Academic Quality and Workforce Division

60×30TX
Texas Higher Education Coordinating Board

Strategies to Incentivize Institutions of Higher Education to Develop Degree Programs in Cybersecurity

A Report to the Texas Legislature,
Per Senate Bill 64, 86th Texas Legislature

In Collaboration with the Department of Information Resources

September 2020

This page has been left blank intentionally.

Texas Higher Education Coordinating Board

Agency Mission

The mission of the Texas Higher Education Coordinating Board (THECB) is to provide leadership and coordination for Texas higher education and to promote access, affordability, quality, success, and cost efficiency through *60x30TX*, resulting in a globally competitive workforce that positions Texas as an international leader.

Agency Vision

The THECB will be recognized as an international leader in developing and implementing innovative higher education policy to accomplish our mission.

Agency Philosophy

The THECB will promote access to and success in quality higher education across the state with the conviction that access and success without quality is mediocrity and that quality without access and success is unacceptable.

The THECB's core values are:
Accountability: We hold ourselves responsible for our actions and welcome every opportunity to educate stakeholders about our policies, decisions, and aspirations.
Efficiency: We accomplish our work using resources in the most effective manner.
Collaboration: We develop partnerships that result in student success and a highly qualified, globally competent workforce.
Excellence: We strive for excellence in all our endeavors.

Please cite this report as follows: Texas Higher Education Coordinating Board. (2020). Strategies to Incentivize Institutions of Higher Education to Develop Degree Programs in Cybersecurity. Austin, TX.

This page has been left blank intentionally.

Table of Contents

Figure

Table

Appendices

Executive Summary

The Texas higher education plan, *60x30TX*, contains four broad goals: 1) an educated population; 2) completion; 3) marketable skills; and 4) student debt. *60x30TX* is designed to ensure that a competitive and prosperous future remains for students seeking to better their lives and the lives of their families. The second goal of *60x30TX* states that at least 550,000 students in 2030 will complete a certificate or associate, bachelor's, or master's degree from an institution in Texas (THECB, 2015). The type of degree students complete is equally important. Research indicates that completing a credential or degree beyond a high school diploma improves employment outcomes and earnings for individuals (Belfield, 2017).

There is a growing need for graduates of certificate and degree programs in cybersecurity. According to Cybercrime Magazine (2016), only three percent of U.S. bachelor's degree graduates have cybersecurity-related skills. Cybersecurity Ventures, the world's leading researcher and publisher covering the global cyber economy (Cybersecurity Ventures, 2019), estimates there will be 3.5 million unfilled cybersecurity jobs in 2021. Recent data from the National Center for Education Statistics showed that of the 1.9 million students who graduated with a bachelor's degree in 2018, only 64,405 earned a degree in computer and information sciences, a skill set relevant to cybersecurity. Approximately 3.6 million students graduated from U.S. high schools in 2019, and of those, only 66 percent went on to attend college. If only three percent of college students continue to enroll in computer science programs related to cybersecurity, the shortage of workers in this under-employed area will get worse (Knoll, 2019). The Bureau of Labor Statistics states that cybersecurity has a high-growth projection rate of 28 percent from 2016 to 2026. In addition, an entry-level position in cybersecurity requires a workforce certificate or an associate degree. In 2019, the median annual salary of a cybersecurity professional is $95,510, and with more education and experience, salaries increase.

Senate Bill (SB) 64 passed by the 86th Texas Legislature, Regular Session, required the Texas Higher Education Coordinating Board (THECB), in collaboration with the Department of Information Resources (DIR), to explore ways to incentivize Texas higher education institutions to develop more certificate and degree programs in the area of cybersecurity and submit a report detailing strategies to the lieutenant governor, the speaker of the House of Representatives, the presiding officer of each legislative standing committee with primary jurisdiction over higher education, and each governing board of an institution of higher education not later than September 1, 2020. This report satisfies that legislative directive.

The THECB and DIR conducted two surveys and a focus group session in February 2020 to collect data on the development of degree programs in cybersecurity at Texas institutions of higher education (IHEs), and make recommendations to help incentivize the development of additional degree programs in cybersecurity.

The THECB and DIR identified 33 IHEs in Texas that offer cybersecurity degree programs and their points of contact. The contacts included department chairs, coordinators, professors, and deans. Using these contacts, the THECB sent out an email requesting their participation in the focus group, and 24 contacts volunteered to participate. The THECB held the focus group on February 12, 2020. Before the focus group discussion, the THECB sent out a survey to all the IHEs that offer cybersecurity programs and another survey to the IHEs that do

not offer such programs. To increase likelihood of responses, the surveys were conducted anonymously. The THECB used both the survey and the focus group discussion to ask participants to respond to a set of questions regarding the development of a cybersecurity program, as well as their suggestions on possible incentives for IHEs to start a cybersecurity degree program. Based on the review of the surveys and the input of the focus group, the THECB staff, in consultation with the DIR staff recommend the following:

Recommendations

Recommendation 1. Provide state funding. Institutions with existing cybersecurity degree programs secured funding through external grants, institutional sources (tuition or department budget), or an industry partner. Institutions without existing cybersecurity degree programs stated that lack of funding (for labs, equipment, and qualified faculty salaries) is a major reason cybersecurity programs have not been implemented on their campuses.

Recommendation 2. Create partnerships with industry. Institutions with industry partnerships indicated that local industry partners requested the programs due to market demand for cybersecurity professionals. To partner with local industries in their areas, institutions created advisory groups and committees to help address the need for cybersecurity degree programs and graduates.

Recommendation 3. Develop standardized curriculum. The National Institute of Standards and Technology released the National Initiative for Cybersecurity Education (NICE) framework that establishes a taxonomy and common lexicon for cybersecurity. Institutions should align curriculum with these established standards.

Recommendation 4. Ensure clear articulation pathways (high school to college). Based on staff research, surveys, and the focus groups, the minimum requirement for entering the cybersecurity field and securing a financially stable job is at the certificate and associates degree level. The THECB should work with the Texas Education Agency to develop articulation pathways from high school to college.

Introduction

The second goal of the Texas higher education plan, *60x30TX*, states that at least 550,000 students in 2030 will complete a certificate or associate, bachelor's, or master's degree from an institution in Texas (THECB, 2015). The type of degree students complete is equally important. Research indicates that completing a credential or degree beyond a high school diploma improves employment outcomes and earnings for individuals (Belfield, 2017).

For Texas students, choosing the right postsecondary degree is necessary to ensure the state remains competitive at the national and international levels. The demand for information security graduates is on the rise nationwide. Information security has become an important part of the nation's security infrastructure. Several threats have affected businesses and organizations across the state in recent years. According to the report, *Economic Impact of Cybercrime-No Slowing Down*, published by the Center for Strategic and International Studies in partnership with McAfee (a private cybersecurity company), cybercrime costs organizations an estimated $445 to $608 million worldwide each year (McAfee, 2018). The ISC², a worldwide professional cybersecurity organization, estimates there is a shortage of approximately 2.93 million qualified cybersecurity professionals globally (ISC², 2019).

