Future Directions : 2022 Summit

The Role of Community Colleges in Cybersecurity Education

June 26-28, 2022 in Alexandria, Virginia

NSF

NATIONAL CYBERWATCH CENTER

CSSIA
National Support Center for Systems Security and Information Assurance

NCYTE CENTER

Thank you to our summit sponsors!

us bank®

ISACA®

CSA cloud security alliance®

EC-COUNCIL | ACADEMIA

JONES & BARTLETT LEARNING
An Ascend Learning Company

stanly CC
COMMUNITY COLLEGE

ISACA®
Los Angeles Chapter

cisco™ Networking Academy

NDG

NSF

The **Future Directions: 2022 Summit** - ***The Role of Community Colleges in Cybersecurity Education*** is funded by a National Science Foundation Advanced Technological Education Grant #1937905.

Table of Contents

Summit Sponsors 1

Table of Contents 2

Welcome Messages 3

Organizing Institutions 4

Summit Agenda 5

Presidents Forum & Pathways Panel 8

Concurrent Session Topics 9

Keynote Speakers 17

Presenter Bios 21

Poster Reception 31

Alexandria Floorplan 33

Welcome!

The National Cybersecurity Training & Education Center (NCyTE) is excited to welcome you to our two-day Future Directions 2022 Summit!

We are thrilled to be able to gather in-person with so many leaders and stakeholders in cybersecurity education to examine the essential role community colleges play in addressing the growing, critical shortage of qualified cybersecurity workers in the U.S.

In 2002, the National Science Foundation (NSF) and the American Association of Community Colleges co-sponsored a workshop and resulting report titled, 'Protecting Information: The Role of Community Colleges in Cybersecurity Education.' Nearly 20 years later, cybersecurity education has evolved dramatically – and, along with it, the cybersecurity threats and needs of the nation. Community colleges use innovative outreach initiatives and relevant curriculum programming to reach untapped, diverse, potential new student populations that they traditionally serve. These strategies are a vital component in closing the workforce gap.

Over the next two days, we look forward to working with some of the most influential minds in cybersecurity education to discuss the progress and impacts of community colleges on workforce development that directly support national and economic security, and contribute to recommendations for the future. This Summit is organized by the National Cybersecurity Training & Education Center (NCyTE) in partnership with the Center for Systems Security & Information assurance (CSSIA) and the National CyberWatch Center.

Preventing Discrimination, Harassment, and Bullying

Please read carefully through the following expectations for participants in The Role of Community Colleges in Cybersecurity Education: Future Directions 2022 Summit.

The Organizers of The Role of Community Colleges in Cybersecurity Education: Future Directions 2022 Summit are committed to the principles of diversity, integrity, civility, and respect in all of our activities. We look to you to be a partner in this commitment during your Summit participation by helping us to maintain a professional and cordial environment. All forms of discrimination, harassment, and creating a hostile environment or bullying are prohibited in any Summit activity. This commitment applies to all participants in all settings and locations in which Summit work and activities are conducted, including meals, receptions, focus groups, presentations, and other work and social functions where Summit participants, volunteers, sponsors, vendors, hotel employees or guests are present.

Relevant Definitions

Relevant definitions regarding discrimination, harassment, creating a hostile environment / bullying and related considerations are available upon request.

Reporting and Resolution

Any violation of this Summit policy should be reported. If you experience or witness discrimination, harassment, or bullying, please report the incident to Janice Walker, Senior Personnel/Special Projects Director for Cybersecurity Grants, Whatcom Community College (WCC); phone: 360.383.3282; email: jwalker@whatcom.edu

Organizing Institutions

NCyTE CENTER

The National Cybersecurity Training and Education Center (NCyTE) at Whatcom Community College (WCC) is an Advanced Technological Education (ATE) National Center, grant-funded by the National Science Foundation (NSF).

NCyTE advances cybersecurity education in the U.S. by supporting technological innovation, creating and disseminating resources, and providing professional development and tools to support faculty, community colleges, and the workforce pipeline of tomorrow.

NCyTE is focused on building a comprehensive network of higher education institutions, businesses, and government agencies dedicated to developing and maintaining a robust cybersecurity workforce.

CSSIA
National Support Center for Systems Security and Information Assurance

The Center for Systems Security and Information Assurance (CSSIA) is a National Science Foundation (NSF) Advanced Technological Education (ATE) National Resource Center. Since 2003, CSSIA has provided students with real-world learning experiences in information assurance and network security through several program improvement supportive initiatives.

CSSIA National Resource Center Goals:

- Maintain and develop cybersecurity related curriculum content including instructional materials, assessment instruments, lab activities and and virtual student skills competition environments.
- Building a national infrastructure of qualified cybersecurity educators.
- Developing national infrastructure remote virtualization lab environment and content.
- Increase the number of minority, women, veterans and other underrepresented groups in the cybersecurity and information assurance professions.

NATIONAL CYBERWATCH CENTER

A consortium of higher education institutions, public and private schools, individual cybersecurity practitioners, businesses, and government agencies focused on collaborative efforts to advance cybersecurity education and strengthen the national cybersecurity workforce.

Our roles include: advocating for cybersecurity education programs; building cybersecurity education and workforce development programs; collaborating with educational institutions, businesses, government entities, and professional organizations; and coordinating collaborative cybersecurity education, assessment, and research programs.

Summit Agenda

Day One - June 26, 2022

TIME	EVENT	LOCATION
9:00 am – 1:00 pm	Effective Change Management: Strategies for successful cybersecurity project and grant implementation workshop *restricted to new NSF ATE grantees	Rosemont
5:00 pm – 6:00 pm	Conference Registration Opens Sponsor Set-up Sponsor Check-in	Old Town Ballroom Foyer Old Town Ballroom Foyer Old Town Ballroom
6:00 pm – 8:00 pm	No-host Dinner	Local Restaurants

Day Two - June 27, 2022

TIME	EVENT	LOCATION
7:00 am – 8:00 am	Conference Registration Opens Breakfast	Old Town Ballroom Foyer Rosemont
8:00 am – 8:10 am	Welcome – Center Directors	Old Town Ballroom
8:10 am – 8:20 am	Welcome – Dr. Corby Hovis, Program Director, National Science Foundation	Old Town Ballroom
8:20 am – 8:30 am	Welcome – Dr. Kathi Hiyane-Brown, President, Whatcom Community College	Old Town Ballroom
8:30 am – 9:10 am	Opening Keynote – Hack the Gap: Fixing Cybersecurity's Broken Talent Pipeline— *Will Markow*	Old Town Ballroom
9:10 am – 9:25 am	**Welcome – Center Directors**	
9:25 am – 11:15 am	**Concurrent Sessions – Author Presentation & Focus Group Discussion**	
	Workforce Study: Community College Cybersecurity Alumni - Where Are They Now? — *Dr. John Sands, Moraine Valley Community College*	Old Town West
	CyberCorps Scholarship for Service Program: The Expanding Role of Community Colleges— *Kim C. Muschalek, San Antonio College*	Arlandria
	Community College Leadership Roles, Including the Impact of the NSA/DHS CAE Program on Community Colleges — *Corrinne Sande, Whatcom Community College*	Old Town Central

