WORKFORCE STUDY: COMMUNITY COLLEGE CYBERSECURITY ALUMNI

WHERE ARE THEY NOW?

John Sands, Moraine Valley Community College
Corrinne Sande, Whatcom Community College

ABSTRACT

Community colleges have increased the number of cybersecurity professionals that graduate from their programs each year. These individuals are finding employment in every sector of our economy and are addressing the nation's shortage. The federal government led by the NIST/NICE Project have been able to better define the nations cybersecurity workforce through a list of 52 specialized cybersecurity work roles. This study was designed to examine the type of cybersecurity jobs filled by community college graduates and how they align to the NICE frameworks job roles. This study was conducted as a partnership between the National Cybersecurity Training and Education Center (NCyTE) and the Center for Systems Security and Information Assurance (CSSIA) and was funded by the NSF. The study examined graduates from 12 of the nation's top community college cybersecurity programs. The study is based on student interviews and self-identification of their current cybersecurity work roles. Doctoral candidates from Dakota State University interviewed the alumni and collected survey data. The results were analyzed and published by Dr. John Sands and Corrinne Sande. The study reveals the type of positions community college students are prepared for. The study highlights current trends and identifies potential opportunities for community college graduates.

RATIONALE

This study, like many others is addressing the worldwide growing threat of cybercrime and the nation's shortage of cybersecurity professionals. What distinguishes this study from others is specifically focusing on the contributions community college cybersecurity programs are making in addressing the worldwide shortage of cyber professionals. The cybersecurity workforce In the US is growing yet is currently not able to keep up with the national demand. While the cybersecurity workforce shortage continues to grow, the challenge faced by organizations, businesses and individuals is expanding at an alarming rate. In 2017, 447 million consumer records were reported stolen. This is an increase of 126% over the prior year. Nearly 60 million Americans were affected by identify theft last year according to a survey by the Harris Polls. The fastest growing threat, ransomware, costs have predicated to hit 20 billion dollars in 2021 up from 11.5 billion in 2019. Ransomware attacks increased by 350% in 2018 alone. Each of these statistics clearly reveals the cyber threat is expanding and affecting all aspects of business and individual privacy. Businesses and individuals are reacting by investing in new technologies, products and the employment of an ever-expanding cybersecurity workforce.

Figure 1: AACC membership database, January 2019. Represents regionally accredited primarily associate degree

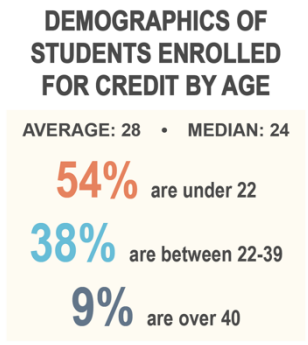


Figure 2: NCES (2018). 2015-16 National Postsecondary Student Aid Study (NPSAS:16)

The cybersecurity workforce gap has been well studied and is expected to continue to grow even as many of our nation's cybersecurity programs have grown stronger and are graduating more students. It is estimated that 3% of the nation's college graduates pursue occupations in the cybersecurity industry. There is consensus that community colleges have potential of contributing to solving the cybersecurity workforce shortage. This consensus is based on several unique aspects of the community college institution. As of 2018, there were approximately 941 public community colleges in the United States. (*Figure 1*) Approximately 28% of community college students graduate in their program of study. Unlike 4-year institutions, the average age of the community college student is 28 years old and the median age is 24. (*Figure 2)* A significant portion of community college students are working professionals interested in changing careers. These students bring a wealth of workforce experience and cultural diversity. As of fall, 2018, just under 7 million students were enrolled in 2-year post-secondary institutions and 839,855 completed an associate degree and 549,149 completed career and technical certificates. About 42,600 students earn an associates degree each year. Thirty seven percent of community college students are full time while 63% are part time students.