Data from the U.S. Bureau of Labor Statistics (BLS) estimates a national average of 12,800 openings for information security analysts each year from 2018 to 2028, with an employment increase of 32 percent. The Texas Workforce Commission (TWC) indicates a state average of 820 annual job openings for information security analysts each year from 2016 to 2026, with an employment increase of 34 percent. This is more than twice the average projected employment growth for all occupations. In addition, employment for information security professionals is projected by the BLS to grow 56 percent specifically in the computer systems design and related services field through 2026. In 2019, Texas institutions statewide produced 477 degrees in cybersecurity. According to TWC's estimates, Texas is producing 343 fewer graduates than available job positions, indicating a shortage of graduates in the cybersecurity field.

Senate Bill 64

The 86th Texas Legislature, Regular Session, passed Senate Bill (SB) 64, which mandated, "The board in collaboration with the Department of Information Resources shall identify and develop strategies to incentivize institutions of higher education to develop degree programs in cybersecurity." SB 64 directed the THECB, in collaboration with the Department of Information Resources, to submit a report detailing the strategies to incentivize institutions of higher education to develop degree programs in cybersecurity to the lieutenant governor, the speaker of the house of representatives, the presiding officer of each legislative standing committee with primary jurisdiction over higher education, and each governing board of an institution of higher education not later than September 1, 2020. This report satisfies that legislative directive.

Background of Cybersecurity

What is Cybersecurity?

On February 9, 2016, President Barack Obama announced the formation of the Commission on Enhancing National Cybersecurity (Obama, 2016). The commission was formed April 13, 2016 (Daniel, Felten, Scott, 2016) and officially defined cybersecurity as:

> "The process of protecting information and information systems by preventing, detecting, and responding to unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" (Commission on Enhancing National Security, 2016).

Why is cybersecurity important?

In 1969, the Advanced Research Projects Agency Network (ARPANET), the first version of what would become the internet, came online and digitally connected geographically disparate users for the first time (Defense Advanced Research Projects Agency, 2020). It was comprised of innovations and technology that laid the foundation for the networks still used today. While it may seem like a more modern problem, in 1972 ARPANET had the world's first virus (Matthews, 2019). The virus was what is known as a worm, a self-replicating program that spreads between systems. Now known as "Creeper," it was not malicious, simply displaying a message on a user's screen before moving to another system. Shortly after, the first anti-virus program, Reaper, was created, specifically to remove Creeper (Dominguez, 2018). While these two events did not start the cybersecurity industry, in hindsight, the need for modern cybersecurity was inevitable.

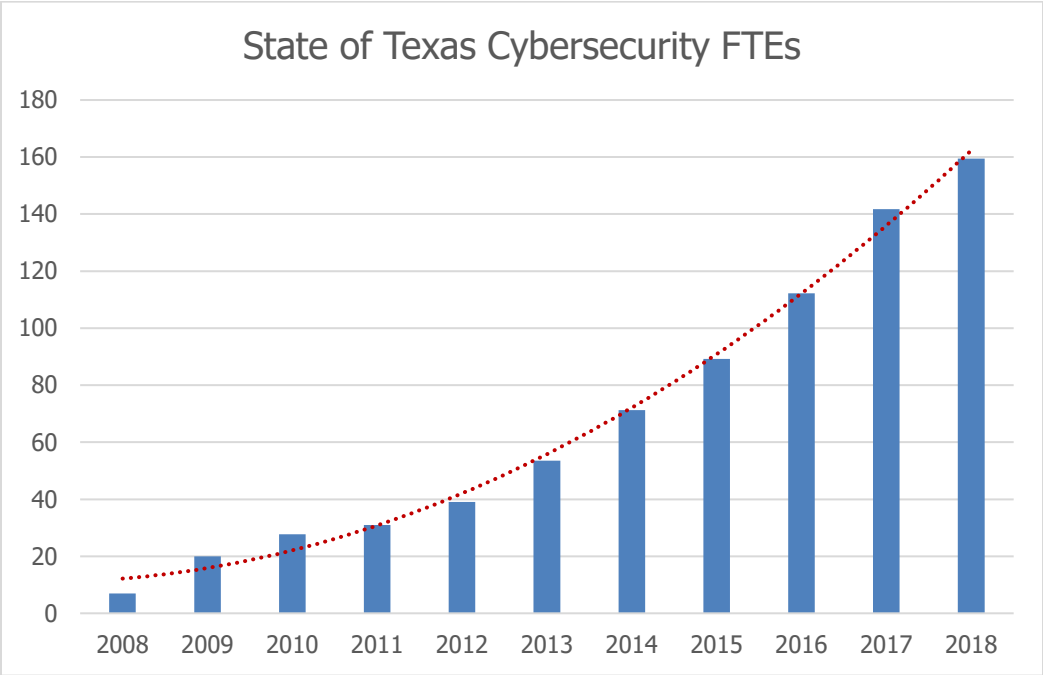
Today, from the coffee shop down the street to the power plants that are providing electricity in homes and offices, to the battlefield, and even in elections, information systems have permeated nearly every facet of modern life. For almost every information system, there is someone trying to breach its security. Bad actors do so for many reasons, including financial gain (Pagliery, 2015), testing security for future massive attacks (Das, 2019), and stealing secrets (Burgess, 2018). The global costs of cyberattacks also are climbing, with estimates showing a projected increase from $3 to $5 trillion by 2024 (Juniper Research, Ltd, 2019).

With costs of cyberattacks in the trillions, cybersecurity has become a hot job market. There are an estimated one million professionals working in cybersecurity, but there are far more cybersecurity jobs available (National Initiative for Cybersecurity Education, n.d.). In Texas, there are more than 40,000 cybersecurity openings, and the national workforce is looking for half a million cybersecurity professionals. With a growth rate of more than 30 percent projected for the sector, the talent pool is dry (Lloyd, 2017).

Due to a lack of qualified staff able to perform the work, the average pay for cybersecurity professionals is climbing fast. In 2018, the average security analyst earned $102,470 (U.S. Bureau of Labor Statistics, 2019), almost double the national average wage (U.S. Bureau of Labor Statistics, 2019). The salaries are even higher for more senior cyber talent. Employers are desperate for qualified staff and increasing the availability of degrees in cybersecurity will help ensure Texas produces the highly paid employees they desire.

The state of Texas' workforce demonstrates this trend. Before 2008, Texas did not have any information technology classifications directly correlating to cybersecurity; now it has four. Using reports from the Texas State Auditor's Office, between 2008 and 2018, the average increase in the number of cybersecurity employees was 42 percent (Figure 1).

Figure 1. State of Texas Cybersecurity Full-Time Equivalents (FTEs)



Source: Texas State Auditor's Office

Degree Levels and Job Correlation

With cybersecurity professionals in such high demand, employers are substituting education for experience, typically on a year-to-year basis. Certifications that prove a candidate's technical knowledge and experience in the field are enough for entry- to senior-level analysts. For example, if a candidate gets additional certifications in specific technologies, that candidate may qualify to be employed as a cybersecurity auditor, cybersecurity engineer, or cybersecurity architect.