Summit Agenda

Day Two - June 27, 2022

TIME	EVENT	LOCATION
9:25 am – 11:15 am	CTE K-12 Pathways of Study in Cybersecurity: The Role of Community Colleges — *Deanne Wesley, North Carolina Central University and Chuck Bales, Moraine Valley Community College*	Old Town East
	National Trends of Community Colleges Offering Bachelor's Degrees: What Are the Current and Future Impacts on the National Cyber Workforce? — *Kyle Jones, Sinclair Community College and Ernest Friend, Florida State College at Jacksonville*	Rosemont
	The Successes and Challenges Faced by Community Colleges in Addressing the Evolving Cybersecurity Work Roles — *Stephen Miller, Eastern New Mexico University - Ruidoso Branch*	Del Ray
	[Invitation only] Presidents & Special Guests focus group: Challenges and Opportunities — *hosted by Kathi Hiyane-Brown, WCC ***	Carlyle Suite
11:15 am – 11:30 am	**Transition / Break**	
11:30 am – 12:20 pm	Focus Group Report Outs	Old West Ballroom
12:20 pm –1:45 pm	Lunch	Old Town Ballroom
1:15 pm –1:45 pm	Mid-Day Keynote - Community College Leadership — *Lynne Clark*	Old Town Ballroom
1:45 pm – 2:00 pm	**Transition / Break**	
2:00 pm – 3:50 pm	**Concurrent Sessions – Author Presentation & Focus Group Discussion**	
	New Models for Cybersecurity Teaching & Training: The Case for National Action — *Owen McNally, Austin Community College*	Old Town Central
	The Challenges in Building Stronger Community College Cyber Articulation Agreements — *Margaret Leary, Northern Virginia Community College*	Del Ray
	The Achievements and Obstacles in Building a Diverse Cybersecurity Workforce— *Dr. Kristine Christensen, Moraine Valley Community College, and Dr. Rebecca Caldwell, Winston-Salem University*	Rosemont

Day Two - June 27, 2022

TIME	EVENT	LOCATION
2:00 pm – 3:50 pm	Examination of Community College and Government & Industry Partnerships — *Dr. John Sands, Moraine Valley Community College*	Old Town East
	Innovations in Cybersecurity Classroom Practices: A Spotlight on Community Colleges — *Mike Qaissaunee, Brookdale Community College*	Arlandria
	Evidence-Based Assessment: The Role of Extracurricular Activities in Preparing Students for the Cybersecurity Workforce — *Jake Mihevc, Mohawk Valley Community College*	Old Town West
3:50 pm – 4:05 pm	**Transition / Break**	
4:05 pm – 4:50 pm	Focus Group Report Outs	Old West Ballroom
4:50 pm – 5:00 pm	Wrap-up Remarks	Old Town Ballroom
5:00 pm – 6:00 pm	**Transition / Break**	
6:00 pm – 7:30 pm	Poster / Networking Reception	Outdoor Courtyard

Day Three - June 28, 2022

TIME	EVENT	LOCATION
8:00 am – 9:00 am	Breakfast	Rosemont
9:00 am – 9:30 am	Closing Keynote: Well, Here We Are..... Where Now?— *Murray Kenyon*	Old Town Ballroom
9:30 am – 9:45 am	**Transition / Break**	
9:45 am – 10:45 am	Pathways Panel – What's Working to Expand the Pipeline. *Panelists: Albert Palacios (Department of Education), Lazaro Lopez (Illinois Community College Board), Ashley Greeley (NSA), Davina Pruitt-Mentle (NICE, NIST)*	Old Town Ballroom
10:45 am – 11:00 am	**Transition / Break**	
11:00 am – 12:30 pm	Action Plan, Lunch & Closing Remarks – Center Directors	Old Town Ballroom

** Presidents Forum: Challenges and Opportunities **

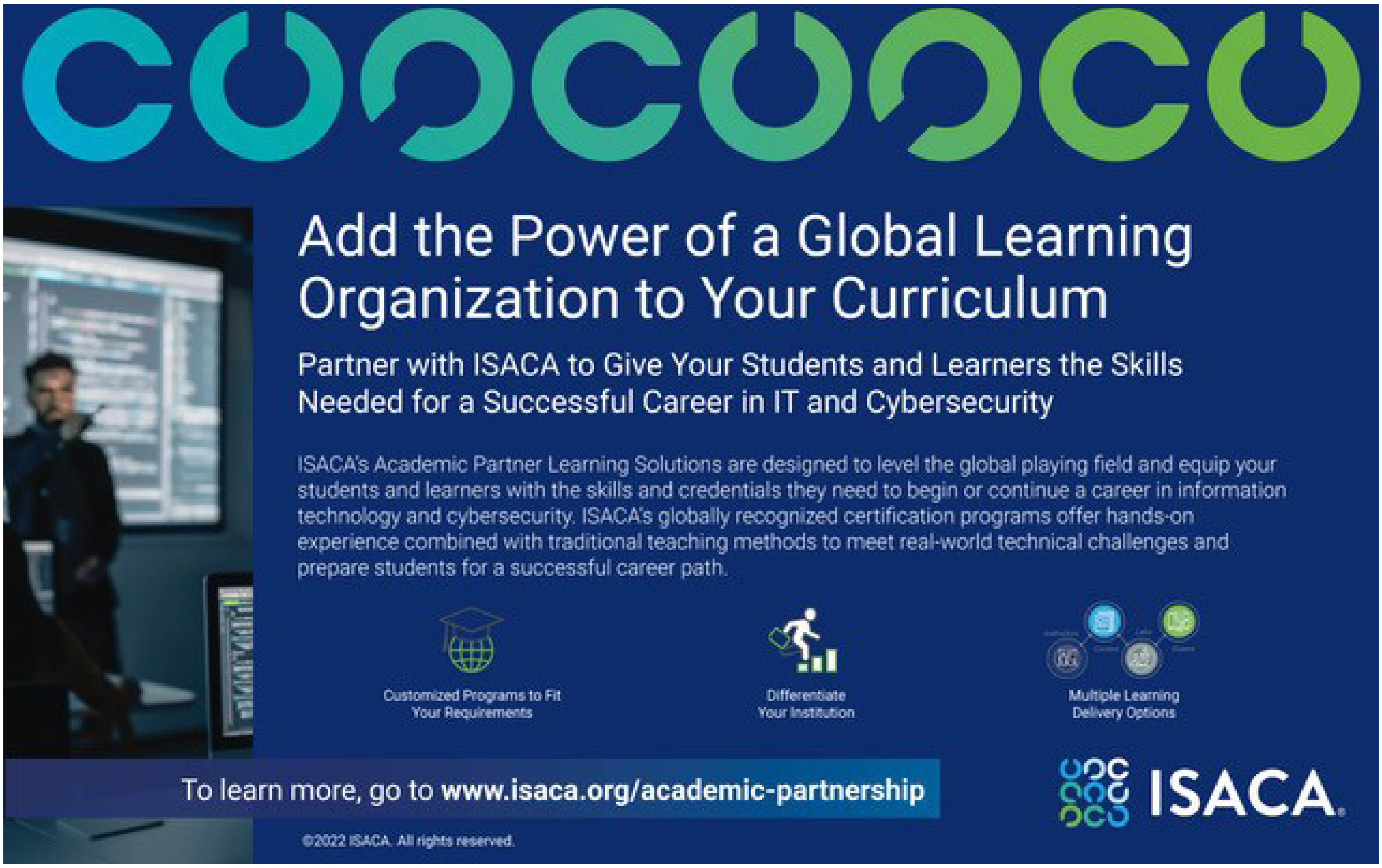
About the Focus Group:
This focus group will explore the obstacles and opportunities that college administrators from across the nation face in positioning their institutions to rapidly meet the growing cybersecurity workforce gap. Successful innovations, outcomes and recommendations will be explored.

** Pathways Panel – What's Working to Expand the Pipeline **

About the Panel:
Join our panel of experts as they discuss challenges, opportunities and the key elements to building and expanding successful cybersecurity education pathways for students from high school to college, careers and beyond.

Pathways Panelists:
Albert Palacios, Education Program Specialist, Department of Education
Lazaro Lopez, Chair, Illinois Community College Board
Ashley Greeley, K12 Projects Lead, National Security Agency (NSA)
Davina Pruitt-Mentle, Lead for Academic Engagement National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST)

Moderator:
Corrinne Sande, NCyTE Center at Whatcom Community College



Concurrent Session Topics →

Workforce Study: Community College Cybersecurity Alumni-Where Are They Now?

Topic 1

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.

Presented by Dr. John Sands, Moraine Valley Community College

CyberCorps Scholarship for Service Program: The Expanding Role of Community Colleges

Topic 2

With the passing of the 2018 National Defense Authorization Act (HR2810), the nation's leaders have recognized the expanding role of community colleges and community college students in the NSF's CyberCorp® Scholarship for Service (SFS) program. This article will document why the community college student population can contribute to addressing the nation's federal cybersecurity workforce shortage.