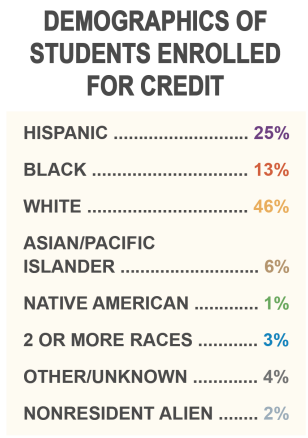


Figure 3: NCES (2018). IPEDS Fall 2017 Enrollment Survey.

The US has a total cybersecurity workforce of approximately 716,000 and a reported shortage of 314,000 according to CyberSeek (https://www.cyberseek.org/heatmap.html). It is predicted that women will represent 20% of the global cybersecurity workforce by the end of 2019. This is up from 11%.

This is a similar trend in attendance at community colleges. Community college populations are majority women and in 2018, 56% of community college students were female. (*Figure 4*)

Over the last 15-20 years, community colleges across the nation have established and operated cybersecurity programs. There has been minimal research examining the effectiveness and impact of these programs. This study specifically tracks community college alumni recording their current employment and the alignment of their current occupation to the NIST/NICE 52 job roles.

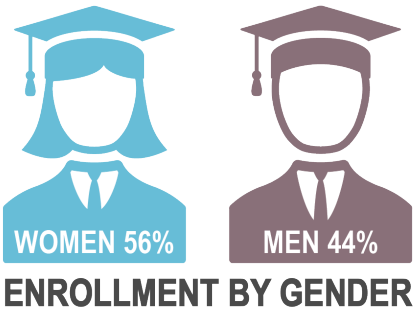


Figure 2: NCES (2018). IPEDS Fall 2017 Enrollment Survey [AACC analysis]

RESEARCH METHODOLOGY

Study Design

The design of this study was based on narrative inquiry of recent community college graduates from cybersecurity programs. The research team selected 12 leading community college cybersecurity programs from across the country. Each program was represented by an institutional gatekeeper that worked with the research team in identifying employed program graduates. The 12 institutions included in the study are listed in the table below.

COLLEGE	GATEKEEPER
Brookdale Community College	Michael Qaissaunee
College of Southern Nevada	Margret Taylor
City College of San Francisco	Richard Wu
Florida State College in Jacksonville	Ernie Friend
Forsyth Technical College	Deanne Wesley
Ivy Technical College	Jiri Jirik/Pam Schmelz
Johnson County Community College	Andrew Lutz
Moraine Valley Community College	Kevin Vaccaro
Prince George Community College	Casey O'Brien
San Antonio Community College	Kim Muschalek
Sinclair Community College	Kyle Jones
Whatcom Community College	Corrinne Sande/Stephen Troupe

Each institution self-selected the participants in the study to reflect successful students that found employment in the cybersecurity sector after graduation. The narrative included individual interviews with each graduate. These interviews were phone interviews and took between 20 minutes and a half hour. The study contracted with PhD candidates enrolled in a cybersecurity program at Dakota State University. These researchers were enrolled in a methods class as part of their doctoral coursework. Each researcher participated in processing institutional review board documentation and helped design an online instrument to collect relevant data from the interviews. Researchers followed a protocol that required collection of specific data and allowed for follow up inquiry to gain a deeper understanding of the data collected.

Hypothesis

The hypothesis of this study was to determine which of the 52 NICE cybersecurity work roles community college graduates are currently able to fulfill. Each study participant was asked to provide personal contact information, information about their current employer, their current title, the type of program they graduated from and which work role they have or currently fulfilling within their organization.

Acknowledging Biases and Conflicts

Conflict of interest has been the subject of discussion and concern in almost all social studies. Avoiding conflict of interest in order to achieve sound, unbiased science is in the vested interest of the social scientific community as well as the general public. However, creating a system in which scientific decisions are made in an ethical manner while free of bias and conflict is a challenge. This study was funded by the National Science Foundation Division of Undergraduate Education within the Advanced Technological Education Program. This program primarily funds community and 2-year college technical programs. The study was conducted by community college staff from Moraine Valley Community College and Whatcom Community College. The purpose of the study was not to promote community college programs but to identify the impact of their programs and the challenges they face in preparing students for today's cybersecurity workforce.