Bachelor's degrees are required by just over half of employers (National Center for O*NET Development, 2019) and can help qualify candidates for the same cybersecurity analyst, cybersecurity auditor, cybersecurity engineer, and cybersecurity architecture roles, although companies may also want a certification with the degree. These degrees often have an added benefit of enabling a candidate to obtain management-level positions, such as Chief Information Security Officer. Depending on the degree, the job pool may also expand to programming the cybersecurity systems, performing forensic investigations, or becoming a penetration tester. A bachelor's degree is statutorily required to become a manager for a private investigations company (Texas Association of Licensed Investigators, 2012), an important role for forensic investigations (see licensure section below).

Master's degrees provide opportunity for the same positions but expand the available job pool to teaching at junior and community colleges, as well as opening more research roles. Doctoral degrees are primarily for those looking to be researchers or full-time professors.

Certification and Licensure

Unlike lawyers, nurses, and doctors, there are no licensure or accreditation requirements to practice or work in the cybersecurity field. There are a few notable exceptions, depending on the role of the individual and their place of employment.

If the practitioner is in Texas and performing forensic investigations, an individual does not need a license if "preparing for or responding to a cybersecurity event"(86th Texas Legislature, 2019). If the individual performs any other forensic investigations, the Texas Department of Public Safety has clarified that the individual needs a private investigator license per Texas Occupation Code, Section 1702.104 (Texas Department of Public Safety, 2019). In order to obtain a private investigator license, the applicant must own or be employed by a licensed agency, and a licensed agency must employ a licensed manager (which can be the owner/applicant). The manager must have at least three years of experience in investigations and a bachelor's degree.

There are also professional certification requirements for Department of Defense (DoD) employees. In 2004, the DoD published Directive 8140.01, which established baseline certification and training requirements for DoD employees assigned to certain roles (Department of Defense, 2015). The department issued a new directive, 8570.01-M, in 2015 to "update and expand the established policies and assigned responsibilities for managing the DoD cyberspace workforce" (Department of Defense, 2005). The DoD also publishes a mapping of minimum certifications to positions for their workforce (Defense Information Systems Agency, n.d.).

Methodology

Purpose

Senate Bill 64 (SB 64), passed by the 86th Texas Legislature, Regular Session, requires the Texas Higher Education Coordinating Board (THECB) to collaborate with the Department of Information Resources (DIR) and consult with institutions to identify and develop strategies to incentivize institutions of higher education to develop degree programs in cybersecurity. The THECB and DIR conducted two surveys and a focus group in February 2020 to collect data on the development of degree programs in cybersecurity at Texas institutions of higher education (IHEs), as well as recommendations and possible incentives for the development of additional degree programs in cybersecurity.

Approach

The THECB and DIR identified 33 IHEs in Texas that offer cybersecurity degree programs and their points of contact. The contacts included department chairs, coordinators, professors, and deans. The THECB sent out an email requesting participation in the focus group, and 24 individuals volunteered to participate. The THECB held the focus group session on February 12, 2020. Before the focus group discussion, the THECB surveyed the IHEs that offer cybersecurity programs and also surveyed IHEs that do not offer the program. To promote the likelihood of a higher response rate, the surveys were conducted anonymously. The THECB used both the survey responses and the focus group discussion to ask participants to respond to a set of questions regarding the development of the cybersecurity program, as well as their suggestions on possible incentives for IHEs to start a cybersecurity degree program. The surveys are included as Appendix A.

Location of the Focus Group

The focus group was held at the THECB offices at 1200 East Anderson Lane, Austin, Texas, on February 12, 2020, from 10 a.m. to 3 p.m.

Structure of the Focus Group

In order to encourage the focus group discussion, the THECB divided the 24 participants into five small groups. Each group included participants from both two-year and four-year IHEs to promote a productive conversation. A staff member from either the THECB or DIR joined each focus group as a facilitator, and one of the participants in each focus group served as a notetaker.

At the start of the focus group, the main facilitator for the session introduced the leadership of the THECB's Division of Academic Quality Workforce, provided the background and context for SB 64, and allowed attendees to introduce themselves. Each attendee was given the list of seven questions to discuss. The group facilitators allocated time to discuss each question, ensuring each participant had an opportunity to share their thoughts and insights. The notetaker captured the main ideas or themes for each question. The list of questions used at the focus group is provided in Appendix B. The themes that emerged from each focus group are included in Appendix C.

Samples and Analyses

A total of 24 individuals participated in the focus group meeting, including 14 individuals from two-year IHEs, 7 individuals from four-year IHEs, and 3 representatives from state and national agencies.

A total of 23 individuals completed the survey that was distributed to the IHEs that offer a cybersecurity program, and 55 individuals completed the survey that was sent out to the IHEs that do not offer a cybersecurity program.

The data analyses were based on the survey data and notes created at the focus group. THECB staff looked for emerging themes across the data. Through this process, the THECB utilized participants' voices to understand the development and implementation of the cybersecurity programs, as well as the possible incentives that IHEs may need to start additional cybersecurity degree programs.

Limitations

Data collected from the focus group and surveys cannot be generalized, because the experiences of the people who participated may not necessarily be representative of the larger population of IHEs and stakeholders. Also, the number of participants in the focus group and surveys is not comprehensive and cannot reflect the experiences and the opinions of the entire community. Lastly, not all participants answered every question in the surveys or focus group.

Focus Group and Survey Outcomes

Because the findings from the focus group discussions and survey responses sent to the IHEs that offer a cybersecurity program shared similar themes, this section combines the focus group discussions and survey responses that are relevant to SB 64:

- What prompted your institution to establish a cybersecurity program?
- What motivated your institution to start its cybersecurity program?
- Who were the key individuals (ex. dean, provost, chair, outside stakeholders, etc.) involved in the development of the degree program in cybersecurity?
- How did you determine there was a need for your degree program?

Overall, the main reasons that the IHEs established cybersecurity programs were the demand from industry and government, workforce demand, and student demand. The institutional officials reported the most important driver for starting a cybersecurity program was the demand from industry, which they understood would provide job opportunities for their students. The participants identified the industry advisory committee, dean, faculty, vice president, and department chair as the key individuals involved in the development of the programs. In addition to the demand and key players that started the program, the participants mentioned their IHEs had available funding and personnel to develop the program.

- How did you assess the student demand for your cybersecurity program?

By and large, the participants felt that industry demand for a cybersecurity program was a strong motivator for them to start the program. Thus, many respondents assessed student demand by surveying students, as well as tracking the increase in the enrollment numbers in cybersecurity or computer maintenance courses. These were important indicators for the institutions to offer the program.

- How did you develop the curriculum for your cybersecurity program?

