Evaluation of the Trade Adjustment Assistance Community College and Career Training

WAYNE COUNTY COMMUNITY COLLEGE DISTRICT'S "GENERATION CYBER"

SUBMITTED TO

WAYNE COUNTY COMMUNITY COLLEGE DISTRICT
Dr. James Robinson, Project Director

PREPARED BY

ICF
Dr. Astrid Hendricks, Dr. Miriam Jacobson,
Dr. Yvette Lamb, Lead Project Directors

September 26, 2018

Acknowledgments

The authors gratefully acknowledge the help of many individuals who contributed to this report including Dr. James Robinson, Project Director of Wayne County Community College District's Generation Cyber, Dr. Shawna Forbes , Wayne County Community College District Vice Chancellor for Continuing Education and Workforce Development, and Ms. Mary Ann Troy, Generation Cyber Recruitment and Placement Specialist. Substantive technology information was provided by Dell, VMware, Ixia, TestOut, Mavi Interactive, and the Midwest Colloquium for Information System Education.

At ICF, staff contributing to the report include Dr. Miriam Jacobson, Dr. Astrid Hendricks, Dr. Yvette Lamb, Andreea Mitran, Bryana Carroll, and Gabi Kirsch. A special thanks to Nanette Antwi-Donkor, Dr. Kathy Karageorge, and Nicole Wright for their leadership and contributions to this project.

This evaluation was funded by the U.S. Department of Labor's Employment and Training Administration, Trade Adjustment Act Community College Training (TAACCCT) program.

TABLE OF CONTENTS

"…whatever the sphere in which the data are being collected, we can understand events only when they are situated in the wider social and historical context."

– A. Bryman, *Quantity and Quality in Social Research*

PREFACE

Between 2014 and 2018 Wayne County Community College District (WCCCD) developed a cybersecurity training program, Generation Cyber, using funding from the U.S. Department of Labor's Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant program. The goal of Generation Cyber was to help train today's workforce in industry-recognized skills and hands-on experience that help lead individuals and families to self-sufficiency. The program aimed to target trade-affected workers, other dislocated workers, and unemployed veterans in Wayne County, Michigan. WCCCD's Generation Cyber was incubated in a very dynamic and rapidly changing technology and cybersecurity environment. Some would describe these dynamics as "flux and transformation."[1] To fully grasp the impact of the change that transpired during this period, it is critical to understand the context and environment in which technology and cybersecurity unfolded and developed as WCCCD's Generation Cyber program was implemented and to situate the program in a wider social and historical context.

This Preface provides that context and is intended to support understanding the findings of the evaluation. The Preface describes perspectives from national and regional contexts for historical purposes and explores the perspectives of staff involved throughout the development of Generation Cyber. Finally the Preface provides the perspectives of technology partners involved in the development of the cybersecurity laboratories on the WCCCD campus--a significant infrastructure resource critical to the success of a training and certification program.

Sources of information for the Preface include a review of current literature on cybersecurity, training, and certification; a review of public and private research documents published between 2011 and 2018; and most importantly, interviews with partners/vendors involved with the creation of the Generation Cyber learning laboratory and Cyber environment and key Generation Cyber project staff from WCCCD.

The National and State Contexts

Almost every week in the news, Americans hear about another cybersecurity attack. In 2017, it appeared as if no information was safe from hackers, from personal information hacks (e.g., Equifax) to hacks of government intel (e.g., Wikileaks).

[1] "Flux and transformation" is a metaphor used by Gareth Morgan to describe how organizations or phenomena evolve in order to address chaos and complexity.

Cybersecurity is an issue that affects almost every person, company, and governmental organization in the United States, and more and more resources are being poured into the protection of these entities. A report from Cybersecurity Ventures revealed that the cost of global cybersecurity will exceed one trillion dollars between the years 2017 to 2021.[2] In 2011, the Executive Office and the National Science and Technology Council (NSTC) released a report, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, which aimed to prioritize and understand the needs and importance of cybersecurity capabilities.[3]

National Demand for Cybersecurity Workforce

With cyberattacks on the rise, employers across the United States have expressed the need for a larger cybersecurity workforce. The demand for frontline workers[4] in cybersecurity increased by almost 170 percent from 2010-2016, despite a slight dip from 2014-2016.[5] By 2022, it is estimated that 1.8 million more people will need to be trained to meet the shortage of cybersecurity professionals across the globe.[6]

According to Cyberseek, from April 2017 to March 2018, there were 301,873 online job listings for cybersecurity-related positions. The top cybersecurity job titles included Cybersecurity Engineer, Cybersecurity Analyst, Network Engineer/Architect, and Cybersecurity Manager, among others.[7] Frontline cybersecurity workers such as these, which make up over 76 percent of cybersecurity-related postings, earn an average salary double the national median hourly wage ($40.09 compared to $21.60).[8]

NATIONAL FAST FACTS

1.8 million more individuals will be needed in the cybersecurity workforce by 2022

64% of cybersecurity job openings require a bachelors degree

41% of cybersecurity openings are not in professional services

Defining Cybersecurity Professions

Multiple national initiatives have arisen from the need for a larger cybersecurity workforce, including the National Initiative for Cybersecurity Education (NICE), which is led by the National Institute of Standards and Technology (NIST), as a partnership between the government, private sector, and educational institutions to increase the number of cybersecurity professionals working to protect the United States from cyberattacks.

Before the inception of NICE, US government departments and agencies gathered to create a framework that aims to distinguish categories of cybersecurity and related work. It is comprised of seven categories (see Exhibit A), 33 specialty areas,

[2] Morgan, S. (2017). *2018 cybersecurity market report*. Cybersecurity Ventures. Retrieved from https://cybersecurityventures.com/cybersecurity-market-report/

[3] National Science and Technology Council (NSTC). (2011). *Trustworthy cyberspace: Strategic plan for the Federal Cybersecurity Research and Development Program*. Report prepared by the National Science and Technology Council, Executive Office of the President. Retrieved from https://www.nitrd.gov/pubs/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

[4] Frontline workers refers to individuals directly working on technical design and cybersecurity strategies.

[5] Workforce Intelligence Network. (2017). *Cybersecurity skills gap analysis: National and Advance Michigan region data.* Retrieved from https://winintelligence.org/report/cybersecurity-report/

[6] National Institute of Standards and Technology. (2017). *Cybersecurity workforce demand.* Retrieved from https://www.nist.gov/sites/default/files/documents/2017/11/16/workforce_demand_111617_final.pdf

[7] Cyberseek. (2018). *Cybersecurity supply/demand heat map.* Retrieved from https://www.cyberseek.org/heatmap.html

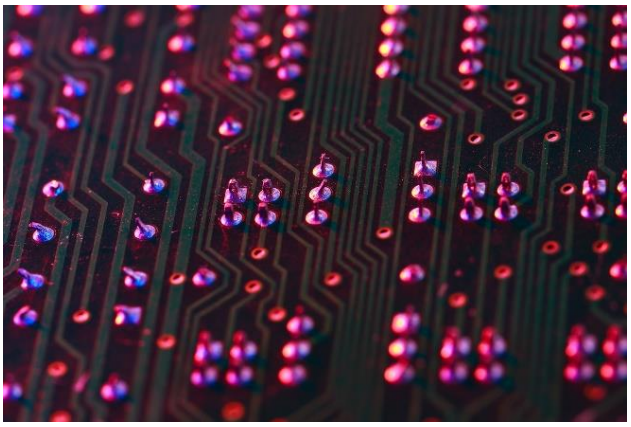
[8] Workforce Intelligence Network. (2017). *Cybersecurity skills gap analysis: National and Advance Michigan region data.* Retrieved from https://winintelligence.org/report/cybersecurity-report/

and 52 work roles to provide the public, private, and academic sectors with a better understanding of the cybersecurity field and where the work is done.[9] This common lexicon was developed to keep job descriptions and curriculums consistent across recruiters, employers, and academic institutions.

Exhibit A: Categories of Cybersecurity and Related Work Functions

The Value of Certifications

The cybersecurity industry has come to recognize the importance of credentialing and certification for "new collar" technology jobs. Traditionally, the majority of cybersecurity job openings nationally require a bachelor's degree and employers have valued bachelor's degrees with traditional, theoretical backgrounds typically provided in four-year academic STEM programs over two-year degrees or certificate programs. IBM is one company that has recognized the significant skills gap and workforce shortage and has addressed this by creating "new collar" jobs, which prioritize skills and ability over higher degrees.[10] Since they started this approach, more than 20 perecent of their US hiring has been of "new collar" professionals. Moreover, in a 2017 survey of IT professionals, 55 percent reported practical/hands-on experience was the most important attribute of a qualified applicant.[11] Certification programs and two-year degrees can be valuable to employers because they can provide students with hands-on experience and tailored assessments. Certifications specifically provide continued learning opportunities through renewals and provide a consistent measure of knowledge, skills, and abilities across the country.



Community College Training

Community Colleges are at the forefront of preparing diverse pools of people for the needs of the workforce. The U.S. Department of Labor Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant program was designed to help community colleges build workforce capacity for today's industry demands as well as build the capacity of Community Colleges to have the necessary infrastructure for training. Every U.S. state received funding for over four years and, as a result, established over 2,600 programs which aimed to train

[9] National Institute of Standards and Technology. (2017). *NICE cybersecurity workforce framework.* Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

[10] Van Zadelhoff, M. (2017). *Cybersecurity has a serious talent shortage. Here's how to fix it.* Retrieved from https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

[11] ISACA. (2017). *State of cybersecurity 2017: Workforce trends and challenges.* Retrieved from https://www.isaca.org/cyber/Documents/State-of-Cybersecurity-infographic_res_eng_0217.pdf

workers eligible under the Trade Adjustment Assistance (TAA) for Workers program.[12] One program to emerge from the TAACCCT grants, was WCCCD's Generation Cyber in Detroit, Michigan.

Recommendation 1.5 (Presidential Report, 5/11/2017, p9) The Federal government should launch a vigorous effort to recruit cybersecurity workers from large and diverse pools of candidates who are underutilized or underrepresented in the cybersecurity workforce. This includes veterans, women and minorities.

There are eight TAACCCT grantees, including WCCCD, that focused on implementing cybersecurity and emerging technologies training programs, totaling $75 million nationwide (about 4% of the $1.9 billion TAACCCT allocation). TAACCCT cybersecurity programs have been launched in Maryland, Hawaii, Massachusetts, Michigan, Missouri, and Virginia. Each of these career pathway programs are job-driven and most include training partnerships in their communities.

TAACCCT training programs are generally free to individuals who qualify, including low-income individuals, underemployed or unemployed adults, trade-affected workers, dislocated workers, and unemployed veterans. Cybersecurity programs vary in focus but primarily provide participants with hands-on training and entry-level and stackable certifications. In some instances, internships, career planning, and job placement support are also provided.

State Demand for a Cybersecurity Workforce

Not only is the demand for a robust cybersecurity workforce a national priority, individual states are undertaking aggressive strategies to create a workforce able to fill needed jobs. Michigan Governor Rick Snyder launched the Michigan Cyber Initiative in 2011 to place cybersecurity as a central issue in Michigan's priorities, raising awareness and implementing creative solutions. The report titled, *Leading the Nation: An interagency, public-private collaboration (2015),* outlines state priorities in cybersecurity. Similar to other states, the demand for cybersecurity professionals is higher than the number of those qualified and looking for employment. Between July 2015 and June 2016, according to the Workforce Intelligence Network (WIN) report, *Cybersecurity Skills Gap Analysis: National and Advance Michigan Regional Data (2017),* there were 6,789 cybersecurity-related job postings in the state of Michigan. The majority of these job posts were for frontline cybersecurity workers, those that work directly with the design and implementation of cybersecurity strategies. These are the people who work with security platforms, address virtual threats, and develop programming related to security. Other occupational categories with fewer job postings (although not insubstantial) were: cyber-sensitive service workers, physical security and access workers, and indirect cyber-related workers.

In Michigan, top employers for these frontline cybersecurity jobs are within the auto, finance, defense, media, university, and health industries. As Detroit is commonly called the Motor City, the big auto companies are among the employers looking to hire the most cybersecurity professionals in the region: particularly, General Motors, Ford Motor Company, and Fiat Chrysler Automobiles. As vehicles continue to become more technologically advanced, the need for a trained cybersecurity workforce will increase so that these companies can ensure that consumers are able to execute the technology without interference. Beyond the auto industry, healthcare organizations like Blue Cross Blue Shield of Michigan, Ascension-Healthcare, and Henry Ford Health System are also main employers

[12] Employment and Training Administration, United States Department of Labor. (2011). *Trade Adjustment Assistance Community College and Career Training grant program: Program summary*. Retrieved from https://doleta.gov/taaccct/

of cybersecurity professionals as protecting confidential patient information continues to be a necessity. These cybersecurity positions require individuals to have the knowledge and skills, and specific certifications to prove competency including certifications in CompTIA Network+, CompTIA Security+, Certified Ethical Hacker, Cisco Certified Network Associate, and Certified Authorization Professional.

As of June 2017, training for cybersecurity positions were available at multiple community colleges in Southeast Michigan. In addition to the Wayne County Generation Cyber training, Washtenaw Community College, located in Ann Arbor, Michigan, offers the same number of certifications. They also partner with Eastern Michigan University to allow students who complete the associate degree to transition seamlessly into a 4-year degree program. Other community colleges offer cybersecurity related certifications including Henry Ford College, Oakland Community College, and Schoolcraft College.

While the availability of certifications at these providers is important, certifications in cybersecurity are only one part of the conversation about how to qualify for cybersecurity jobs. Eighty-six percent of the job postings in Michigan that mention a desired level of educational attainment specified they wanted a bachelor's degree. Just as many job posts (83%) require applicants to have at least three years of experience. From a national perspective, only 11 percent of posts are open to applicants with a high school degree only or vocational training.

While these community colleges in Michigan offer certifications, WCCCD is the only community college that boasts a cyber environment for students to use to improve their skills through additional training within their training course time. If students at these other programs want to experience training through a cyber environment, they would have to access it through other means, for example the Merit Network,[13] which provides this opportunity at a few different locations in Southeast Michigan. While many Michigan universities sit on the board of Merit Network, a Merit Network representative explained that the cyber environment is not a common tool used in university curriculums and that schools must set up a practicum with Merit Network in order to use their services.

Many universities in Southeast Michigan offer 4-year bachelor's degree programs in computer and information science, which provide some training within cybersecurity. In 2015, the University of Michigan awarded 344 bachelor's degrees in cybersecurity. In addition, Michigan State University awarded 135, and Wayne State University awarded 132. While these universities in total educate a large number of students with the knowledges and skills that could be relevant to careers in cybersecurity, these numbers do not reflect the total number of students going into cybersecurity from these institutions. Further, creating a robust cybersecurity workforce requires not only job-related education, but also credentials, hands-on practice ,and experiences deriving from identifying a diverse workforce. The WCCCD Generation Cyber story that follows provides insight into what is needed to support the development of a robust cybersecurity workforce.

