PACIFIC
Research & Evaluation, LLC

Final Evaluation Report

Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant: Round 2

CyberSecurity Career Pathways Program

Utah Valley University

Prepared by

Pacific Research and Evaluation, LLC
3507 SW Corbett Avenue
Portland, Oregon 97239

Date: September, 2016

Table of Contents

Executive Summary

TAACCCT Program/Intervention Description and Activities

The CyberSecurity Career Pathways Program at Utah Valley University (UVU) was funded through a $3 million, four-year Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant from the US Department of Labor (DOL). In 2009, the American Recovery and Reinvestment Act amended the Trade Act of 1974 to authorize the TAACCCT Grant Program. The CyberSecurity Career Pathways grant was awarded in October 2012 and, with a no-cost extension and institutional support, supported services through June 2016.

The Information Systems and Technology (IST) Department at UVU and its partners in industry and workforce services created the CyberSecurity Career Pathways program to address the lack of adequate CyberSecurity training in the region, the shortage of faculty and laboratory facilities at UVU to support cyber training, a lack of training in flexible modalities and delivery methods, and barriers to learning for TAA-eligible populations.

Three primary components of the CyberSecurity Career Pathways Program at UVU included: 1) The development or modification of CyberSecurity courses and programs, 2) The enhancement of student support services, and 3) The leveraging of relationships with local industry partners. The program was designed with multiple entry and exit points to employment. The following six credentials can be awarded and were either created or modified using grant funding: 1) Certificate of Proficiency in Information Technology, 2) Certificate of Completion in Network Administration, 3) Associate in Applied Science (AAS) in Information Systems and Technology, 4) Bachelor's of Science in Information Technology with an emphasis in Network Administration and Security, 5) Bachelor's of Science in Information Technology with an emphasis in Information Security Management, 6) Post-baccalaureate Graduate Certificate in CyberSecurity.

The support services that were enhanced through the CyberSecurity grant include the addition of an academic advisor dedicated at least half time to CyberSecurity students as well as mentors, tutors, and additional lab support. The program also provided support to students through funding to take industry certification tests. The CyberSecurity grant team engaged the Utah Department of Workforce Services (DWS) along with several local industry partners early in the grant process and fostered these relationships throughout the grant to create courses and programs that truly meet the needs of the local workforce and prepare students for immediate entry into CyberSecurity careers.

The majority of students served by the CyberSecurity Career Pathways grant were male (89.7%) and Caucasian (80.9%). The mean age of students was 28 at the time of enrollment, and just over half attended the programs full-time (56.7%). A total of 743 unique students were served during the first three years of the grant.

Evaluation Design Summary

UVU partnered with Pacific Research and Evaluation (PRE) to conduct the third party evaluation of the CyberSecurity Career Pathways program. PRE designed and executed a comprehensive plan for the implementation and impact evaluation components required by DOL and collected additional data to inform continuous program improvements throughout the life of the grant. The implementation evaluation focused on the initial assessment of the program plan and curriculum as well as an ongoing assessment of how the programs were implemented. The implementation evaluation addressed the following questions:

- Analyze the steps taken by the institution to create and run the training program.
- Assess the operational strengths and weaknesses of the project after implementation.
- How was curriculum selected, used, or created?
- How programs and program design were improved or expanded using grant funds?
- What delivery methods were offered?
- What was the program administrative structure?
- What support services and other services were offered?
- Did grantees conduct an in-depth assessment of participant's abilities, skill, and interests to select participants into grant programs?
- What assessment tools and process were used
- Who conducted the assessment?
- How the assessment results were used?
- Were assessment results useful in determining the appropriate program and course sequence for participants?
- Was career guidance provided and if so, through what methods?
- What contributions did each of the partners make in terms of: 1) Program Design, 2) Curriculum Development, 3) Recruitment, 4) Training, 5) Placement, 6) Program Management, 7) Leveraging of Resources, 8) Commitment to Program Sustainability?
- What factors contributed to partners' involvement or lack of involvement in the program?
- What contributions from partners were most critical to the success of the grant program?
- Which contributions from the partners had less of an impact?

The methods used to collect data to assess these formative evaluation questions included: Project Team Focus Group, Student Survey, Student Focus Group, Staff Focus Group, Staff Phone Interviews, Advisory Board Phone Interviews, Advisory Board Focus Group, and Quarterly Report Surveys.

The impact study utilized a historical comparison cohort method of evaluating TAACCCT program outcomes. PRE worked with the UVU Institutional Research department to obtain student outcome data for both the participant and comparison cohorts and worked with UVU to create a data request of DWS to provide PRE with the appropriate data for conducting the employment data analyses. The student cohorts were compared on the following outcomes: Program Completion, Retention in Program of Study, Credential(s) Earned, Wage Increase, Entered Employment, and Retained Employment.

Implementation Findings

The CyberSecurity Career Pathways program was created based on the needs of the industry which led to the close partnership between the university and an industry partner advisory board to help design the program and develop curriculum. The grant team at the university was assembled based on experience in grants management and CyberSecurity, and there was minimal turnover in grant team members over the course of the grant. The advisory board was a strength of the program throughout the course of the grant, and members included representatives from various local Information Technology organizations including Adobe, Spectra, and UtiliSec. The most crucial partner contributions related to program design and curriculum development, but advisory board members also played an important role in recruitment, training, placement, and commitment to program sustainability.

Support services and other services offered as part of the CyberSecurity Career Pathways program included student access to traditional advising services, as well as student mentoring and tutoring and funding for industry certification exams. Evaluation results showed that mentoring and tutoring services were beneficial to students but the team struggled to keep these positions staffed. In terms of career guidance, students had access to campus resources in addition to their professors, many of whom have experience working in the field of CyberSecurity. Students could also work with the advisor at DWS during the early stages of the grant but this position was eliminated in year three in lieu of an additional academic advisor for CyberSecurity students.

The CyberSecurity Career Pathways program had several operational strengths including strong partnerships with industry partners, sustainability of new credentials through the institution, and low turnover in the grant team. Operational weaknesses of the program included the length of time required for obtaining institutional approval and accreditation for the post-baccalaureate certificate and issues with advising services provided through the program.

Participant Impacts & Outcomes

Academic outcomes of participants showed that students in CyberSecurity programs often enrolled or had plans to enroll in further education, which may be related to the stackable nature of the credentials. In terms of employment outcomes, results showed both students and staff are confident that the CyberSecurity Career Pathways program is preparing students for employment in in the field of CyberSecurity upon exiting the program.

Results of the impact study showed positive results for CyberSecurity Career Pathways participants. Students in the grant program were significantly more likely to complete their academic program or be retained in their program of study than a historic comparison cohort, with nearly 65% of the treatment group completing or retained compared to less than 45% of the comparison cohort. The treatment group also had better employment outcomes than a comparison cohort, with 79.5% of incumbent workers receiving a wage increase, and 71.4% of those who entered employment after exiting the program staying employed three terms after exiting. These data show the CyberSecurity Career Pathways program is setting participants up for long-term employment success.

Conclusions

Although TAACCCT grant funding at UVU concluded in June 2016, PRE would like to offer the following insights regarding the continuation of the CyberSecurity credentials that were developed as part of the CyberSecurity Career Pathways TAACCCT grant. These insights are based solely on the data collected through the evaluation activities referenced in this report.

1. The student tutoring and mentoring positions for CyberSecurity students seemed to be beneficial to students involved in the CyberSecurity credentials. However, the university struggled to find and keep qualified students employed in this position throughout the grant period due to well-qualified students preferring higher paying, full-time positions. PRE encourages UVU to continue exploring models for supporting students enrolled in the CyberSecurity program. If there is an

option to offer academic credit for student tutoring and mentoring positions, this may be incentive for qualified students to offer this support.

2. The industry partner advisory board was a crucial part of the success of the CyberSecurity Career Pathways program. The evaluation teams recommends continuing to engage this group and hold advisory board meetings moving forward. This will allow the program to be current with the needs of the industry and possibly increase the number of local hires from the CyberSecurity program at UVU. The advisory board may also offer support for the development of the master's degree program.

3. A final insight regarding the CyberSecurity program at UVU is regarding the development of a master's degree program in CyberSecurity. The evaluation team heard feedback from stakeholders at various levels including students and staff that a master's degree would be beneficial for the region and utilized by large numbers of students. PRE recommends the university continue with plans to develop the master's program as it will be a valuable addition to the stackable credentials developed as part of the TAACCT grant.

Introduction

The CyberSecurity Career Pathways Program at Utah Valley University (UVU) was funded through a $3 million, four-year Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant from the US Department of Labor (DOL). In 2009, the American Recovery and Reinvestment Act amended the Trade Act of 1974 to authorize the TAACCCT Grant Program. On March 30, 2010, President Barack Obama signed the Health Care and Education Reconciliation Act, which included $2 billion over four years to fund the TAACCCT program.

TAACCCT provides community colleges and other eligible institutions of higher education with funds to expand and improve their ability to deliver education and career training programs that can be completed in two years or less, are suited for workers who are eligible for training under the TAA for Workers program, and prepare program participants for employment in high-wage, high-skill occupations. Through these multi-year grants, DOL is helping to ensure that our nation's institutions of higher education are helping adults succeed in acquiring the skills, degrees, and credentials needed for high-wage, high-skill employment while also meeting the needs of employers for skilled workers. DOL is implementing the TAACCCT program in partnership with the Department of Education. The CyberSecurity Career Pathways grant was awarded in October 2012 and, with a no-cost extension and institutional support, supported services through June 2016.

The Information Systems and Technology (IST) Department at UVU and its partners in industry and workforce services created the CyberSecurity Career Pathways program to address the lack of adequate CyberSecurity training in the region, the shortage of faculty and laboratory facilities at UVU to support cyber training, a lack of training in flexible modalities and delivery methods, and barriers to learning for TAA-eligible populations.

In year two of the grant, UVU partnered with Pacific Research and Evaluation (PRE) to conduct the third party evaluation of the CyberSecurity Career Pathways program. PRE designed and executed a comprehensive plan for the implementation and impact evaluation components required by DOL and collected additional data to inform continuous program improvement throughout the life of the grant. The evaluation plan as executed is summarized below.

Research Plan

PRE's evaluation methodology included an implementation evaluation to assess formative components of program implementation and an impact evaluation which utilizes participant outcomes and historical cohorts as comparison to assess the impact of the CyberSecurity programs on participants in terms of key student outcomes.

Formative Evaluation

The evaluation plan included two types of formative evaluation: one with a focus on the initial assessment of the program plan and curriculum, and an ongoing assessment of how the program is implemented. The initial assessment gathered background data regarding the development of the CyberSecurity program. Specifically, qualitative information was collected from the implementation team and the partner organizations through a staff focus group and advisory board interviews.

The ongoing assessment focused on the operational strengths and weaknesses of the programs upon implementation. Formative data regarding staffing, delivery methods (assessment, recruitment, and career guidance), participation, and partner contributions were collected from UVU staff, partner organizations, and students through the staff interviews and focus groups, advisory board interviews and focus groups, and student surveys and focus groups. The following table summarizes the methods used for addressing each of the formative evaluation questions.