The participants identified several resources to which they referred when developing the curricula for their cybersecurity programs. Examples included seeking guidelines and relevant information from the National Institute of Standards and Technology, National Initiative for Cybersecurity Education, Centers of Academic Excellence in Cybersecurity, and National Security Agency; consulting with faculty and industry representatives who have expertise in the field; attending conferences and meetings with practitioners; reviewing job postings; and researching other cybersecurity programs in Texas and other states.

- How did you secure the finances to run your cybersecurity program?

The respondents identified two main sources from which they seek funding: 1) grant opportunities such as local funding, Perkins Grant, and National Science Foundation grants; and 2) department budget. Overall, the participants commented operating a cybersecurity program is costly, and they make continuous attempts to secure funding.

- What obstacles were encountered in starting the cybersecurity program?

When participants were asked about the obstacles they encountered in starting their cybersecurity programs, they answered that hiring qualified professionals to develop the curriculum and teach in the new programs was the most challenging. Other notable obstacles were establishing partnerships between the IHEs and industry, securing funding to run the program, and having adequate facilities.

- What are the areas that your program is currently improving/planning to improve? (Please rank the areas in order from 1 to 5)

Table 1. Areas of that Texas programs are currently or planning to improve

	1	2	3	4	5	Total
Building public and/or private partnerships between college and industry	1	6	1	2	6	16
Recruiting students	2	3	2	5	2	14
Meeting requirements for Center for Academic Excellence	5	2	3	3	1	14
Hiring professionals to develop curriculum and teach	6	5	0	0	3	14
Providing/upgrading facilities	1	2	1	3	3	10
Securing funding to run the program	1	0	3	4	2	10
Improving student outcomes	3	1	2	1	2	9
Enhancing ranking/reputation of the program	0	2	3	2	2	9
Articulating the purpose and goals of the program	1	1	2	3	2	9
Promoting equity and access	0	1	1	1	3	6
Increasing affordability	0	0	1	2	0	3
Other	1	0	0	0	1	2

Source: Responses from the THECB survey of institutions with cybersecurity programs, 2020.

The following additional questions were posed to the focus group members:

- What could the state of Texas (Texas Legislature/Texas Higher Education Coordinating Board/Department of Information Resources) do to encourage the development of additional cybersecurity programs in Texas?
- How might an institution be encouraged to start a cybersecurity degree program?
- What are some incentives/strategies an institution may need to start a cybersecurity program?

When the participants were asked what may encourage the development of additional cybersecurity programs in Texas, they shared their anecdotes about the difficulty in hiring qualified full-time faculty. Interestingly, two-year and four-year IHEs had different definitions for "qualified" faculty. That is, for two-year IHEs, a qualified full-time faculty meant a professional with relevant experience; four-year IHEs required the faculty to have a certain educational credential (i.e., at least a master's degree). By and large, the participants agreed that institutions could not simply overcome the vast difference between the salaries offered by industry and those offered by the IHEs.

Another concern the participants shared was the lack of a curriculum blueprint. The respondents believed that having the curriculum established would remove the burden from faculty and staff members. Particularly, the representatives from the two-year IHEs said their

students often cannot transfer most of their courses and must retake courses once they transfer to four-year IHEs. Thus, having the state's participation by providing a clear degree plan and a pathway from the two-year to four-year degree, as well as from college to employment, is critical.

Additionally, the participants said securing paid internships for their students was difficult, especially for the students with the Associate of Applied Science degrees or certificates. Thus, having a strong partnership between college and industry is essential.

Overall, the respondents expressed the need for funding and interventions from the state to overcome these challenges and promote additional cybersecurity programs.

Survey Outcomes

The survey outcomes presented in this section are from the survey that was distributed to the institutions that do not offer cybersecurity programs:

- Has your institution recently considered offering a degree program in cybersecurity?

Response	%	Count
Yes	78%	43
No	22%	12
Total	100%	55

More than 70 percent of institutions responded that they recently considered offering a cybersecurity program.

- Which of the following make starting a cybersecurity program difficult? (Please check all that apply.) (31 of 55 responses from IHEs)

Response	%	Count
Hiring professionals to develop curriculum and teach	21%	21
Securing funding to start the program	17%	17
Hiring staff to start the program	17%	17
Establishing public and/or private partnerships between college and industry	16%	16
Providing/upgrading facilities	13%	13
Meeting requirements for Center for Academic Excellence	7%	7
Articulating the purpose and goals of the program	6%	6
Other	5%	5

When asked which factors make starting a cybersecurity program difficult, the respondents chose hiring professionals to develop curriculum and teach as the most difficult factor, followed by securing funding and hiring staff to start the program. The respondents said the following:

- There are few cybersecurity job opportunities in our service area. Also, our existing IT programs do include elements of cybersecurity, and our resources are limited to add additional programs that are perhaps duplicative.
- We currently have a minor in cybersecurity as a step and may build on this to meet demand if resources are available.
- Labor market demand data.

Overall, the participants listed cost and lack of qualified faculty in the area as the main factors that prohibit them from offering a cybersecurity program. In addition, they mentioned there is not a large demand for the cybersecurity program in the community for them to start the program.

- What are some examples of incentives and/or resources your institution may need to start a cybersecurity degree program?

Regarding the incentives and resources an IHE may need to start a cybersecurity program, the respondents answered they would need a clear guideline from the state to define what constitutes a cybersecurity program and how to maintain excellence in training and educating students. In addition, the respondents expressed a great need for consistent funding to provide labs, software, and supplies to students and hire faculty and graduate teaching assistants with expertise in cybersecurity.

Strategies

The second goal of the Texas higher education plan, *60x30TX*, states that at least 550,000 students in 2030 will complete a certificate or associate, bachelor's, or master's degree from an institution in Texas (THECB, 2015). For Texas students, choosing the right postsecondary degree is necessary to ensure the state remains competitive at the international and national levels. The demand for information security degrees is on the rise nationwide. Information security has become an important part of security infrastructure. In Texas alone there are over forty-thousand cybersecurity openings, and the national workforce is looking for half a million cybersecurity professionals. With a growth rate of over 30 percent projected for the sector, the talent pool is dry (Lloyd, 2017). Research and collected data support the need for additional cybersecurity degree programs in Texas. Based on the review of the surveys and the input of the focus group, the THECB staff, in consultation with the DIR staff recommend the following:

Final Report Recommendations

The THECB and DIR conducted two surveys and a focus group in February 2020 to collect data on the development of degree programs in cybersecurity at institutions of higher education (IHEs) to identify and develop strategies to incentivize institutions of higher education to develop degree programs in cybersecurity. Below are the strategies recommended by the THECB and DIR, based on input from the institutions:

Recommendation 1. Provide state funding. Institutions with existing cybersecurity degree programs secured funding through external grants, institutional sources (tuition or department budget), or an industry partner. Institutions without existing cybersecurity degree programs stated that lack of funding (for labs, equipment, and qualified faculty salaries) is a major reason cybersecurity programs have not been implemented on their campuses.