The author will document the impact of the current CyberCorps® program and the expanding role of community college students in these programs. In 2018 the National Defense Authorization Act specifically addressed using community colleges to recruit veterans and/or individuals looking to change careers and possessing undergraduate or graduate degrees in other fields of study. The article also documents the unique opportunity community colleges offer in expanding workforce diversity.

The expansion of the SFS program to community colleges offers a greater opportunity to expand these programs to many of the 1,100 community and technical colleges in the United States. The study was conducted by Kim Muschalek from San Antonio College. San Antonio College is one of the schools currently participating in the SFS Community College Cyber Program (C3P) authorized by HR2810. The author will document the impact of the current CyberCorps® program and the expanding role of community college students in these programs.

Presented by Kim C. Muschalek, San Antonio College

Community College Leadership Roles, Including the Impact of the NSA/DHS CAE Program on Community Colleges

Topic 3

NSA launched the Centers of Academic Excellence in Information Assurance (now Cyber Defense) Education program in 1999. While initially only open to Universities, in 2010 the CAE2Y designation was created and community colleges had the ability to become CAEs. Community colleges have been at the forefront in applied cybersecurity education and have assumed leadership roles especially involving the CAE. Several community colleges serve as CAE regional resource centers and two community colleges serve as national centers. These community colleges provide mentoring, peer reviewers, program development and other services to universities and community colleges alike.

The NCyTE center contracted with Seattle Jobs Initiative to conduct a study of the impact of the CAE on institutions and the surrounding economic region. This article will report the results of this study along with providing highlights of the leadership role of community colleges and their contribution to the national cybersecurity workforce.

Presented by Corrinne Sande (Whatcom Community College)

CTE K-12 Pathways of Study in Cybersecurity: The Role of Community Colleges

Topic 4

A career pathway describes an educational ecosystem consisting of multiple elements of an effective and efficient pathway of study for students, intending to lead to a specific career field. Pathway elements typically include secondary and post-secondary school courses, and workforce learning programs, such as internships and apprenticeships. The United States Department of Education created a Career Pathways framework that grouped occupations within associated career clusters. Occupations within a pathway share common knowledge, skills, and abilities. Well-designed Career Pathways enable students to gain an early start towards a targeted career, earn professional credentials while still in school, and shorten the time required to complete academic studies and enter the workforce. Career pathways have been shown to greatly increase career awareness and interest, as well as workforce capacity for high-demand fields. The challenge faced by the cybersecurity academic community is the absence of a formal career cluster framework for the cybersecurity field. When the Career Pathways framework was developed there was no placement within the framework for many of today's high-demand career fields like cybersecurity due to the fact that careers like cybersecurity were not established or a recognized profession at that time.

This paper will provide an overview of pathways of study and how they benefit the workforce. We will discuss our findings from our investigation of cybersecurity programs of study from community colleges across the United States and share thoughts from leading CTE stakeholders. We will discuss the elements of a model cybersecurity pathways, and highlight states with successful models, such as Texas and Ohio. We will also examine opportunities to strengthen career pathways in cybersecurity and the unique challenges in building these model programs of study for cybersecurity. Resources were provided by the Department of Education in the 1990s in order to help build momentum for Career Pathways and aid in development and dissemination. New and emerging technology, such as cybersecurity, need similar resources and funding in order to help develop cybersecurity career pathways models and support dissemination and training.

Presented by Dr. Deanne Cranford-Wesley (North Carolina Central University) and Chuck Bales (Moraine Valley Community College)

National Trends of Community colleges Offering Bachelor's Degrees: What Are the Current and Future Impacts on the National Cyber Workforce?

Topic 5

Over the last 10 years, there has been a trend in the United States in which community colleges have been given the opportunity to offer bachelor's degrees within their institutions. This endeavor has helped increase the number of individuals with bachelor's degrees offering hands on experience and training. This document focuses on the history of community college and why community colleges can offer bachelor's degrees. This document will also take an in-depth look at three leading community colleges in the country that have gone through the process and are now offering bachelor's degrees associated with cybersecurity.

Currently 28 states allow community colleges to award bachelor's degrees. Collectively these college produce over 21,000 bachelor completers.[3] "The Inside Higher Ed survey asked a broad set of questions about community college bachelor's degrees at a time when half the states have now enabled two-year institutions to award such degrees. The survey found that 75 percent of community college presidents would like to see their campuses offer bachelor's degrees, even though only one in 10 reported offering four-year degree programs on their campuses. Only 1 percent of respondents said their college offers a wide range of four-year degree programs. Eighty percent of community college presidents agreed that their institutions are in a strong position to offer bachelor's degrees to students who would not otherwise have access to those degrees because of four-year universities' higher costs or distance from where students live."[1]

Community colleges are adept at quickly meeting regional workforce needs and providing affordably bachelor degrees. Many of the bachelor degrees at community colleges are workforce based applied programs. Due to the strong demand for cyber security technicians many states are allowing community colleges to create cyber related bachelor degrees. State education board policies generally dictate the degree area and number of bachelors an educational institution can offer. "States typically spell out a program approval process and criteria, and some include data collection and reporting processes in their policies. When considering community college bachelor's policies, state leaders must often navigate contentious debates over the traditional missions of two- and four-year institutions and how the overlapping and competing roles of the two sectors continue to evolve."[2]

Presented by Kyle Jones (Sinclair Community College) and Ernie Friend (Florida State College at Jacksonville)

1. https://bit.ly/inside-higher-ed-survey
2. https://files.eric.ed.gov/fulltext/ED556034.pdf
3. https://nces.ed.gov/collegenavigator/?s=all&l=93&ct=1&ic=2

The Successes and Challenges Faced by Community Colleges in Addressing the Evolving Cybersecurity Work Roles

Topic 6

The cybersecurity work roles are continually changing to meet the needs of the public and private sectors. Community colleges play a key role in meeting these changes in a timely matter. In my fifty-five years' experience in the Information Technology (IT) workforce as an IT professional, manager, and educator, it has become apparent how community colleges are a powerful resource that address not only entry level jobs but incumbent worker and employer needs, multidiscipline career changing training, and veteran pathways in cybersecurity. The NIST/NICE Framework currently lists fifty-two work roles that cover the seven workforce categories. CyberSeek has five common cybersecurity feeder roles, and there are many other security roles and job titles that can be found online by searching "cybersecurity work roles".

This paper will cover a study of how community colleges currently and in the future will meet the student and employer requirements for cybersecurity work roles, tasks and knowledge, skills, and abilities. The study will capture key topic information with interviews from NIST/NICE leaders, industry representatives, faculty, and student and graduate interviews. The information will include both the multi-disciplinary nature of cybersecurity and the specialization of cybersecurity work roles. The study will provide answers and best practices addressing the challenges community colleges face today and will face in the future in quality curriculum and programs to provide a productive cybersecurity workforce. This includes what types of resources, funding, and support would provide the greatest impact for success.

Presented by Stephen D. Miller (NCyTE & Eastern New Mexico University – Ruidoso)

New Models for Cybersecurity Teaching and Training: The Case for National Action

Topic 7

Multiple and convergent data indicate not only a serious and worsening shortage of cybersecurity professionals, but also an under-recognized deficit of cybersecurity teachers and trainers. In order to evaluate possible explanations for barriers and disincentives to cybersecurity faculty recruitment, training and retention, a questionnaire was administered to 31 cybersecurity subject matter experts. The participants were also queried about the viability of differing approaches to develop cybersecurity faculty, as well as the use of novel techniques and technologies to augment training. Major findings indicate that 90% of these experts strongly or somewhat agreed that a major factor making it hard to develop and retain faculty who are teaching cybersecurity is the compensation differential compared to being part of an industry cybersecurity team. Data also show 96% strongly or somewhat agreed that the low status and pay of adjunct and other part-time professionals is a barrier to having adequate information security teachers. About 80% of the respondents strongly or somewhat agreed with the proposition that mainstream media sources should be cultivated, and original content developed, to represent information security teachers in a positive light. Still other responses suggest support for having top information security industry professionals, who are recognized experts, drafted to train new information security teachers; for identifying recently completed Master's and PhD students as trainable potential information security faculty; for private sector corporations investing more resources in developing information security teachers and trainers; and for use of memes and other youth-friendly "viral" media to spread awareness of cybersecurity.