Table 1. Evaluation Methods

Evaluation Question	Evaluation Method	Timeline
Analyze the steps taken by the institution to create and run the training program.	Staff Focus Group Advisory Board Phone Interviews	Year 2 Year 2
Assess the operational strengths and weaknesses of the project after implementation.	Staff Focus Group Advisory Board Phone Interviews Advisory Board Focus Groups Staff Phone Interviews Student Survey Student Focus Group	Year 2 & 4 Year 2 Year 3 & 4 Year 3 Year 2 & 4 Year 3
How was curriculum selected, used, or created?	Staff Focus Group Advisory Board Phone Interviews	Year 2 Year 2
How programs and program design were improved or expanded using grant funds?	Staff Phone Interviews Staff Focus Group Advisory Phone Interviews	Year 3 Year 2 Year 2
What delivery methods were offered?	Staff Phone Interviews	Year 3
What was the program administrative structure?	Staff Focus Group Staff Survey	Year 2 Year 2
What support services and other services were offered?	Student Survey Staff Phone Interviews	Year 2 & 4 Year 3
Did grantees conduct an in-depth assessment of participant's abilities, skill, and interests to select participants into grant program?	Staff Focus Group	Year 2
What assessment tools and process were used?	Staff Focus Group	Year 2
Who conducted the assessment?	Staff Focus Group	Year 2
How the assessment results were used?	Staff Focus Group	Year 2
Were assessment results useful in determining the appropriate program and course of sequence for participants?	Staff Focus Group	Year 2
Was career guidance provided and if so, through what methods?	Student Survey Student Focus Group Staff Phone Interviews	Year 2 & 4 Year 2 Year 3
What contributions did each of the partners make in terms of: • Program Design • Curriculum Development • Recruitment • Training • Placement • Program Management • Leveraging of Resources • Commitment to Program Sustainability	Staff Survey Advisory Board Phone Interviews Advisory Board Focus Group Staff Focus Group	Year 2 Year 2 Year 3 & 4 Year 4
What factors contributed to partners' involvement or lack of involvement in the program?	Staff Focus Group Advisory Board Interviews Advisory Board Focus Group	Year 4 Year 2 Year 3 & 4

Evaluation Question	Evaluation Method	Timeline
Which contributions from partners were most critical to the success of the grant program?	Staff Focus Group Advisory Board Focus Group Staff Phone Interviews	Year 4 Year 3 & 4 Year 3
Which contributions from partners had less of an impact?	Staff Focus Group Advisory Board Focus Group	Year 4 Year 3 & 4

Data Collection Tools

Table 2 summarizes the methods used for collecting data to address the formative evaluation questions and provide continuous program improvement data over the course of the grant. Each of these methods is described in more detail below.

Table 2. Summary of Data Collection Methods

Activity	Year 1 (2012-13)	Year 2 (2013-14)	Year 3 (2014-15)	Year 4 (2015-16)
Project Team Focus Groups		✓		✓
Student Survey		✓		✓
Student Focus Groups		✓		
Staff Focus Groups			✓	
Staff Phone Interviews			✓	
Advisory Board Phone Interviews		✓		
Advisory Board Focus Groups			✓	✓
Quarterly Report Surveys		✓	✓	

Project Team Focus Groups

Project team focus groups were conducted in years two and four of the grant. Six staff members participated in the year two focus group. The following topics were covered: 1) Steps taken by the institution to create and run the training program, 2) Administrative structure of the program, 3) Selection of program curriculum, 4) Selection of students for the program, 5) Expectations of students in the program, 6) Strengths of the program, and 7) Constraints experienced. Seven members participated in the final project team focus group in year four. Those participating held various roles at UVU including program manager, instructors, and academic advisors in the CyberSecurity program. The following topics were covered: 1) Program strengths, 2) Preparation for students to work in CyberSecurity, 3) Program fit for displaced workers, 4) Available advising resources, 5) Useful aspects of the advisory board, 6) Areas for improvement, 7) Hopes for program sustainability, and 8) Additional comments about the program. The protocols for both the year two and year four project team focus groups are presented in Appendix A.

Student Surveys

In the second year of the grant, the institutional research department at UVU distributed a survey to students in who had participated in a class through the CyberSecurity Career Pathways program during the first two years of the TAACCCT grant period. A total of 43 students responded to that survey. In the fourth year of the grant, an online student survey was distributed by PRE to students who enrolled in the following three courses: IT 2700, IT 3700, IT 4700 in the 2014-15 academic year or the fall term of the 2015-16 academic year. Students who were currently enrolled in one of the above courses were offered extra credit for their participation. A total of 92 students responded to the survey in year four. Survey questions can be found in Appendix B. The sample size for each student survey year is presented in Table 3.

Table 3. Student Survey Sample Size

Year	Administration Date	n
Year 2 Survey	Spring, 2014	43
Year 4 Survey	Fall, 2015	92

Student Focus Groups

Student focus groups were conducted in year two of the grant. Fourteen students participated in the two focus group sessions and represented a variety of program and emphasis areas, the most common being IT with an emphasis in Network Administration & Security, followed by IT with an emphasis in Computer Forensics & Security. The following topics were explored during these focus groups: 1) Program participation, 2) Program recruitment, 3) Experience with advising services, 4) Education plans, 5) Career plans, 6) CyberSecurity program opportunities, 7) Barriers to program completion, 8) Suggestions for improvement, and 9) Additional comments. See the student focus group protocol in Appendix C.

Staff Phone Interviews

Staff phone interviews were conducted during August and September of 2015. Seven interviews were conducted with various staff that play a wide variety of roles including faculty, advisors, administrators, and support staff. The following topics were explored during the interviews, and the full interview protocol can be found in Appendix D: 1) Strengths of the program, 2) Preparation of students to enter the field, 3) Program fit for displaced and traditional workers, 4) Advising resources, 5) Career guidance, 6) Useful aspects of the advisory board, 7) Areas for improvement, 8) Program sustainability, and 10) Additional comments.

Advisory Board Phone Interviews

Interviews were conducted over the phone during the winter of 2014. Ten individuals participated in the interviews, representing nine partnering organizations. The interviews were conducted with individuals from Adobe, Condition Zebra, Inc., Department of Workforce Services, Mountain America Credit Union, National Security Agency (NSA), Paraben Corporation, SecurityMetrics, Inc., Spectra, and Symantec. Partners were asked a series of questions related to their involvement in the CyberSecurity Career Pathways program at UVU. Interview topics included which program elements they were involved with (design of the program or curriculum, recruitment, or other areas), factors that contributed to their involvement, expectations for the new or expanded program elements (students participation, the impact on their company and what positions students would likely enter within their organization), the program impacting the IT industry in the region, the strengths of the program, barriers or challenges with the program and other feedback. See the interview protocol in Appendix E.

Advisory Board Focus Groups

PRE conducted an advisory board focus group in years three and four. In November of year three, PRE attended an advisory board meeting and facilitated a focus group with members with questions related to continuous program improvement efforts and sustainability. The second advisory board focus group took place in March of 2016. This group focused on the industry partner level of involvement throughout the grant period, the impact of the program on industry, sustainability of partner involvement, program successes and identification of barriers of the program. Questions addressed in both of the advisory board focus groups can be found in Appendix F.

Quarterly Report Surveys

PRE distributed a quarterly report survey during years two and three of the grant in order to gather information from various CyberSecurity Career Pathways staff for the DOL quarterly reports. The surveys asked staff to report progress made on relevant strategies during that quarter and provide any additional grant updates. PRE received surveys from three to six individuals quarterly, and compiled and synthesized the results into a summary document to assist the project team with quarterly reporting requirements.

Impact Evaluation

Due to the fact that participants were enrolled in the CyberSecurity Career Pathways program and TAACCCT grants place an emphasis on recruiting TAA-eligible students, it was not feasible to conduct an impact evaluation that included true random assignment. Thus, PRE developed a quasi-experimental historical comparison cohort method of evaluating TAACCCT program outcomes. This method allowed us to compare outcomes for participants in the grant-funded training with participants in historical cohorts that were comparable on key dimensions such as learning objectives (program completion and credential attainment), as well as employment outcomes. These student cohorts were compared on the following outcomes:

- Program Completion
- Retention in Program of Study
- Credential(s) Earned
- Wage Increase
- Entered Employment
- Retained Employment

The final impact study compared the year one participant cohort, broken down by program enrollment (AS/AAS in Information Technology, BS in Information Technology and in Information Systems) to a historical cohort of students who started in corresponding programs in the year of 2008-09 at UVU. Each program was analyzed separately for a three-year time period of program enrollment. PRE examined both educational and employment outcomes for the two groups. Educational outcomes included: program completion or program retention and credential attainment. Employment outcomes included: unemployed students gaining employment after program completion, employment retention for nine months after program completion, and wage increases for those students who were employed while going through the program. PRE worked with the UVU Institutional Research department to obtain student educational outcome data for both participant and comparison cohorts and worked with UVU to create a data request of Department of Workforce Services (DWS) to provide PRE with the appropriate data for conducting the employment data analyses. Table 4 presents the treatment and comparison cohorts selected for the impact analysis as well as the number of students in each of the cohorts.

Table 4. Impact Analysis Cohorts

Participant Cohort (2012/13 Followed Through Spring 2015)	n	Historical Comparison Cohort (2008/09 Followed Through 2012)	n
AS/AAS in IT	73	AS/AAS in IT	83
BS in IT/IS	215	BS in IT/IS	208
Aggregate Participant Cohort	288	Aggregate Comparison Cohort	291

CyberSecurity Career Pathways Program Development

Three primary components of the CyberSecurity Career Pathways Program at UVU will be reviewed below, including: 1) The development or modification of CyberSecurity courses and programs, 2) The enhancement of student support services, and 3) The leveraging of relationships with local industry partners. The program was designed with multiple entry and exit points to employment. The following credentials can be awarded:

- Certificate of Proficiency in Information Technology
- Certificate of Completion in Network Administration
- Associate in Applied Science (AAS) in Information Systems and Technology
- Bachelor's of Science in Information Technology with an emphasis in Network Administration and Security
- Bachelor's of Science in Information Technology with an emphasis in Information Security Management
- Post-baccalaureate Graduate Certificate in CyberSecurity

The support services that were enhanced through the CyberSecurity grant include the addition of an academic advisor dedicated at least half time to CyberSecurity students as well as mentors, tutors, and additional lab support. The program also provided support to students through funding to take industry certification tests. The CyberSecurity grant team engaged the Utah Department of Workforce Services along with several local industry partners early in the grant process and fostered these relationships throughout the grant to create courses and programs that truly meet the needs of the local workforce and prepare students for immediate entry into CyberSecurity careers.

Course and Program Development

The six credentials listed above were either added to the IST course schedule or modified using the grant funding. The sections below detail the steps taken by UVU to create and run the CyberSecurity Career Pathways program; the administrative structure of the program; how curriculum was selected, used, or created; how programs were designed or improved using grant funds; and what delivery methods were offered.

Analyze the steps taken by the institution to create and run the training program

The steps taken by UVU to develop the CyberSecurity Career Pathways program were driven by the need for this type of training program in the region. A member of the grant team noted this in the initial project team focus group: “There has been a lot of discussion about the need for CyberSecurity training in our area. An advisory board member was instrumental in some discussions in Washington D.C., and he brought back information….We also knew that the National Security Agency (NSA) was coming into the area." The fact that TAACCCT grants were being provided specifically to community colleges was another reason the team decided to apply for the grant to fund their CyberSecurity program. One staff member noted, "Another piece unique to our state is that the community college system is attached to the university system. We are in a unique position at UVU, because the TAACCCT grants are targeted at community colleges so we were able to apply at our campus instead of the University of Utah. That hasn't gone unnoticed, because the University of Utah would have loved to have had this grant, but they couldn't compete." Finally, the team acknowledged that they were in a good position in terms of institutional capacity to support such a grant so the timing for the program was right.