Recommendation 2. Create partnerships with industry. Institutions with industry partnerships indicated that local industry partners requested the programs due to market demand for cybersecurity professionals. To partner with local industries in their areas, institutions created advisory groups and committees to help address the need for cybersecurity degree programs and graduates.

Recommendation 3. Develop standardized curriculum. The National Institute of Standards and Technology released the National Initiative for Cybersecurity Education (NICE) framework that establishes a taxonomy and common lexicon for cybersecurity. Institutions should align curriculum with these established standards.

Recommendation 4. Ensure clear articulation pathways (high school to college). Based on staff research, surveys, and the focus groups, the minimum requirement for entering the cybersecurity field and securing a financially stable job is at the certificate and associates degree level. The THECB should work with the Texas Education Agency to develop articulation pathways from high school to college.

Conclusion

The Texas Workforce Commission (TWC) indicates a state average of 820 annual job openings for information security analysts each year from 2016 to 2026, with an employment increase of 34 percent. This is more than twice the average projected employment growth for all occupations. In 2019, Texas institutions statewide produced 477 degrees in cybersecurity. According to TWC's estimates, Texas is producing 343 fewer graduates than available job positions, which means there is a shortage of graduates in the cybersecurity field.
These findings and recommendations are aligned with and support the completion goals of the *60x30TX* higher education plan.

References

(ISC)2. (2019). *Strategies for Buildig and Growing Stong Cybersecurity Teams.* Clearwater: (ISC)2 Cybersecurity Workforce Study.

86th Texas Legislature. (2019, September 1). *Texas Occupations Code Chapter 1702. Private Security*. Retrieved from Texas Constitution and Statutes: https://statutes.capitol.texas.gov/Docs/OC/htm/OC.1702.htm

Belfield, C. a. (2017). *The labor market returns to sub-baccalaureate college: A review.* New York: Center for Analysis of Postsecondary Employment and Earnings.

Burgess, M. (2018, July 11). *A dumb security flaw let a hacker download US drone secrets*. Retrieved from Wired: https://www.wired.co.uk/article/router-hacking-drone-reaper-military-secrets

Commission on Enhancing National Cybersecurity. (2016, December 1). *Report on Securing and Growing the Digital Economy.* Retrieved from National Institute of Standards and Technology: https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

Daniel, M., Felten, E., & Scott, T. (2016, April 13). *Announcing the President's Commission on Enhancing National Cybersecurity.* Retrieved from National Archives: https://obamawhitehouse.archives.gov/blog/2016/04/13/announcing-presidents-commission-enhancing-national-cybersecurity

Das, D. (2019, November 4). *An Indian nuclear power plant suffered a cyberattack. Here's what you need to know.* Retrieved from The Washington Post: https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/

Defense Advanced Research Projects Agency. (2020, February 14). *ARPANET and the Origins of the Internet*. Retrieved from Defense Advanced Research Projects Agency: https://www.darpa.mil/about-us/timeline/arpanet

Defense Information Systems Agency. (n.d.). *DoD Approved 8570 Baseline Certifications*. Retrieved from DoD Cyber Exchange: https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/

Department of Defense. (2005, December 19). *DoD 8570.01-M Information Assurance Workforce Improvement PRogram.* Retrieved from Executive Services Directorate: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf

Department of Defense. (2015, August 11). *DoDD 8140.01 Cyberspace Workforce Management.* Retrieved from Executive Services Directorate: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf?ver=2019-06-06-120639-863

Dominguez, A. (2018, October 10). *History of computer viruses: Creeper and Reaper.* Retrieved from Pandora FMS Enterprise: https://pandorafms.com/blog/creeper-and-reaper/

Juniper Research, Ltd. (2019, August 27). *Business Losses to Cybercrime Data Breaches To Exceed $5 Trillion By 2024*. Retrieved from Juniper Research: https://www.juniperresearch.com/press/press-releases/business-losses-cybercrime-data-breaches

Knoll, S. (2019, March 6). Only 3 Percent Of U.S. Bachelor's Degree Grads Have Cybersecurity Related Skills. Cybercrime Magazine. https://cybersecurityventures.com/only-3-percent-of-u-s-bachelors-degree-grads-have-cybersecurity-related-skills/

Lloyd, M. (2017, March 21). *Negative Unemployment: That Giant Sucking Sound In Security*. Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2017/03/21/negative-unemployment-that-giant-sucking-sound-in-security/#789e76cf7206

Matthews, T. (2019, April 18). *A Brief History of Cybersecurity*. Retrieved from Cybersecurity Insiders: https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/

McAfee. (2018). *Economic Impact of Cybercrime-No Slowing Down.* Washington, D.C.: Center for Strategic and Insternational Studies.

National Center for O*NET Development. (2019, December 12). *15-1122.00 - Information Security Analysts*. Retrieved from O*NET OnLine: https://www.onetonline.org/link/summary/15-1122.00

National Initiative for Cybersecurity Education. (n.d.). *Cybersecurity Supply/Demand Heat Map*. Retrieved February 14, 2020, from CyberSeek: https://www.cyberseek.org/heatmap.html

Obama, B. (2016, February 9). *Executive Order -- Commission on Enhancing National Cybersecurity.* Retrieved from National Archives: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity

Pagliery, J. (2015, May 14). *Hackers are draining bank accounts via the Starbucks app*. Retrieved from CNN: https://money.cnn.com/2015/05/13/technology/hackers-starbucks-app/

Texas Association of Licensed Investigators. (2012). *Texas Licensing Requirements*. Retrieved February 18, 2020, from Texas Association of Licensed Investigators: https://www.tali.org/texas-licensing-requirements

Texas Department of Public Safety. (2019, September). *Agency Opinions Related to Private Security*. Retrieved from Texas Department of Public Safety: https://www.dps.texas.gov/RSD/PSB/Laws/psb_opin_sum.htm

Texas State Auditor's Office. (2008). *An Annual Report on Classified Employee Turnover for Fiscal Year 2008.* Retrieved from https://www.sao.texas.gov/SAOReports/ReportNumber?id=09-703

Texas State Auditor's Office. (2009). *An Annual Report on Classified Employee Turnover for Fiscal Year 2009.* Retrieved from https://www.sao.texas.gov/SAOReports/ReportNumber?id=10-702

Texas State Auditor's Office. (2010). *An Annual Report on Classified Employee Turnover for Fiscal Year 2010.* Retrieved from https://www.sao.texas.gov/SAOReports/ReportNumber?id=11-702

Texas State Auditor's Office. (2011). *An Annual Report on Classified Employee Turnover for Fiscal Year 2011.* Retrieved from https://www.sao.texas.gov/SAOReports/ReportNumber?id=12-701

Texas State Auditor's Office. (2012). *An Annual Report on Classified Employee Turnover for Fiscal Year 2012.* Retrieved from https://www.sao.texas.gov/SAOReports/ReportNumber?id=13-704

Texas State Auditor's Office. (2013). *An Annual Report on Classified Employee Turnover for Fiscal Year 2013.* Retrieved from https://www.sao.texas.gov/SAOReports/ReportNumber?id=14-701