Opinion was more divided on using AI software to do training via chatbots, on importing more trainers and teachers via immigration, on retraining groups including retired university or college professors with PhDs and technical backgrounds to become information security teachers, and whether resources in this area are scarce due to expenses associated with the growing administrative sector. Recommendations based on these data are proposed, with a focus on investments in teaching and training appropriately scaled to the ongoing security needs of both public-sector institutions as well as private entities, such as for-profit corporations.

Presented by Owen McNally (Austin Community College)

The Challenges in Building Stronger Community College Cyber Articulation Agreements

Topic 8

Key differences exist between traditional, transfer-oriented degree programs and applied degree programs at Community Colleges. While applied degree programs tend to provide employers with job candidates who possess the required skills to "hit-the-ground-running", more than 76% of employers require a 4-year degree for employment. The structural differences between Applied Associate degrees and Bachelor of Science degrees result in significant articulation challenges for students seeking to continue their studies beyond community colleges. This is especially true in Cybersecurity disciplines, where the majority of 4-year Cybersecurity programs are placed in transfer-oriented Computer Science departments while most 2-year programs exist in applied degree programs, such as Information Technology.

This study examines articulation challenges between two- and four-year institutions. NSA institutional data was examined to identify successful articulation programs and public data from EMSI was analyzed to address the effectiveness of Computer Science and Cybersecurity programs at meeting cybersecurity workforce needs. Interviews were conducted with NSA Centers of Academic Excellence Points of Contact (POC). This study presents successful articulation models and makes recommendations for increasing articulation opportunities between 2- and 4-year institutions.

Presented by Margaret Leary (Northern Virginia Community College)

The Achievements and Obstacles in Building a Diverse Cybersecurity Workforce

Topic 9

The cybersecurity workforce continues to experience extreme shortages while the frequency, sophistication, and severity of cyberattacks continue to intensify, putting national and individual security at risk. While national initiatives are in place to address the cybersecurity workforce shortage, there continues to be a lack of female and minority representation in this field.

This study will examine the current state of diversity in the cybersecurity workforce, highlight both empirical and anecdotal findings of research focused on attracting and retaining both women and minority cybersecurity professionals, and will discuss strategies that community colleges can employ to address the shortage of individuals with cybersecurity skills while increasing the number of female and minority participating in this workforce.

Key stakeholders of successful projects and initiatives will be interviewed and their responses and suggestions for capacity building will also be reported. Lastly, lessons learned from successful frameworks and organizations aimed at capacity building in both academia and the workforce will be discussed.

Presented by Dr. Kristine Christensen (Moraine Valley Community College) and Dr. Rebecca Caldwell (ADMI and Winston Salem State University)

An Examination of Community College and Government Partnerships

Topic 10

From their inception community colleges required strong partnerships in their local communities including business partnerships, industry organizations and local, state and federal government agencies. This tradition is still true especially in the cybersecurity field. In today's cybersecurity workforce approximately 82% of entry-level jobs require candidates to have a college credential of industry recognized certification. This study examines the critical partnerships between community colleges, local businesses, government agencies and industry organizations.

The author examines the role of business partnerships, the impact and benefits to both businesses and the community college cybersecurity programs and the benefit to the students in these programs. The author also examines the multitude of partnerships between community college cybersecurity programs and local, state and federal agencies. Government agencies now play a greater role in protecting our nation's critical infrastructure and our citizens from cyber-based attacks. The author examines the role government agencies play in defining workforce frameworks, identifying critical cybersecurity program elements and designation requirements, funding faculty development, funding career awareness programs, providing student with government scholarships, and many other initiatives.

The author also examines the relationships between cybersecurity industry organizations and community college cybersecurity programs. In this examination, the author explores certification programs, student skills competitions and industry sponsored cybersecurity bootcamps serving community college students. The author will also discuss the benefits and issues with cybersecurity industry organization sponsored certifications and how certifications can benefit community college students.

Presented by Dr. John Sands (Moraine Valley Community College)

Innovations in Cybersecurity Classroom Practices: A Spotlight on Community Colleges

Topic 11

The lead author for this paper, a Mechanical Engineer by training, transitioned to teaching Networking and Information Technology in 2000 and to Cybersecurity shortly thereafter. In addition to nearly 20 years of teaching cybersecurity, the lead author has extensive experience in curriculum development and securing grant funding to support cybersecurity education.

This paper will discuss the unique nature of cybersecurity and the difficultly in teaching the required skills and knowledge. In addition to the rapid pace of change in the field of cybersecurity, there are technology requirements and institutional constraints that must be overcome. The challenge is to create a robust space for students to learn cybersecurity, while balancing the safety of networks and systems and institutional concerns.

We will document some of the different approaches that have been adopted to teach cybersecurity, extending from single station approaches to statewide cyber ranges. We will detail products and technologies, approaches to teaching concepts, developing skills and assessing student learning. Included will be well-known national cyber ranges, cloud-based and home-grown solutions, competitions, grant-funded initiatives, public-private partnerships and commercial solutions. Additionally, we will capture perceptions of educators, students and business and industry leaders and need for and effectiveness of these various solutions.

Presented by Mike Qaissaunee (Brookdale Community College). Additional contributor: Lonnie Decker (Davenport University)

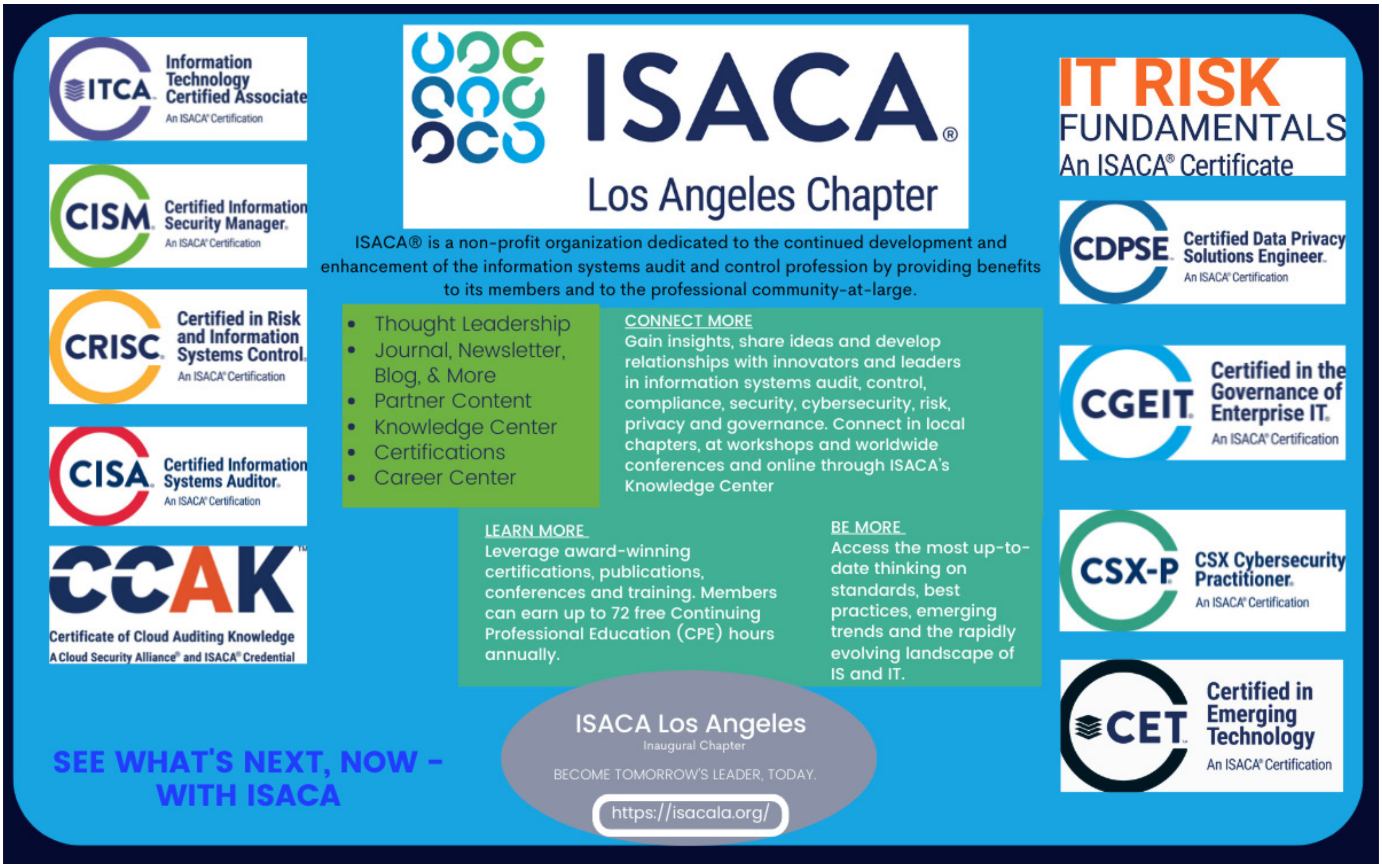
Evidence-Based Assessment: The Role of Extracurricular Activities in Preparing Students for the Cybersecurity Workforce