The assembly of the industry advisory board was another key aspect to the creation and administration of the CyberSecurity program. The program utilized the advisory board to determine what curriculum would meet the needs of industry standards as detailed in later sections of this report. The staff member responsible for creating the advisory board described what companies were represented by the advisory board at the start of the grant: "The advisory board for the program has several members from international, national, and local companies working in CyberSecurity. Some of the companies include the National Security Agency (NSA), Security Metrics, Symantec, Harobin, Adobe, and UtiliSec. We also have an informal connection with Carnegie Melon." A couple of advisory board members noted they have been involved with UVU for several years; one board member noted he contributed to the grant writing process:

> "I began work on presenting the need for a CyberSecurity training program to UVU back in 1997, and ever since, have been trying to get the deans to understand the need for this mission-critical program. After three deans, it's good to see one come in and take charge. I wrote the initial curriculum and the grant to the Department of Labor, which provided the three million dollars."
>
> *CyberSecurity Advisory Board Member (Y2)*

Advisory board members also contributed to the creation of the CyberSecurity program through support with hiring staff in early stages of the grant. One advisory board member provided a recommendation for the program manager and another advisory board member assisted with the interviews and selection of the staff member hired for a hybrid position between the Department of Workforce Services and the college. Other ways advisory board members helped with the creation of the training program included feedback regarding the different tracks or credentials, providing ideas for increasing student enrollment, and meeting industry demand as suggested by an advisory board member in year two:

> "At my first meeting, we talked about the lab and training, library resources, approval process, as well as about hacking and what to do to address it. They also talked about increasing student enrollment, which would lead to increasing classroom size, professors, and the curriculum and turning the program into additional semesters if needed. Employers talked about the need for the program, and what they're looking for in an employee."
>
> *CyberSecurity Advisory Board Member (Y2)*

Program administrative structure

In terms of the administrative structure of the grant, the CyberSecurity Career Pathways team was assembled based on previous grant experience, role within the university, and expertise in the field of

CyberSecurity. This grant team included the Director of Career and Technical Education, the Associate Dean for the College of Technology and Computing, the Information Systems and Technology Department Chair, a content specialist hired as the CyberSecurity Program Manager, and a Career/Technical Education Business Assistant.

In the early stages of the grant, the team described their rationale for assigning the role of the project manager to an administrative staff member rather than a faculty member: "On a previous grant we had a faculty member who served that role of project manager and it drained faculty resources because they had to learn those processes and distracted faculty from doing their job. It was a blessing to have Career and Technical Education office take over because they are familiar with the process." This structure allowed for the faculty members to focus on program needs and not worry about the reporting and grant management details as noted by one team member: "I don't have to worry about the accountability piece and I can focus on what the program needs and what we think we should do." There was minimal turnover in the CyberSecurity grant team over the course of the project.

How was curriculum selected, used, or created?

The new and modified credentials that were developed through the CyberSecurity Career Pathways program were highly driven by industry need. One staff member noted that discussions with the advisory board around industry demand were crucial in curriculum selection:

> "I've met with advisory board members regularly to discuss the curriculum, what their organization felt new hires were lacking in that area, and what their pain points were as far as security information assurance, and trends they are seeing. I work with both the advisory board members and other parties that are not officially associated with this but I know professionally. So, that's where a lot of curriculum came from: industry demand. We are trying to provide a program that meets the needs in the local area and nationally as well."
>
> *CyberSecurity Program Manager (Y2)*

Advisory board members echoed their involvement in curriculum selection and noted various levels of involvement. Involvement ranged from assisting with writing initial curriculum, providing general recommendations for content to include, to reviewing and making recommendations. One advisory board member commented on this involvement: "We went through the overall curriculum as a board making recommendations. We made a nice assessment of what's relevant and there was a lot discussed about security and auditing." Another noted, "I was asked to join the board of advisors about a year ago. I've attended meetings and provided comments and feedback about curriculum. I met with the program manager at lunch to talk about goals for the program, and what I think would be important for my company." Other advisory board members provided less direct contributions to curriculum selection but were present for discussions about curriculum and provided general guidance or review as noted by one member: "I just reviewed the type of classes and required courses for the curriculum. I gave more general contributions."

How were programs design or improved using grant funds?

The CyberSecurity Career Pathways grant primarily worked to modify existing credentials within the IST department including the certificates and the modifications made to the associate and bachelor degree programs. These modifications included curriculum development for new courses that focus on CyberSecurity and the ability to provide the emphases in Network Administration and Security or Information Security Management. The goal in the original statement of work was to create curriculum for eight new courses to be included in the associate and/or bachelor degree programs. Modifications also included creating a computer lab for CyberSecurity and forensics which was completed by early in year two of the grant as reported by a team member on their quarterly report survey:

> "The computer forensics lab with 37 workstations was built and is scheduled to start spring semester. Due to the fact that the computers came in under the expected cost and resulted in a surplus of funds, another equipment request for a second lab has been approved. We are moving forward with placing a bid for the additional computer lab."
>
> *CyberSecurity Project Team Member (Y2)*

The team also spent a significant amount of time in the development of the post-baccalaureate graduate certificate in CyberSecurity which did not exist in any form prior to the grant and is the only graduate certificate of its kind in the region. Regarding the post-baccalaureate certificate, a staff member said, "I think one of the strengths of the CyberSecurity program is the post-baccalaureate certificate. It is a high-level administration type of situation where you don't get stuck at an entry level position in CyberSecurity – you can jump right into high-level or mid-level management." Additionally, staff members mentioned the development of this certificate paved the road for the creation of a master's degree program in CyberSecurity: "The grant really laid the foundation for the master's degree. I think without the post-baccalaureate certificate this wouldn't be something we would be so far along with."

What delivery methods were offered?

One of the primary strategies identified in the CyberSecurity Career Pathways grant statement of work was to prepare four existing courses for hybrid delivery. In the first staff focus group, team members discussed their plans to incorporate online classes into the curriculum. One staff member said, "Some existing classes and IT classes will be offered online at least once a year, so we're working with the faculty on the methods for those online courses." Early within year two of the grant, progress had been made towards identifying the courses that would be prepared for hybrid delivery. A year two status report provided the following update:

> "Courses have been identified and discussions are taking place between internal stakeholders and subject matter experts to determine expectations in order to create quality hybrid courses. Contracts are being worked on for faculty working in this area; however, there are concerns in this area and a suggestion made was to bring in OER experts."
>
> *CyberSecurity Project Team Member (Y2)*

By quarter two of year three, the project status report summary indicated that the four courses had been selected and that three were in the process of hybrid development. One had been completed and was implemented during the fall semester of year three. By the end of grant year three, the team reported additional courses were being modified for hybrid delivery.

CyberSecurity Students

Characteristics

The following table summarizes the number of students enrolled in CyberSecurity credentials in the first three years of the grant.

Table 5. Number of Students Enrolled in CyberSecurity Credentials

Credential	Number of Students
Certificate in Information Technology	9
Certificate in Network Administration	21
AS in Information Systems and Technology	28
AAS in Information Systems and Technology	71
BS in Information Systems	330
BS in Information Technology	315

Table 6 presents the concentration of degrees for students in the CyberSecurity program. These data were available for the majority of students (n = 589). The most common degree concentration was Network Administration and Security, which includes CyberSecurity focused courses along with the networking and system administration courses.

Table 6. Degree Concentration

Concentration	Number of Students
Business Intelligence Systems	220
Computer Forensic and Security	61
Database Admin and Security	8
Database Administration	2
Geographic Information Systems	7
Healthcare Information Systems	29
Information Security Management	4
Network Admin and Security	250
Web Admin and Security	8

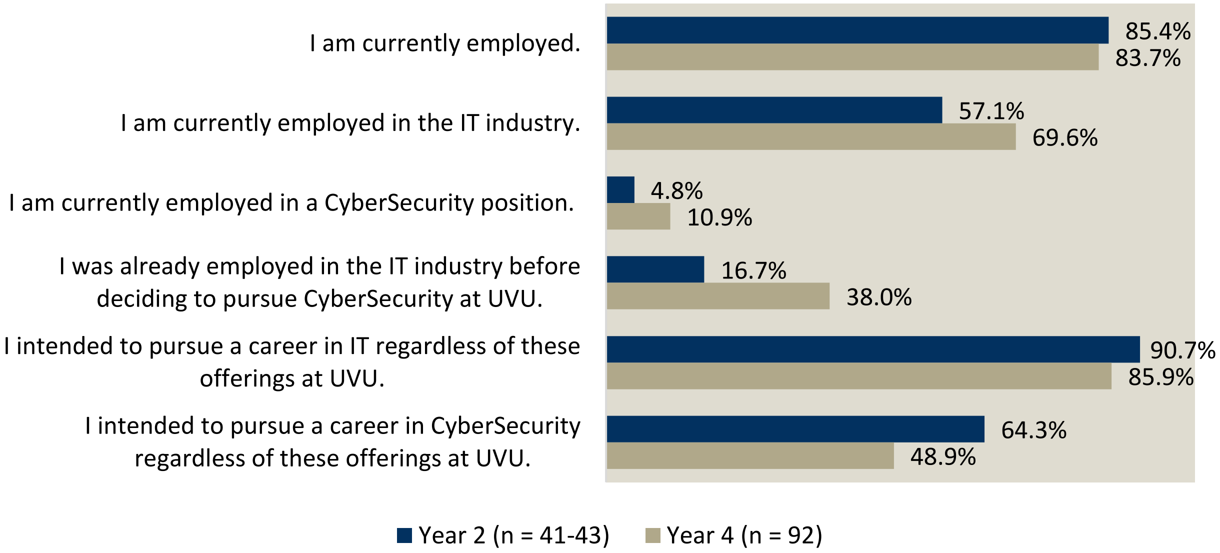
Student Demographics

PRE received student demographic data from institutional research at UVU for 743 students who participated in the credential programs through year three of the grant. The majority of these students were male (89.7%) and Caucasian (80.9%). Nine percent (8.7%) of students were Hispanic, 3.8% of students were Asian, and 2.6% of students were black. Less than two percent (1.5%) of students identified as American Indian or Pacific Islander, and the remaining 2.5% of students identified as more than one race or did not report their race. The mean age of students was 28 at the time of enrollment, but the age range of students served by the CyberSecurity Career Pathways program varied widely from 17 to 69. Just over half of all CyberSecurity students attended the programs full-time (56.7%), and the remaining students attended the program part-time (43.3%).

Student Employment Characteristics

The student survey in years two and four asked a series of questions about employment characteristics as shown in Figure 1. The majority survey respondents were employed during their time in the program and of those who were employed, about half were working within the IT industry. Only a small group of CyberSecurity students each year reported being employed in a CyberSecurity position while they were at UVU. Though the majority of CyberSecurity students at UVU intended to pursue a career in IT, the new offerings did impact the career trajectory of some students.

Figure 1. CyberSecurity Student Employment Characteristics
(% Yes)



Eligibility Requirements and Recruitment

Selection of Students for the Program

The only CyberSecurity program credential with an eligibility requirement is the graduate certificate, which requires students to have a bachelor's degree in IT or a related field. Conversely, the other remaining credentials all have open enrollment, which is the case for all other undergraduate programs at UVU. For these credential programs, students are required to take some prerequisite courses before progressing through the program. One staff member commented on open enrollment at UVU: "We're an open-enrollment university; the program doesn't have any requirements, so anyone who wants to enroll is welcome." In discussions around whether an assessment will be used for program enrollment purposes, staff members in the year two focus group discussed the Work Keys assessment for purposes of demonstrating improvement and competences but not for enrollment purposes.

Program Marketing

Facilitating student awareness about the CyberSecurity Career Pathways program was one of the primary grant strategies. Early recruitment efforts included ensuring students were aware of the program and what it includes by promoting it in classrooms and through press releases, and by reaching out to companies with TAA-eligible workers. One team member commented on recruitment early in the grant period: "The community as a whole knows because there have been press releases. Our president continues to put it out in front of everyone. It's a big deal in our area."