Trustworthiness of Data

The trustworthiness of qualitative research generally is often questioned by positivists, perhaps because their concepts of validity and reliability cannot be addressed in the same way in naturalistic work. Nevertheless, several writers on research methods, notably Silverman [1], have demonstrated how qualitative researchers can incorporate measures that deal with these issues, and investigators such as Pitts [2] have attempted to respond directly to the issues of validity and reliability in their own qualitative studies.

Questioning the validity of survey data is often one of the first reactions when survey results are shared. One way to avoid accepting the new information is to simply choose to consider it as invalid. Nonetheless, it is important to be able to understand and convey that the science behind collecting data through self-reporting methods is valid and reliable. The research team took steps to designing this study to increase data collection accuracy and question potential data outliers.

Each researcher performing interviews came to the study with a background in cybersecurity, cybersecurity education or support or management of cybersecurity education programs. Researchers also had a working knowledge of the NIST/NICE framework and the 52 work roles examined in the study. Finally, researchers were provided research protocols that encouraged follow up questions to better understand responses and to clarify and substantiate data outliers.

Data Collection Instrument & Protocol

The Data Collection process began with the development of an online survey. The online survey included the following items:

- Contact information for each participant interviewed including email address, phone number and mailing address.
- Academic information including the school they attended, the programs they graduated from and the academic credentials they earned.
- Industry certifications earned.
- Their perception of workforce preparedness after completing academic program.
- Ability and timeline to find employment in cybersecurity occupation.
- Current job title and organization they work for (if able to share it).
- Initial position with current company and any upward mobility.
- Workforce training or mentorship participated in.
- Years employed in cybersecurity.
- Description of current job responsibilities.
- Name of the division they are employed with.

The second half of the survey has students self-identify which of the 52 NICE work roles they have or currently fulfill.

NICE Specialty Area	Work Role
Securely Provision (SP)	
Risk Management (RSK)	Authorizing Official/Designating Representative
	Security Control Assessor
Software Development (DEV)	Software Developer
	Secure Software Assessor
Systems Architecture (ARC)	Enterprise Architect
	Security Architect
Technology R&D (TRD)	Research & Development Specialist
Systems Requirements Planning (SRP)	Systems Requirements Planner
Test and Evaluation (TST)	System Testing and Evaluation Specialist
Systems Development (SYS)	Information Systems Security Developer
	Systems Developer
Operate and Maintain (OM)	
Data Administration (DTA)	Database Administrator
	Data Analyst
Knowledge Management (KMG)	Knowledge Manager
Customer Service and Technical Support (STS)	Technical Support Specialist
Network Services (NET)	Network Operations Specialist
Systems Administration (ADM)	System Administrator
Systems Analysis (ANA)	Systems Security Analyst

NICE Specialty Area	Work Role
Oversee and Govern (OV)	
Legal Advice and Advocacy (LGA)	Cyber Legal Advisor
	Privacy Officer/Privacy Compliance Manager
Training, Education, and Awareness (TEA)	Cyber Instructional Curriculum Developer
	Cyber Instructor
Cybersecurity Management (MGT)	Information Systems Security Manager
	Communications Security (COMSEC) Manager
Strategic Planning and Policy (SPP)	Cyber Workforce Developer and Manager
	Cyber Policy and Strategy Planner
Executive Cyber Leadership (EXL)	Executive Cyber Leadership
Program/Project Management (PMA) and Acquisition	Program Manager
	IT Project Manager
	Product Support Manager
	IT Investment/Portfolio Manager
	IT Program Auditor
Protect and Defend (PR)	
Cybersecurity Defense Analysis (CDA)	Cyber Defense Analyst
Cybersecurity Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist
Incident Response (CIR)	Cyber Defense Incident Responder
Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst
Analyze (AN)	
Threat Analysis (TWA)	Threat/Warning Analyst
Exploitation Analysis (EXP)	Exploitation Analyst
All-Source Analysis (ASA)	All-Source Analyst
	Mission Assessment Specialist
Targets (TGT)	Target Developer
	Target Network Analyst
Language Analysis (LNG)	Multi-Disciplined Language Analyst
Collect and Operate (CO)	
Collection Operations (CLO)	All Source-Collection Manager
	All Source-Collection Requirements Manager
Cyber Operational Planning (OPL)	Cyber Intel Planner
	Cyber Ops Planner
	Partner Integration Planner
Cyber Operations (OPS)	Cyber Operator
Investigate (IN)	
Cyber Investigation (INV)	Cyber Crime Investigator
Digital Forensics (FOR)	Law Enforcement /Counterintelligence Forensics Analyst
	Cyber Defense Forensics Analyst