Topic 12

Community colleges are uniquely positioned to meet the national demand for a skilled cybersecurity workforce. Cybersecurity is an incredibly dynamic field, and the industry connections that are at the heart of the community college mission are a priceless asset in keeping education current and aligned with workforce needs. Further, cybersecurity is an applied discipline, and community colleges excel at providing practical education experiences based on the latest tools and techniques. As the demand for skilled cybersecurity professionals has increased, employers have increasingly valued extracurricular activities as both a means of skills validation and as an opportunity to observe a prospective employee perform in the context in which they will work.

Community colleges have taken an active role in the development and implementation of extracurricular activities within cybersecurity education. This study will review and summarize some of the most significant benefits extracurricular activities contribute to the cybersecurity education community. It will explore the impact of extracurricular activities in student development, share any common characteristics of successful activities, and note challenges to future implementations. The study will provide a perspective on work currently underway to refine the evidencing of competencies within extracurricular activities. The findings of the study may prove helpful to employers interested in external validation of a skillset, educators aspiring to enhance the student experience within their programs, and students who seek to test their knowledge and skills in a practical, applied context.

Presented by Jake Mihevc (Mohawk Valley Community College)


ITCA Information Technology Certified Associate An ISACA® Certification
CISM Certified Information Security Manager. An ISACA® Certification
CRISC Certified in Risk and Information Systems Control. An ISACA® Certification
CISA Certified Information Systems Auditor. An ISACA® Certification
CCAK™ Certificate of Cloud Auditing Knowledge A Cloud Security Alliance® and ISACA® Credential
ISACA®
Los Angeles Chapter
IT RISK FUNDAMENTALS An ISACA® Certificate
CDPSE Certified Data Privacy Solutions Engineer. An ISACA® Certification
CGEIT Certified in the Governance of Enterprise IT. An ISACA® Certification
CSX-P CSX Cybersecurity Practitioner. An ISACA® Certification
CET Certified in Emerging Technology An ISACA® Certification
SEE WHAT'S NEXT, NOW – WITH ISACA
ISACA Los Angeles
Inaugural Chapter
BECOME TOMORROW'S LEADER, TODAY.
https://isacala.org/

ISACA® is a non-profit organization dedicated to the continued development and enhancement of the information systems audit and control profession by providing benefits to its members and to the professional community-at-large.

- Thought Leadership
- Journal, Newsletter, Blog, & More
- Partner Content
- Knowledge Center
- Certifications
- Career Center

CONNECT MORE
Gain insights, share ideas and develop relationships with innovators and leaders in information systems audit, control, compliance, security, cybersecurity, risk, privacy and governance. Connect in local chapters, at workshops and worldwide conferences and online through ISACA's Knowledge Center

LEARN MORE
Leverage award-winning certifications, publications, conferences and training. Members can earn up to 72 free Continuing Professional Education (CPE) hours annually.

BE MORE
Access the most up-to-date thinking on standards, best practices, emerging trends and the rapidly evolving landscape of IS and IT.

Keynote Speakers

Opening Keynote Presentation

Hack the Gap: Fixing Cybersecurity's Broken Talent Pipeline

Presented by: Will Markow

Managing Director – Human Capital Management and Emerging Technologies

Will Markow leads the Emerging Technologies and Human Capital Management practice at Burning Glass Technologies where he oversees Burning Glass's research and consulting efforts focused on the impact of emerging technologies on the workforce.

Will's research with Burning Glass is routinely featured in national media outlets – such as the Wall Street Journal, New York Times, and Washington Post – and he has led dozens of custom research projects for Fortune 100 companies, technology vendors, training providers, workforce development organizations, and government agencies. He has also advised multiple White House administrations on key issues related to the future of work.

In addition, Will is an internationally recognized commentator on the cybersecurity talent shortage and, in partnership with CompTIA and the National Initiative for Cybersecurity Education, leads the development of Cyberseek.org, an interactive online tool providing definitive data on the cybersecurity workforce across the United States.

Presentation Overview:

The cybersecurity talent pipeline is broken. Demand for cybersecurity jobs has grown over 90% in the past five years but new graduates of cybersecurity programs have grown only 44%, exacerbating what was already one of the most severe talent shortages in the economy. Compounding this shortage is widespread demand for workers with rare combinations of skills and credentials, which blocks new workers from entering the field. As a result, employers are feeling the pain: cybersecurity jobs take 20% longer to fill than other IT jobs and pay 16% more – translating to a salary premium of nearly $13,000 per year. Nonetheless, employers still request heightened education and experience requirements, with over 85% of cybersecurity job openings requesting at least a bachelor's degree or at least 3 to 5 years of previous work experience. This further constrains the pool of workers from which employers may recruit. In this keynote, we will explore research and data on the cybersecurity workforce from Burning Glass Technologies and CyberSeek.org – an interactive supply and demand heatmap and career pathway for cybersecurity jobs across the U.S. We will explore some of the key factors driving a wedge between supply and demand for cybersecurity jobs in North America and beyond, and identify opportunities for employers, educators, policymakers, and individuals to fix the cybersecurity talent pipeline and grow the next generation of cybersecurity workers.

Mid-day Keynote Presentation

Community College Leadership

Presented by: Lynne Clark

Chief, Center for Cybersecurity Education, Innovation and Outreach, National Security Agency

In twenty years at NSA, Lynne has worked in Operations Security, risk management and information assurance, and managed the Information Assurance Directorate personnel and recruiting programs. She is the recipient of the Meritorious Civilian Service Award, was twice awarded the Joint Meritorious Unit Award for special projects in support of the Department of Defense, and the National Intelligence Meritorious Unit Citation for support to the Intelligence Community.

Currently Lynne is the Chief, for the Center for Cybersecurity Education, Innovation and Outreach (CEIO) for the National Security Agency. The Center is responsible for management of the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program, the GenCyber and STARTALK summer programs, the Service Academy Intern Program, Service Academy Visiting Professors and other NSA academic outreach programs.

Closing Keynote Presentation

Well, Here We Are... Where Now?

Presented by: Murray Kenyon

Vice President, Cybersecurity Partnership Executive Information Security Services US Bank

Murray W. Kenyon is Cybersecurity Partnership Executive in Information Security Services at U.S. Bank, where he fosters partnerships with Government, Trade Associations, Information Sharing and Analysis Centers, Educational Institutions, and other Non-Profits focused on Cybersecurity in the nation's critical infrastructure. Murray is a seasoned leader of national-level cybersecurity initiatives, with 35+ years of experience—in both the Federal Government and Private Sector—in cybersecurity, geo-political analysis, intelligence operations, information sharing, and critical infrastructure protection.