By the beginning of year three, a CyberSecurity Career Pathways website had been created, approved, and launched. Information regarding the program, transferability, articulation, and contact information was made available on the website. In addition, with the support of the technology and computing marketing director, a CyberSecurity pull-up banner was designed and positioned in a high-traffic area of an IST hallway. By the end of year three, staff reported on additional marketing efforts that had been made for the program:

> "There has been a large amount of progress on this strategy. The website has been updated and has additional traffic, and Rivetal has been conducting outreach for the program through newspaper ads and fliers. The advertisement is increasing awareness of the program and the updates to the website have led to more accurate and timely information being provide to those who inquire."
>
> *CyberSecurity Staff Member (Y3)*

TAACCCT Grant Components

CyberSecurity Career Pathways Credentials

As noted previously, a series of credentials were established through the CyberSecurity Career Pathways grant at UVU with a goal of meeting the needs of students at varying levels of CyberSecurity knowledge. These include entry level certificates that can be completed in less than a year and offer employer/industry recognized credentials. Students could complete earn a two-year degree in the form of an AAS in Information Systems and Technology or earn a BA in either Information Technology with an emphasis in Network Administration and Security or a BA in Information Systems with an emphasis in Information Security Management. Finally, for those student looking for post-graduate education, the CyberSecurity Career Pathways grant developed a Post-baccalaureate Graduate Certificate in CyberSecurity. Each of these credentials is described in more detail below and all credentials will be sustained moving forward.

Entry-Level Certificates

The entry-level certificates included in the CyberSecurity Career Pathways program consist of the Certificate of Proficiency in Information Technology and the Certificate of Completion in Network Administration. These entry-level certificates provide students with the opportunity to gain knowledge and quickly earn a credential that can be added to their résumé. While they are not specifically focused on CyberSecurity, the certificates provide foundational knowledge necessary for success in a variety of technology fields. The courses in these credentials lead directly into and can be applied to the Associate in Applied Science (AAS) in Information Systems and Technology program.

Associate in Applied Science (AAS) in Information Systems and Technology

UVU's AAS program provides the essential coursework and knowledge to provide a strong foundation upon which to build a CyberSecurity education. Coursework includes topics such as network administration, Linux, and information security.

BS in Information Technology or Information Systems

UVU's ABET accredited Bachelor of Science programs in Information Technology and Information Systems both have emphases designed for those interested in CyberSecurity. The Information Technology emphasis in Network Administration and Security includes CyberSecurity focused courses along with the networking and system administration courses essential for IT professionals. The Information Systems emphasis in Information Security Management includes important CyberSecurity courses for students focused on enabling business with technology. From web application security to information security analytics, the IS courses provide deep insight on how CyberSecurity affects businesses.

Post-baccalaureate Graduate Certificate in CyberSecurity

Designed for working professionals, UVU's graduate certificate is an intensive year-long program focused exclusively on graduate-level CyberSecurity content. Classes are held twice a week in the evening and include Cybersecurity Operations, Advanced Network Defense and Countermeasures, Cybersecurity Management, and more.

Student Support Services

Aside from the instructional development and enhancements made as part of the CyberSecurity Career Pathways program, student support services are a significant component of the TAACCCT grant, and UVU provided both academic advising and career guidance as detailed below.

What support services and other services were offered?

Students in the CyberSecurity Career Pathways program were offered services to support academic and employment success. These services included traditional academic advising, career guidance, mentoring, tutoring, and monetary support for certification testing.

In the early stages of the grant, UVU shared plans to partner with the Department of Workforce Services (DWS) in hiring an advisor that would be employed half-time by each of the organizations. By year two of the grant an advisor has been hired for this position and activities in this role included promoting the program to IT students, meeting with students, and training other staff on Work Keys. A goal of partnering with DWS was to help students in a variety of ways and provide funding for student tuition, which is not available through the grant. Although the grant team had positive intentions with the hybrid position, it did not end up working out logistically. By the spring of year three, the status reports indicated a lack of clarity surrounding advising due to the fact that the college lost a full-time academic advisor and the hybrid position was left to be the primary advisor for some students. This change led to inconsistencies in advising services that students were receiving, and as a result, the college decided to hire a new full-time academic advisor within the college and eliminate the hybrid position with DWS. By the end of year three, the department had one full-time and one half-time advisors working with students and there were discussions about making the half-time advisor full-time for the IST department.

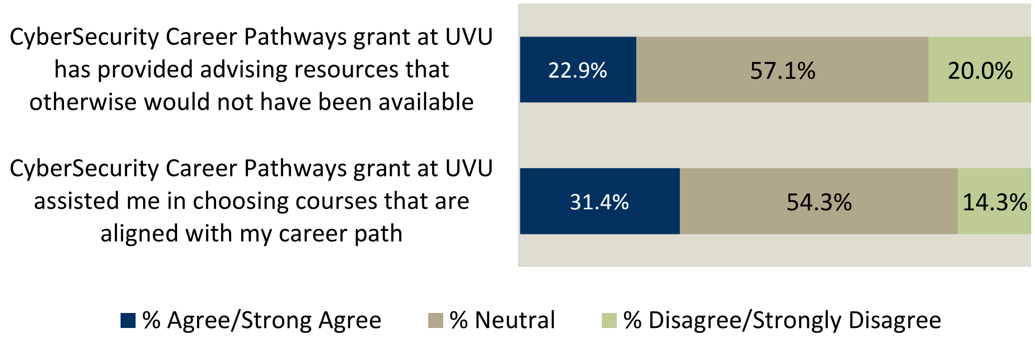
Student Experience with Advising Services

Students provided feedback regarding advising services on the student surveys and during student focus groups in year two and four. Students indicated that advisors helped guide them to their current program of study through a discussion of their interests and employment opportunities in the region. One student stated an advisor helped the student in setting their schedule: “I’ve been to my advisor so many times. At the beginning I had her help me set my schedule, and she planned it out for me. I've gone back in to fix little pieces.” Another student provided positive feedback regarding experiences with advisors at UVU by indicating they have been helpful: “They’ve been really great. I’ve had to switch advisors, but they’ve been good at helping me.”

In the year two focus groups, a few students described having negative experiences with UVU advising, citing reasons such as the advisor not being able to answer questions, a lack of experience working in the field in which they are advising, difficulty transferring credits, and, for students who were already employed, receiving information about lower-level employment opportunities rather than scholarship opportunities.

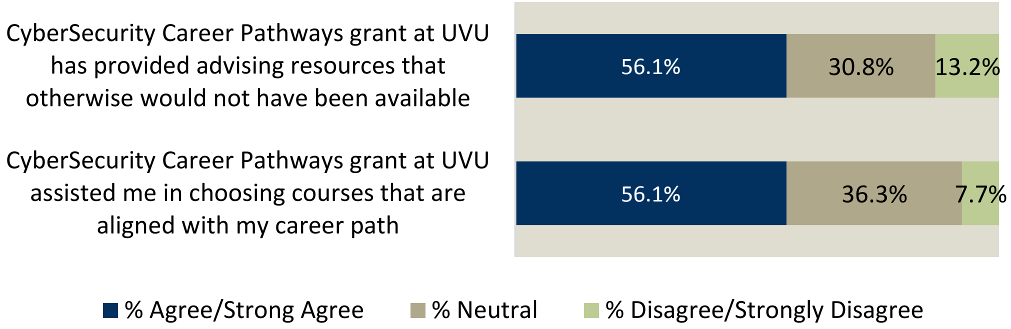
As shown in Figure 2, twenty-three percent (22.9%) of students who responded to the survey in year two indicated they had received advising resources through the grant program that otherwise would not have been available and 31.4% of students indicated the CyberSecurity Career Pathways grant has provided assistance in choosing courses aligned with their career path. It is important to note the high level of neutral responses. Low levels of agreement and neutral responses are not surprising as the grant funds were being used to fund standard advising positions, and students might not know if they were seeing an advisor funded through the grant.

Figure 2. Year 2 Student Perceptions of Advising Services
(n = 35)



In year four, student feedback regarding advising services showed perceived improvement in services and resources provided. Fifty-six percent (56.1%) of students indicated the CyberSecurity Career Pathways program at UVU has provided assistance in choosing courses aligned with their career path and that they have received advising resources that otherwise would not have been available to them (see Figure 3).

Figure 3. Year 4 Student Perceptions of Advising Services
(n = 91)



Staff Feedback on Advising Resources

In terms of staff feedback on advising services, focus group participants in year three indicated that advisors had not been able to promote the program to students due to the delay in approval for the post-baccalaureate certificate of the program. The cumbersome institutional approval and accreditation process provided challenges in the recruiting and retention of students in these new programs. One staff member commented on the program’s ability to hire a second advisor who is partially funded by the grant, resulting in a smaller student to advisor ratio for those existing students. The university was also able to bring on additional advising staff to specifically help students from the program:

> “We have 1.5 advisors assigned to IT as a whole, with a focus of .5 of an advisor assigned to working with students who are interested in CyberSecurity. We encourage them to come in once a semester to make sure they are on the right path but we don’t force them to. I email with students as well. We plan out their classes to get them to graduation, and we have to revamp that plan when life happens.”
>
> *CyberSecurity Staff Member (Y3)*

One staff member mentioned some of the outside agencies UVU collaborates with to provide advising services to students including the Department of Workforce Services and the LDS Employment Services, which is one of the largest private employment services in valley. They are also working with the VA and other veterans groups, and have done outreach to disadvantaged communities, as stated by a staff member in a year three interview: “It is not just advising we are providing at the university, but also the mentoring we are providing to community advisors to help them reach out in their focus groups and targeted audiences to look at what the onramp is to get into the program.”

Student Mentoring and Tutoring

One of the goals of the TAACCCT grant at UVU was to hire and train students to act as tutors and mentors to students in the CyberSecurity programs. By the beginning of the second year of the grant, two students had been hired part time to provide math, IS, and IT assistance to students and were receiving positive feedback from faculty and students. As the second year progressed, staff experienced difficulty in identifying qualified individuals to fill additional open positions, and turnover of the student tutors exacerbated this issue. One staff member explained that finding qualified candidates was difficult on a quarterly report: “It has been difficult to find qualified students to hire for this position. The majority of upper level students who would be qualified for a tutor or mentor position aren't interested in a part-time job." It was difficult for the program to get these well-qualified students interested in the position as it was not feasible to increase the salary for the position.

Funding for Industry Certification Testing

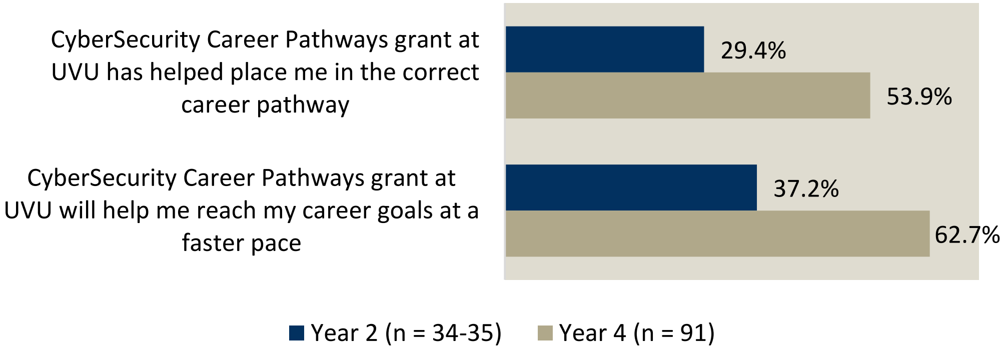
Another support service UVU provided as part of the CyberSecurity Career Pathways grant was funding for students to take industry certification tests. The university offered vouchers to cover 80% of the cost of certain industry certification exams. Staff worked with industry partners to determine which industry certification tests would be offered at the beginning of the grant. When funding was first offered for the certification exams at the end of the second year of the grant, interest from students was low, and this continued to be an issue throughout the grant period. By the end of the grant period, an estimated number of 100 students had taken advantage of this opportunity. One staff member commented on the importance of students taking the industry certification tests during the final project team focus group:

> "There was an increase in demand in students getting industry certifications. We had a lot of students take advantage of those vouchers. It balances out the formal, academic education with some validated industry certification. It also validates what we are doing because they are able to pass these real world certifications."
>
> *CyberSecurity Project Team Member (Y4)*

Was career guidance provided and if so, through what methods?