[13] The Merit Network is a nonprofit organization that is governed by Michigan's 12 public universities: Central Michigan University, Eastern Michigan University, Ferris State University, Grand Valley University, Lake Superior State University, Michigan State University, Michigan Technological University, Northern Michigan University, Oakland University, University of Michigan, Wayne State University, and Western Michigan University. While Merit Network offers a variety of services to Michigan organizations, they also offer 17 cybersecurity certification opportunities and the Michigan Cyber Range. The certifications and the cyber range offered by Merit are hosted at Pinckney High School, Velocity Hub & Cyber Institute in Sterling Heights, and Wayne State University ATEC in Warren. Merit Network created the Michigan Cyber Range in partnership with the State of Michigan.

The WCCCD Generation Cyber Story

In the following portions of the Preface, we examine the context surrounding the implementation of Generation Cyber from two perspectives—the experience of WCCCD project staff as they developed and put into action Generation Cyber and the experience of WCCCD's technical partners who developed the cyber training infrastructure needed to carry out training.

The push at the national and state levels for highly effective training programs that result in a robust cybersecurity workforce was launched with processes, beginning in 2010-2011, to understand what skills and knowledge would be needed for cybersecurity jobs. Although not yet fully realized at the inception of the WCCCD Generation Cyber program, the beginnings of a clearly defined cybersecurity career pathway would be the intended goal. Simultaneously, Detroit was pursuing a path of rebuilding and revitalizing local industry—manufacturing, health care, finance—that required both robust technology and strong cybersecurity to protect it. WCCCD joined others in addressing the gaps in capacity.

The Internal WCCCD Context

For Wayne County Community College District (WCCCD), the push at the national, state, and local levels has provided an opportunity to develop a solution to fit both the national and state need and to address local demand. The U.S. Department of Homeland Security, for example, has identified the nation's community colleges as the optimal setting to respond to the critical need for a cybersecurity workforce that is theory-based yet more importantly, practice/hands on ready. Community colleges have historically been quick to respond and accustomed to preparing students for workforce and employer needs. In fact, WCCCD senior staff describe the primary objective of community colleges as "preparing [students] for the workforce."

Having reviewed data surrounding cybersecurity jobs in Southeast Michigan, WCCCD was well aware that the jobs were defined but the skill set needed to carry out the jobs was not evident. Their perspective was that people were being prepared with master's degrees—they could identify a cyber threat—but not practiced in stopping a threat. The opportunity to develop the proper blend of theory and hands-on, "stick time" was central to WCCCD's academic mission. It also aligned with WCCCD's mission to prepare the workforce for those jobs that are needed by their area employers.

> "Our responsiveness to our employers is always at the forefront. That's the crux of who we are. We are here to be responsive, to create the workforce that is needed in a short period of time through a boot camp model or a semester model. Community colleges are absolutely capable of preparing the [cybersecurity] workforce." – WCCCD Staff

In order to take advantage of this opportunity to create a cybersecurity training program, WCCCD would need to develop a curriculum, hire and train faculty, create a cybersecurity training platform, and develop certification processes—at the same time keeping a rate structure that is cost efficient. To accomplish all of this, a funding source would need to be identified.

Building Generation Cyber

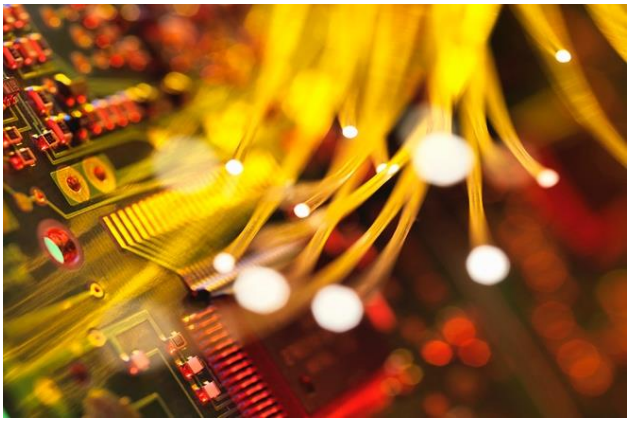
The Trade Adjustment Assistance Community College and Career Training (TAACCCT) program funded by the U.S. Department of Labor seemed tailored to the needs of WCCCD to launch a cybersecurity training program and provide the resources for capacity building for infrastructure and curriculum development. The funding program provided resources to build the technology for learning laboratories and computer labs and to create a cybersecurity curriculum for students. It targeted Trade Adjustment Assistance (TAA) workers who had real world work experience and were in need of retraining for current employment opportunities.

With labor market information and job reports from industry-related resources indicating that there were vast job openings for cybersecurity in the Detroit and Southeast Michigan areas and with excitement building around Detroit as a "comeback" city, WCCCD brought together a partnership to submit and ultimately win TAACCCT funding. They named the project "Generation Cyber" noting that "this generation is all about technology—our young people are very much connected to the world of cyberspace—it was so very new—it was a play on the younger generation and their love of technology—they were born into technology".

Once they secured TAACCCT funding, they proceeded to build Generation Cyber layer by layer. They created an official Advisory Council that actively contributed to the implementation of the TAACCCT grant. The members of the Advisory Council were representatives of the industries WCCCD thought would be ready to hire their cyber students. They targeted representatives from manufacturing, healthcare, IT companies, and the banking and financial sectors. In addition to industry, they included senior WCCCD administrative staff, WCCCD IT staff, representatives from state and federal agencies (NIST, Michigan Merit Computer Network, and CyberWatch to name a few), local political leadership, and other community colleges and baccalaureate granting institutions. The Advisory Council, from WCCCDs perspective, represented the best people to inform what was going on currently and would be able to inform WCCCD about trends and changes in the cybersecurity field.

While the federal government has pushed cybersecurity as an issue of importance, WCCCD's Generation Cyber program also responds to state priorities of increasing the number of highly skilled workers to fit the demands of gaps in the workforce. Understanding which employers hire cybersecurity professionals helps paint the picture of what jobs WCCCD would be positioning students to apply for in Generation Cyber.

WCCCD secured critical technology partners who built the technology learning platform for Generation Cyber (see details in the next section on external context). In addition to the technology learning infrastructure, TAACCCT funding supported the renovation of space on two WCCCD campuses for learning laboratories at their downtown and western campuses. The TAACCCT funding was different from other federal programs, allowing the opportunity to "build out dedicated space for the program that required a huge renovation plan and processes at two campuses… [it's] not often that we get to do a full build out." However, the process of following Department of Labor guidelines and securing proper Department of Labor permissions was slow to come to resolution resulting in delays of approximately one year before actual renovation work began on the learning laboratories.



Curriculum and Training

Efforts during the first year also involved creating the curriculum and training aspects of Generation Cyber, grounding the process in the critical knowledge, skills and practice that were expected at national (NIST/NICE) and state levels.

Generation Cyber was initially developed as a credit bearing program resulting in an associate degree that trained TAA workers in five cybersecurity programs in combination with other training that would result in the associate degree. It was structured as a competency based design (see

evaluation report for added detail). Students would take three to four electives related to technology over a 15-week time period. They would learn from real world instructors—people who worked in the industry—and be supported by those instructors. In the learning labs located in the downtown and western campuses, a wide range of state of the art technology was made available to students. These included virtual networks, VMware, simulations, and access to third party certifications (i.e., TestOut) that students would be able to sit for without the high cost of using other certifying bodies. WCCCD aimed to infuse game-based learning into Generation Cyber to provide critical hands-on experiences for their participants.

The curriculum followed the guidelines and standards of the WCCCD curriculum committee, adhering to the same rigor as other credit bearing curricula across the community college district. This process reinforced the vision of Generation Cyber to be a rigorous program that wasn't for everyone.

Over time, due to changing participant demographics, including TAA designated workers, incumbent workers and WCCCD IT students, Generation Cyber expanded to become a one-year certificate program providing a short-term certificate if students passed three classes and successfully sat for a third party certification using the TestOut platform.

Certifications and Credentials

Certifications and credentials are very important in the cybersecurity field. WCCCD's Generation Cyber focused on the "Securely Provision" and "Operate and Maintain" categories of cyber training (see Exhibit A) which tended to have the largest number of job opening at the state and national levels at the time. "Securely provision" refers to jobs focusing on the conceptualization, design, and building of a secure information technology (IT) system. "Operate and maintain" refers to occupations that support, administer, and maintain IT systems' performance and security. They offered students the ability to gain certifications in CompTIA Network+, Certified Ethical Hacker, Cisco Certified Network Associate, and Certified Authorization Professional, providing students with the opportunity to gain some foundational qualifications to enter the workforce as a cybersecurity professional.

"The certifications are relevant because the industry is constantly changing. It demonstrates their (i.e., Generation Cyber participants) ability to learn. Employers want people who are trainable, so when you have the discipline to go through a structured program and then test out of that program and earn a certificate, it tells the employer you're trainable and current. The credentials are important to employers for employability." – WCCCD Partner

Practice through Cloud Computing, Game-based Learning, and Virtual Desktops

The technology that WCCCD put in place is considered the "top of the line," consisting of simulations, game-based learning, and opportunities for participants/students to share desktops to compete with and learn from one another. One contractor developed malware—"the bad stuff"—to provide hands-on practice in detecting and stopping viruses and other harmful agents that might constitute a cyberattack. The vision was that participants/students would form weekend groups to practice using all of the technology available to them in the cyber labs. In reality, there wasn't sufficient time in the grant and the curriculum for the full potential of these technology features to be fully utilized. Going forward, however, it is anticipated that future cybersecurity trainees will benefit from all of the technology developed for Generation Cyber.

Building Staff Capacity through Training and Credentials

To support the curriculum and training infrastructure, the TAACCCT grant provided resources for WCCCD to be able to train faculty in cybersecurity. For Generation Cyber, two to three faculty with the

appropriate skill set were needed to teach the curriculum. WCCCD initially did not have faculty with cybersecurity credentials to be able to take on the load of teaching the cybersecurity program. Faculty training was a major component of the capacity building undertaken through the TAACCCT grant. Faculty training continued throughout the implementation of Generation Cyber in order to meet the teaching and training demands of the program as well as to respond to faculty attrition. They offered faculty training through a contract with one of their Advisory Council partners—the Center for Cybersecurity and Intelligence Studies (CCSIS). The Generation Cyber training was not the easiest curriculum to teach. Faculty not only had to master the content of the curriculum but they also needed to be able to navigate the labs. It is a rigorous program, but faculty who successfully completed and passed the credentialing exams were effective in delivering the training.

The Pipeline and Recruitment

WCCCD was challenged throughout the implementation of Generation Cyber to identify a strong pipeline from which to recruit and select participants. Generation Cyber participants were initially recruited from the key target audience of TAA workers in need of immediate jobs. However, the recruitment process surfaced a key marketing issue—not many TAA workers knew what cybersecurity was and they wanted training for quick turnaround jobs, not in jobs requiring longer term certifications and credentials.

> "If you said to someone, are you interested in the [cybersecurity] field? There's no specific picture to give someone that says this is what you'll be doing in the field of cybersecurity." – WCCCD Staff

WCCCD shifted to the recruitment of incumbent workers which had limited success but did not provide a sufficiently large or steady stream of potential participants. WCCCD shifted again towards the recruitment of students that were already accepted in WCCCD IT programs, focusing efforts on anyone that was interested in IT, gaming, and the types of critical skills that would be used in cybersecurity training.

The pipeline and recruitment issues were a persistent challenge for Generation Cyber throughout implementation. Adding to the challenge was the nature of the cybersecurity field and its career pathways that were broad and undefined during the Generation Cyber implementation process. As one staff member indicated, "it became more apparent that the changes in the industry and in working with recruiting students, this program [Generation Cyber] required daily research as to what was going on in the industry both at a national and certainly at a local level in southeast Michigan." This challenge was perceived to have an impact not only on creating a strong pipeline for Generation Cyber, but also for placing participants completing the program in the entry-level "new collar" jobs that employers were seeking to fill.

Engaging Employers

Recruitment, training, and providing hands-on practice with the credentialing process were all meant to lead to the final step of placement of Generation Cyber participants into an entry-level cyber position in the Detroit area. WCCCD used its network of the Generation Cyber Advisory Council to engage employers in the targeted areas they were training participants—manufacturing, healthcare, and finance/business—to help find cyber jobs for its credentialed completers. What they encountered was a critical misalignment between employer job needs and the cybersecurity job specifications used for hiring purposes.

> "The cybersecurity industry wasn't conducive to entry-level positions. Very few positions allowed for an associate degree…You need a bachelor's degree, certifications plus two years of experience." – WCCCD Partner

From WCCCD's perspective, their program was designed based on labor information available at the outset of the program which guided the kind of curriculum and certifications they offered. However, between the time they wrote the curriculum and were approved to implement it, the industry had a shift in what they defined as entry-level credentials. This was further exacerbated by decades of escalating digital sabotage with words like "hacking", "viruses", and "phishing" becoming common ways to describe the sabotage. The cybersecurity field was continuously evolving, experiencing "flux and transformation" that affected what constituted job specifications for hiring purposes.

WCCCD realized that engaging employers around a continuously changing cybersecurity environment was challenging and having an impact on their ability to place Generation Cyber graduates into jobs. On the demand side, employers needed to better understand what jobs were actually needed and what constitutes a cybersecurity job versus other information technology positions. Further, employers needed to address what human resources (HR) processes were needed to employ and onboard cybersecurity positions, particularly in much needed entry-level positions. To address this knowledge gap, WCCCD undertook a process to educate its employers by creating a cybersecurity awareness and training program using some of the assets of Generation Cyber. It was called "foundational" training and provided employers and their HR staff with an understanding of the changing landscape of cybersecurity and the type of training that Generation Cyber provides for participants.

On the supply side, with their Generation Cyber students, there was a need to push them to go beyond the preparatory credentialing processes that was part of the Generation Cyber training. Generation Cyber provided extensive preparatory training on the major credentials accepted for cybersecurity positions through the TestOut platform. However, students would still need to "sit" for certification by third party standardized cybersecurity certifying bodies. While students would incur additional costs to take these third party certifications, they were the only ones that employers and government acknowledge as professional certification.

A significant learning about employee engagement from the perspective of Generation Cyber staff and partners was the importance of having HR representatives as part of the Advisory Council. An HR Department's understanding of the difference between cybersecurity and IT, as well as having HR involved in the design of entry-level specifications for cybersecurity positions, are important to successful placement. Generation Cyber staff and Advisory Council members often referred to a need to address the "misalignment" between HR standards for hiring IT positions versus developing processes for entry-level cybersecurity positions. Understanding the value of an associate degree, various certifications, and levels of experience are perceived to be the direction needed to correct the misalignment.

External Partnerships Create Needed Technology Infrastructure

A shared vision and mission is a crucial part of a partnership. As a TAACCCT grantee, WCCCD's vision for a cybersecurity program motivated their external partnerships with many industry leading experts in IT hardware, software, and cloud infrastructure.

Each WCCCD partner expressed enthusiasm for Generation Cyber and recognized the importance of filling a noticeably large skills gap within the cybersecurity industry. Exhibit B details each external partner's role. Aside from a brief collaboration between Dell, VMware, and Ixia, each partner worked in a separate capacity to create the infrastructure for the Generation Cyber program.