Prior to joining U.S. Bank, Murray was Senior Vice President for Technology Risk Management, leading the Cybersecurity Program at the Financial Services Roundtable (now the Bank Policy Institute). Before entering the Private Sector, Murray spent 33 years in analytic, staff, leadership, and executive positions at the National Security Agency (NSA), including as the Senior Executive Account Manager for the Financial Sector. Murray received his Bachelor of Arts from Asbury University, and earned Master of Science degrees from the Joint Military Intelligence College and the National War College. He serves on the National Visiting Committee for the National Cybersecurity Training and Education Center (NCyTE), and on the Advisory Boards for Cybersecurity education at New York University's Tandon School of Engineering, the University of West Florida's Center for Cyber Security, and Carroll County (Maryland) Community College.

Presentation Overview:

Eighteen years ago, ***Protecting Information: The Role of Community Colleges in Cybersecurity Education*** painted an accurate picture of the very challenging situation the nation faced regarding the need to expand the knowledge and skills of the technical workforce in basic—and more advanced—aspects of computer security. That report articulated a place for community colleges in providing "technical education about cybersecurity issues…for employment in a wide range of fields." Arguing—convincingly—that community colleges are well suited for educating information technology professionals in cybersecurity in an agile, need-based fashion, and that their ties with business and industry give them a unique position in the overall cybersecurity education effort, the community colleges laid out an ambitious set of program recommendations aimed at helping address the shortage of qualified cybersecurity practitioners the nation and world need. No doubt, the program adjustments resulting from these recommendations have made an important contribution.

But, let's be honest. If you miss the date on that report and its contemporaneous references, your first impression might be that it was written last year…or last month. The challenge of developing the cybersecurity workforce remains, the scarcity of qualified applicants for cybersecurity positions in companies across critical (and non-critical) infrastructure persists, the need for already employed practitioners to hone their skills every year has in no way abated. And, dismayingly, the threat actors just keep getting better and better. What can we do?

Leveraging his extensive background, Murray will share his thoughts on how the community colleges can continue to expand the value they provide in the ongoing fight to secure critical information and infrastructure across the "good guy" space.

Presenter Bios

→

Presenters

Chuck Bales

Professor and Program Coordinator of Automation and Engineering Technology at Moraine Valley Community College

Mr. Bales has taught and developed curriculum for mechanical design, CAD, automation, and engineering technology for over 20 years. Mr. Bales holds a Bachelor's and Master's degrees in Mechanical Engineering from the University of Florida and a Bachelor's degree in Industrial Technology from Southern Illinois University at Carbondale.

As a program coordinator, full-time faculty member, and academic researcher, he has developed and taught numerous engineering and technology courses and created several new degree and certificate programs at the college. Mr. Bales has been actively involved in grants as a co-principal investigator, researcher, and developer for the Department of Education, National Science Foundation, National Security Agency, and the US Department of Labor since 1994. He also holds numerous professional certifications in the fields of information technology and networking, manufacturing and robotics, and computer-aided design.

Corrinne Sande

Whatcom Community College and PI/Director of NCyTE

Whatcom Community College's Director of Computer Science and Information Systems, Corrinne Sande is the director of the National Cybersecurity Resource Center funded by the National Security Agency, and Principal Investigator for CyberWatch West, a National Science Foundation–funded Advanced Technological Education (ATE) regional center that works to grow and strengthen the nation's cybersecurity workforce. Ms. Sande also serves as a Co-Principal Investigator of Catalyzing Computing and Cybersecurity in Community Colleges (C5).

Through Ms. Sande's efforts, Whatcom Community College became the first National Center of Academic Excellence in Cyber Defense—Two-Year Education (CAE2Y) on the West Coast. She holds several industry certifications, and she co-organizes the Pacific Rim Collegiate Cyber Defense Competition (PRCCDC) with Highline College.

In recognition of her outstanding work as an advocate for cybersecurity education, Ms. Sande received the 2016 Pacific Region Faculty Award from the Association of Community College Trustees (ACCT)

Presenters

Dr. Deanne Cranford-Wesley

Director Cybersecurity at North Carolina Central University(NCCU) and formally Associate Dean Davis iTEC/Cyber Security Center at Forsyth Technical Community College.

Dr. Cranford-Wesley manages the Cybersecurity concentration in the School of Business, Computer Information System Program at NCCU. She directs operation in the innovative cybersecurity lab and is the advisor for the Women in Cybersecurity (Wicys) student chapter at NCCU. During her tenure at Forsyth Technical Community College, she managed 10 technical programs in the Davis iTEC Cybersecurity Center and also taught in the cybersecurity program. She developed curriculum for post-secondary education as well as K-12. She also led efforts on behalf of the Center of Academic Excellence and Regional Resource Center, where one of her initiatives focuses on the K-12 cybersecurity pipeline. She has designed curriculum for K-12 programs as a consultant in the 4-year space. She is a previous member of the CyberWatch Cybersecurity Task Force.

Dr. Cranford-Wesley previously worked as Department Coordinator and Associate Professor in the 4-year space for 12 years. She currently is an executive board member for the NC TECH Association, an Executive Board member for the NC Chamber, and a member of the Executive Board for the Colloquium of Information System Security board. Dr. Cranford-Wesley is a cybersecurity professional and has appeared as a subject matter expert on Fox8 and Time Warner News discussing innovations in cybersecurity and cyber-attacks. In August 2019, she appeared on WXI12 discussing the value of a GenCyber Girls Camp hosted by Forsyth Technical Community College.

Dr. Cranford-Wesley has a vast amount of experience in curriculum design, grant writing, and program evaluation. She has a PhD in Education Leadership with a focus in Instructional Technology and is a published author of various technology related articles. Furthermore, she has obtained the following certifications throughout her career: IC3, Security+, Cisco Certified Network Professional (CCNP), Cisco Certified Network Associate (CCNA), and Cisco Certified Instructor (CCAI).

Presenters

Ernest “Ernie” Friend

Instructional Program Manager, Florida State College at Jacksonville

Mr. Friend’s 35-year career in information technology has been punctuated with extensive partnerships in the development of innovative workforce development and career preparation programs. As the Instructional Program Manager at Florida State College at Jacksonville (FSCJ), Mr. Friend has worked with notable international technology leaders such as Cisco, EMC, VMware, Citrix and Redhat to create specializations in Voice, Security, Virtualization/Cloud, Open Source Operating Systems, and data science. Working with his staff and faculty he has used virtualization technologies to web-enable some of the most advanced technical hands-on academic curriculum.

Mr. Friend was selected as the 2018 National Science Foundation (NSF) HI-TEC Educator of the Year. As a board member of the National Convergence Technology Center, Mr. Friend contributes significantly, in collaboration with international business interests, to the national dialog defining skill sets required for emerging information technology occupations. Mr. Friend has led or participated in more than a dozen National Science Foundation and Department of Labor grants centered on creating new curriculum, faculty professional development, and student engagement in high technology fields. He served on the U.S. Department of Commerce National Institute of Standards and Technology (NIST) committee designing new standards for Cybersecurity, and his college’s computer networking program, which he leads, received recently the National Security Agency (NSA) designation as a Center of Academic Excellence.

Mr. Friend has assisted seven Florida colleges and universities in creating network virtualization academic programs. He has served as a consultant to the Florida Senate Education Committee on the need for enhanced collegiate programs and improved vendor certification programs in network virtualization and cloud computing. He was appointed by the Florida State Senate President to the University Of Florida Board Of Governors Advisory Board for online programs.

Mr. Friend holds a Bachelor’s of Science degree in Electronics Management from Southern Illinois University and a Master’s of Science degree in Cybersecurity form the University of South Florida. His foundations in information technology leadership were earned through 10 years of service in the United States Navy, providing technical support and instruction on the latest military aircraft.

He has been employed for more than 25 years at Florida State College at Jacksonville where he manages an advanced networking associate’s degree, Bachelors of Applied Science degree in Computer Networking and Computer Information Technology at the College’s technology-focused Downtown Campus.