Texas State Auditor's Office. (2014). *An Annual Report on Classified Employee Turnover for Fiscal Year 2014.* Retrieved from https://www.sao.texas.gov/SAOReports/ReportNumber?id=15-703

Texas State Auditor's Office. (2015). *An Annual Report on Classified Employee Turnover for Fiscal Year 2015.* Retrieved from https://www.sao.texas.gov/SAOReports/ReportNumber?id=16-702

Texas State Auditor's Office. (2016). *An Annual Report on Classified Employee Turnover for Fiscal Year 2016.* Retrieved from https://www.sao.texas.gov/SAOReports/ReportNumber?id=17-704

Texas State Auditor's Office. (2017). *An Annual Report on Classified Employee Turnover for Fiscal Year 2017.* Retrieved from https://www.sao.texas.gov/SAOReports/ReportNumber?id=18-703

Texas State Auditor's Office. (2018). *An Annual Report on Classified Employee Turnover for Fiscal Year 2018.* Retrieved from https://www.sao.texas.gov/SAOReports/ReportNumber?id=19-703

U.S. Bureau of Labor Statistics. (2019, March 29). *Information Security Analysts*. Retrieved from Occupational Employment Statistics: https://www.bls.gov/oes/current/oes151122.htm

U.S. Bureau of Labor Statistics. (2019, April 2). *May 2018 National Occupational Employment and Wage Estimates*. Retrieved from Occupational Employment Statistics: https://www.bls.gov/oes/current/oes_nat.htm

Appendices

Appendix A

Cybersecurity Program Survey

Senate Bill 64 (SB 64), passed by the Texas 86th Legislature, Regular Session, requires the Texas Higher Education Coordinating Board (THECB) to collaborate with Department of Information Resources and consult with institutions to identify and develop strategies to incentivize institutions of higher education to develop degree programs in cybersecurity. Institutions are asked to please answer the following survey questions to help develop strategies and recommendations that will encourage the development of additional degree programs. Please note institutions will not be identified, and data will be aggregated and kept confidential.

1. What prompted your institution to establish a cybersecurity program?
   _____

2. Who were the key individuals (ex. dean, provost, chair, outside stakeholders, etc.) involved in the development of the degree program?
   _____

3. How did you determine there was a need for your degree program?
   _____

4. How did you assess the student demand for your cybersecurity program?
   _____

5. How did you determine the strategic plan for your cybersecurity program? If your program has a mission statement and/or strategic plan, please include it in your response.
   _____

6. How did you articulate the purpose and goals of your cybersecurity program to potential students?
   _____

7. How did you develop the curriculum for your cybersecurity program?
   _____

8. How did you secure the finances to run your cybersecurity program?
   _____

9. What are the areas that your program is currently improving/planning to improve? (Please rank the areas in order from 1 to 5)

▢ Hiring professionals to develop curriculum and teach

- ▢ Meeting requirements for Center for Academic Excellence
- ▢ Building public and/or private partnerships between college and industry
- ▢ Articulating the purpose and goals of the program
- ▢ Securing funding to run the program
- ▢ Recruiting students
- ▢ Enhancing ranking/reputation of the program
- ▢ Providing/Upgrading facilities
- ▢ Increasing affordability
- ▢ Promoting equity and access
- ▢ Other _____

10. What could the State of Texas (Texas Legislature/Texas Higher Education Coordinating Board/Department of Information Resources) do to encourage the development of additional cybersecurity programs in Texas?

11. How might an institution be encouraged to start a cybersecurity degree program?
    _____

Survey for IHEs with No Cybersecurity Program

Senate Bill 64 (SB 64), passed by the Texas 86th Legislature, Regular Session, requires the Texas Higher Education Coordinating Board (THECB) to collaborate with Department of Information Resources and consult with institutions to identify and develop strategies to incentivize institutions of higher education to develop degree programs in cybersecurity. Institutions are asked to please answer the following survey questions to help develop strategies and recommendations that will encourage the development of additional degree programs. Please note institutions will not be identified, and data will be aggregated and kept confidential.

1 Has your institution recently considered offering a degree program in cybersecurity?

o Yes

o No

Display This Question: If Has your institution considered offering a degree program in cybersecurity? = Yes

2-1 Which of the following make starting a cybersecurity program difficult? (Please check all that apply.)

▢ Hiring professionals to develop curriculum and teach

▢ Meeting requirements for Center for Academic Excellence

▢ Establishing public and/or private partnerships between college and industry

▢ Articulating the purpose and goals of the program

▢ Securing funding to start the program

▢ Hiring staff to start the program

▢ Providing/upgrading facilities

▢ Other _____

Display This Question: If Has your institution considered offering a degree program in cybersecurity? = No

2-2 Please tell us why your institution had not considered offering a degree program in cybersecurity.

3 What are some examples of incentives and/or resources your institution may need to start a cybersecurity degree program?

_____

Appendix B

SB 64 Focus Group Questions

1. What motivated your institution to start its cybersecurity program?
    a. List 1-3 motivators (each person in the group, eliminate the same answer responses)

2. What obstacles were encountered in starting the cybersecurity program?
    a. List 1-3 obstacles (each person in the group, eliminate the same answer responses)

3. Does your program have capacity to increase its enrollment?

4. The top three expenses associated with your cybersecurity program are: (circle top three among the group)
    a. Personnel (faculty, program administration, staff)
    b. Student support
    c. Supplies and materials
    d. Library and IT resources
    e. Equipment
    f. Facilities
    g. Other (If other, please specify)

5. What type of internships or experiential learning experiences are available to students and how do they find out about them?

6. What are some incentives/strategies an institution may need to start a cybersecurity program?

7. What else do institutions need to know when they consider starting a cybersecurity degree programs?

Appendix C

Focus Group Final Comments

1. What motivated your institution to start its cybersecurity program?

- Group 1

  - Industry/workforce need
  - Regional need
  - Student demand

- Group 2

  - Workforce request
  - Program advisors
  - Ability to advance

- Group 3

  - Industry interest
  - Legislative interest
  - Student interest when taking related courses in networking

- Group 4

  - Industry demand for employees
  - Social-economic need for cybersecurity (ex. News about attacks, personal attacks)
  - Availability of funding (ex. seed money)

- Group 5

  - Workforce demand
  - Student demand
  - Workforce opportunities

2. What obstacles were encountered in starting the cybersecurity program?

- Group 1

  - Finding qualified faculty/instructors
  - Disconnect in academia – teaching requires masters' degree, but industry doesn't
  - Getting upper administration to support/understand the importance of cybersecurity

- Group 2

  - Qualified faculty
  - Lack of standardized curriculum

- Group 3

  - Hiring
  - Retention of qualified faculty
  - Aligning post-degree certifications with instructional part

- Group 4

  - Curricular challenges – complex field; rapidly changing; different aspects; hard to identify textbooks to match learning outcomes
  - Not a well communicated state vision for cybersecurity – need standardization
  - Articulation agreements/student pathways need to be more clearly defined
  - Funding challenges