Exhibit B: Roles of the WCCCD Technology Partners

Dell	Dell provided vlan hardware for storage in user devices and updated software for the hardware.
VMware	VMware designed a simulated environment, also known as a cyber range, to launch and defend cyber attacks.
Ixia	Ixia provides the malware called Breaking Point that allows you to send attack traffic and simulate cyber attacks.
TestOut	TestOut is a virtual curriculum and testing package that was selected as an instructional aid to monitor student performance.
Mavi Interactive	Mavi Interactive provided competitive and immersive cybersecurity simulation games.

Exploring New Territory

Generation Cyber led the way on numerous fronts within cybersecurity education, by working innovatively with their external partners, and pushing to advance educational and technological boundaries. Generation Cyber blazed a trail for future cybersecurity professionals and community colleges looking to start their own cybersecurity programs.

Trailblazing in the Community College Landscape

Some external partners shared they had not worked with community colleges in the past. For VMWare, their partnership with WCCCD served as an affirmation project. While WCCCD originally considered using the VMware Academic Program (VMAP), a free software licensing program that allows academic institutions to use VMware products, VMware staff quickly realized that VMAP was not going to meet Generation Cyber's advanced needs for cybersecurity training. Instead, VMware created a customized virtual cyber environment for students to launch and defend cyber attacks in a completely safe and isolated environment. Within months of implementing their cloud-based cyber environment at WCCCD, they received multiple inquiries from community colleges across the country to implement a similar technology platform.

Ixia had previously worked with academic institutions, but primarily four-year institutions. WCCCD was one of the first few community colleges they worked with. Similarly, staff from Dell reported not having had worked with community colleges on a cybersecurity project like this, but rather with professional firms to train employees. While the product delivered to WCCCD was not different for Dell or Ixia, the customer (WCCCD) was unique in its structure, vision, and needs.

Other companies like Mavi Interactive and TestOut had previously worked with community colleges and provided WCCCD with products they previously used with other academic institutions. Though no new products were created out of the partnership with TestOut, TestOut worked with WCCCD to provide tailored products. Mavi Interactive sold specific games to WCCCD, but consistently improved their games and adjusted the games based on WCCCD's consistent feedback.

On the Cloud

Many of the external partners shared that Generation Cyber did away with "old school" methods and implemented a cloud-based system across the board. As a representative from Dell put it, "the technologies they implemented were the cream of the crop for this industry."

> "Wayne County Community College District went above and beyond to stay on cutting edge."
> – WCCCD Partner

VMware and Dell recognized the unique need for a virtual system for WCCCD early on. The cybersecurity industry has been moving to cloud-like functionality, where the purchase and use of virtual space functions

act like a vending machine. Users can buy space easily (with the click of a button) and use a series of services immediately thereafter, rather than use a physical system that requires users to purchase hardware and physically install it. This flexibility was appealing to WCCCD for a couple of reasons. WCCCD offers Generation Cyber on two campuses – Downtown Campus and Western Campus – which are on different sides of town. The alternative to the cloud-based system was a physical system that requires hardware to be connected, which did not meet WCCCD's needs. WCCCD worked with VMware to implement a cloud-based infrastructure to connect these two campuses.

WCCCD and VMware agreed the best option for them was to create a fully isolated virtual security lab, also known as a cyber environment. While the coordination of the physical networking and IT teams to describe how this virtual environment would work slowed down the process slightly, the team worked with the Generation Cyber Project Director to determine the design.

Ixia used the hypervisor (cyber environment) VMware installed to run their Breaking Point Virtual Edition software. This was possible due to VMware's strong server, which can host multiple operating systems (e.g., Linus, Windows), essentially allowing WCCCD to operate a network in an isolated box in order to keep the malware contained. As a representative from VMware explained, "we built here what is essentially called in the medical world a glove box, where you stick their arms in the gloves inside the glass box and manipulate things like viruses. They pull their hands out, but everything stays in the box. We created that in a virtual space, a virtual glove box." This virtual glove box provided WCCCD the opportunity to manipulate computer viruses and other threats without exposing other computer systems at WCCCD to the harmful effects of the malware.

The representative from VMware called the cyber range a "virtual glove box." This image of a glove box illustrates how one isolates harmful material in a medical setting.

In order to train the next generation of "cyber environment warriors," WCCCD used Breaking Point to send attack traffic to simulate cyber attacks. The Breaking Point platform has over 35,000 different attacks, including evasions, which are what attackers use to "cover their tracks." This kind of platform cannot be taken lightly; the malicious threats created in this virtual lab could be misused if the software fell into the wrong hands. WCCCD staff, as part of the Breaking Point software implementation, attended a three-day intensive training with a world-renowned trainer. Ixia staff noted that it was obvious WCCCD "knew what they were doing" and were prepared to take on the responsibility of protecting the software.

Simulated Exercises

To complement the Breaking Point software, WCCCD worked with TestOut to include an interactive e-book for students to learn cybersecurity concepts and prepare for certifications. Video lectures and demonstrations by instructors can be used to accompany the e-book. IT professionals in the field inform the curriculum; TestOut surveyed the cybersecurity industry and incorporated the qualifications and skills graduates need to succeed in a cybersecurity career.

As part of the curriculum, students also experience simulations in a virtual lab (separate from the cyber environment) to explore the cybersecurity concepts

they learn in the classroom. Instructors control the issues and viruses students face within this virtual lab. WCCCD worked closely with TestOut to evaluate and select the elements of the TestOut curriculum they wanted to use. WCCCD also received a custom exam that students are able to take to receive TestOut's certification, and to help them prepare for their official CompTIA certification. While TestOut is not a certifying body, their exams are developed in partnership with CompTIA, a "3rd party certification company that provides the most industry recognized exams and…sets industry standards." The exams differ in that TestOut's exam evaluates performance skills, while CompTIA is a traditional exam. As part of their partnership with WCCCD, TestOut continues to provide technical support for students and instructors.

WCCCD also worked with Mavi Interactive to provide cybersecurity gamified exercises within a simulation format, which supplemented TestOut's simulations. This gamified and competitive platform was hosted on 25 high-end Windows portable tablets (used on carts in classrooms). At first, WCCCD implemented two games but now that number has grown with the program. While Mavi Interactive had worked with other academic institutions, WCCCD was different. WCCCD was active in the implementation phase, providing feedback and requesting additional or advanced programming functionality.

Mavi's Interactive games are designed by subject matter experts to be used as a training tool towards certification (though Mavi Interactive is not a certifying body). Students receive instruction on how to complete exercises within the games and work their way through various difficulty levels which are used in different parts of the semester to test students' knowledge of cybersecurity concepts. WCCCD's intention to integrate the classroom – from games to e-books to hands-on experience – created a cohesive and comprehensive approach to cybersecurity education.

The involvement of each external partner helped build WCCCD's capacity in creating a state of the art cybersecurity training facility to complement learning theory.

Ready for the Next Attack

Each day there are hundreds of new attacks created by hackers, making the process of training new cybersecurity experts challenging. Each new attack can have new elements, evasions, or viruses. External partners recognized that there is little value in teaching students old material; the attacks students learn to fight today may be irrelevant tomorrow. External partners emphasized that the process of learning cybersecurity must be fluid and dynamic. The ability for students to be exposed to new and incoming security threats increases their employability and success in their future jobs.

Regular and Frequent Updates

To meet the changing needs of this industry, WCCCD ensured their software was capable of providing their students with relevant hands-on experience. TestOut's simulations, Mavi's Interactive games, VMware's cyber environment, and Ixia's Breaking Point malware all provide students a variation of hands-on experience, but each are updated to stay relevant.

TestOut regularly redesigns their curriculum objectives to meet the objectives of the CompTIA certification exam which is updated every few years. Mavi Interactive adapts to industry changes and new threats by advancing their game and creating deeper cybersecurity threat awareness.

VMware's virtual systems let instructors copy, delete, and be fluid with the threats students can practice with; for example, students can practice on "day 0 attacks" in which a new bug can be run in the virtual lab within moments of its discovery.

Ixia keeps up with the constantly changing cybersecurity landscape by sending biweekly updates to their Breaking Point virtual edition software. Ixia

sends application and threat intelligence updates virtually so WCCCD receives the latest and worst attacks to simulate within the cyber environment.

Continuous Communication, Leadership, and a Dash of Passion

WCCCD's leadership and dedicated staff provided a base for the initial success of Generation Cyber – they radiated passion, demonstrated strong leadership, and effectively communicated their vision. Their vision drove the program to create the external partnerships that are still in existence today. Each partner we interviewed shared at least once in their interview, the excitement and passion that radiated from the Generation Cyber team.

Know What You Want

WCCCD's project director and project coordinator often met with potential and existing external partners to share their vision for the Generation Cyber project. External partners gained a deeper understanding of Generation Cyber's goals and objectives, as well as the role they were to play in the development of the project. When approaching external partners, WCCCD shared their particular needs for their program, and provided feedback on existing WCCCD programs to create a customized curriculum and hands-on experience for students.

Thorough Trainings and Support

Almost every external partner provided a variation of training for staff. Breaking Point sent a world-renowned product specialist trainer to provide training for their simulation software. Dell also provided training services for their software which allowed for virtual desktop infrastructure (i.e., multiple desktop software with defined storage).

VMware provided trainings on their products, and recently published an e-book that drew from their experience with WCCCD on how to safeguard your campus.

> "You don't have to be a R1 research university to start up one of these programs—you can be a community college and do it with the assistance of a grant." – WCCCD Partner

Conclusion

In 2018, there has been about 215,371 cybersecurity job openings. Many of these openings are "new collar" positions ideally suited for individuals with "the technical and soft skills needed to work in a contemporary technology industry through nontraditional education paths."[14] WCCCD's Generation Cyber program intends to be on the forefront of feeding the pipeline for these new collar positions. Their experience developing Generation Cyber under the Department of Labor's TAACCCT capacity building grant demonstrates the push and pull needed to work within community colleges as academic institutions and with external partners, employers, and HR professionals as the beneficiaries of their efforts. WCCCD's Generation Cyber, according to its project director, has allowed them to be at the table in their region, defining important alliances, and supporting large manufacturers in Detroit and their Tier 1 suppliers by providing well-trained and skillful workers.

This Preface provided a glimpse of the social and historical context in which WCCCD's Generation Cyber was developed and implemented. The third party evaluation that follows provides an in-depth analysis of the implementation and outcomes achieved by the program.

[14] New-collar worker. (2018). Retrieved from https://en.wikipedia.org/wiki/New-collar_worker

References

Bryman, A. (1988). *Quantity and quality in social research.* London, UK: Unwin Hyman.

Cybersecurity and Information Assurance Research and Development Senior Steering Group; and the Cybersecurity and Information Assurance Interagency Working Group. (2011). *Trustworthy cyberspace: Strategic plan for the Federal cybersecurity research and development program.* National Science and Technology Council.

IBM Corporation. (2013). *Cybersecurity education for the next generation.* Armond, NY: IBM Corporation.

ICF. (2017). Wayne County Generation Cyber Trade Adjustment Act Community College and Career Training interim report. Fairfax, VA: ICF.

Michigan Cyber Initative 2015. (2015). *Leading the Nation: An interagency, public-private collaboration*. Retrieved from https://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf

Morgan, S. (2017). *2018 Cybersecurity market report.* Cybersecurity Ventures. Retrieved from https://cybersecurityventures.com/cybersecurity-market-report/

Newhouse, W., Keith,S., Schribner, B., & Witte, G. (2017). *National initiative for cybersecurity. Education (NICE) cybersecurity workforce framework.* NIST Special Publication 800-181. US Department of Commerce.

National Science and Technology Council (NSTC). (2011). *Trustworthy cyberspace: Strategic plan for the federal cybersecurity research and development program.* Report prepared by the National Science and Technology Council, Executive Office of the President. Retrieved from https://www.nitrd.gov/pubs/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

Ponemon Institute. (2014). *2014 Best schools for cybersecurity*. Traverse City, MI: Ponemon Institute LLC.

United States of America: Department of Commerce and Department of Homeland Security. (2017). Supporting the growth and sustainment of the nation's cybersecurity workforce: Building the foundation for a more secure American Future.

Workforce Intelligence Network. (2017). Cybersecurity skills gap analysis: National and advance Michigan region data.

WAYNE COUNTY COMMUNITY COLLEGE DISTRICT'S "GENERATION CYBER"

Evaluation Report

ICF

Wayne County Community College District

EXECUTIVE SUMMARY

Introduction

In 2014, the Wayne County Community College District (WCCCD) was awarded a Trade Adjustment Assistance Community College Career Training Grant (TAACCCT) from the United States Department of Labor to implement a cybersecurity training initiative, called WCCCD Generation Cyber (Generation Cyber). ICF was hired as the third party evaluator to assess the implementation and outcomes of the program. Generation Cyber aimed to provide cybersecurity training and credentials to the workforce in Wayne County, Michigan. The training would benefit the local industry by providing a workforce with needed skills in cybersecurity, and also prepare students for a career pathway that would lead to increased earnings and benefits, stable employment, and potentially further education. In addition, the program was designed to increase the institutional capacity of WCCCD to train the cybersecurity workforce by developing curriculum, creating cybersecurity labs, training faculty, and establishing strong partnerships with the local industry.

Evaluation Methodology

The evaluation was designed to capture the implementation and outcomes of Generation Cyber and identify potential lessons learned and implications for WCCCD and other Cybersecurity training programs. The evaluation team used a mixed methods approach that included interviews and focus groups with different program stakeholders (staff, faculty, partners, and students) along with quantitative data about students in the program from baseline student surveys and college administrative data.

Implementation Findings

The implementation findings described how the program developed and changed over the grant period, successes and challenges to program implementation, and institutional capacity building.

- Generation Cyber implemented most of the expected components of their program model, such as lab-based and multi-mode instruction, stacked credentials, multiple educational pathways, partnership engagement, and career and training supports for students.

- There were a few changes made to the program, which were designed to better meet the needs of its students. For example, Generation Cyber removed a baseline screening assessment, since students already could demonstrate their preparedness through taking prerequisite courses. In addition, the program broadened its target population to include community college students at large, and also found they had been successful in recruiting women and older adults.

- Generation Cyber developed a cybersecurity program at their college that was sustainable beyond the grant period. Staff plan to continue to offer the courses and use the cyber labs developed during the grant, and also continue to conduct cyber awareness workshops for incumbent workers. In the future, they plan to expand their work with industry partners, and update the curriculum over time to align with emerging technological innovations in the cybersecurity field.

Outcome Findings

The evaluation captured initial trends on student training outcomes. However, it was too early at the time of the evaluation to fully assess the program's effects on student employment, given the short time that the program had been implemented.

- Students completed the new cybersecurity training courses during the grant. While the majority of students completed one or two cybersecurity courses, some completed all five. Almost all of the students who attempted to earn a 3rd party certification were able to do so, and one student earned an associate degree.

- Staff found that while they were training students with the skills and certifications that would prepare them for cybersecurity jobs, many companies limited hiring for entry level jobs to those who had a Bachelor's degree and multiple years of experience.