The major focus of this instrument is to identify the type of positions leading cybersecurity community college program graduates are able to fulfill when aligned to the NICE work roles. The instrument should also help identify which programs and credentials result in graduates' career options. The research

designers understand other variables come into play including which industries and companies exist within each community college region.

Protocol

The protocol established for the study required each researcher to complete all IRP institutional policies, procedures and forms. The team at Whatcom Community College collected and stored this information. Researchers were informed that some participants would not be able to share some employment data including the company and division they are employed with. Others may have limitations in sharing their current job roles and responsibilities. Each researcher was briefed on the NICE framework including the seven categories of work specialization areas and the 52 work roles so they would be better able to answer questions subjects may have in understanding the different work roles. The NICE specialization framework spreadsheet was also shared with researchers and participants. The protocol also encouraged researchers to have follow up questions to dig deeper into interview responses that could be classified with outlier data or unexpected responses.

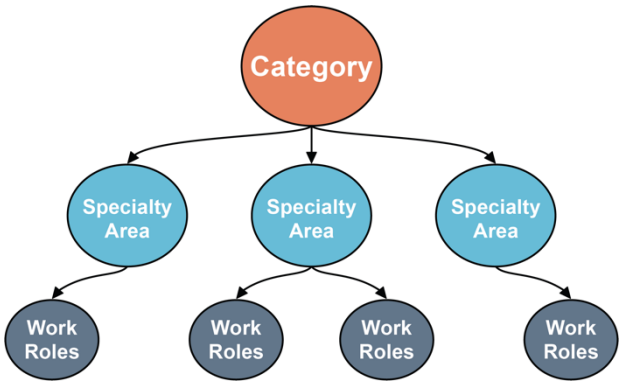
STUDY PARTICIPANTS

Participants

The study participants were limited to graduates of one of twelve contributing community colleges. Each community college gatekeeper identified twelve to fifteen graduates. The gatekeepers had firsthand knowledge that these individuals found employment in the cybersecurity occupation. Second, the gatekeepers reached out and informed each graduate that their name was submitted to participate in this study. As a result, the survey had a much higher than normal participation rate. Approximately 82.4% of the graduates agreed to participate and 67.2% were able to complete the entire survey. There was a small percentage of participants that could not share details of their employment status due to security restrictions. In total, 88 participants fully completed the survey. All participants in this study had graduated their programs within the last 10 years. A large percentage of the graduates completed an associate's degree and technical certificates.

ANALYSIS

All data was collected using an online survey tool. This tool incorporated data aggregation features, graphing and simple comparative analysis. The focus of the study was to analyze factors that prepared students for their current work roles. The study also analyzed student employment data when aligned to the NICE framework. This includes alignment to the workforce categories, specialty