As illustrated in Figure 4, 29.4% of students credited the CyberSecurity Career Pathways grant with placing them in the correct career pathway in a year two survey, and this percentage increased to 53.9% in year four. There was also an increase in the percentage of students who reported the CyberSecurity Career Pathways grant will help them reach their career goals at a faster pace, from 37.2% in year two to over 60% in year four. This shows another improvement from the beginning stages of implementation in the TAACCCT funded programming and services.

Figure 4. Student Perceptions of Career Guidance
(% Agree/Strongly Agree)



Staff Feedback on Career Guidance

Staff mentioned the UVU campus career services center as a source of career guidance for students in the CyberSecurity program. This department provides assistance with internships through an internship specialist who goes into classes each semester and keeps students abreast of internship opportunities by posting weekly "hot internships" on a list serve which students can subscribe to. The department also helps with employment placement after graduation by sharing job readiness and employment opportunities through their career passport program. In addition, department advisors, who mainly counsel students on course plans and graduation requirements, provide some career guidance for students as well.

Staff also shared that they provide career guidance to students during classes. Faculty talk about job opportunities during class, and regularly mentor, provide guidance, and write letters of recommendation for students who are looking for jobs and applying for graduate programs. One staff member also shared that they have personal connections with companies, which helps students to gain employment: "I'm also there for connections with actual businesses the university has partnerships with. Sometimes students get job offers from those partnerships. The department also gets emails from local companies looking for people."

Another staff member shared information about a speaker series put on by the CyberSecurity program to talk to the students about career paths and opportunities:

> "We bring speakers in that are working in the cyber industry to talk to the students about what they do, what jobs there are, and what the trends are. We try to bring people in from each one of the companies on our advisory board, as well as the NSA and the governmental groups. To me, that is the best way to reach the students so they can understand what is actually happening in the industry. We have had a number of CyberSecurity firms come to our career fairs meet with the students and share potential opportunities."
>
> *CyberSecurity Staff Member (Y3)*

Students also benefit from the experiences of their instructors, many of whom have backgrounds working in the field. They are able to teach the curriculum based on their professional, real-world experience, as opposed to instructors who have been career academics. As one staff member put it, "The actual people from the industry are helping to prepare our students."

Overall, the staff believe students are supplied with beneficial training and resources to have successful careers in CyberSecurity. This preparation has shown to be appropriate for displaced workers, non-traditional students and people new to the industry. The staff expressed that they put a high degree of effort in providing students with guidance and opportunities for mentorship in their department.

Industry Connections

Connections with local industry partners in the form of an advisory board was an area of strength for the UVU CyberSecurity Career Pathways program, as evidenced by the many references to the advisory board in previous sections of this evaluation report. Advisory board members included representatives from the National Security Administration, Adobe, EMC, Spectra, UtiliSec, and various other local organizations. As one member of the advisory board noted, "I think we've got a pretty good representation of industries." This sentiment was also expressed by university staff members, and one commented, "The advisory board that we put together is a huge strength, because we found the right people." Over the course of the grant, staff and industry partners were asked to reflect on the contributions that the advisory board made to the CyberSecurity program at UVU in terms of:

- Program Design

- Curriculum Development
- Recruitment
- Training
- Placement
- Commitment to Program Sustainability

Program Design

As described earlier, the industry partners heavily influenced the design of the CyberSecurity credentials at UVU, including assisting with identifying credentials to be part of the program, as described by an advisory board member at the beginning of the grant: “I have been attending meetings and providing feedback at the meetings about the different tracks, program goals, expectations, and insight from my experience as a security professional who is a hiring manager.” This ability to influence the program design was appreciated by industry partners, as mentioned by another member of the board:

> “We were involved in identifying the different tracks as part of the CyberSecurity program. It came up by them asking very specific questions like ‘If you needed to hire someone today, what kind of skills would you need?’ We used those discussions to talk about the courses, the direction they were going, and what those different tracks were. I really liked having that input.”
>
> *CyberSecurity Advisory Board Member (Y4)*

Curriculum Development

Advisory board members discussed being involved with curriculum development at varying levels, including writing pieces of the curriculum, reviewing course outlines, and making suggestions for topics to be included. Staff mentioned that this feedback on the curriculum was crucial to the CyberSecurity program as it helped ensure the students are gaining skills necessary for employment:

> “I’ve met with advisory board members regularly to discuss the curriculum, what their organization felt new hires were lacking in that area, and what their pain points were as far as security information assurance, and trends they are seeing. We are trying to provide a program that meets the needs in the local area and nationally as well.”
>
> *CyberSecurity Project Team Member (Y2)*

One advisory board member mentioned the curriculum will have to constantly be updated to keep up with the rapid changes in the CyberSecurity industry: “I think a constantly evolving curriculum is in order. This is an industry that is going to evolve pretty rapidly for many, many years, so staying on top of the curriculum and courses and keeping it current is going to be a pretty important thing.” This is an important reason for UVU to continue partnering with the industry to inform the CyberSecurity program moving forward.

Recruitment

Advisory board members were involved with recruitment of students for the CyberSecurity program at UVU. One member said they have recommended the program to individuals in their organization as well as potential employees, “We have referred our own employees to the program as well as potential employees that we thought would benefit from that skill and had other good aptitudes that would make good employees for us that we wanted to have with a CyberSecurity background.”

Training

In terms of involvement with training, advisory board members have been guest lecturers in the new CyberSecurity courses, as discussed by one staff member: “We have had advisory board members come in as part of a lecture series. I have had people from partner organizations and affiliated organizations (not official partners) come in to do guest lectures. We have had a lot of interest in doing guest lectures and presentations. Students love that and they like seeing a new perspective, and it is good for networking.”

Placement

Several industry partners involved with the advisory board mentioned they have hired interns from the CyberSecurity programs as well as graduates of the program. During the final project team focus group, a staff member mentioned the partners who have hired students from the program have been able to provide additional feedback on the training: “There was a lot of influence [from the advisory board], and there is continuing influence from those who have hired the students.”

Commitment to Program Sustainability

When discussing commitment to program sustainability, several advisory board members discussed their wishes that the advisory board will continue to provide guidance for the program moving forward:

> “We are really excited that the program will continue. I would hope that there would continue to be an advisory board. I know the College of Technology and Computing has a board at that level, but I would hope that a more CyberSecurity focused group could stay engaged from industry to continue to advise the program as we move through the rapid changes in the industry. I think it is really important for this area, so the board should continue.”
>
> *CyberSecurity Advisory Board Member (Y4)*

Another member of the advisory board mentioned they will continue to provide feedback on the CyberSecurity program after the grant ends: “For my participation, it doesn’t matter if it is through this grant or not, my continual feedback is always there. I am always happy to help out.” Staff members mentioned they hoped to gain financial support from industry partners, and that one partner has already contributed in the form of a scholarship for CyberSecurity students: “I know our development people have been looking at trying to get monetary sustainability. As far as wanting the program to continue and see it grow, there is a lot of interest [from partner organizations]. Now the questions is about how they can make that happen. One organization provided a scholarships specifically for CyberSecurity.”

What factors contributed to partners’ involvement or lack of involvement in the program?

In general, partners were satisfied with their involvement in the CyberSecurity Career Pathways program. As one partner said in the final focus group, “I think we were invited to be involved in as much as we could. The staff were very good at sharing information, sharing ideas, and offering opportunities to get more involved. I think it was done very well.”

There were several factors that led to members of the advisory board being less involved than they would have liked. First, lack of time made it difficult for partners to attend meetings, as one partner noted: “I think the frustrating thing for me has been not being able to attend the group sessions so a lot of my feedback ends up being more one-on-one because of my travel schedule.” A staff member also mentioned this issue: “Our partner organizations have full plates. Everyone is really, really busy. Schedules are difficult to align.”

Another factor that limited partners' level of involvement in the program was a lack of knowledge about CyberSecurity. The local representatives from large companies were not always subject matter experts, as one member of the advisory board discussed:

> "CyberSecurity is a multibillion dollar division for our company, and I am a general manager that spans multiple other divisions for our company, not a subject matter expert. It was a little difficult for me to get the right subject matter experts engaged. I was the local person who could provide the interface and the relationship, but I was constantly trying to broker the conversation between people like Robert and the subject matter experts in the relevant groups inside this big company."
>
> *CyberSecurity Advisory Board Member (Y4)*

Finally, UVU staff mentioned a lapse of communication between the college and the partners as a challenge of partner engagement. Staff mentioned it would be useful to be able to allocate more time to maintaining open communication and relationships with partner organizations:

> "When we reach out and go talk to partners or have meeting, we get a lot of good information, but it is hard to maintain that line of communication. We have all those people on the advisory board and other organizations that are interested, so it is almost a full time job to keep on top of those relationships. When you are teaching classes and developing new things, the communication is easy to let slide off. You get a bunch of good feedback, it trickles off and you realize I haven't talked to anyone for a while, so it goes in waves. That would be something that would be useful is more time to dedicate to that."
>
> *CyberSecurity Project Team Member (Y4)*

Which contributions from partners were most critical to the success of the grant program?

The partner organizations involved with the advisory board made a number of significant contributions to the CyberSecurity program at UVU as evidenced by the sections above. One of the contributions that was critical to the success of the grant was feedback on the program design and curriculum development. This input was important to creating up-to-date credentials:

> "Most of the courses we have are brand new courses that address the correct challenges of CyberSecurity and the dynamic environment that we work in. I believe this is a huge advantage to our program. For instance, we have a course that I taught and developed called Application Security. I have been involved with other institutions and none of them had that kind of course. That was totally developed working with the advisory board because they said there was a need for that and this is where the field is headed."
>
> *CyberSecurity Staff Member (Y3)*

In addition, the advisory board input on curriculum development was useful in determining the specific skills students need to know in order to meet employer needs:

> "Because they are out there on the front line working in the industry, we can turn to them for advice in fine tuning the curriculum or changing it if we are completely off base on what the demand is for specific skills. That is what we use them for the most – to make sure we are going in the right direction and preparing students to be employable."
>
> *CyberSecurity Staff Member (Y3)*

Program Strengths

Strengths of the CyberSecurity Career Pathways program included the strong relationships with industry partners, the continuation of the newly created credentials, and the continuity in grant team members. Noted in the section on industry partnerships and throughout this report, UVU developed strong relationships with relevant local companies through the advisory board. This board was able to provide support for the grant program in many major ways, including providing feedback on program design and curriculum development. Advisory board members helped to ensure the program is preparing students to graduate with skills that meet the needs of employers. Additionally, the advisory board members are committed to continuing to provide advice and support after the grant funding ends, which is advantageous as the curriculum will need to be constantly updated because the field of CyberSecurity is rapidly changing.

In terms of program sustainability, all the new credentials put in place by the CyberSecurity Career Pathways program will be sustained through permanent university funding channels. An advisory board member said, "We are really excited that the program will continue and it has the appropriate funding from the university to continue."

A final strength of the program was the continuity in the project team over the course of the grant. There was minimal turnover from this team which allowed the program to avoid any hiring or training delays and created strong partnerships with the advisory board.