- Staff started actively working with partners to figure out how to solve the misalignment between the demand for a cybersecurity workforce with these hiring restrictions. Regardless, staff and faculty shared success stories of students who had been able to find employment and start a career pathway that would build on their cybersecurity training.

Conclusions and Implications for Workforce Training Initiatives

The evaluation showed how the Generation Cyber program achieved its goals and adapted over the four-year grant to better meet the needs of its students and the local industry. The evaluation provides several implications for other workforce training initiatives, particularly in the cybersecurity area.

- A dynamic program model is essential when training students for a field changing as rapidly as cybersecurity. In cybersecurity, there are new developments every few months, which can require teaching different strategies and using the latest software to make sure students are armed with the most up-to-date skills. However, making the necessary adaptations over time requires significant investments in time and funding to be able to purchase equipment and undergo curriculum approval processes. Program administrators and funders should recognize the need to build in time for the program development process, and should also focus on effectively coordinating to move the project forward.

- Cybersecurity training potentially benefits a wide range of adults, including those who are new to the field and longer term incumbent workers. The college found that to recruit students they needed to broaden their focus to different audiences who were interested and would benefit from the training, such as community college students, incumbent workers, and older adults.
- Engaging internal and external partners are important at all stages of program development. Generation Cyber found they needed to interface and leverage multiple departments in their college, for example, to purchase equipment and meet the grant reporting requirements. They also described different ways that industry partners contributed to the program such as designing the labs, providing input on curriculum, teaching students about career opportunities, connecting students to career opportunities, and doing outreach for the program in the field.

INTRODUCTION

In 2014, the Wayne County Community College District (WCCCD) was awarded a Trade Adjustment Assistance Community College Career Training Grant (TAACCCT) from the United States Department of Labor to implement a cybersecurity training initiative, called WCCCD Generation Cyber (Generation Cyber). The grant was intended to allow WCCCD to develop a pipeline of skilled workers who could address current and future cybersecurity threats in a wide range of industries. ICF was hired as the third party evaluator to assess the implementation and outcomes of the program. This report describes the evaluation methodology and findings as well as potential implications for WCCCD and other workforce training programs.

WCCCD TAACCCT Program

Program Goals and Intended Impacts

Generation Cyber aimed to provide cybersecurity training and credentials to the workforce in Wayne County, Michigan. The training would benefit the local industry by providing a workforce with needed skills in cybersecurity, and also prepare students for a career pathway that would lead to increased earnings and benefits, stable employment, and potentially further education. In addition, the program was designed to increase the institutional capacity of WCCCD to train the cybersecurity workforce by developing curriculum, creating cybersecurity labs, training faculty, and establishing strong partnerships with the local industry.

Program Activities

Generation Cyber developed and evolved over the course of the grant. In the original model, a broad set of activities were planned. The expectation was that WCCCD would create cybersecurity classes, with multi-modal, lab-based instruction. These courses would lead to industry-recognized cybersecurity certificates, or an associate degree, and students would have the option to stack certificates earned to build up their qualifications during their training. The staff would engage an advisory council that included industry representatives to review the curriculum and provide feedback. The program would also connect students with employment opportunities and employer partners. In the program model, students would need to take an assessment called the Llobet, to determine their readiness for Generation Cyber, and then would take a foundation class if they were not ready to enroll. However, as described below, neither of those components were relevant for the final program model and were not utilized. We developed a logic model in 2015 to describe the vision for the program early on in the grant, which served as a framework for the third party evaluation (see Appendix A).

EVALUATION METHODOLOGY

Purpose of the Evaluation

The evaluation was designed to capture the implementation and outcomes of Generation Cyber and identify potential lessons learned and implications for WCCCD and other Cybersecurity training programs. The evaluation team used a mixed methods approach that integrated perspectives of different program stakeholders (staff, faculty, partners and students) along with quantitative data about students in the program.

Key Evaluation Questions and Methodology

Implementation Study

An implementation study was conducted to document the implementation processes, capture how closely the implementation aligned with the initial Generation Cyber program model, understand successes and challenges with implementation, and describe how institutional capacity was built. Exhibit 1 below shares the implementation evaluation questions that were addressed in the study.

Exhibit 1: Implementation Evaluation Questions

Topic	Questions
Describing and mapping the implementation process	▪ How is the particular curriculum selected, used, modified, or created? ▪ How has the program improved or expanded using grant funds? What delivery methods are offered? What is the program administrative structure? What support or other services are offered? ▪ Is an in-depth assessment of participants' abilities, skills, and interests conducted to select participants into the grant program? Is an assessment of participants' logic and reasoning knowledge and abilities conducted as a partial condition to program admission? What assessment tools and processes are used to screen the participants? Are the assessment results useful in determining the appropriate program and course sequence for participants? ▪ What contributions does each partner (e.g., employers, workforce system, others) make in terms of program design, curriculum development, recruitment, training, placement, program management, leveraging resources, and commitment to program sustainability?
Assessing implementation fidelity	▪ How closely do the programs replicate the major and ancillary components of the Generation Cyber program model? What changes were made to the implementation strategy? Why? ▪ What are the variations in implementation in the two different campuses?

Topic	Questions
Identifying successes and challenges to implementation	▪ What program outputs are generated throughout the life of the grant? What barriers hinder output achievement? What factors unexpectedly improve output achievement? ▪ What are the successes and obstacles to program performance? ▪ How should program processes, tools, or systems be modified to improve performance? ▪ What factors contribute to partners' involvement or lack of involvement in the program? Which contributions from partners are most critical to the success of the grant program? Which contributions from partners have less of an impact? ▪ How satisfied are program partners, staff, and participants with the program? Why?
Institutional capacity-building	▪ What are some successful elements that build institutional capacity of WCCCD (e.g., new faculty, professional development for faculty and staff, new equipment)? How can the program expand or enhance institutional capacity? Are continuous feedback loops being utilized to share information and make critical decision about Generation Cyber?

Using the logic model and early conversations with program staff as a guide, the evaluation team developed interview and focus group protocols to assess stakeholders' perspectives on program implementation, including successes and challenges as the program developed. In the third and fourth year of the grant, the evaluation team conducted interviews with staff and partners and conducted focus groups with enrolled students. Exhibit 2 below shows the number of each group of stakeholders that participated each year. In addition, the evaluation findings were informed by interviews conducted in a separate study used to develop the preface above.

Exhibit 2: Stakeholders Interviewed

Stakeholder Group	Number Interviewed	
	Grant Year 3	Grant Year 4
Program Staff	3	2
Faculty	2	2
Students	8	3
Industry Partners	0	2

Note. This table does not include interviews conducted for the study reported in the preface. Data from those interviews may have informed some of the findings below.

Outcome Study

An outcome study was conducted to understand how the program affected students' education and employment outcomes. Exhibit 3 shares the outcome evaluation questions. To answer these questions, the evaluation collected baseline and follow-up surveys and also obtained college administrative data. However, because insufficient follow-up surveys were collected, they were not included in the analyses. To help address the limited follow-up information, we supplemented the outcome data with stakeholder interviews, by including a small number of questions about student outcomes on the interview protocols.

The baseline survey was administered each semester during courses starting in February 2017. While we attempted to survey students during their first course in Generation Cyber, some students were surveyed shortly after their first course ended. However, the baseline survey data still provided a picture of student background characteristics and perspectives towards the start of their engagement in the program. The findings below include 65 student baseline survey responses, after removing duplicate responses and responses where students had started the survey but not completed any questions.

Exhibit 3: Outcome Evaluation Questions

Topic	Questions
Education Outcomes	▪ To what extent does Generation Cyber increase completion and retention rates? ▪ To what extent does Generation Cyber result in increases in the number and percent of students who pursue additional education? ▪ To what extent does Generation Cyber increase certification rates? ▪ To what extent does Generation Cyber improve mastery of industry and occupational skills or other program-related credentials?
Employment/ Career Outcomes	▪ To what extent does Generation Cyber lead to higher quality employment outcomes (e.g., employment rates and earnings, promotions)? ▪ To what extent does Generation Cyber decrease the time lapse between graduation/completion and job placement? ▪ To what extent does Generation Cyber decrease the time needed to attain credentialing? ▪ To what extent does Generation Cyber put participants on stable and strong career pathways, as defined by increases in promotions and benefits, as well as declines in the receipt of public assistance?

Limitations

There are certain limitations in the study that provide context for interpreting the findings.

The student focus groups only included 11 students (eight in Year 3 and three in Year 4), and the baseline student survey only included 65 students. The students who participated in data collection may not represent the views of all students who participated in the program. In addition, for the baseline student survey, some of the questions were skipped by a large proportion of students (e.g., questions about employment barriers) and therefore the data below only represents the view of a small number of students.

The evaluation also provides mainly qualitative information about student employment outcomes from interviews with program stakeholders. Quantitative data on student employment outcomes were not available during the study because the evaluation team did not receive follow-up surveys that they could use to assess student employment after program completion.

In understanding program outcomes, it is also important to recognize that the evaluation assessed the program at an early stage in its development. The program was still evolving for most of the grant period, and initial program implementation was delayed by external factors, such as the time required for equipment purchases and curriculum approval (see the Preface for more detail). By the time the evaluation data collection was conducted, many students who

participated had not yet completed the program nor had sufficient time after they finished to achieve meaningful employment outcomes. A future study would be needed to more fully understand the program's potential impact on student career outcomes.

EVALUATION FINDINGS

This section shares findings developed from the data collected about: 1) Student Characteristics, 2) Program Implementation, and 3) Program Outcomes. Further description of program context and development is available in the Preface above.

Student Characteristics

Demographics

The study gathered information about the students participating in the program from the college's administrative data and the baseline survey. Exhibit 4 below shares the demographics of students in the study found in each sample. For both samples, the majority of students were men, were under 30, and were Black/African-American. However, the program also included 29% of women in both samples, and about a fifth of the students were over 40 years of age. Demonstrating that the program included students from groups that tend to have employment barriers, the baseline survey data showed that a small proportion of students had a disability (3%) or had served in the military (6%) (See Exhibit 5).

Exhibit 4: Student Demographics

	Administrative Data (N=124)	Baseline Survey (N=65)
Gender		
Male	70%	66%
Female	29%	29%
Other	1%	-
Do not wish to disclose*	-	5%
Age		
18-24	48%	33%
25-30	16%	18%
31-40	16%	20%
41-50	4%	15%
51-60	16%	7%
61 or older	0%	8%
Race/Ethnicity**		
Black/African-American	65%	60%
Asian/Pacific Islander	1%	20%

	Administrative Data (N=124)	Baseline Survey (N=65)
White/Caucasian	8%	17%
Hispanic	3%	-
Native American/Alaskan Native	1%	-
Other	21%	-
Do not wish to disclose*	-	8%

Sources: WCCCD Administrative Data and Baseline Survey
*This category was only assessed in the survey and not in the administrative data.
**For the survey, students could select more than one race/ethnicity.
Administrative Total N=124, Baseline Total N=65.

Exhibit 5: Student Characteristics

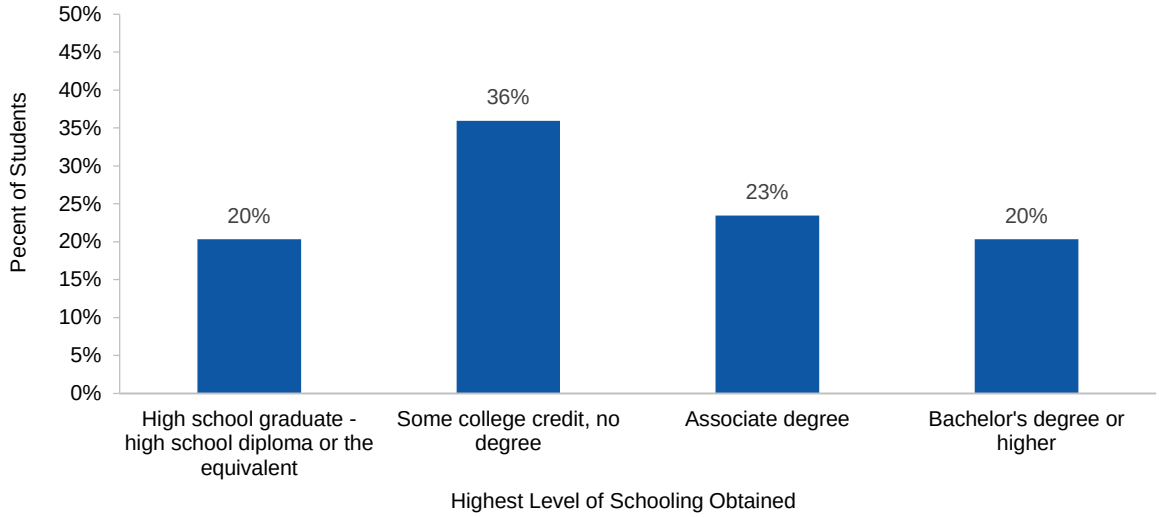
	Percent of Students
Do you have a disability?	
Yes	3%
No	89%
Do not wish to disclose	6%
US Military Service	
Never served in the military	83%
Only on active duty for training in the Reserves or National Guard	3%
On active duty in the past but not now	3%
Do not wish to disclose	11%

Source: Baseline Survey. Disability question total N=64, US Military Service question total N=65.

Prior Vocational Training and Education

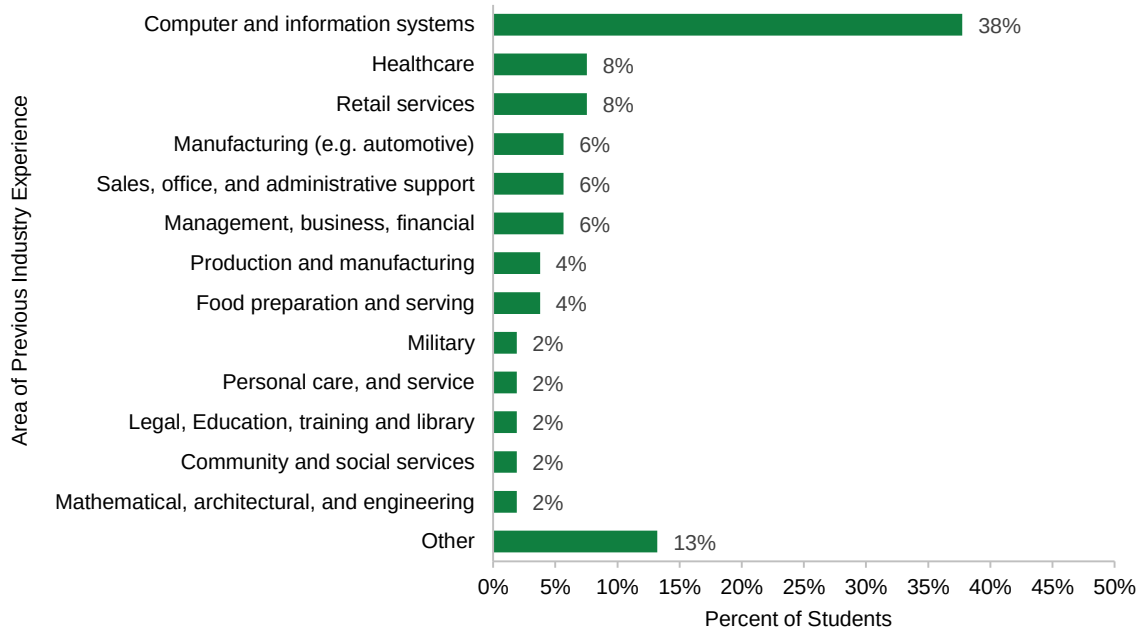
As shown in Exhibit 6, students began the program with a range of educational backgrounds and almost half (43%) already had an associate degree or higher. While 20% said they were a high school graduate, it is likely these students also had some college credit, since students were required to take two prerequisite college courses before starting Generation Cyber. Most of the students (80%) did not hold certifications or licenses at the beginning of the program. However, the majority of students (85%) reported that they had a paying job at some point before the program started (Total N=65).