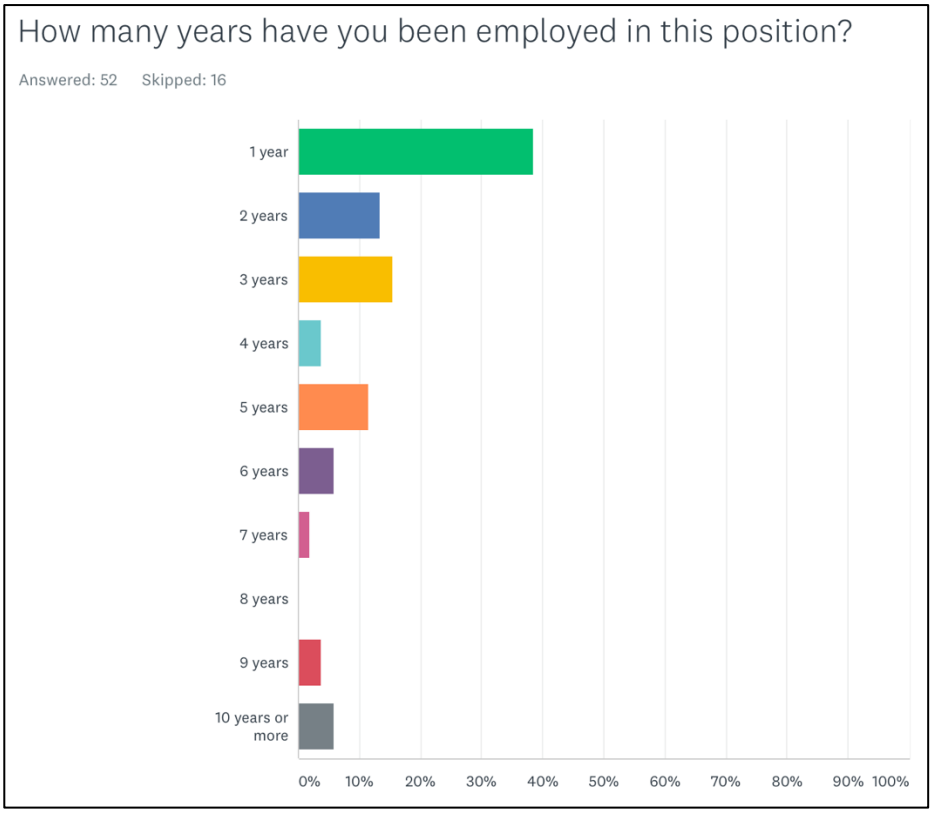


areas and 52 work roles. The analysis also included exploration of data outliers and unexpected survey results. In general, it was expected based on the nature of the work that the majority of students graduating community college technical programs would align to two of the seven workforce categories. The two categories include operate and maintain and protect and defend.

FINDINGS

The study asked students to identify factors that prepared them for the workforce. These factors included the type of academic credentials they earned, industry certifications received and their perception of preparedness for the cybersecurity workforce upon graduation.

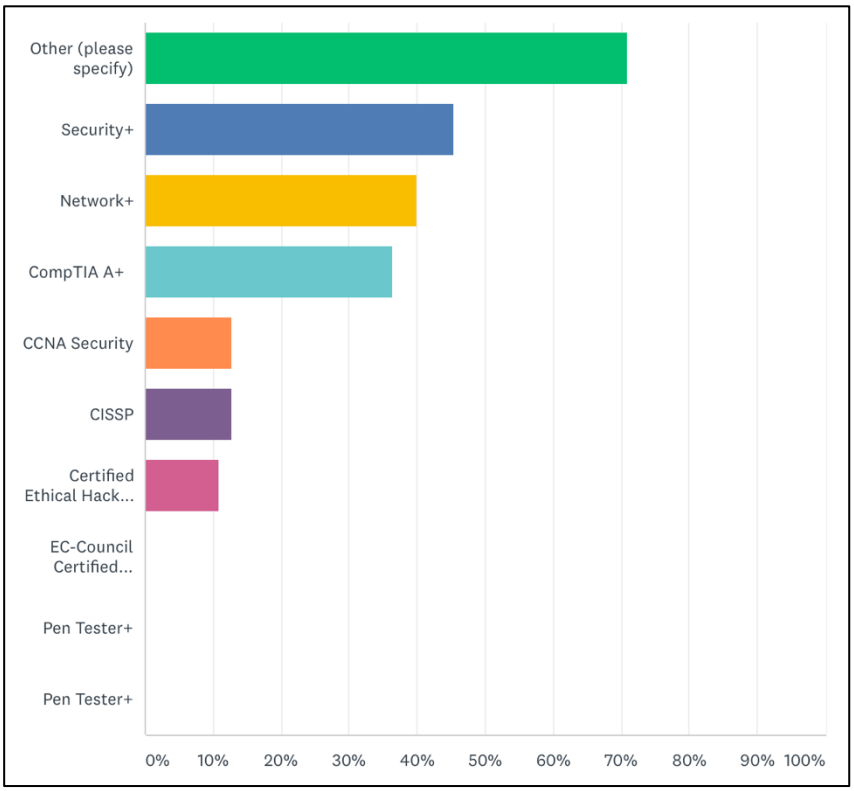
Students in the survey all graduated within the last 10 years and the chart below provides a breakdown of number of years since graduation.