Presenters

Jake Mihevc

Dean of ScienceTechnology, Engineering and Math at Mohawk Valley Community College

Jake launched the college's Cybersecurity AS program in 2014 and helped it achieve the Center of Academic Excellence in Cyber Defense designation in 2016. He is also the Director and PI of the Northeast Regional Resource Center for the NSA/DHS Center of Academic Excellence program. Jake is a co-founder of the Central New York Hackathon, a regional cybersecurity competition that brings over 100 students from eight cybersecurity programs together each semester to test their skills. He is an active member of the National Initiative for Cybersecurity Education Workgroup and has worked to expand cybersecurity competitions nationwide.

Dr. John Sands

Department Chair and Professor, Moraine Valley Community College and Director/ PI of CSSIA

John Sands has over 30 years of experience in education and workforce research in the areas of data communications, manufacturing technologies, information technology, information security management and cybersecurity. He currently serves as the department chair and professor of information technology at Moraine Valley Community College. John also serves as the Principal Investigator/Executive Director of the Center for Systems Security and Information Assurance (CSSIA), an NSF/ATE National Support Center. John's team has studied the technology workforce needs both in the local Chicago metropolitan region and nationally as the Principal Investigator of CSSIA. He holds a Ph.D. from Colorado State University and several industry certifications.

As a department chair, full time faculty member, and academic researcher, he has developed and taught numerous online technology courses using an integrated virtual teaching and learning environment. Dr. Sands has served as the executive director of one of the most successful Cisco System - Networking Academy Training Centers in the country. John also possesses a very strong background in developing and implementing online curriculum for both students and faculty and has been the recipient of several awards in the area of innovation and teaching. Professor Sands also has received several academic awards including the Master Teacher of the Year, Innovator of the Year and the Career Pathways Partnership Excellence Award - Best Dual Credit Program.

Presenters

Kim C. Muschalek

San Antonio College

Kim C. Muschalek, has over 24 years of higher education experience in computer applications management and computer science. She is a Microsoft Operations Specialist and Certified Adobe instructor and is qualified to teach Cisco Networking Certification classes. Kim has experience teaching client operating systems (Windows and Linux), TCP/IP, network design and architecture, and hardware configuration and software integration.

In 1995, Kim joined the faculty at San Antonio College. She has mentored the San Antonio College/ Information Technology and Security Academy (ITSA) CyberPatriot Team for 6 years and taught cyber security concepts and team strategies aimed at solving real-world cyber security issues. Kim has been the Computer Information Systems/Computer Science program coordinator since 2016. She is currently the PI for the National Science Foundation Scholarship for Service C3P Pilot Program and the Director of the South Central CAE Regional Resource Center.

Dr. Kristine Christensen

Professor of Management Information Systems at Moraine Valley Community College

Dr. Kristine Christensen is a professor of Management Information Systems at Moraine Valley Community College, where she has taught and developed curriculum in website development, user interface design principles, programming, networking, robotics, and engineering technology for the past twenty years. She has a passion for teaching a diverse group of learners and enjoys the challenges and rewards of helping people develop their knowledge, skills, and abilities so that they can reach their potential and be successful in their future lives and careers. She encourages underserved student populations to enter the information technology and cybersecurity fields, and she provides support and mentorship to them as a way to help bring more diversity and equity to the IT and cyber workforce.

Dr. Christensen also serves as Moraine Valley's Director of Faculty Development and is responsible for designing, developing, and evaluating professional development programs for faculty and staff. She has been actively involved in research and curriculum development for grants awarded by the National Science Foundation, National Security Agency, and the National Centers of Academic Excellence in Cybersecurity. She holds a Bachelor of Science in Business with a double major in Human Resource Management and Industrial Psychology from Valparaiso University, a Master of Business Administration with an emphasis in Consulting from Eastern Illinois University, a Master of Science in Management Information Systems with a focus in Computer Programming and Electronic Commerce from Governors State University, a Master of Science in Teaching and Learning from St. Francis University, a graduate certificate in Online Communications and Web Design from the University of Florida, and a Ph.D. in Community College Leadership from Old Dominion University. In addition to her academic credentials, she has earned numerous professional certifications in information technology and networking, manufacturing and robotics, programming, and web development.

Presenters

Kyle Jones

Chair & Associate Professor of Sinclair Community College's Computer Science and Information Technology department.

He worked in the IT field for over 15 years before coming to education. In his experience has worked as a small business PC repair technician to a Fortune 500 Sr. Security Infrastructure Administrator Mr. Jones holds a CompTIA Strata, A+, Network+, Security+, CySA certification, as well as an ITIL Foundations. He holds an Associate in Network Engineering from Sothern State, a Bachelor of Business from Wilmington College, and a Master's degree in Information Assurance and Security from American Public University. He is a CAE2Y Principal Investigator as well at the Principle Investigator for the Community College Scholar for Service Program and the PI for the Community College Cyber Scholarship for Service program. Also, Mr. Jones has been featured as a public speaker on cybersecurity topics. Most recently, he participated in a roundtable discussion hosted by the Dayton Business Journal on the present landscape of cybersecurity, and he was featured on WDTN Dayton-Channel 2 in a vignette about "Good Cyber Hygiene." His previous work experience ranges from working for small PC repair shops to Fortune 500 Datacenters.

Margaret Leary, Ph.D, CISSP, CEH, CRISC, CIPP/G

Chair, Cybersecurity, Northern Virginia Community College

Dr. Margaret Leary is a Professor of Cybersecurity at NVCC, where she has taught and developed curriculum for IT and Cybersecurity for over 20 years. She has more than 30 years' experience consulting and working in the IT and Cyber fields, serving as a senior cybersecurity policy advisor to Federal agencies in the Washington, D.C. region, including various studies on e-Authentication, identity theft, and privacy.

She serves on the Leadership Team for the National CyberWatch Center, an NSF-funded consortium of higher education, government, and businesses focused on advancing cybersecurity education/research and strengthening the national cybersecurity workforce and is the Director of an NSA Center of Academic Excellence National Resource Center, training faculty at 2- and 4-year institutions to review applications for institutions seeking CAE-CD and CAE2Y designation. She was appointed as Cyber Faculty In-Residence to the Governor's Office in 2015 to assist with increasing the number of community college cybersecurity programs in Virginia and was awarded a State Council for Higher Education Virginia (SCHEV) Outstanding Faculty Award in 2017. She serves on a variety of cybersecurity education and industry working groups and Advisory Boards.

Presenters

Mike Qaissaunee

Professor and Chair of the Engineering and Technology Department and Director of Brookdale's Cyber Center at Brookdale Community College.

At Brookdale, Mike has written and been awarded multiple National Science Foundation (NSF) grants and Department of Education (DoE) grants including:

- Collaborative Research: Community College Accelerated CyberCorps® Pilot Program (NSF),
- Building a Virtual Lab Environment to Provide Cybersecurity Students with Improved Hands-on Skills (DoE/FIPSE),
- Building a Pipeline of Cyber Warriors Through Education and Competition Offered Through Community Colleges (NSF),
- E-books and Mobile Apps for Technician Education (NSF), and
- Mid-Atlantic Institute for Telecommunications Technologies (NSF).

The National Security Agency (NSA) has also provided support for GenCyber Cybersecurity camps for high school students in Summer 2016, 2017, 2018, and 2019.

Professor Qaissaunee co-authored a 10th-grade Engineering and Technology textbook, has been active at his own campus and around the country in promoting the adoption of new technologies in and approaches to teaching and learning and has conducted workshops and presented keynote addresses at more than 60 conferences nationwide. Qaissaunee is the recipient of the People Who Made a Difference in Security award from the SANS Institute, two Educator of the Year awards, and Brookdale's Barringer award, which recognizes career contributions to the college. Mike received his undergraduate and graduate degrees in Mechanical Engineering from the University of Delaware (Newark, DE).