Exhibit 6: Student Education Level



Source: Baseline Survey. Total N=64.

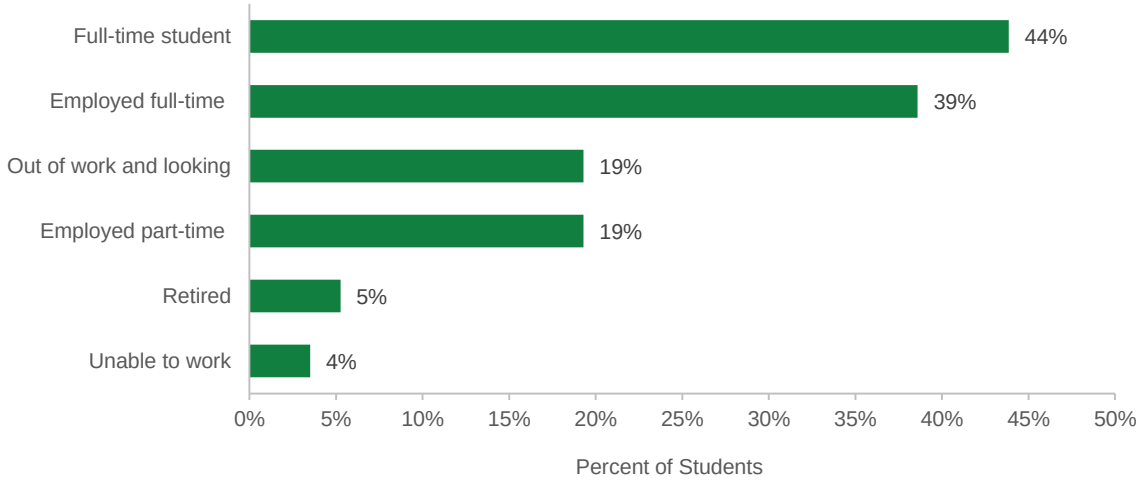
Exhibit 7: Student Professional Background



Source: Baseline Survey. Total N=53.

The most common area of students' professional background (see Exhibit 7) was computer and information systems (38%), which makes sense since Cybersecurity is an area within that field, and because students were often recruited directly from the college's Computer and Information Systems program (as described further below). Exhibit 8 shows the employment status of students when they enrolled for the course. Students include those who had been full-time students (44%) and those who worked full-time (40%), along with some who were unemployed and looking for work (19%) and some who were employed part-time (19%).

Exhibit 8: Student Employment Status When Enrolled

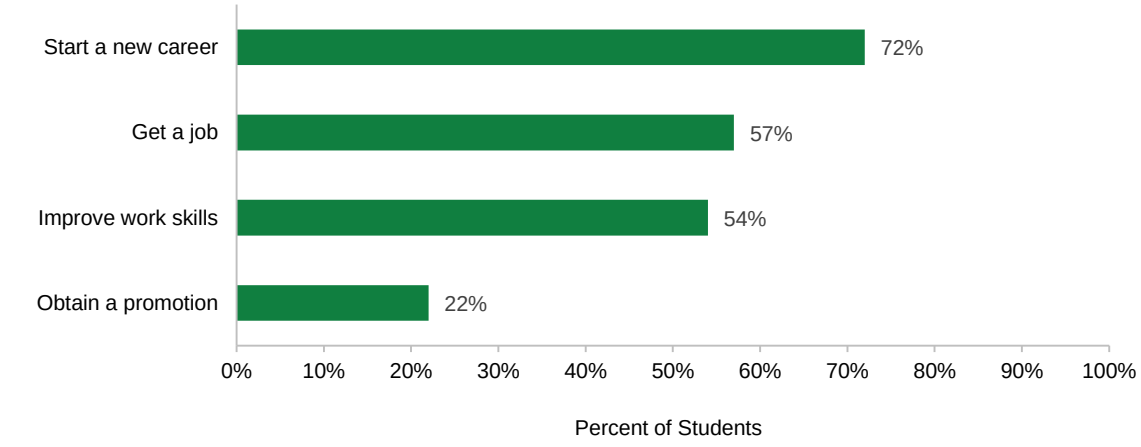


Source: Baseline Survey. Total N=57. Students could select more than one category.

Employment Goals

When asked their goals for completing the program, the majority of students reported that they wanted to start a new career (72%), get a job (57%) or improve work skills (54%). A smaller proportion of students indicated that they wanted to obtain a promotion (22%) (See Exhibit 9). These findings suggest that most students saw participation in Generation Cyber as a way to start a new career pathway or obtain a job, rather than to be promoted in their current professional position.

Exhibit 9: Goals for Participating in the Cybersecurity Program



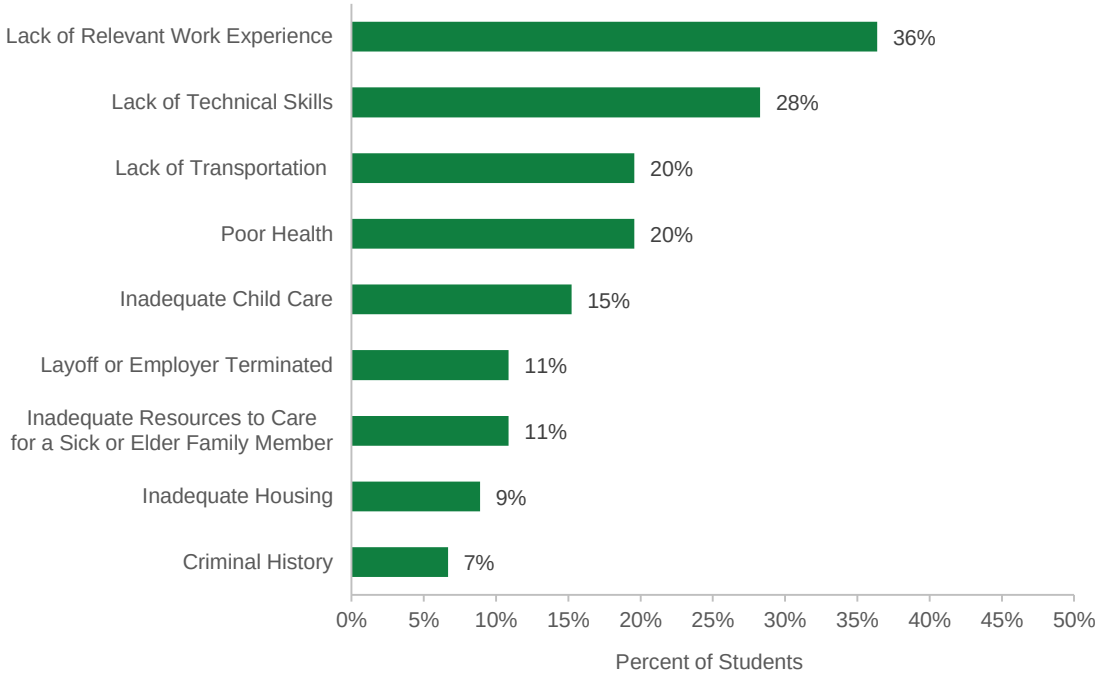
Source=Baseline Surveys. Total N=65

Employment Barriers

While most students had been employed before, many also reported having barriers to employment. In the baseline survey, students were asked the extent to which circumstances affected their ability to secure and maintain employment. Exhibit 10 shows the percent of

students who reported that they experienced each barrier to any extent. The most common barriers were a lack of relevant work experience (36%) and a lack of technical skills (28%), which were areas that Generation Cyber was designed to address. The next most common areas were lack of transportation (20%) and poor health (20%).

Exhibit 10: Employment Barriers



Source: Baseline surveys. The total N ranged from 44 to 46.

Program Implementation

The preface above describes the process used for program development. This section focuses more on describing program implementation after the initial development phase.

Curriculum and Instruction

Before offering training, WCCCD needed to undergo an extensive program development process involving multiple partners (see Preface for more detail), which included, for example, advisory council meetings, purchasing equiptment, adapting software with technology partners, building labs, training faculty, and writing and getting approval for course curriculum. After their initial development phase, WCCCD conducted a pilot of their Network+ course in Spring 2016, and then again in Summer 2016. In Fall 2016, the course was officially launched. Over the next year and a half, the college added in additional courses that students could take once they completed earlier courses in the sequence. The initial launch of the courses was delayed by multiple challenges and other contextual factors, such as delays in ordering equipment to develop the labs and time required to obtain approval for their for-credit courses (see Preface).

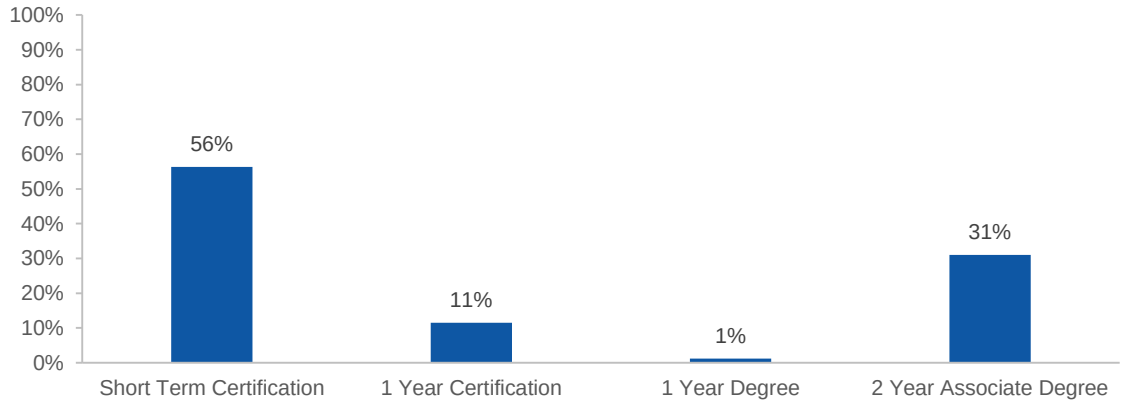
Exhibit 11 lists five new cybersecurity courses that were developed during the grant. Before starting these courses, students needed to take two prerequisites in the Computer Information Sciences (CIS) program: 1) Introduction to Computer Information Systems (CIS 110), and 2) Networking Essentials (CIS 240). Some courses were available in an accelerated format, which lasted for seven weeks, while others were offered in a longer format that was 15 weeks long. Network+, for example, was offered in both the longer and accelerated format, allowing students multiple options with which to engage with the first course in the sequence.

Exhibit 11: New Cybersecurity Classes Developed:

- Network+ (CIS 270)
- Security+ (CIS 272)
- Certified Ethnical Hacker (CIS 274)
- Cyber Network Associate (CIS 276)
- Certified Authorization Professional (CIS 278)

Students could earn industry-related certifications after completing each course, making students potentially more marketable for employers. Generation Cyber also offered an associate degree program that combined the new courses with existing courses in their Computer Information Systems (CIS) courses. Essentially, the Cybersecurity program offered students three educational pathways: a two-year associate degree in Applied Science, a one-year certificate, or short-term certificates that can be completed in three months. Exhibits 12 and 13 show the type of programs in which students participated in and their enrollment status. Over half (56%) enrolled in the short-term certification program and most of the remaining students (31%) were in a two-year associate degree program. There were also a combination of students who participated in the program full-time (67%) and part-time (33%).

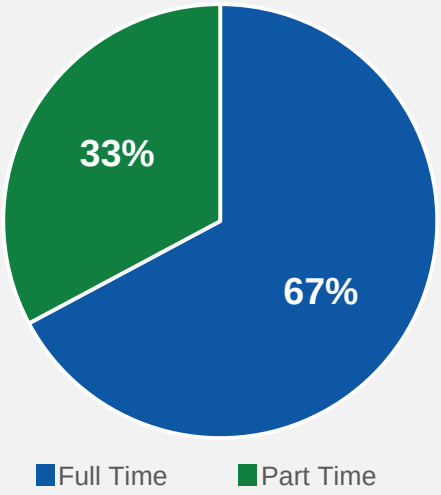
Exhibit 12: Program in which Students Were Enrolled



Source: Administrative Data. Total N=87.

In addition to receiving college certificates, students could complete exams to receive third-party certifications from nationally recognized institutions (e.g., CompTIA Security+). Stakeholders described how certifications were valuable because they allowed students to demonstrate competency in an area to an employer in a short period of time. As one faculty member said, "Employers want to see [certifications]. We have talked to them about how that adds value to their resume, even if they don't have work experience to show an employer. But, to have the certification is critical."In the interviews, instructors described their instructional approach. Their courses used both lecture and hands-on activities. Especially later on in the grant, the instructors incorporated simulations and game-based learning activities that allowed students to practice solving cybersecurity problems (See Preface). Students and instructors talked positively about these activities, in that they helped them learn the actual skills students would need for the workplace. Students in the focus groups mentioned that some of their peers had difficulty being able to keep up with the courses if they missed class. As one staff member explained, with the students it can be common for there to be challenges in balancing work and school and in getting to class. The staff member also shared, "[TestOut] is an excellent curriculum and software, but also very time consuming. That has been a challenge to students. The amount of time is overwhelming for some students; before you develop intuitiveness for the hands-on nature of the work, it can be a lot for students to handle."

Exhibit 13: Part- and Full-Time Enrollment



Source: Administrative Data. Total N=64.

The program also expanded its reach outside of the college, by offering a short-term workshop for incumbent workers. This program was called a Cyber Bootcamp and aimed to build awareness of cybersecurity issues among professionals. These workshops were potentially applicable to a wide range of employees, not just those whose job focuses on cybersecurity issues; staff shared how given the current cyber threats across industries, broad employee awareness was critical to preventing attacks early on. As one staff member explained, "There's such a link between [cybersecurity] and so many other fields – it impacts everyone's jobs." These workshops were also a way to educate employers about what their training program offered and encourage them to recruit employees from their training program.