Program Constraints

In the early stages of implementation, program constraints included the time it took to receive institutional approval and accreditation of the post-baccalaureate certificate in CyberSecurity. UVU was not able to advertise the program before the approval and accreditation process was complete. A staff member mentioned that by the middle of year three they were still not able to advertise the certificate: "We can't promote the [post-baccalaureate] CyberSecurity certificate or even talk about its existence until we get the accreditation for it. We have people asking questions, but we have no resources and can't mention the post-baccalaureate program on our webpage." This inability to advertise led to less interest in the program than anticipated for the first year, but staff members were hopeful that the recent advertising efforts will increase interest in the program in the near future:

> "There is low enrollment but we figured it was better to offer the classes and get the word out that way than to not offer them and try to build up enrollment before we did it. We are almost two semesters behind of where we wanted to be. The advertisement of the program is getting good feedback now and I expect the program to grow rapidly as it gets out there. You will probably see 15-20 students in the spring or next fall."
>
> *CyberSecurity Staff Member (Y3)*

Advising was another program constraint for the CyberSecurity Career Pathways program. The university had plans to partner with DWS to hire a hybrid advisor to work with students and provide funding for tuition, which is not available through the grant. However, the position did not end up working out as the program lost a full-time academic advisor, leaving the hybrid position as the only advising services, and the college decided to hire a full-time advisor and eliminate the hybrid position. These changes led to inconsistencies in advising services. Additionally, the grant planned to hire student tutors and mentors to assist students in the CyberSecurity program. However, the staff experienced difficulties with finding and keeping qualified students employed as those with enough experience to tutor preferred full-time, higher paying positions. Both of these issues may have led to low student awareness and utilization of support services.

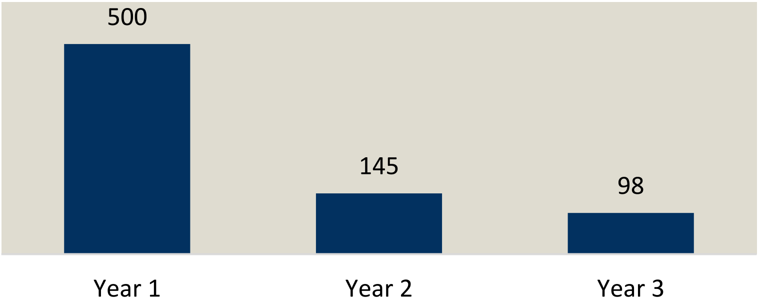
TAACCCT Outcomes

TAACCCT grants are geared towards the attainment of both academic and employment outcomes for participants. Education outcomes include program completion, continued enrollment, credential earned, and further enrollment in education. Employment outcomes include wage increases for incumbent workers as well as entered and retained employment for non-incumbent workers. The education and employment outcomes specific to the CyberSecurity Career Pathways participants are detailed in the sections below.

Academic Outcomes

Education outcome data were made available to PRE through institutional research at UVU for CyberSecurity Career Pathways students through the end of year three of the grant. There were additional students who participated in the credential programs after the data pull that are not included in this report. Figure 5 breaks down then number of unduplicated students enrolled during each year of the grant through year three. The year one total is higher as it includes students who were enrolled in all relevant IST courses when the grant started whereas years two and three totals include only new students who enrolled in each of those years.

Figure 5. Number of Students Unduplicated by Year



Number of Completers and Credential Earned

The number of CyberSecurity students completing a credential during each year of the grant is presented in Table 7 by credential type. The program did not track credentials earned through certification testing so the number of completers is equal to the number of credentials earned in this grant. Those student completing degrees in other majors were involved in CyberSecurity grant funded classes but did not complete and IT/IS related credential.

Table 7. Number of Completions by Credential

	Year 1 2012-13	Year 2 2013-14	Year 3 2014-15
Certificate in Information Technology	0	1	8
Certificate in Network Administration	5	5	8
AS in Information Systems Technology	4	17	9
AAS in Information Systems Technology	4	16	4
BS in Information Systems	18	32	27
BS in Information Technology	39	35	38
Other Major	16	21	24
Total	86	127	118

Number of Students Retained

Table 8 shows the number of students who were retained after years one and two of the grant by credential. Numbers of students retained are high for this grant as the focus is on two and four year credential programs.

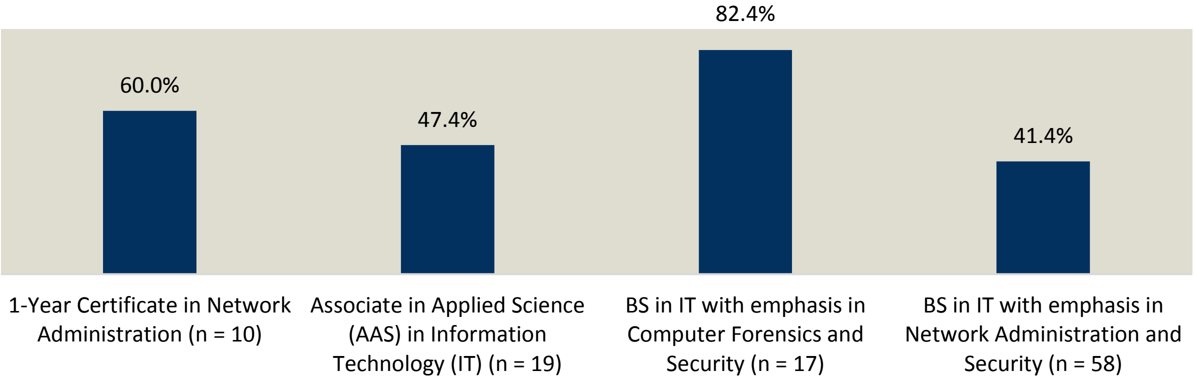
Table 8. Number of Retained Students

	Retained at the start of Year 2	**Retained at the start of Year 3**
AAS Information Systems/Technology	64	28
AS Information Systems/Technology	15	17
BS Information Systems	157	181
BS Information Technology	135	82
Total Retained	371	308

Enrollment in Further Education

Since the CyberSecurity Career Pathways program was designed to offer stacked credentials, many students enrolled in further education after completion of their credential. National Clearing House data showed that at the end of year three, 126 students had enrolled in further education. PRE asked students about intentions to pursue additional credentials in the year four student survey and as shown in Figure 6, a large number of students do have plans to pursue additional education. When students were asked what credential they plan to pursue, the most popular response from the BS students was to pursue a Master's degree in an IT field and specifically within CyberSecurity.

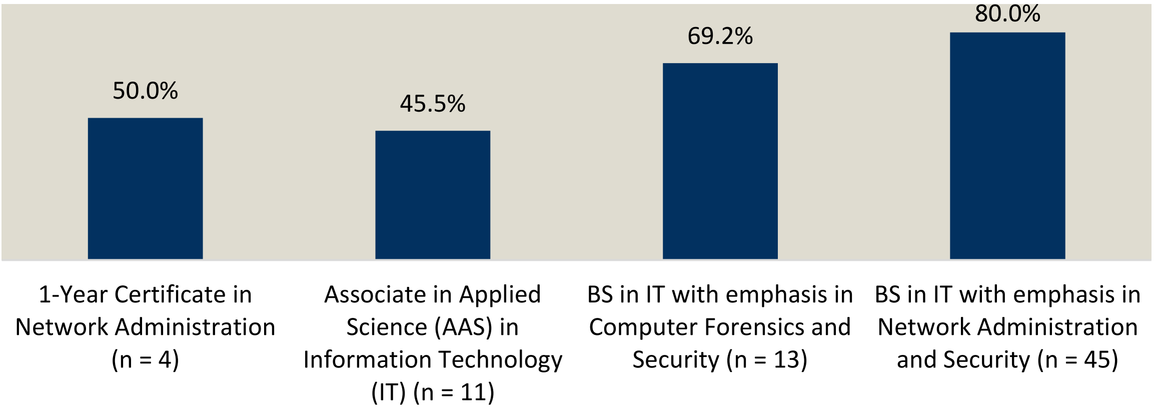
Figure 6. Student Plans to Pursue Another Credential



Employment Outcomes

Participation in CyberSecurity programs led to positive employment outcomes for many students, including a salary increase upon entering or completing the program, as reported by year four student survey respondents in Figure 7. For those employed students who were pursuing Bachelor's degrees in IT, the majority of students anticipated a wage increase upon completion of their degree. In addition, students reported receiving job opportunities as a result of their involvement within the CyberSecurity credential programs. One student said, "Instructors have helped me decide what classes to take and I got a job through a project I did for a class."

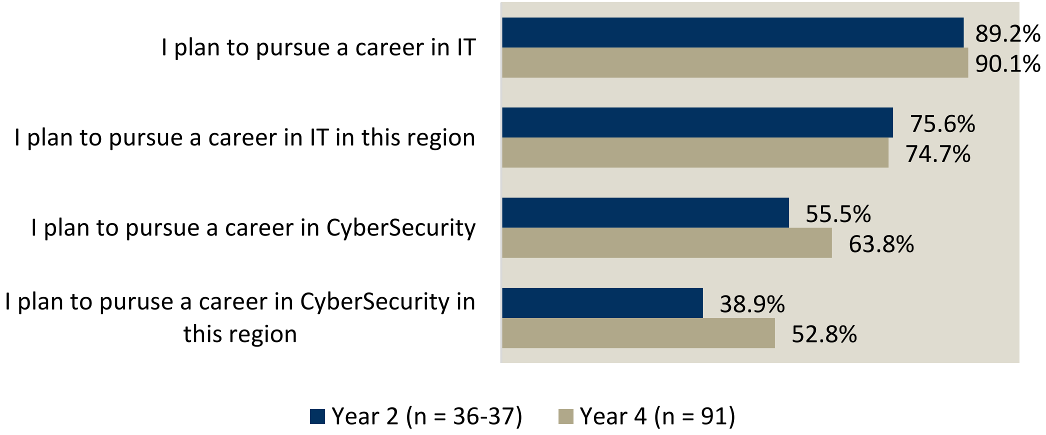
Figure 7. Student Anticipated Wage Increase



Career Plans

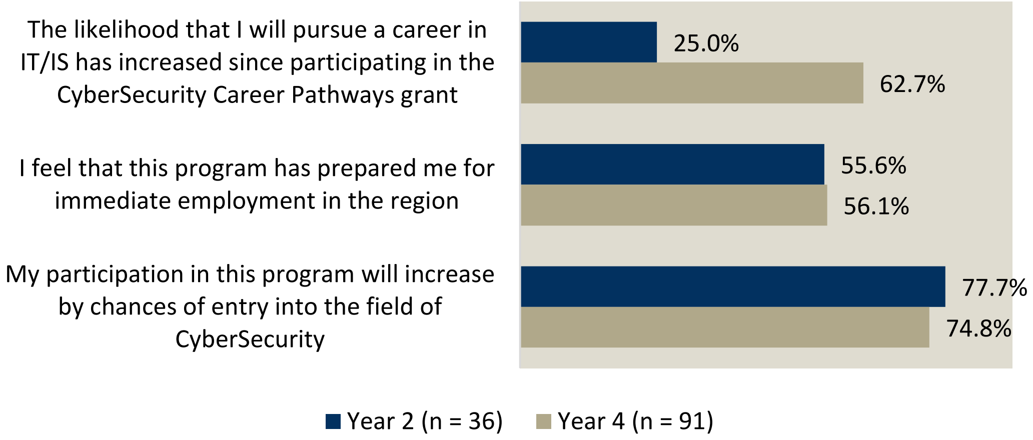
Additional contextual data regarding employment were collected through PRE's student surveys. Students were asked about their plans to pursue a career in IT/IS and CyberSecurity in the region in both the second and fourth years of the grant. Across both years, a majority of students participating in the survey planned to pursue a career in IT/IS (89.2% and 90.1%) and approximately 75% of students planned to pursue this type of work in the region. In year four, approximately two-thirds of participants (63.8%) planned to pursue a career in CyberSecurity and 52.8% planned to do so in the region, both higher than the rates in year two.