When students were asked to identify their perception of workforce readiness based on graduation from their programs, 65% felt strongly that their programs prepared them for their current role in the cybersecurity workforce and 19% agreed that the programs well prepared them for these positions. Therefore, 16% of the respondents were neutral or negative with their opinion of preparedness based on graduation in their programs. The study also had students self-identify the type of academic degrees or certificates earned during their academic program at once of the twelve community colleges. Sixty seven percent of the participants earned an associate of applied science degree, 86% of the participants

identified completion of a two-year degree which would include AAS, AA or AS. Fourteen percent of the participants graduated without completing a two-year degree but did identify completion of technical academic certificates. Each participant also was asked to self-identify which cybersecurity related industry certifications they hold. The chart below represents the results.

Security + was the most popular certification earned at 45.45%. CCNA Security at 12.7%, CEH was 10% and CISSP was 12.7%. Other industry certifications were self-identified but not listed in the survey including Linux, Microsoft, Palo Alto and Cisco certifications. Overall, 73% of survey participants earned at least one certification, 46.4% earned at least two certifications and 24.9% earned three or more certifications.



The primary focus of this study was to identify how community college cybersecurity graduates current employment aligned to the NIST/NICE framework. Each student was asked to review the entire list of 52 work roles and self-identify which of those work roles they have or are currently fulfilling with their current employer. Participants were asked to review the associated knowledge and skills if there was confusion or questions interpreting each of the individual work roles. The following data is a summary of the student responses.

WORKFORCE STUDY DATA			
NICE Specialty Area	**Response**	**Work Role**	**Response**
Securely Provision (SP): 86 Total Responses			
Risk Management (RSK)	14	Authorizing Official/Designating Representative	5
		Security Control Assessor	9
Software Development (DEV)	10	Software Developer	5
		Secure Software Assessor	5
Systems Architecture (ARC)	28	Enterprise Architect	11
		Security Architect	17
Technology R&D (TRD)	7	Research & Development Specialist	7
Systems Requirements Planning (SRP)	7	Systems Requirements Planner	7
Test and Evaluation (TST)	9	System Testing and Evaluation Specialist	9
Systems Development (SYS)	11	Information Systems Security Developer	7
		Systems Developer	4
Operate and Maintain (OM): 213 Total Responses			
Data Administration (DTA)	21	Database Administrator	13
		Data Analyst	8
Knowledge Management (KMG)	9	Knowledge Manager	9
Customer Service and Technical Support (STS)	47	Technical Support Specialist	47
Network Services (NET)	62	Network Operations Specialist	62
Systems Administration (ADM)	53	System Administrator	53
Systems Analysis (ANA)	21	Systems Security Analyst	21
Oversee and Govern (OV): 143 Total Responses			
Legal Advice and Advocacy (LGA)	5	Cyber Legal Advisor	3
		Privacy Officer/Privacy Compliance Manager	2
Training, Education, and Awareness (TEA)	18	Cyber Instructional Curriculum Developer	7
		Cyber Instructor	11
Cybersecurity Management (MGT)	30	Information Systems Security Manager	24
		Communications Security (COMSEC) Manager	6
Strategic Planning and Policy (SPP)	14	Cyber Workforce Developer and Manager	4
		Cyber Policy and Strategy Planner	10
Executive Cyber Leadership (EXL)	2	Executive Cyber Leadership	2
Program/Project Management (PMA) and Acquisition	74	Program Manager	14
		IT Project Manager	24
		Product Support Manager	22
		IT Investment/Portfolio Manager	0
		IT Program Auditor	14