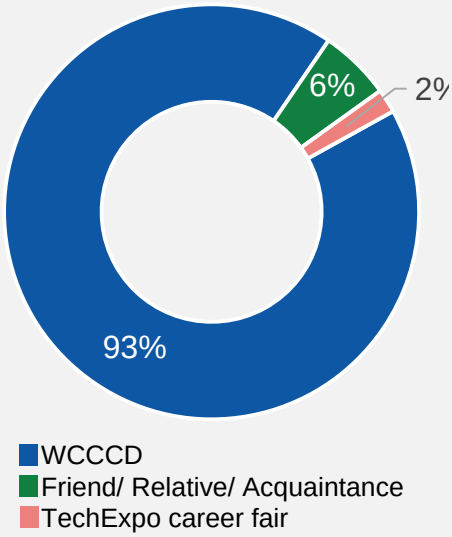
One challenge staff and faculty described was how they had to keep up with ongoing changes in the cybersecurity field. Every few months, there were changes in technology and new strategies, and it was important that students' skills reflected the most recent innovations. As one staff member shared, "we need to be so in tune to the fact that it is such a dynamic field… [and] students need the most relevant, up-to-date information." However, the pace with which faculty

could update course curriculum was limited by the lengthy process required for course approval, and the costs of purchasing new software and equipment.

Recruitment and Enrollment

The program engaged in multiple strategies to recruit students, such as attending industry and community events, producing radio and print ads, sending out emails, and outreach with industry partners. Ultimately they found that the most successful strategy was to recruit students from their Computer Information Science (CIS) program. This is reflected in the baseline surveys, where almost all students (93%) had heard about the program from the college (WCCCD) (see Exhibit 14). Accordingly, the college expanded their recruitment beyond trade-affected workers, dislocated workers, and unemployed veterans, who were the original targets for the grant, to focus on community college students.

Exhibit 14: How did you hear about this program?



Source: Baseline Survey. Total N=55

Staff also noted that they had success in recruiting women and older adults to the program. As one staff member shared, “The blend has been older individuals with younger students, and they have been very helpful and encouraging to the younger students. Cyber also lacks diversity traditionally, and we are developing a stronger female component. We just had one single mom, who is very excited about cyber.” There were a few challenges in recruitment, described in greater detail in the preface, that made it more difficult to recruit students. This included, for example, that cybersecurity was not initially considered an official program at their school, and students may have been concerned that their course costs would not qualify for financial aid. This was especially a concern since TAACCCT did not fund students’ tuition or materials, and many students could not afford to pay these costs on their own.

Career and Training Support Services

Students in the program had access a wide variety of academic, career, and other types of support services (See Exhibit 15). Students mentioned that job fairs, resume workshops, and interview assistance were particularly helpful for their career preparation. Students also benefited from having staff and partners visit classrooms to talk about Cyber-related careers and the necessary skills and qualifications, and to connect students to industry resources and other partners. For example, staff informed students about statewide cybersecurity training platforms like the Michigan Cyber Range, pursued relationships with IT recruitment firms, and incorporated industry publications into the classrooms. Staff observed that students might not be taking

advantage of available services. As one staff member shared, "In my experience in totality, working with universities and community college students in general, students can know there's a resource and never go to it. You have to make sure it's the right resource and lead them to it." Similarly, one student explained, "Most of the material and the resources we have—if you go out and look for it, you will find it. If you are willing to do the work, it is there for you."

Exhibit 15: Examples of Student Supports Available

Area	Example Supports
Training Services	▪ Instructor out-of-class support ▪ Online tutoring ▪ Reading support ▪ Other support services (e.g., housing, food, transportation)
Career Services	▪ Job fairs ▪ Resume workshops ▪ Interview preparation ▪ Soft skills training ▪ Job placement

Participant and Program Assessment

WCCCD's shift towards recruiting students from their CIS program led to changes in their intake assessment practices. Initially, the program planned to administer an assessment to determine students' readiness for the cybersecurity program, called the Llobet. However, once the program began enrolling students, staff realized it was no longer an applicable assessment. Given that students were recruited from the school's CIS program (See Preface), they had already had an opportunity to develop their capabilities through the CIS coursework. Rather than use a separate assessment, the program decided to require students to get a B in two pre-requisite courses (CIS 110 and CIS 240) before enrolling in the first course in the cybersecurity sequence (CIS 270).

Exhibit 16: Program Assessment Methods

- Student feedback
- Visiting classes
- In class participation
- Homework assignments
- Hands-on project work
- Course exams
- Certification exams

In the courses, faculty conducted multiple assessments to understand student progress (See Exhibit 16). They used traditional quizzes, real-world lab simulations through TestOut, and practice certification tests to assess student performance (See Preface). Faculty believed that the labs in particular were useful to understand students' skills, since they reflected how they dealt with actual cyber problem solving.

All students who completed the platform coursework received a certificate and were then prepared to take a 3rd party certification exam. While not required, faculty with experience

working in the cybersecurity industry reported that companies like to see national certifications on student resumes. Teachers saw the best results on national exams when students took the test close to the end of the program while the material was still fresh and thus encouraged students to take the exam soon after completing the program. One staff member said that while the program prepared students well for national certification, the biggest barrier was student self-confidence. Some students did not feel ready to take the national exam, even though their teachers believe they will pass with the skills they have acquired.

Program staff also used assessment to continue to build the program and reflect on how to optimize the design, for example, by obtaining student feedback or visiting classes to see how they were going. One staff member shared, "We have used an iterative process all along – constantly reflecting on this prototype. Both rapid prototyping as well as iterative processes; to be open, to receive feedback as we continue to develop and adapt strategies for everything from recruitment to the best time for students to take certification exams."

Partnership Engagement

WCCCD engaged many partners as they developed and implemented Generation Cyber. Exhibit 17 below lists the different partners they worked with, both internal partners within their college, and external partners. Some of the program staff began the grant with already strong partnerships with the industry and these continued to strengthen during the grant.

Program Development

> "They have a lot of good local contacts and multiple locations throughout the county which is a great plus for students."
>
> – Industry partner

As described above (See Preface), WCCCD worked with technology companies and their internal staff to develop the cybersecurity equipment and labs to teach the curriculum. This was important to be able to use the latest technologies and also make them align with a community college setting. During the development stage, WCCCD also started to meet with an advisory council with employers and others involved in the cybersecurity industry to get input on their curriculum as it was being developed. For example, the advisory council provided input on the type of 3rd party certifications they should offer to make students more marketable to employers. Partners also played a role in training faculty in the cybersecurity content they were going to teach and helping them to get certified themselves.

Program Implementation

While partners continued to play a role in ongoing program development, they also took on additional roles once the trainings were implemented. For example, partners also played a role in soft skills training. Industry partners who sat on boards or coalitions could help connect students to professional resources such as national educational colloquiums or large local employers seeking cybersecurity professionals. One staffing agency was planning to offer soft skills workshops for students in the future, and they had already provided soft skills training content for the college to implement themselves.

Staff shared how internal partners at their university were also critical to program implementation. They leveraged career and training services for their students to provide access to a range of supports to serve student needs. IT staff at their institution continued to help with the technology infrastructure as the program continued, and other departments played different roles in the grant, such as how the institutional research department helped with program assessment.

Job Placement

Through outreach to companies, WCCCD marketed their program and worked to correct the misalignment between hiring requirements and the skills of their students (See Preface). Through their outreach, they identified staffing firms and employers that would be potentially interested in hiring their students. Towards the end of the grant, WCCCD was also working with these entities to recruit incumbent workers into their programs to provide upskilling and further training. Staff expressed interest in further developing relationships with technology and cybersecurity firms in the area to help students understand what cybersecurity professionals do and to potentially secure hiring agreements for Generation Cyber students.

Exhibit 17: Type of Generation Cyber Partners

Type	Examples
Internal Partners	▪ Educational Affairs Division ▪ IT staff ▪ Internal Evaluation Division ▪ Student Services ▪ Continuing Education and Workforce Development ▪ College leadership
External Partners	▪ Technology companies ▪ Book publishers ▪ Cybersecurity professionals ▪ Staffing agencies ▪ Employers ▪ Staff at other higher education institutions ▪ Educational organizations (e.g. National Initiative for Cybersecurity Education and National Institute of Standards and Technology)

Capacity Building and Sustainability

Through the program activities, WCCCD established a cybersecurity program that staff will continue after the grant ends. Staff expect the program courses will still be offered and will continue to use the same instructional approach. However, they expect to make refinements to respond to emerging industry needs and continue to optimize the courses for students. Staff plan to continue to increase the number of employers they work with and expand the role of industry partners in program implementation and recruitment of incumbent workers into their programs in both short-term workshops and their regular courses.

The preface above describes the many capacity building activities that Generation Cyber engaged in during the grant, such as the development of partnerships, labs and training technology, and curriculum; faculty training, and outreach to build awareness of what their training program offered. As a result, they established the capacity to offer cybersecurity training to their local area, and expect to have a valuable impact in the long-term in addressing regional needs for a trained cybersecurity workforce.

> "We're going to continue working with them on helping them to provide soft skills to their students and helping to place them."
>
> – Industry partner

Program Outcomes

Training Outcomes

At the time this report was developed, students had only been enrolled in the program for less than two years, so findings on student training outcomes are still preliminary. However, the findings share some early trends based on the data available. According to the college's administrative data, within the nearly two years since the program started enrolling students, 17 had attempted to earn a 3rd party certification (14%), and 16 of those had earned a 3rd party certifications, showing that almost all of those who attempted 3rd party certifications were able to obtain them. One student had also earned an associate degree, however, given how the program had begun enrolling students less than two years ago, there had not been much time for students to earn the degree. Highlighting the short- and longer-term options available to students, by the end of the grant, the college had some students who had completed all 5 new cybersecurity courses (10%, n=13), while most had completed one (40%, n=50) or two (22%, n=27) courses.

Employment Outcomes

For this report, we did not have quantitative data on employment outcomes, such as the number of students employed. However, through the stakeholder interviews, we gathered qualitative information on how the program prepared students for employment and a successful career pathway. The students interviewed spoke highly of the skills developed in the program, their job prospects, and their opportunities for advancement within the field. In general, they believed they would not have issues finding a job, although they expressed concern about their lack of experience. Similarly, staff and faculty described how there was a misalignment between the training provided and the qualifications for entry level cybersecurity jobs. Most entry level cybersecurity jobs required not only certification, but also a bachelor's degree and multiple years of experience. While the cybersecurity program gave them desirable skill sets and certifications and prepared them for jobs, it was difficult for the WCCCD students to obtain a job in cybersecurity, specifically. Overall, instructors reported that they tried to emphasize to their students that this program is a pathway that provides a strong foundation in cybersecurity skills, and students should develop their own path and pursue opportunities within the field.

CONCLUSION

Summary of Findings

The evaluation gathered data to understand the implementation of Generation Cyber and its outcomes, based on information available at the time of the evaluation.

Implementation Findings

The evaluation described how the program developed and changed over the grant period, successes and challenges to program implementation, and institutional capacity building. This section summarizes a few overall trends.

- Generation Cyber implemented most of the expected components of their program model, such as lab-based and multi-mode instruction, stacked credentials, multiple educational pathways, partnership engagement, and providing career and training supports for students. There were a few changes made to the program, which were designed to better meet the needs of its students. For example, Generation Cyber removed a baseline screening assessment, since students already could demonstrate their preparedness through taking prerequisite courses. In addition, the program broadened its target population to include community college students at large, and also found they had been successful in recruiting women and older adults.

- There were multiple external challenges that affected program implementation. For example, the program had delays in getting their curriculum and equipment orders approved, which lengthened the time until the courses could be launched. In addition, recruitment was affected by students' concerns about the costs of courses and uncertainties about whether financial aid would cover them. Throughout the grant, the program responded to these and other challenges by adapting the program model and working with internal and external partners to make ongoing progress with program implementation.

- Generation Cyber developed a cybersecurity program at their college that was sustainable beyond the grant period. Staff planned to continue to offer the courses and use the cyber labs developed during the grant, and also continue to conduct cyber awareness workshops for incumbent workers. In the future, they plan to expand their work with industry partners, and update the curriculum over time to align with emerging technological innovations in the cybersecurity field.

Outcome Findings

The evaluation captured initial trends on student training outcomes from college administrative data, along with stakeholder perspectives on employment outcomes and associated contextual factors. However, as noted above, it was too early at the time of the evaluation to fully assess the program's effects on student employment, given the short time that the program had been implemented.

- While the majority of students completed one or two cybersecurity courses, some completed all five. Almost all of the students who attempted to earn a 3rd party certification were able to do so, and one student earned an associate degree.

- Staff found that while they were training students with the skills and certifications that would prepare them for cybersecurity jobs, many companies limited hiring for entry level jobs to those who had a Bachelor's degree and multiple years of experience. Staff started actively working with partners to figure out how to solve the misalignment between the demand for a cybersecurity workforce with these hiring restrictions. Regardless, staff and faculty shared success stories of students who had been able to find employment and start a career pathway that would build on their cybersecurity training.

Implications for Workforce Training Initiatives

The evaluation provides several implications for other workforce training initiatives, particularly in the cybersecurity area.

- **A dynamic program model is essential when training students for a field changing as rapidly as cybersecurity.** In cybersecurity, there are new developments every few months, which can require teaching different strategies and using the latest software to make sure students are armed with the most up-to-date skills. However, making the necessary adaptations over time requires significant investments in time and funding to be able to purchase equipment and undergo the curriculum approval processes. Program administrators and funders should recognize the need to build in time for the program development process, and should also focus on effectively coordinating to move the project forward.

- **Cybersecurity training potentially benefits a wide range of adults, including those who are new to the field and longer term incumbent workers.** The college found that to recruit students, they needed to broaden their focus to different audiences who were interested and would benefit from the training, such as community college students, incumbent workers, and older adults.

- **Engaging internal and external partners is important at all stages of program development.** Generation Cyber found they needed to interface and leverage multiple departments in their college, for example, to purchase equipment and meet the grant reporting requirements. They also described different ways that industry partners had contributed to the program such as designing the labs, providing input on the curriculum, teaching students about career opportunities, connecting students to career opportunities, and doing outreach for the program in the field.