Figure 8. Student Career Plans
(% Agree/Strongly Agree)



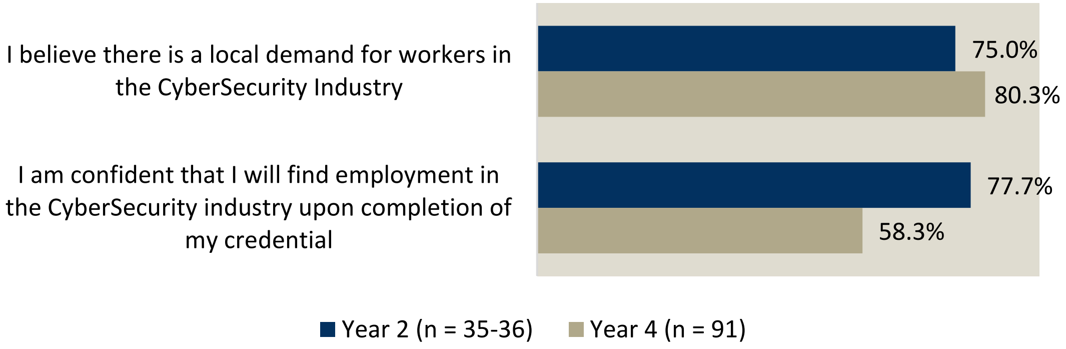
Students were asked a series of questions related to industry demand, program preparation, and likelihood of finding employment upon completion of the credential in both years two and four. In year two, only 25.0% of students credit the grant program as increasing the likelihood of pursuing an IT/IS career, and this number increased to 62.7% by year four. At both time points, just over half of students believed their classes prepared them for immediate employment in the region. (See Figure 9.)

Figure 9. Employment Potential
(% Agree/Strongly Agree)



A majority of students believed there was a local demand for work in CyberSecurity at both time points (75.0% and 80.3%), as illustrated in Figure 10. In year four, 58.3% of students believed they would find employment in the CyberSecurity industry upon completion of their credential, which was a decrease from earlier in the grant when 77.7% of students believe they would find employment.

Figure 10. Industry Demand
(% Agree/Strongly Agree)



Preparation of Students in the CyberSecurity Pathways Program

In terms of how the program prepares students for entry into the field of CyberSecurity, staff explained that the program prepares students for entry-level work in the field, gives them knowledge employers are interested in, and provides students with more awareness about security concerns.

A staff member also noted that the grant provided funding that allowed that them to participate in training that has resulted in embedding the topic of security in their instruction, even when the course is not necessarily focused on security, which gives students further knowledge on the subject:

> "I've utilized the grant as a faculty member for some development activities such as participating in a training course for the CSSIP exam. The experience with courses like that and the training ends up being put into all my classes; I teach IS and IT classes and they may not specifically be a security class, but if it is about networking we talk about security and if it's about health information systems we talk about security. I think pretty much all the faculty who had some of the training that the grant has provided would say the same thing."
>
> *CyberSecurity Staff Member (Y3)*

Program fit for Displaced Workers

According to staff, one of the main ways the UVU CyberSecurity program is a good fit for workers who have been displaced from computer or IT jobs is that students immediately learn employable skills. This allows displaced workers to reenter the workforce quickly and benefit from learning the newest technology, which could also be useful to people currently working in the field who are trying to get a promotion. Another way staff believe this program is a good fit for displaced workers is it helps them to build on skills they already have by allowing them to test out of classes, which gets them back into the workforce faster. In addition, the advanced classes in CyberSecurity are new subject material for most returning workers. This keeps students interested in furthering their education.

Another staff member mentioned that in addition to updating displaced workers on new technology and changes in the field since they were trained, the class schedules are a good fit for these individuals: "At UVU our demographic is the nontraditional student, so we seem to attract folks who are either displaced or working in an industry they don't want to be in and they can come back at night. It is geared schedule-wise to help that kind of person complete the program." Staff members indicated that nontraditional students make up over half of the population in the CyberSecurity program, including dislocated workers and individuals looking for a change in career.

One faculty member gave a specific example of a students who is a veteran and was able to attend the UVU program because it provided financial assistance. This financial assistance also benefits workers who have been displaced from IT/computer jobs: "I had a situation with one of my students who is a veteran and is able to take these CyberSecurity courses because the tuition is being covered."

Program fit for Workers Entering the Field

Staff were also asked how the CyberSecurity program is a good fit for more traditional students who are entering the CyberSecurity field for the first time. A theme in responses was that the program curriculum is designed to teach students employable skills. In addition, the program stays current with trends in the industry so the skills students learn are relevant when they enter the field. In addition, the program teaches basic skills that are the building blocks for more advanced skills. One staff member illustrated this benefit here:

> "I think it is really good for them because they can move into the more advanced CyberSecurity, and have the ability to shift into different areas. For instance, a company in the area used to be traditional software coding and testing, and now they are incorporating a large CyberSecurity component, and that is something that a standard IT or IS program is not going to provide for the student. A student that takes our courses in cyber and has a background in IT can move into other programs and entry level jobs that are highly paid and highly skilled and it gives them a great pathway as they continue their degree to move up in different organizations."
>
> *CyberSecurity Staff Member (Y3)*

Another way the program is a good fit for students who are just entering the CyberSecurity field is the diversity in degree options. This allows students to exit the program into the workforce at any point in their education, which is beneficial to those entering the field, as one staff member stated, "The fact that you can go for one year and have a certificate and some basic understanding of CyberSecurity is a plus for someone who is just trying to get a job in the industry." Staff reported that lower level certificates and degrees are a great way to get a start in the CyberSecurity industry. That process is described by a staff member here: "The program is structured with the five CyberSecurity offerings, with something for everyone. If you are just entering the field, we have something to get you up to speed, and if you are willing to gain more advanced knowledge then you can go for our bachelor's or graduate certificate, and at some point you can even go for a master's degree. The vision is to have something that appeals to various stakeholders in terms of educational needs and their skill level and background."

Program Impact

In order to examine the impact of the CyberSecurity Career Pathways program on student education and employment outcomes, PRE utilized a quasi-experimental comparison cohort design with historical comparison groups. This method allowed us to compare outcomes for participants in the grant-funded training with participants in historical cohorts that were comparable on key dimensions such as learning objectives, credential attainment, and certification outcomes. PRE worked closely with the project team and the UVU institutional research department to determine the best comparison group for each of the treatment groups. Table 9 presents the treatment and comparison cohorts selected for the impact analysis. For the impact study, the treatment group consisted of participants who were enrolled in one the following four CyberSecurity credentials during the first year of the grant: AS in IT, AAS in IT, BS in IT or BS in IS. The historical comparison group consisted of participants who were enrolled in one of these four credentials four years prior to the start of the grant (2008-09). The student cohorts listed in Table 9 will be compared on the outcomes of:

- Program Completion
- Retained in Program of Study
- Credential Earned
- Wage Increase
- Entered Employment
- Retained Employment

Table 9. Impact Analysis Cohorts

Participant Cohort (2012/13 Followed Through Spring 2015)	n	Historical Comparison Cohort (2008/09 Followed Through 2012)	n
AS/AAS in IT	73	AS/AAS in IT	83
BS in IT/IS	215	BS in IT/IS	208

Participant Cohort (2012/13 Followed Through Spring 2015)	n	Historical Comparison Cohort (2008/09 Followed Through 2012)	n
Total Treatment	288	**Total Comparison**	291

Academic Impact

In order to examine the impact of the CyberSecurity Career Pathways program on student academic outcomes, PRE compared completion rates, retention rates, and credential earned for each of the two treatment and historical comparison cohorts, and for the treatment and comparison groups overall. A chi-square test of independence was conducted to test for significant differences between groups and the threshold for significance was p < .05. The tables below present this information and an asterisk denotes a significant difference between cohorts.

Completion and Retention

The treatment cohort for students pursuing a BS in IT/IS showed a higher completion rate when compared to its historical cohort whereas the AS/AAS treatment and historical cohorts showed little difference in completion rates. Overall completion rates for treatment and comparison students in the impact analysis showed a significant difference with 42.4% of treatment group students completing their program of study compared to 30.2% of the comparison group students.

Table 10. Program Completion

Treatment Cohort	n	%	Historical Comparison Cohort	n	%
AS/AAS in IT	17	23.3%	AS/AAS in IT	19	22.9%
BS in IT/IS	105	48.8%*	BS in IT/IS	69	33.2%
Total Treatment	122	42.4%*	**Total Comparison**	88	30.2%

For the outcome of retention, both treatment cohorts showed higher rates of retention compared to their historical cohorts. Overall retention rates for treatment and comparison students in the impact analysis showed a significant difference with 27.8% of treatment group students retained in their program of study compared to 15.8% of the comparison group students.

Table 11. Retention

Treatment Cohort	n	%	Historical Comparison Cohort	n	%
AS/AAS in IT	28	38.4%*	AS/AAS in IT	12	14.4%
BS in IT/IS	52	24.2%*	BS in IT/IS	34	16.3%
Total Treatment	80	27.8%*	**Total Comparison**	46	15.8%

PRE also examined differences between treatment and comparison cohorts for the outcomes of completion and retention combined. Students were included in the sample if they either completed or were retained in their program during the impact study timeframe. When examining those students who either completed or were retained, both treatment cohorts showed higher rates compared to the historical cohorts. Overall rates for those completing or retained in their program of study for treatment and comparison students in the impact analysis showed a significant difference with 64.6% of treatment group students either completing or retained compared to 43.6% of the comparison group students.

Table 12. Completed OR Retained

Treatment Cohort	n	%	Historical Comparison Cohort	n	%
AS/AAS in IT	40	54.8%*	AS/AAS in IT	30	36.1%
BS in IT/IS	146	67.9%*	BS in IT/IS	97	46.6%
Total Treatment	186	64.6%*	**Total Comparison**	127	43.6%

Credential Earned

When examining the outcome of credential earned, the historical AS/AAS in IT cohort showed a higher percentage of students earning credentials than the treatment cohort. The opposite is true for the BS in IT/IS with the treatment group showing a higher percentage of students earning a credential (48.8%) when compared to the historical cohort (39.9%). Overall, the rate of credential earned for the treatment group was slightly higher than the comparison group, but there was not a significant difference between the two groups.

Table 13. Credential Earned

Treatment Cohort	n	%	Historical Comparison Cohort	n	%
AS/AAS in IT	17	23.3%	AS/AAS in IT	29	34.9%
BS in IT/IS	105	48.8%	BS in IT/IS	83	39.9%
Total Treatment	122	42.4%	**Total Comparison**	112	38.5%

Employment Impact

In order to examine the impact of the CyberSecurity Career Pathways program on student employment outcomes, PRE compared the employment outcomes of wage increase, entered employment, and retained employment for each of the treatment and historical comparison cohorts and for the treatment and comparison groups overall. A chi-square test of independence was conducted to test for significant differences between groups and the threshold for significance was p < .05. The tables below present this information and an asterisk denotes a significant difference between cohorts.

Wage Increase

The employment outcome of wage increase was calculated only for incumbent workers, which was defined as those students who were employed during the quarter prior to program entry. Wage increase was determined by comparing a student's wage the quarter prior to enrollment to their wage during the quarter after completion. As shown in Table 14, the BS in IT/IS treatment group cohort showed a higher rate of wage increases when compared to its historical comparison cohort. The overall difference in rate of wage increase for treatment and comparison cohorts was almost 10% and was statistically significant.

Table 14. Wage Increase

Treatment Cohort	n	%	Historical Comparison Cohort	n	%
AS/AAS in IT Incumbent (n = 57)	44/57	77.2%	AS/AAS in IT (n = 62)	49/62	79.0%
BS in IT/IS Incumbent (n = 177)	142/177	80.2%*	BS in IT/IS (n = 150)	100/150	66.7%
Total Treatment (n = 234)	186/234	79.5%*	**Total Comparison (n = 212)**	149/212	70.3%

Entered and Retained Employment

The outcomes of entered and retained employment were calculated for non-incumbent students who completed their program of study. Table 15 presents the number of non-incumbent completers in each cohort.

