhinzer, N. and A. M. Russo, "An exploration of employer perceptions of graduate student employability," Education & Training, 60(1), 104-120, 2018, http://dx.doi.org/10.1108/ET-06-2016-0111

[24] T. Coulson, M. Mason, and V. Nestler, "Cyber capability planning and the need for an expanded cybersecurity workforce," Communications of the IIMA, 16(2), 2019, https://doi.org/10.58729/1941-6687.1401

[25] S. I. Erwin, "Shortage of talent could cripple cybersecurity plans," National defense, Vol. 94, Number 669, pp. 12-, 2009.

[26] J. Fan, "Legal policies failing on data breaches?–An empirical study of U.S. information security law implementations," Procedia Computer Science, 221, 971–978, 2023, https://doi.org/10.1016/j.procs.2023.08.076

[27] S. Furnell, "The cybersecurity workforce and skills," Computers & Security, 100, 1-7, 2021, https://doi.org/10.1016/j.cose.2020.102080

[28] M. Glas, G. Messmann, and G. Pernul, "Complex yet attainable? An interdisciplinary approach to designing better cyber range exercises," Computers & Security, 144, 103965-, 2024, https://doi.org/10.1016/j.cose.2024.103965

[29] J. Hiller, K. Kisska-Schulze, and S. Shackelford, "Cybersecurity carrots and sticks," American Business Law Journal, 61(1), 5–29, 2024, https://doi.org/10.1111/ablj.12238

[30] B. Hoanca and B. Craig, "Building a K-16-Industry partnership to train IT professionals," Journal of Information Systems Education, 30(4), 232-241, 2019.

[31] A. Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications. Sebastopol, CA: O'Reilly Media, Inc., 2024.

[32] B. Holland, "Special Issue: Higher Education and Workforce Development – Comparative approaches for diverse industries: Introduction: The theoretical context of higher education and workforce development," Industry & Higher Education, 33(6), 359–361, 2019, https://doi.org/10.1177/0950422219885201

[33] K. Jones, A. Namin, and M. Armstrong, "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, 2018, https://doi.org/10.1145/3152893

[34] S. Jontz, "Cybersecurity education receives a makeover," Signal, 69(8), 35-, 2015.

[35] R. C. Joseph, "Data breaches: Public sector perspectives," IT Professional, 20(4), 57–64, 2018, https://doi.org/10.1109/MITP.2017.265105441

[36] U. Kannan and R. Swamidurai, "Integrating cybersecurity concepts across undergraduate computer science and information systems curriculum," ASEE Annual Conference, 2021, [Online] https://par.nsf.gov/servlets/purl/10264185

[37] P. A. McQuaid and S. Cervantes, "How to achieve a seasoned cybersecurity workforce," Software Quality Professional, 21(4), 4-10, 2019.

[38] M. Mukherjee, N. T. Le, C. Yang-Wai, and W. Susilo, "Strategic approaches to cybersecurity learning: A study of educational models and outcomes," Information, 15(2), 117, 2024, https://doi.org/10.3390/info15020117

[39] National Security Agency, "National Centers of Academic Excellence in Cybersecurity," National Centers of Academic Excellence, 2022. [Online] Available: https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

[40] S. Nepal, J. Hernandez, R. Lewis, A. Chaudhry, B. Houck, E. Knudsen, R. Rojas, B. Tankus, H. Prafullchandra, and M. Czerwinski, "Burnout in cybersecurity incident responders: Exploring the factors that light the fire," Proceedings of the ACM on Human-Computer Interaction, 8(CSCW1), 1–35, 2024, https://doi.org/10.1145/3637304

[41] "New cyber academy looks to tackle security skills shortage," Computer Fraud & Security, 2013(9), 3–3, 2013, https://doi.org/10.1016/S1361-3723(13)70077-0

[42] S. Okada, Y. Katano, Y. Kozai, and T. Mitsunaga, "Predicting and visualizing lateral movements based on ATT&CK and quantification theory Type 3," Journal of Cases on Information Technology, 26(1), 1-14, 2024, https://doi.org/10.4018/JCIT.340722

[43] U. C. Okolie, C. A. Nwajiuba, B. Eneje, M. O. Binuomote, C., Ehiobuche, and D. Hack-Polay, "A critical perspective on industry involvement in higher education learning: Enhancing graduates' knowledge and skills for job creation in Nigeria," Industry & Higher Education, 35(1), 61–72, 2021, https://doi.org/10.1177/0950422220919655

[44] B. Payne and E. Mienie, "RASCLS vs. Ransomware: A counterintelligence framework for cybersecurity education," Journal of Homeland Security Education, 16, 1-5, 2023.