APPENDIX A: WCCCD Logic Model

Wayne County Community College District (WCCCD) Generation Cyber Logic Model: Developed in 2015

INPUTS

PROGRAM AND PARTNERS

- U.S. DOL (TAACCCT funding)
- WCCCD current and new faculty
- Cybersecurity steering committee
- Michigan Economic Development Corporation
- Detroit Employment Solutions Corp.
- Southeast Michigan Community Alliance

PROGRAM RESOURCES

- New technology
- New and existing WCCCD courses
- Learning communities

PROGRAM PARTICIPANTS

- U.S. veterans
- TAA-eligible workers
- Dislocated workers

ACTIVITIES

PROGRAM AND PARTNERSHIP DEVELOPMENT

- Industry-oriented curricula review and feedback by Advisory Council
- Training and employment opportunities by employer partners

DEGREE/ CERTIFICATE PROGRAM

- Multi-modal, competency-based curricula with at-home scenario labs
  - Initial assessment leads to foundation classes or new curricula
- Cyber Certificate
- Cyber AA Degree
- Third Party Certifications/Stackable & Latticed Credentials

OUTPUTS

IMPROVEMENTS

- More credentialed students
- More students enrolled in higher education
- Higher employment and retention after completing TAACCCT
- Higher wages for those already employed upon enrollment
- More sector-based partnerships

SHORT-TERM OUTCOMES

PROGRAM AND PARTNERS

- More qualified cybersecurity workers
- Improved programming
  - Faculty recruitment and training
  - Evidence-based curricula
  - Industry partnerships

PROGRAM PARTICIPANTS

- Increased cybersecurity skills and certifications
- Competitive in job market

INTERMEDIATE OUTCOMES

PROGRAM AND PARTNERS

- WCCCD has sustained curriculum, supported faculty, and Associate degree program
- Employers have more satisfaction with workforce
- Best practices for training and TAA curriculum are being used

PROGRAM GRADUATES

- Pursue higher education and training
- Improve employment and job retention rates
- Increase earnings and benefits

LONG-TERM OUTCOMES

PROGRAM AND PARTNERS

- Employers know WCCCD is a reliable resource for workforce pipeline
- Detroit has a stronger cybersecurity field and more institutional collaboration

PROGRAM GRADUATES

- Sustainable and transferrable skills
- Increased quality of life and financial self-sufficiency

CONTEXT: The Detroit Metropolitan area has high unemployment (7.9% in April 2014), together with a high number of TAA certifications (218 in Detroit) and workers, a changing industry landscape, and a labor supply that lacks the skills and education needed to successfully gain and retain employment in the current landscape of job opportunities. Local workforce development agencies and employers have identified a demand for trained and educated Cybersecurity workers in the Detroit region. WCCCD has been funded by DOL to develop training and pathways leading to industry-recognized credentials in the high-demand field of cybersecurity in the Detroit region.

ASSUMPTIONS: The Wayne County Generation Cyber (WCGC) program will focus its efforts on developing knowledge, skills, and abilities for *two* of the seven National Cybersecurity Workforce Framework occupational categories: Securely Provision and Operate and Maintain. Evidence-based strategies in the design of the program includes an emphasis on Competency Assessment tied to Aptitudes, Pathways and Competencies which links aptitude and prior experience to success in the WCGC program and in the field of cybersecurity. The program is expected to also build the institution's capacity, enabling WCCCD to train existing faculty, hire new staff and faculty, secure new technology resources, launch an Associate degree program in cybersecurity, and strengthen partnerships within the local cybersecurity sector.

APPENDIX B: WCCCD Generation Cyber Interview Protocols: Year 4

Project Manager Interview Facilitation Guide

My name is {introduce self and note-taker}. We are from ICF, a team that is evaluating the Wayne County Generation Cyber program.

As you may know, the program is training students to gain employment in the growing IT and cybersecurity industry. We are studying how the program is helping students achieve certifications and certificates, get and retain jobs, and how the program has been implemented at the college. Today, we want to learn about your role in the program, your perspective on how the program is working. We have a few questions and expect it will take about 30-45 minutes to go through them.

I'll be asking you questions and {note taker name} is here to take notes on our conversation. To help us take notes today, we would like to record our interview, would that be ok with you? (yes or no)

Before we begin, we want to remind you that your participation in this interview is voluntary and the information you share with us will be kept confidential. Specifically, this means that:

1. you can decline to answer any questions, or stop at any time;
2. we will not connect your name with what was said any written reports; and
3. only evaluation staff will have access to the interview data.

In our reports, we will only provide overviews or anecdotes from any interviews we conduct with faculty and staff, thus your interview will be a part of a larger dataset. At no time will we report or present the information you share with us in any form that will identify you specifically.

Interview Questions:

Program Structure and Development

1. Please describe your current role in the grant. Has it changed over the last year? If so, how?
   Probe: Think about your role working with:
   - Advisory board
   - Workforce partners (e.g., WIBs)
   - Staff
   - Instructors
   - Employers

2. Looking at the current list of courses from the materials we sent you, have there been any changes to the program offerings?
   - In the past year, have there been any changes to the curricula?
   - If there were changes in the curricula, how were they selected and developed? Why did these changes occur?
3. Tell me about the process used to monitor the program and make any necessary mid-course corrections.
4. How are you assessing student abilities before they enter the program?
5. Can you describe how the program is currently monitoring student performance and whether this has changed since last year?
   - Student readiness to take certification exams?
   - Student readiness for the work environment?
   - Course completion and certificates earned?
   - Post-employment outcomes?
6. Please describe your work with outside partners, such as those in the industry.
   - What role did those partners play in your program's development and implementation?

Sustainability

7. Has your program been discussing plans for sustaining the program after the grant ends? If so, how?
8. Will any of the following program elements likely be sustained? How?
   - Recruitment and intake processes
   - Courses offered and curriculum
   - Instructional methods, including online and technology-enabled learning
   - Credentials offered
   - Career and academic support services
   - Partnerships with industry and others
9. During the course of the TAACCCT grant, were there any changes to policy or practice at your college as a result of your program? If so, please describe.
10. Have you, or are you planning to pursue new sources of funding to sustain your program? Have you secured new funding? Which sources are you pursing/have secured?
11. Have you established organizational buy-in, for example from college leadership, to sustain your program?
12. After the grant ends, will you have sufficient personnel, such as staff, instructors, and [if applicable] partners, to continue to operate the program effectively? Please describe.
13. What will be the most important factors in allowing you to sustain the program? What challenges do you anticipate if any?

14. How likely is your district going to try to scale your program? Beyond your district? Please describe.

Overall Assessment

15. How are you feeling about the grant right now?
    - With which areas are you most pleased?
    - What are your biggest concerns?
    - What are the biggest challenges?
16. How do you feel your program has helped participants' employment outcomes, such as career readiness and employment, and wage increases? Please describe.
17. Do you have any example success stories to share about a participant in your program?

Outcomes & Data Specialist Interview Facilitation Guide

My name is {introduce self and note-taker}. We are from ICF, a team that is evaluating the Wayne County Generation Cyber program. As you may know, the program is training students to gain employment in the growing IT and cybersecurity industry. We are studying how the program is helping students achieve certifications and certificates, get and retain jobs, and how the program has been implemented at the college. Today, we want to learn about your role in the program and your perspective on how the program is working. We have a few questions and expect it will take about 30 minutes to go through them.

I'll be asking you questions and {note taker name} is here to take notes on our conversation. To help us take notes today, we would like to record our interview, would that be ok with you? (yes or no)

Before we begin, we want to remind you that your participation in this interview is voluntary and the information you share with us will be kept confidential. Specifically, this means that

1. you can decline to answer any questions, or leave at any time;
2. we will not connect your name with what was said any written reports; and
3. only evaluation staff will have access to the interview data.

In our reports, we will only provide overviews or anecdotes from the interviews, thus the interviews are will be connected to other data; however, we will not report or present the information you share with us in any way that will identify you specifically.

Interview Questions:

1. Has your role evolved over the last year? If so, how?
2. Are you receiving the resources and supports you need to conduct your role?
   - Are there any that you were receiving that you are not currently?
   - Are there any that are new this year that you were not receiving previously?
3. Can you describe how you are monitoring student academic performance through the academic year?
   - Student readiness to take certification exams?
   - Student readiness for the work environment?
   - How often do you track students' progress in the program?
   - What aspects of the data tracking systems/ processes work well?
   - What challenges have you had with tracking student progress?
   - What changes have you made to the program based on the data?
4. Describe how you are using data or information from the employer partners to make program improvements. Has that changes since last year? If so, how?

Overall Assessment

5. How are you feeling about the grant right now?
   - With which areas are you most pleased?
   - What are your biggest concerns?
   - What are the biggest challenges?
6. How do you feel your program has helped participants' employment outcomes, such as career readiness and employment, and wage increases? Please describe.
7. Do you have any example success stories to share about a participant in your program?

Wayne County Generation Cyber Program Completion and Retention Coach Interview Facilitation Guide

My name is {introduce self and note-taker}. We are from ICF, a team that is evaluating the Wayne County Generation Cyber program. As you may know, the program is training students to gain employment in the growing IT and cybersecurity industry in Wayne County. We are studying how the program is helping students achieve certifications and certificates, get and retain jobs, and how the program has been implemented at the college. Today, we want to learn about your role in the program, your perspective on how the program is working. We have a few questions and expect it will take about 30 minutes to go through them.

I'll be asking you questions and {note taker name} is here to take notes on our conversation. To help us take notes today, we would like to record our interview, would that be ok with you? (yes or no)

Before we begin, we want to remind you that your participation in this interview is voluntary and the information you share with us will be kept confidential. Specifically, this means that:

1. you can decline to answer any questions, or leave at any time;
2. we will not connect your name with what was said any written reports; and
3. only evaluation staff will have access to the interview data.

In our reports, we will only provide overviews or anecdotes from the interviews, thus the interviews are will be connected to other data; however, we will not report or present the information you share with us in any way that will identify you specifically.

Interview Questions:

1. What is your current role in the program?
   - Has your role evolved over the last year? If so, how?
2. Can you describe how you are monitoring student performance through the academic year?
   - E.g. their readiness to take certification exams?
   - Their readiness for the work environment?
3. In your interactions with students, are there any common challenges that seem to arise across the cohort?
   - How have you been able to help students overcome those challenges?
   - Are there any other supports you think students need? If so, what supports?
4. [If applicable] Please describe your work with outside partners, such as those in the industry.
   - What role did those partners play in your program development and implementation?
5. Are you involved in discussions about sustaining the program after the TAACCCT grant ends? [if no, skip the next question.]

6. Will any of the following program elements be sustained? If yes, how?
   - Recruitment and intake processes
   - Courses offered and curriculum
   - Instructional methods, including online and technology-enabled learning
   - Credentials offered
   - Career and academic support services
   - Partnerships with industry and others

Overall Assessment

7. How are you feeling about the grant right now?
   - With which areas are you most pleased?
   - What are your biggest concerns?
   - What are the biggest challenges?
8. How do you feel your program has helped participants' employment outcomes, such as career readiness and employment, and wage increases? Please describe.
9. Do you have any example success stories to share about a participant in your program?

Curriculum-Related Faculty Interview Guide

My name is {introduce self and note-taker}. We are from ICF, a team that is evaluating the Wayne County Generation Cyber program. As you may know, the program is training students to gain employment in the growing IT and cybersecurity industry in Wayne County. We are studying how the program is helping students achieve certifications and certificates, get and retain jobs, and how the program has been implemented at the college. Today, we want to learn about your role in the program, your perspective on how the program is working. We have a few questions and expect it will take about 30 minutes to go through them.

I'll be asking you questions and {note taker name} is here to take notes on our conversation. To help us take notes today, we would like to record our interview, would that be ok with you? (yes or no)

Before we begin, we want to remind you that your participation in this interview is voluntary and the information you share with us will be kept confidential. Specifically, this means that:

1. you can decline to answer any questions, or leave at any time;
2. we will not connect your name with what was said any written reports; and
3. only evaluation staff will have access to the interview data.

In our reports, we will only provide overviews or anecdotes from the interviews, thus the interviews are will be connected to other data; however, we will not report or present the information you share with us in any way that will identify you specifically.

Interview Questions:

1. What courses do you teach?
   - What are your responsibilities in the Cybersecurity program?
2. Have you been involved in any developments to the course over the past year?
   - How have the curricula themselves evolved, if at all?
   - Why have these changes been made? Probe: For example, did the curriculum change to align with industry standards?
3. How did the program determine students' abilities before entering the program?
4. What tools do you use to assess student learning and performance? Are these the same tools you used last year?
5. [If applicable] Please describe your work with outside partners, such as those in the industry.
   - What role did those partners play in your program's development and implementation?
6. How well do you think the course is preparing students to work in the cybersecurity sector?
   - How do you think the course is preparing students for certifications?
   - What aspects of the class are exposing them to the work environment/on-the-job challenges?

7. Are you involved in discussions about sustaining the program after the TAACCCT grant ends? [if no, skip the next question.]
8. Will any of the following program elements be sustained? If yes, how?
   - Recruitment and intake processes
   - Courses offered and curriculum
   - Instructional methods, including online and technology-enabled learning
   - Credentials offered
   - Career and academic support services
   - Partnerships with industry and others

Overall Assessment

9. How are you feeling about the grant right now?
   - With which areas are you most pleased?
   - What are your biggest concerns?
   - What are the biggest challenges?
10. Do you have any example success stories to share about a participant in your program?

Student Focus Group Moderator's Guide

My name is {introduce self and note-taker}. We are from ICF, a team that is evaluating the Wayne County Generation Cyber program. As you may know, the program is training students to gain employment in the growing IT and cybersecurity industry. We are studying how the program is helping students achieve certifications and certificates, get and retain jobs, and how the program has been implemented at the college. A focus group is a discussion that involves us asking you for your opinions about a program. The focus group will last one hour. We appreciate you taking time to assist with this evaluation because your input on how this program works is important. Today, we want to hear your opinions on the program, how it is working, what is working well, and what you think might need to change.

Before we begin, we want to remind you that your participation in this focus group is voluntary and the information you share with us will be kept confidential. Specifically, this means that:

1. you can decline to answer any questions, or leave at any time;
2. we will not connect your name with what was said any written reports; and
3. only evaluation staff will have access to the interview data.

There will be no penalty or repercussions for what you or others share in this focus group. In our evaluation reports we will only provide overviews of what was learned and will connect anecdotes to other data we have collected. We will not report or present the information you share with us in any way that will identify a specific person.

As a reminder, as you agreed to during the focus group recruitment process, the focus group will be recorded for research purposes. This recording will not be shared with Wayne County staff or faculty. If you no longer want to be recorded, you are free to leave the session at this time.

Focus Group Facilitation Rules

What we discuss today is private. We ask that you don't talk about what was said here today outside of this room. That includes not sharing information about what you said, or what others said.

To help the focus group work, we would like to ask each of you to:

1. During the focus group, use your first names only when necessary.
2. Be respectful of other participants and the facilitators. This includes being respectful about not sharing outside of this room without the participant's permission.
3. Fully participate to the best of your abilities by sharing your expertise and experiences with your peers.
4. Ask questions and make suggestions that will help everyone.
5. Turn off cell phones and/or pagers or place them on vibrate.

Questions

1. What first attracted you to the WCGC training?
   - How did you learn about WCGC (e.g., flyer, word of mouth, local workforce agency or One-Stop Center, Recruitment Specialist, or other)?
2. Once you heard about the program, what did you have to do to enroll (e.g., complete an application process, take assessment tests, be interviewed)?
   - What did you like? What didn't you like (for each stage)?
3. How do you like your training classes so far?
   - How do you find the pace of classes? (too fast, too slow, just right)
   - Are the classes appropriate in terms of: i) the times they are offered, ii) length, iii) location, and iv) resources available?
4. How do you like the different methods used to teach you about cybersecurity (e.g., the use of web technology, hands on learning, game technology)?
   - What do you like or dislike about each of these methods?
   - Is there anything you think should change?
5. What do you think about the quality of the classes?
   - How do you find the instructors?
     - Are they knowledgeable in cybersecurity topics?
     - Are they prepared to teach the material and able to convey their knowledge to you?
   - What do you think of the course materials and curricula?
   - Are there any other resources you might need to be successful?
6. Are the classes increasing your knowledge of cybersecurity?
   - Do you think what you are learning will help you pass 3rd party certifications?
   - Do you think you will be able to apply the knowledge learned in the real world or work environment?
   - Do you plan to complete the Wayne County cybersecurity certificate? If no, why not?
7. Have you received individual coaching, tutoring, or career and job placement services?
   - How often have you used these services?
   - How were they helpful?
8. What types of challenges have you had with the training?
   - Have you needed any other services (e.g., childcare, transportation assistance)?
9. Overall, are you satisfied with the WCGC program thus far?
   - How do you think it will help you?
   - If there is anything you could change, what would it be?