Table 15. Non-Incumbent Completers

Treatment Cohort	n	Historical Comparison Cohort	n
AS/AAS in IT	15	AS/AAS in IT	21
BS in IT/IS	38	BS in IT/IS	79

The AS/AAS in IT treatment cohort showed lower rates of entered and retained employment when compared to the historical cohorts. The BS in IT/IS treatment cohort showed lower rates of entered employment but higher rates of retained employment than its historical cohort. Overall, the rate of entered employment was slightly lower for the treatment group, but the rate of retained employment was higher for the treatment group.

Table 16. Entered and Retained Employment

Treatment	Entered		Retained		Comparison	Entered		Retained	
	n	**%**	**n**	**%**		**n**	**%**	**n**	**%**
AS/AAS in IT	2/15	13.3%	1/2	50%	AS/AAS in IT	6/21	28.6%	4/6	66.7%
BS in IT/IS	12/38	31.6%	9/12	75.0%	BS in IT/IS	20/79	34.5%	14/20	70.0%
Total	14/53	26.4%	10/14	71.4%	**Total**	26/79	32.9%	18/26	69.2%

The results of the impact study showed positive outcomes for the CyberSecurity Career Pathways participants. The treatment group cohorts showed higher percentages of program completion and program retention. With treatment group percentages at 65% for these outcomes combined, the majority of students enrolled in these new or modified programs are achieving these educational outcomes. The treatment group students showed good employment outcomes as well with 80% of incumbent workers earning a wage increase and 71% of those who entered employment, being retained for at least two quarters. These results suggest that the CyberSecurity Career Pathways program is setting students up for long-term employment.

Evaluation Insights

Although TAACCCT grant funding at UVU concluded in June 2016, PRE would like to offer the following insights regarding the continuation of the CyberSecurity credentials that were developed as part of the CyberSecurity Career Pathways TAACCCT grant. These insights are based solely on the data collected through the evaluation activities referenced in this report.

1. The student tutoring and mentoring positions for CyberSecurity students seemed to be beneficial to students involved in the CyberSecurity credentials. However, the university struggled to find and keep qualified students employed in this position throughout the grant period due to well-qualified students preferring higher paying, full-time positions. PRE encourages UVU to continue exploring models for supporting students enrolled in the CyberSecurity program. If there is an

option to offer academic credit for student tutoring and mentoring positions, this may be incentive for qualified students to offer this support.

2. The industry partner advisory board was a crucial part of the success of the CyberSecurity Career Pathways program. The evaluation teams recommends continuing to engage this group and hold advisory board meetings moving forward. This will allow the program to be current with the needs of the industry and possibly increase the number of local hires from the CyberSecurity program at UVU. The advisory board may also offer support for the development of the master's degree program.

3. A final insight regarding the CyberSecurity program at UVU is regarding the development of a master's degree program in CyberSecurity. The evaluation team heard feedback from stakeholders at various levels including students and staff that a master's degree would be beneficial for the region and utilized by large numbers of students. PRE recommends the university continue with plans to develop the master's program as it will be a valuable addition to the stackable credentials developed as part of the TAACCT grant.

Appendix A. Project Team Focus Group Protocols

Year 2 Project Team Focus Group Questions

1. Can you tell us about the steps that were taken by the institution to create and/or run this training program?
2. What is the administrative structure of the program?
3. How was the curriculum for the programs selected or created?
    - How were your partners involved in this?
    - How is it being used?
4. Was an assessment of students' skills, abilities and interests used to select students into the programs?
    - What assessment tools were used?
    - Who conducted the assessment?
    - How were the results used?
5. What are your expectations for students in the funded programs?
    - How do you expect this program to affect TAA-eligible individuals? (e.g., re-entry into the workforce, fast completion)
6. At this point, what would you identify as the strengths to this training program?
    - How about the weaknesses?

Year 4 Project Team Focus Group Questions

1. How has the CyberSecurity Career Pathways program met your expectations for students who participated?
2. Has the CyberSecurity Career Pathways program met the employment demands in the region?
3. What contributions did partnering organizations make?
    - Program design
    - Curriculum development
    - Recruitment
    - Training
    - Placement
    - Program management
    - Leveraging of resources
    - Commitment to program sustainability
4. What factors contributed to partners' involvement or lack of involvement in the program?
    - Which contributions from partners were most critical to the success of the grant program?
    - Which contributions had less of an impact?
5. What successes stand out from your implementation of the CyberSecurity Career Pathways program over the past few years?
6. What have been some of the barriers to successful implementation of these programs?
7. What are your plans for program sustainability?
    - To what extent are practices being imbedded into broader institutional policy and practice?
8. Do you have any other comments?

Appendix B. Student Survey Protocol

1. I am currently employed (Y/N)
2. I am currently employed in the IT industry (Y/N)
3. I am currently employed in a CyberSecurity position (Y/N)
4. I was already employed in the IT industry before deciding to pursue this credential at UVU. (Y/N)
5. I intended to pursue a career in IT regardless of these offerings at UVU. (Y/N)
6. I intended to pursue a career in CyberSecurity regardless of the offerings at UVU. (Y/N)

7. **Which of the following CyberSecurity credentials are you currently pursuing? (Questions 25-31 stem from Question 7)**
    - ○ 1-Year Certificate in Network Administration
    - ○ Associate in Applied Science (AAS) in Information Technology (IT)
    - ○ BS in IT with emphasis in Computer Forensics & Security
    - ○ BS in IT with emphasis in Network Administration & Security
    - ○ Post-baccalaureate Certificate in CyberSecurity
    - ○ I am not pursuing any of these credentials
        - ▪ What is your program of study? (O/E)
8. **Which of the following CyberSecurity credentials do you have plans to pursue? (check all that apply)**
    - ○ 1-Year Certificate in Network Administration
    - ○ Associate in Applied Science (AAS) in Information Technology (IT)
    - ○ BS in IT with emphasis in Computer Forensics & Security
    - ○ BS in IT with emphasis in Network Administration & Security
    - ○ Post-baccalaureate Certificate in CyberSecurity

Please rate your agreement with the following items (Strongly Disagree to Strongly Agree)

9. I plan to pursue a career in IT.
10. I plan to pursue a career in IT in this region.
11. I plan to pursue a career in CyberSecurity.
12. I plan to pursue a career in CyberSecurity in this region.
13. The likelihood that I will pursue a career in IT has increased since participating in CyberSecurity career pathways program.
14. I feel that this program has prepared me for immediate employment in the region.
15. I have gained IT skills that prepared me for industry certification.
16. I have gained knowledge of CyberSecurity that has prepared me for industry certification
17. My participation in this program will increase my chances of entry into the field of CyberSecurity.
18. I believe there is a local demand for workers in the CyberSecurity industry
19. I am confident that I will find employment in the CyberSecurity industry upon completion of my credential.

Thinking about the CyberSecurity Career pathways program in general, please rate your level of agreement with the following items (Strongly Disagree to Strongly Agree)

CyberSecurity Career Pathways at UVU…

20. …has helped place me in the correct career pathway.
21. …has provided advising resources that otherwise would not have been available to me.
22. … has assisted me in choosing courses that are aligned with my career path.
23. … will help me reach my career goals at a faster pace.
24. What type of job are you planning to pursue upon completion of your credential?
    - Computer Support Specialists
    - Computer Systems Analyst
    - Database Administrator
    - Network and Computer Systems Administrator
    - Computer and Information Systems Manager
    - Other ______________________________

For each credential chosen in Question 7 above, ask the following questions:

25. How did you hear about this program at UVU?
26. Why did you decide to pursue this credential?
27. This program is a good fit for me. **(1= SD; 5 = SA)**
    - 11a. If student answers SA or A, ask "Why is this program a good fit for you?"
    - 11b. If student answers SD or D, ask "Why is this program not a good fit for you?"
28. I would recommend this program to another student interested in CyberSecurity. **(1= SD; 5 = SA)**
29. Do you have suggestions for improving this program of study?
30. Upon completion of this credential, do you anticipate that you will receive a salary increase at work. (Y/N/NA)
31. Upon completion of this credential, do you plan to pursue another CyberSecurity credential?
    - If yes, which credential?

Open Ended Questions

32. How did you hear about CyberSecurity career pathways program? (OE)
33. Please describe any career guidance you have received through the CyberSecurity career pathways program? (OE)
34. Please describe any anticipated obstacles to program completion. (OE)
35. Do you have any suggestions for improving the CyberSecurity Career pathways program? (OE)
36. Do you have any other comments about CyberSecurity Career pathways program? (OE)

Appendix C. Student Focus Group Questions

1. What program are you in and what is your emphasis? How long have you been in the program?
2. How did you hear about the CyberSecurity Pathways program at UVU?
3. What kind of advising services have you received at UVU? How was your experience?
4. What are your education plans?
5. What are your career plans?
6. What type of opportunities have you received because of your participation in the program?
7. What do you think the biggest barriers might be in completing this program?
8. Do you have any suggestions for improving the program?
9. Do you have any other comments?

Appendix D. Staff Phone Interview Protocol

1. Can you briefly explain your role in the CyberSecurity program at UVU and how long you have been involved?
2. What do you see as the strengths of the program at this point in time?
3. How does this program prepare students for entry into the field of CyberSecurity?
4. In what ways is this program a good fit for workers who have been displaced from computer/IT jobs?
    - How about for those workers just entering the field?
5. What advising resources have been made available to students through this program?
6. Can you discuss how students have received career guidance through the CyberSecurity program?
7. What has been the most useful aspect of working with the advisory board members in program development?
8. What are the areas for improvement in the program at this point in time?
9. What are your wishes for program sustainability?
10. Do you have any additional comments about the CyberSecurity program?

Appendix E. Advisory Board Phone Interview Protocol

1. Can you start by talking about how you have been involved in the Cybersecurity Pathways program at UVU over the past year?
    - Which program elements?
    - Have you contributed to the design of the program or curriculum?
    - Assisted with recruitment?
    - Other areas of involvement?

2. What factors have contributed to your level of involvement in the Cybersecurity Pathways program? Are there things that have made it easier or more difficult for you to participate? (Is the team easy to work with, has communication been good, anything that could make the process better?)
    - Would you like more or less involvement in the coming year? (elaborate)

3. What are your expectations for the new or expanded Cybersecurity Pathways program at UVU?
    - Expectations for student participation (in the program)
    - Expectations for how this will impact your company?
        i. What positions are these students likely to enter within your organization?

4. How do you see this program impacting the IT industry in your region?

5. What are the strengths of the Cybersecurity Pathways program at this point in time?

6. What are the barriers or challenges of the Cybersecurity Pathways program at this point in time?

7. Do you have any other comments about the Cybersecurity Pathways program at UVU?

Appendix F. Advisory Board Focus Group Protocols

Year 3 Advisory Board Focus Group Questions

1. What are the strengths of the program?
2. How do you envision your involvement with the program?
3. How do you envision your involvement after the grant period ends?
4. What are ways you see to get other organizations involved in the CyberSecurity program at UVU?
5. What are areas of improvement for the program?

Year 4 Advisory Board Focus Group Questions

1. Do you have examples of how the expanded Cybersecurity Career Pathways program at UVU has impacted your organization?
2. Have you made any hires out of the expanded Cybersecurity Career Pathways program?
    - Do you notice any differences in these employees compared to other hires?
3. Is there anything you would like to be more involved with as an advisory board member?
4. What do you see as the role for your organizations after the grant ends?
5. What stands out as the greatest successes of this program?
6. From your perspective, what have been some of the barriers to successful implementation of these programs?
7. Do you have any other comments about the Cybersecurity Career Pathways Program at UVU?