- Group 5

  - Programmatic complexity
  - Faculty resources
  - Sustainability (funding and updating to stay current)

3. Does your program have capacity to increase its enrollment?

- Group 1

  - Yes, but depends on qualified faculty

- Group 2

  - Yes

- group 3

  - No, for ongoing programs
  - Yes, for new program, but will have barriers due to limited space and personnel

- Group 4

  - Yes, but may be limited by faculty availability or lab space
  - Programs are steadily growing

- Group 5

  - Yes, with resource constraints on space, faculty, and qualified students

4. The top 3 expenses associated with your cybersecurity program.

- Group 1

  - Equipment (labs, maintenance)

- Personnel
- Securing facilities

- Group 2

- Personnel, faculty, administrative support
- Facility
- Equipment

- Group 3

- Personnel
- Equipment (dedicated labs)
- Facilities

- Group 4

- Equipment (labs, software) – don't always know what lab equipment is needed
- Personnel and training – finding and training faculty
- Student support – books, materials are expensive

- Group 5

- Personnel (especially faculty)
- Equipment
- Facilities

5. What type of internships or experiential learning experiences are available to students and how do they find out about them?

- Group 1

- Internships for two-year schools; let students know by marketing and recruitment

- Group 2

- Provided by board members
- Need more paid internships for working students

- Group 3

- Only 5-10 percent take internship courses
- Well-developed and well managed in industry but concerns regarding age limitation for dual-credit programs and Nondisclosure Agreements and industry recourse if cyberattack

- Group 4

- Individual placements developed by the program director or department chair through focused outreach efforts (time and labor intensive)
- Some paid, some unpaid

- Group 5

- Important for students to build competencies through experience
- Competitions, co-ops, internships
- Found out through personal relationships

6. What are some incentives/strategies an institution may need to start a cybersecurity program?

- Group 1

- Money differential for faculty
- Marketing
- Partnerships with industry
- Incentives for doing internships

- Group 2

- Grant funding for personnel
- Standardized curriculum
- Corporate partnerships
- Cybersecurity competitions to generate interest in the community and prospective students

- Group 3

- Start-up cost is only 25 percent of the whole cost; need to consider funding for faculty salaries to keep competitive
- Need blueprint for ideal cybersecurity program – hard to get instructors to also develop course materials
- Roadmap (high school, associates, and then bachelors)

- Group 4

- Funding
- Clear student pathways
- Curriculum models

- Group 5

- Incentives
  - ✓ Faculty release time
  - ✓ Funding

- ✓ Increased enrollments/completions
- ✓ Incentives

- Strategies
  - ✓ Understand dynamic nature
  - ✓ Build capacity of existing program
  - ✓ Support STEM in K12

7. What else do institutions need to know when they consider starting a cybersecurity degree program?

- Group 1

  - No response

- Group 2

  - Set aside marketing money for students/staff and to promote program availability

- Group 3

  - Do cost study on enrollment and industry interest

- Group 4

  - Difficult to pick a curriculum and books (lots of products out there)
  - Provide training for program director
  - Guided pathways for students
  - Credit for work experience
  - Build industry relationships (for internships and to have an advisory board about how to develop the program to appeal to local/regional employers)

- Group 5

  - Expectations from state
  - It will be a struggle to find faculty
  - No existing blueprint for program

Additional comments:

- <u>Creation of industry advisory council</u>
  - ✓ Combined degree programs and created a Network and Information Security advisory committee – already have these folks in-house and they're already dealing with the issues
- <u>Academic vs practitioner</u>
  - ✓ Getting people in the industry involved in the program before you start is important
  - ✓ Engaging with cybersecurity professionals (across academics and industry) is important

- Proper resources are important
  - ✓ Faculty and administration are stretched; must look at bringing on new roles (ex. Career coaches)
  - ✓ IT is broad and there are a lot of opportunities
  - ✓ Talking to high schoolers also
- Standardizing curriculum
  - ✓ Matching descriptions to NICE

Appendix D

Comprehensive List of all Cybersecurity Certificate, Degree, and Related Programs Offered by Four-Year Public Institutions

Institution Name	Program Name	Degrees Offered	Start Date	Distance Education
Lamar University	Cybersecurity	BS	9/1/2019	No
Sam Houston State University	Cybersecurity	BS, Graduate Cert.	9/1/2020 (BS) 4/20/2017 (G)	No
Sam Houston State University	Digital and Cyber Forensic Science	PHD	4/20/2017	No
Stephen F. Austin State University	Cybersecurity	MS	9/1/2017	No
Texas A&M University - San Antonio	Cyber Engineering Technology	BS	8/22/2019	No
Texas Tech University	Cybersecurity for Critical Infrastructure	Undergraduate and Graduate Cert.	11/14/2014 (UG) 11/14/2014 (G)	No
The University of Texas at Dallas	Cybersecurity, Technology and Policy	MS	8/17/2020	No
The University of Texas at San Antonio	Cybersecurity	BBA	9/1/2003	Yes
University of Houston -Downtown	Cybersecurity	Graduate Cert.	8/15/2016	No
University of Houston	Cybersecurity	MS	10/4/2002	No
University of North Texas	Cybersecurity	BS, MS	8/15/2020	No

Related Programs

Institution Name	Program Name	Degree Offered	Start Date	Distance Education
West Texas A&M University	Computer Information Systems	MS	9/1/2017	Yes
Sam Houston State University	Data Assurance Digital Investigation	Graduate Cert. Graduate Cert.	1/8/2010 1/8/2010	No
Sam Houston State University	Digital Forensics	MS	6/1/2006	No
Sam Houston State University	Information Assurance and Security	MS	9/1/2008	Yes
The University of Texas at Austin	Information and Security and Privacy	MS	9/1/2015	No

Current Proposals for Cybersecurity Programs Under Review (Not Approved)

Institution Name	Program Name	Degrees Offered	Start Date	Distance Education
The University of Texas at San Antonio	Cybersecurity Science	MS	TBD	No

Appendix E

Comprehensive List of all Cybersecurity Certificate and Degree Programs Offered by Two-Year Public Institutions

Institution Name	Program Name	Degrees Offered	Start Date
Alamo Community College District - NW Vista College	Information Assurance and Cyber Security	Certificate, AAS	1/1/2003
Alamo Community College District - Palo Alto College	Information Assurance & Cybersecurity	Certificate, AAS	6/1/2010
Alamo Community College District - San Antonio College	Information Assurance and Cybersecurity	Certificate, AAS	9/1/2009
Alamo Community College District - St. Philip's College	Information Technology Cybersecurity Specialist	Certificate, AAS	9/1/2004
Alvin Community College	Cybersecurity	Certificate, AAS	6/1/2020
Amarillo College	Computer Networking/Cyber-Security, Computer Cyber Security	Certificate, AAS	9/1/2015
Austin Community College	Local Area Network Systems - Cyber Security Specialization	AAS	9/1/2018
Blinn College District	Cybersecurity	AAS	9/1/2020
Central Texas College	Cybersecurity, Cyberdefense - Information Assurance	Certificate	6/1/2020
Coastal Bend College	Computer Information Technician Networking/Cybersecurity Specialization	Certificate	9/1/2010
College of the Mainland Community College District	Information Technology - Cybersecurity	Certificate, AAS	9/1/2020
Collin County Community College District	Information Systems Cybersecurity Specialization	Certificate, AAS	9/1/2004

Comprehensive List of all Cybersecurity Certificate and Degree Program Offered by Two-Year Public Institutions, Con't.