Employer Partner Interview Guide

My name is [introduce self and note-taker]. We are from ICF International, a team that is evaluating the Wayne County Generation Cyber program. As you may know, the program is training students to gain employment in the growing IT and cybersecurity industry. We are studying how the program is helping students achieve certifications and certificates, get and retain jobs, and how the program has been implemented at the college. Today, we want to learn about your role in the program, your perspective on how the program is working. We have a few questions and expect it will take about 30 minutes to go through them.

I'll be asking you questions and {note taker name} is here to take notes on our conversation. To help us take notes today, we would like to record our interview, would that be ok with you? (yes or no)

Before we begin, we want to remind you that your participation in this interview is voluntary and the information you share with us will be kept confidential. Specifically, this means that:

1. you can decline to answer any questions, or leave at any time;
2. we will not connect your name with what was said any written reports; and
3. only evaluation staff will have access to the interview data.

In our reports, we will only provide overviews or anecdotes from the interviews, thus the interviews are will be connected to other data; however, we will not report or present the information you share with us in any way that will identify you specifically.

Interview Questions

1. Can you briefly describe your company and the kind of work you do?
2. Will you continue to partner with WCCCD after the end of the grant? If so, in what capacity?
3. How did you hear about WCGC?
   - What interested you about the program?
4. What got you or your company involved in the program initially?
   - What has your role been?
   - How long have you been involved?
5. How you have been involved with the WCGC program?
   - Have you been involved with any of the following: program design; curriculum development; recruitment; training; placement; or program management?
   - How satisfied are you with your experience as a grant partner (for example, are you dissatisfied, somewhat satisfied, satisfied)?
     - Please explain.

6. Do you think the students exiting from the Generation Cyber Program will be well prepared for work in the cybersecurity field? What about for your company specifically?
7. Are you employing or do you plan to employ graduates of the Generation Cyber Program?
   - If yes, how big a factor did/will holding a cybersecurity from WCCCD be in your hiring decision?
   - What other factors will you screen for?
   - If currently employing, how are they performing?
   - If currently employing, are there any additional skills that they need to develop?
8. Is there anything additional that WCCCD should do or should have done in working with employer partners to design and implement a cybersecurity program that creates graduates that are prepared to fill in-demand jobs in the cybersecurity?
9. Is there anything else you might want to share about the program or your experience as a partner?

Advisory Group Interview Guide

My name is {introduce self and note-taker}. We are from ICF International, a team that is evaluating the Wayne County Generation Cyber program. As you may know, the program is training students to gain employment in the growing IT and cybersecurity industry. We are studying how the program is helping students achieve certifications and certificates, get and retain jobs, and how the program has been implemented at the college. Today, we want to learn about your role in the program, your perspective on how the program is working. We have a few questions and expect it will take about 30 minutes to go through them.

I'll be asking you questions and {note taker name} is here to take notes on our conversation. To help us take notes today, we would like to record our interview, would that be ok with you? (yes or no)

Before we begin, we want to remind you that your participation in this interview is voluntary and the information you share with us will be kept confidential. Specifically, this means that:

1. you can decline to answer any questions, or leave at any time;
2. we will not connect your name with what was said any written reports; and
3. only evaluation staff will have access to the interview data.

In our reports, we will only provide overviews or anecdotes from the interviews, thus the interviews are will be connected to other data; however, we will not report or present the information you share with us in any way that will identify you specifically.

Interview Questions

1. Can you briefly describe the role of the advisory board in the development and implementation of the WCGC program? (always asked during first interview with new member)
   - When did you get involved with the advisory board?
   - What is your role on the board?
2. How do you see the role of the advisory group after the grant comes to an end? Will it be sustained?
3. How do you think the program performed this year?
   - What worked well/ what may need to change?
4. Tell me about what mechanisms are used to inform the advisory group about the program's implementation, process, and outcomes.
   - What works?
   - What are the challenges?
   - How can it be improved?

5. How are you feeling about the grant right now?
   - With which areas are you most pleased?
   - What are your biggest concerns?
6. Are there any other changes you think need to be made to the program?
   - Are there any areas of the program that need additional attention?

APPENDIX C: Baseline Survey

WCCCD TAACCCT Student Baseline Survey

The Wayne County Community College District has been awarded a Trade Adjustment

Assistance Community College and Career Training (TAACCCT) grant from the U.S. Department of Labor (USDOL) to implement a cybersecurity training program.

As part of the grant requirements, a third party, ICF, is evaluating the Wayne County Generation Cyber (WCGC) program. As part of that evaluation, you are being asked to voluntarily complete this survey to help the college understand how the program is working and how it compares to other programs offered by the college. Your responses to this survey will help WCCCD as well as the Department of Labor learn more about students who are participating in this program and similar programs.

Your participation in this survey is voluntary and the information you share with us will be kept confidential and protected to the extent allowed by law. Specifically, this means that

1. you can decline to answer any questions, or discontinue the survey at any time;
2. we will not connect your name with what was said in any written reports; and
3. we will take all possible measures to ensure that only evaluation staff will have access to the data.

If you have any questions about your rights as a participant in the evaluation, please contact the ICF, Institutional Review Board (IRB) at IRB@icf.com.

If you have questions about the study or surveys, please contact ICF at WCCCDTAACCCTeval@icf.com.

Consent

Please indicate if you agree to participate in the evaluation and this survey.

- ○ Yes, I agree to complete this survey as a part of this evaluation
- ○ No, I do not want to participate in the survey

Generation Cyber

1. Is this your first semester in the Cybersecurity program?

   ○ Yes ○ No

2. Please provide us your full name: _____

3. Which Cybersecurity courses have you already taken?_____

_____

4. At which campus are you enrolled in your Cyber courses for your program?

- ○ Downtown campus
- ○ Downriver Campus
- ○ Eastern Campus
- ○ Western campus
- ○ Mary Ellen Stempfle University Center
- ○ Northwest

5. Before enrolling in the Wayne County Generation Cyber (WCGC) program, did you take the Llobet Reasoning Test (LRT)?

- ○ Yes, enrolled after the first or second attempt at the LRT
- ○ No, enrolled after taking the logic and reasoning course
- ○ No, took CIS 110 & CIS 240
- ○ I don't know/don't remember

Enrollment

6. What degree/certificate program are you enrolled in at WCCCD?

- ○ Complete an associate degree
- ○ Complete a 1 year certificate
- ○ Complete a short term certificate

7. What are your goals for participating in the Cybersecurity program?
(Please select all that apply)

- ○ Improve work skills
- ○ Obtain a promotion
- ○ Start a new career
- ○ Get a job

8. How did you hear about this program?

- ○ TechExpo career fair
- ○ Workforce Investment Board– WIA
- ○ Friend/ Relative/ Acquaintance
- ○ Job fair
- ○ Educational fair
- ○ WCCCD

9. Which of the following was true for you at the time you first entered this college?

- ○ Entered directly from high school
- ○ Entered after working for a period of time (excluding summer work)
- ○ Transferred from another 2-year college
- ○ Transferred from a 4-year college or university
- ○ Entered after completing military service
- ○ Other

Education

10. On the scale below please indicate your CURRENT knowledge/ability.

	Very weak	Weak	Strong	Very strong	N/A
My understanding of the subject matter of my coursework.	○	○	○	○	○
My ability to pass a test demonstrating my understanding of the subject matter	○	○	○	○	○
My ability to apply the concepts of my coursework to a real world problem or situation	○	○	○	○	○

11. What is the highest degree or level of school you have completed? (If currently enrolled, mark the last grade or highest degree received)

- ○ Less than high school, no diploma
- ○ High school graduate - high school diploma or the equivalent (for example: GED)
- ○ Some college credit, no degree
- ○ Associate degree (for example: AA, AS)
- ○ Bachelor's degree or higher (for example: BA, AB, BS, MS)

12. Do you hold any vocational, technical or professional certifications or licenses?

    [A professional certification or license shows you are qualified to perform a specific job and includes things like: Licensed Realtor, Certified Medical Assistant, Certified Construction Manager, a Project Management Professional, or PMP certification, or an IT Certification.]

    - ○ Yes, I hold a Vocational, Technical, or Trade School Diploma/Certification or Professional license
    - ○ No, I do not hold any vocational, technical or professional certifications or licenses

Certifications

Please tell us about the other certifications or licenses you have already acquired.

[A professional certification or license shows you are qualified to perform a specific job and includes things like Licensed Realtor, Certified Medical Assistant, Certified Construction Manager, a Project Management Professional, or PMP certification, or an IT Certification.]

13. In what field of study did you earn this certification? _____

14. Who awarded you this certification or license?

    - ○ Federal government
    - ○ State government
    - ○ Local government
    - ○ Industry
    - ○ Business, company, or nonprofit organization
    - ○ Professional association

15. During the intake process for your current program of study, did you take any prior learning assessments to earn credentials/credits for previous certifications you may have earned or to test out of a class?

    [A prior learning assessment would be a placement test or proof of certification to determine whether you have existing knowledge or a previously earned certification in a specific subject]

    ○ Yes ○ No

    If yes, please state credentials/credits earned:

    _____

Employment Experience

16. In what industry do you have the most experience either through work or volunteering? (Please select one)

- ○ Management, business, financial
- ○ Computer and information systems
- ○ Mathematical, architectural, and engineering
- ○ Retail Services
- ○ Community and social services
- ○ Legal, Education, training and library
- ○ Arts, design, entertainment, sports, and media
- ○ Food preparation and serving
- ○ Personal care, and service
- ○ Other (please specify): _____
- ○ Sales, office, and administrative support
- ○ Farming, fishing, and forestry
- ○ Construction and extraction
- ○ Installation, maintenance, and repair
- ○ Manufacturing (e.g. automotive)
- ○ Healthcare
- ○ Protective services
- ○ Production and manufacturing
- ○ Transportation and material moving
- ○ Military

17. How many years of experience do you have in the industry you chose in the previous question?

Number of years: _____

18. Have you ever held a paying job?

○ Yes ○ No

Employment

19. What was your employment status when you signed up for this class? (please select all that apply)

- ○ Employed full-time for wages, for yourself or an employer (for 30 hours or more)
- ○ Employed part-time for wages for yourself or an employer (for less than 30 hours)
- ○ Homemaker
- ○ Full time Student
- ○ Out of work and looking for work
- ○ Out of work but not currently looking for work
- ○ Retired
- ○ Unable to work

Current Employment

20. Were you working in the cyber security field?

    ○ Yes ○ No

21. What is the name of your employer? _____

22. Please describe your job. _____

    _____

23. How much did you earn when you signed up for this course?

    Annual salary: _____

    Average hourly wage: _____

    Average hours worked per week: _____

24. How long have you worked with this job?

    Years: _____

    Months: _____

Previous Employment

25. Were you previously employed?

    ○ Yes ○ No

26. If you are currently unemployed, why did your last job end? _____

    _____

27. Please indicate on the scale to what extent any of the following circumstances affect your ability to secure and maintain employment.

	To no extent	To a little extent	To a moderate extent	To a large extent	N/A
Poor health (e.g. physical health, mental health/stress)	○	○	○	○	○
Inadequate childcare	○	○	○	○	○
Inadequate resources to care for a sick or elder family member	○	○	○	○	○
Inadequate housing	○	○	○	○	○
Lack of transportation (personal vehicle or no accessible public transportation)	○	○	○	○	○
Layoff or employer terminated	○	○	○	○	○
Criminal history	○	○	○	○	○
Lack of technical skills	○	○	○	○	○
Lack of relevant work experience	○	○	○	○	○
Other (please specify)					

Demographics

28. What is your sex?

- ○ Male
- ○ Female
- ○ Do not wish to disclose

29. What is your date of birth?

Month: _____

Year: _____

30. Are you of Hispanic or Latino origin? (Please select all that apply)

- ○ No, not of Hispanic or Latino origin
- ○ Yes, Mexican, Mexican American, or Chicano origin
- ○ Yes, Puerto Rican
- ○ Yes, Cuban
- ○ Do not wish to disclose
- ○ Yes, another Hispanic, Latino, or Spanish origin - Print origin, for example, Argentinean, Colombian, Dominican, Nicaraguan, Salvadorian, Spaniard, and so on: _____

31. Are you any of these races or ethnicities?

- ○ White
- ○ Black, African Am., or Negro
- ○ American Indian or Alaska Native Asian Indian
- ○ Japanese
- ○ Native
- ○ Hawaiian
- ○ Chinese
- ○ Korean
- ○ Guamanian or Chamorro
- ○ Filipino
- ○ Vietnamese
- ○ Samoan
- ○ Other Asian
- ○ Other Pacific Islander
- ○ Do not wish to disclose
- ○ Other (please specify): _____

32. Do you have a disability?

(A disability is a physical or mental impairment that limits one or more major life functions.)

- ○ Yes
- ○ No
- ○ Do not wish to disclose

33. What is your marital status?

- ○ Now married
- ○ Domestic Partnership
- ○ Widowed
- ○ Divorced
- ○ Separated
- ○ Never married
- ○ Do not wish to disclose
- ○ Other (please specify): _____

34. Have you ever served on active duty in the U.S. Armed Forces, Reserves, or National Guard?

- ○ Never served in the military
- ○ Only on active duty for training in the Reserves or National Guard
- ○ Now on active duty
- ○ On active duty in the past but not now
- ○ Do not wish to disclose

35. Do you have a VA-service connected disability rating?

- ○ Yes
- ○ No
- ○ Do not wish to disclose

36. What is your service-connected disability rating?

- ○ 0 percent
- ○ 10 or 20 percent
- ○ 30 or 40 percent
- ○ 50 or 60 percent
- ○ 70 percent or higher
- ○ Do not wish to disclose

Thank you - can we contact you again?

The survey is now complete. Thank you for your participation. Your thoughts and answers will help us better understand the Wayne County Community College District's training programs.

In order for us to collect additional meaningful data that will help us achieve the goals of this evaluation, we would like to be able to follow up with you in the future. At that time, we will provide you with another consent form, where you can indicate your decision to continue participating in the evaluation and complete another survey.

If you agree to be contacted again, please provide your contact information below so that we can follow up with you in a few months' time.

37. *Do you agree to be contact for future data collections?

○ Yes ○ No

38. If you agree to be contacted again, please provide your contact information:

Name: _____

Address: _____

Best Phone Number: _____

Email Address: _____

Thank you!

Thank you for completing this survey. We appreciate your time.

About ICF

ICF (NASDAQ:ICFI) is a global consulting and technology services provider with more than 5,000 professionals focused on making big things possible for our clients. We are business analysts, policy specialists, technologists, researchers, digital strategists, social scientists and creatives. Government and commercial clients have worked with ICF to overcome their toughest challenges on issues that matter profoundly to their success.