[45] A. R. Rao and A. Elias-Medina, "Designing an Internet of Things laboratory to improve student understanding of secure IoT systems," Internet of Things and Cyber-Physical Systems, 4, 154–166, 2024, https://doi.org/10.1016/j.iotcps.2023.10.002

[46] C. A. Ramezan, "Examining the cyber skills gap: An analysis of cybersecurity positions by sub-field," Journal of Information Systems Education, 34(1), 94–105, 2023.

[47] G. A. P. Rodrigues, A. L. M. Serrano, G. F. Vergara, R. de O. Albuquerque and G. D. A. Nze, "Impact, compliance, and countermeasures in relation to data breaches in publicly traded U.S. companies," Future Internet, 16(6), 201, 2024, https://doi.org/10.3390/fi16060201

[48] R. Sahota, "Cybersecurity: Another essential checklist," Journal of the California Dental Association, 52(1), 2024, https://doi.org/10.1080/19424396.2024.2373973

[49] S. E. Said, "Pedagogical best practices in higher education National Centers of Academic Excellence / Cyber Defense Centers of Academic Excellence in Cyber Defense," ProQuest Dissertations and Theses Global, 2018.

[50] H. Saleem and M. Naveed, "SoK: Anatomy of data breaches," Proceedings on Privacy Enhancing Technologies, 2020(4), 153-174, 2020, https://doi.org/10.2478/popets-2020-0067

[51] J. P. Seara and C. Serrão, "Intelligent System for Automation of Security Audits (SIAAS)." EAI Endorsed Transactions on Scalable Information Systems, 2024, https://doi.org/10.4108/eetsis.3564

[52] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal, R. Kumar and A. K. Raees, "Healthcare data breaches: Insights and implications," Healthcare, 8(2), 133, 2020, https://doi.org/10.3390/healthcare8020133

[53] R. L. Smith and R. M. Honda, "What is the best approach to ensuring the nation's cyber security?; Cyberterrorism is not only a threat, It is a reality?; Strengthen cyberterrorism laws," Roll Call, 2002.

[54] A. Sobel, A. Parrish and R. Rai, "Curricular foundations for cybersecurity," Computer, 52(3), 14-17, 2019, https://doi.org/10.1109/MC.2019.2898240

[55] J. Straub, "Defining, evaluating, preparing for and responding to a Cyber Pearl Harbor," Technology in Society, 65, 101599–, 2021, https://doi.org/10.1016/j.techsoc.2021.101599

[56] J. C. Sun and H. A. Turner, "The complementarity investment in university-industry collaboration," Innovative Higher Education, 48(3), 539–556, 2023, https://doi.org/10.1007/s10755-022-09641-6

[57] The Wall Street Journal, Eastern Edition, "U.S. to give scholarships for cyber-security corps," 2001, [Online] Available: https://www.proquest.com/newspapers/u-s-give-scholarshipsfor-cyber-security-corps/docview/398731473/

[58] G. Towhidi and J. Pridmore, "Aligning cybersecurity in higher education with industry needs," Journal of Information Systems Education, 34(1), 70-83, 2023.

[59] C. V. Van Slyke, G. Clary, S. Ellis and M. Maasberg, "Employer preferences for cybersecurity skills among information systems graduates," Proceedings of the 2019 on Computers and People Research Conference, 131–134, 2019, https://doi.org/10.1145/3322385.3322418

[60] M. Warner, "Cybersecurity: A pre-history," Intelligence & National Security, 27(5), 781–799, 2012, https://doi.org/10.1080/02684527.2012.708530

[61] S. C. Yang, "A curriculum model for cybersecurity master's program: A survey of AACSB-accredited business schools in the United States," Journal of Education for Business, 94(8), 520–530, 2019, https://doi.org/10.1080/08832323.2019.1590296

[62] M. N. Yusuf and A. Yulianeu, "Energizing organizational learning and organizational performance: Human Capital Theory perspective," Quality - Access to Success, 24(192), 82-93, 2023, https://doi.org/10.47750/qas/24.192.11