Institution Name	Program Name	Degrees Offered	Start Date
Dallas County Community College District	Cyber Security Analyst Administrator, Cybersecurity	Certificate, AAS	9/1/2018 (C) 9/1/2017 (AAS)
El Paso County Community College District	Cybersecurity	AAS	9/1/2002
Galveston College	Computer Networking/Cyber-Security Technology, Entry-level and Advanced	Certificate	9/1/2010
Grayson County College	Cyber Security Technician, Cyber Security Administration	Certificate, AAS	9/1/2017
Hill College	Networking and Cybersecurity	Certificate, AAS	9/1/2018
Houston Community College System	Computer Systems Networking - Cybersecurity, Cyber Security Specialization	Certificate, AAS	6/1/2015
Kilgore College	Cybersecurity	Certificate	9/1/2015
Lamar Institute of Technology	Cyber Defense Technology Cyber Security Technology	Certificate, AAS	9/1/2018
Lamar State College - Orange	CISCO Networking Cybersecurity Technician, Cybersecurity Specialist	Certificate	9/1/2016 9/1/2017
Laredo College	Computer Information Systems Network and Cyber Security Technology	AAS	9/1/2015
Lone Star College - CyFair	Cybersecurity	AAS	9/1/2017
McLennan Community College	CISCO Network Administration with Cybersecurity, Network Administration with Cybersecurity	Certificate, AAS	6/1/2019
Navarro College	Cybersecurity, Cybersecurity and Visualization	Certificate, AAS	9/1/2014 (C) 6/1/2015 (AAS)
Paris Junior College	Cybersecurity	Certificate, AAS	9/1/2019
San Jacinto College District - South Campus	Information Technology Cyber Security Specialty(Cert/AAS), Adv. Information Technology Cyber Security Specialty	Certificate, AAS	9/1/2020

Comprehensive List of all Cybersecurity Certificate and Degree Program Offered by Two-Year Public Institutions, Con't.

Institution Name	Program Name	Degrees Offered	Start Date
South Plains College	Cybersecurity	Certificate	9/1/2015
South Texas College	Cybersecurity Specialist, Cybersecurity/Digital Forensics Specialist, Business Computer Systems - Specialization in Cybersecurity Specialist (AAS)	Certificate, AAS	9/1/2017
Tarrant County College - Connect Campus	Information Technology: Cybersecurity	AAS	9/1/2018
Tarrant County College - Northeast Campus	Cybersecurity Specialist Information Technology: Cybersecurity	Certificate, AAS	9/1/2018
Tarrant County College - Northwest Campus	Cybersecurity Specialist Information Technology: Cybersecurity	Certificate, AAS	9/1/2018
Tarrant County College - South Campus	Cybersecurity Specialist Information Technology: Cybersecurity	Certificate, AAS	9/1/2018
Tarrant County College - Southeast Campus	Cybersecurity Specialist Information Technology: Cybersecurity	Certificate, AAS	9/1/2018
Tarrant County College - Trinity River Campus	Cybersecurity Specialist Information Technology: Cybersecurity	Certificate, AAS	9/1/2018
Texas State Technical College - Marshall	Cybersecurity	Certificate, AAS	6/1/2012
Trinity Valley Community College	Cybersecurity	Certificate, AAS	1/1/2020

Appendix F

New Cybersecurity WECM Courses

Course	CIP Code	Title	Year
ITSY 1x00	11.1003	Fundamentals of Information Security	2019
ITSY 1x42	11.1003	Information Technology Security	2019
ITSY 2x00	11.1003	Operating System Security	2016
ITSY 2x01	11.1003	Firewalls and Network Security	2016
ITSY 2x17	11.1003	Wireless Security Development	2016
ITSY 2x30	11.1003	Intrusion Detection	2016
ITSY 2x41	11.1003	Security Management Practices	2016
ITSY 2x42	11.1003	Incident Response and Handling	2016
ITSY 2x43	11.1003	Computer System Forensics	2016
ITSY 2x45	11.1003	Network Defense and Countermeasures	2016
ITSY 2x59	11.1003	Security Assessment and Auditing	2016

Appendix G

Cloud Support and Cybersecurity Program of Study

The Program of Study Curriculum of Cloud Support and Cybersecurity shall consist of no more than 45 identified semester credit hours that transfer and apply when students move from one institution to another and continue in a similar program. Students transferring from one institution to another should be granted credit on the basis of comparable courses completed, not on the specific numbers of credit hours accrued.

Cloud Support and Cybersecurity Program of Study Curriculum

Course Title	*Course #*	*SCH*
Introduction to Computer Technology	CPMT 1303/1403	3-4
(or Introduction to Computers)	(ITSC 1301/1401)	3-4
Introduction to Database	ITSW 1307/1407	3-4
(or Introduction to MySQL)	(ITSE 1303)	3-4
Implementing & Supporting Client Operating Systems	ITNW 1308/1408	3-4
Introduction to Scripting Languages	ITSE 1359	3-4
Programming Logic & Design	ITSE 1329/1429	3-4
Fundamentals of Networking Technologies	ITNW 1325/1425	3-4
(or CCNA 1 Introduction to Networks)	(ITCC 1314/1414)	3-4
Fundamentals of Cloud Computing	ITNW 1309/1409	3-4
Cloud Deployment & Infrastructure Management	ITNW 1336/1436	3-4
Advanced Cloud Concepts	ITNW 2327/2427	3-4
Linux Installation & Configuration	ITSC 1316/1416	3-4
Implementing and Supporting Servers	ITNW 1354/1454	3-4
Information Technology Security	ITSY 1342/1442	3-4
Project Management Software	ITSC 1315/1415	3-4

SUBTOTAL: Discipline Courses	**39-45**
General Education Courses	**15**
Specialty Elective Technical Courses**	**0-6**
(Colleges may select additional courses to complete a maximum of 60 SCH)	
TOTAL (MAX 60 with 15 SCH General Education)	**60**

** Recommended Technical Electives
ITSC 2325 Advanced Linux
ITNW 2329 Application Development for the Cloud
Approved by THECB Board January 23, 2020

60x30TX
Texas Higher Education Coordinating Board

This document is available on the Texas Higher Education Coordinating Board website.

For more information contact:

Dr. Audra Patridge
Academic Quality and Workforce
Texas Higher Education Coordinating Board
P.O. Box 12788
Austin, TX 78711
PHONE 512-427-6232
FAX 512-427-6168
Audra.Patridge@highered.texas.gov