WORKFORCE STUDY DATA (cont.)			
NICE Specialty Area	**Response**	**Work Role**	**Response**
Protect and Defend (PR): 103 Total Responses			
Cybersecurity Defense Analysis (CDA)	33	Cyber Defense Analyst	33
Cybersecurity Defense Infrastructure Support (INF)	18	Cyber Defense Infrastructure Support Specialist	18
Incident Response (CIR)	26	Cyber Defense Incident Responder	26
Vulnerability Assessment and Management (VAM)	26	Vulnerability Assessment Analyst	26
Analyze (AN): 33 Total Responses			
Threat Analysis (TWA)	21	Threat/Warning Analyst	21
Exploitation Analysis (EXP)	7	Exploitation Analyst	7
All-Source Analysis (ASA)	1	All-Source Analyst	1
		Mission Assessment Specialist	0
Targets (TGT)	4	Target Developer	1
		Target Network Analyst	3
Language Analysis (LNG)	0	Multi-Disciplined Language Analyst	0
Collect and Operate (CO): 15 Total Responses			
Collection Operations (CLO)	1	All Source-Collection Manager	1
		All Source-Collection Requirements Manager	0
Cyber Operational Planning (OPL)	7	Cyber Intel Planner	1
		Cyber Ops Planner	2
		Partner Integration Planner	4
Cyber Operations (OPS)	7	Cyber Operator	7
Investigate (IN): 24 Total Responses			
Cyber Investigation (INV)	8	Cyber Crime Investigator	8
Digital Forensics (FOR)	16	Law Enforcement /Counterintelligence Forensics Analyst	5
		Cyber Defense Forensics Analyst	11

The participant responses aligned with many of our pre survey perceptions but there were some significant surprises in several outlying data points. The largest category of responses was as predicted which was Operate and Maintain having 213 work role hits; the two largest being Network Operations Specialist and System Administrator. These job roles, knowledge skills and abilities align directly to the programs offered at each of the twelve participating community colleges. The second highest category was Oversee and Govern with 143 hits. This level was not necessarily expected; however, feedback from business and industry advisory board members have expressed a need for students to be better prepared to support organizations, governance, risk management and compliance programs. The third highest category was Protect and Defend (103). Within this category, Cyber defense Analyst and Cyber

defense Incident Responders drew the greatest number of hits. The categories that drew significantly fewer participant hits were Collect and Operate (15), Investigate (24) and Analyze (33).

In conclusion, the community college cybersecurity workforce study results support the program content and knowledge and skills taught in the twelve participating institutions. The study also indicates community college programs need to better support the knowledge and skills found in the Overseeing Governance category. The majority of study participants identified these work roles in their current positions. Data from the study also indicates community college programs would benefit by incorporating additional specialty skills in the Analyze and Investigate categories. Areas of additional investigation would include tracking, occupational pathways, better understanding career mentoring and learning opportunities and a potential study to investigate associations between industry certifications and specific NICE work roles and/or geographic variables in the NICE framework work roles.

REFERENCES

AACC. (2019). Fast Facts. [online] Available at: https://www.aacc.nche.edu/research-trends/fast-facts/.

Morgan, S. (2019). 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics. [online] Cybercrime Magazine. Available at: https://cybersecurityventures.com/cybersecurity-almanac-2019

MOST of Us Project. (2011). Validity of Self-Report Survey Data. Retrieved from https://www.minnetonkaschools.org/uploaded/Documents/Dist/Tonka_Cares/Reveal_What's_Real/Validity_of_Self_Report.pdf

Newhouse, W., Keith, S., Scribner, B. and Witte, G. (2019). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. [online] Doi.org. Available at: https://doi.org/10.6028/NIST.SP.800-181.

Sands, J. (2019). 2019 NSF Workforce Study of Cybersecurity Alumni. Alexandria, VA: National Science Foundation.

Shenton, A. K. (2004). Strategies for Ensuring Trustworthiness in Qualitative Research Projects. Education for Information, 22(2), 63–75. Available at: https://pdfs.semanticscholar.org/cbe6/70d35e449ceed731466c316cd273032b28ca.pdf