Owen McNally, PhD

Professor at Austin Community College

Owen is a professor, researcher and technology analyst in Austin, Texas. He is the Chair of the EFF-Austin Cybersecurity workgroup, and the Founder of the Data Science vs COVID project. An enduring theme in his work over recent decades is the analysis and evaluation of technology for usability, quality and ethics based on humanistic principles. He joined a series of software development teams as a usability and quality assurance analyst, and subsequently earned an interdisciplinary PhD at the University of Texas at Austin, with a program of work in Medical Cognitive Science. He has taught college level software design, cognitive studies, psychology, research methods, and statistics for the behavioral sciences. In recent years his work has been in software usability, cybersecurity training, medical research, and analysis for investors in energy storage, AI, hospital technology, neurotechnology, and logistics.

Presenters

Dr. Rebecca Caldwell

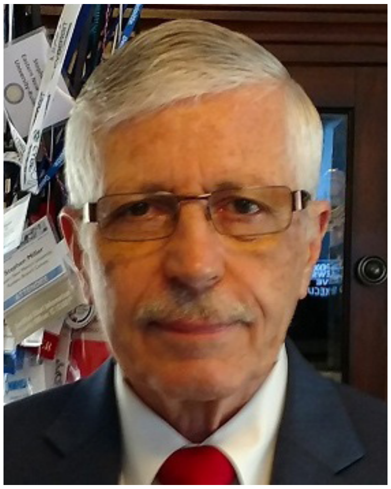
Associate Professor, the Department of Computer Science at Winston-Salem State University

Dr. E. Rebecca Caldwell earned her Ph.D. from the University of North Carolina—Greensboro. Dr. Rebecca Caldwell has over two decades of full-time University-level teaching experience at Winston-Salem State University. She has primarily taught programming classes in various languages. She has been the recipient of numerous awards including the Wachovia Excellence in Teaching Award. During her tenure at Winston-Salem State University, she has played instrumental roles in curriculum development, assessment of student performance, and strategic planning. She has also served on several self-study committees for the Computer Science's ABET accreditation. She has participated on a NSF review panel for proposals submitted to Transforming Undergraduate Education in Science, Technology, Engineering and Mathematics (TUES). Dr. Caldwell also completed the NSF (HBCU UP/QEM Leadership Development Institute. She currently serves as President of The Association of Computer/Information Sciences and Engineering Departments at Minority Institutions (ADMI). Her research interests are in the areas of Computer Science Education, Robotics, Software Engineering, and Cybersecurity.

Grant Experience:

- NSF - NCLSAMP
- NSF Grant – DUE Center for Systems Security and Information Assurance (CSSIA)
- NSF HBCU-UP Targeted Infusion Project: Developing Game-Like Instructional Modules to Enhance Student Learning in Lower Level Core Computer Science Courses
- Winston-Salem State University Research Initiative Program Grant, Using Robotics to Improve Student Satisfaction and Engagement in an Introductory
- NSF Grant - Broadening Participation in Computing Advancing Robotics Technology for Societal Impact (ARTSI) Alliance

Presenters



Stephen D. Miller M.S./ITIL/QM/BPR

Tenured Professor/Director/CoPI CyberWatch West Information Systems/Cyber Security Center of Excellence Eastern New Mexico University – Ruidoso

Mr. Miller has been in the Information Systems Profession since 1966 working in business, government, and education sectors. He has a M.S. MIS Managing Computer Technology from Houston Baptist University, B.S./Business Information Systems Services with (Phi Kappa Phi honors) from the University of Houston – Downtown, and Organizational Management for Improving Organizational Effectiveness Post Graduate Certificate from The Office of Executive Development, Rice University.

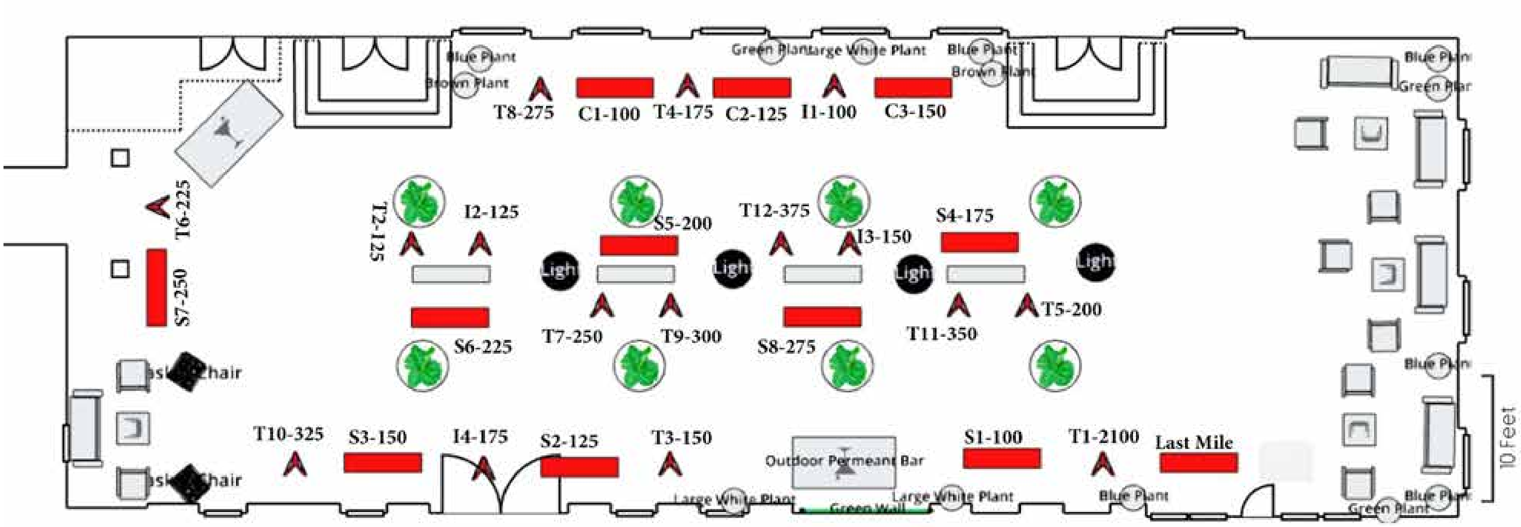
Mr. Miller is currently a tenured Professor, Subject Matter Expert. and Director for Information Systems/Cyber Security Center of Excellence, where he is responsible for developing Information Systems Curriculum, SCADA, Cyber Security program development, research, and teaching. He is also President of BITS Consulting since 2002, providing Information Technology, SCADA, and Computer/Network Security consulting using tools like CSET 8.1, Business Process Re-Engineering ITIL Service Management Tool Kit.

Mr. Miller is retired from ExxonMobil Global Information Systems where he served in management, supervisory and technical roles over his 27 year career, and 13 years with Exxon Pipeline Company. He has been employed at Ford TechRep Division (programmer), U.S. Army 1st Calvary Div. in Vietnam (computer specialist), and Univac Corp. - NASA Mission Control on the APOLLO—including APOLLO 13, and Skylab Missions (Communications and Telemetry Systems Analyst), TRW Controls (Project Manager), United Way of the Coastal Bend (Community Services Director), and self- employed Consulting Company.

Mr. Miller has served or is serving as a member/leader of the following organizations Energy Telecom & Electrical Association, Chairperson Exxon Leadership 2000 Mentor Program & Science and Math Ambassador, Phi Kappa Phi active member, and Gartner Group Quality Study Group. Mr. Miller is a past board member of Albuquerque InfraGard National Infrastructure Protection and current member of InfraGard Houston, InfraGard Oil & Gas, a contributor for the National Institute Cybersecurity Studies and National Initiative for Cybersecurity Education (NICE). Past and current activities include the NIST workshops for the Cybersecurity Critical Infrastructure Framework standards, and recently coauthored a n e-textbook "Framework for SCADA Cybersecurity" ISBN: 9781310309960. Working with George Mason University in developing a Cybersecurity course for Whatcom Community College and NCyTE Center based on the Critical Infrastructure Security and Resilience: The Cyber Dimension course. Mr. Miller is also a presenter for many Cybersecurity conferences throughout the United States.

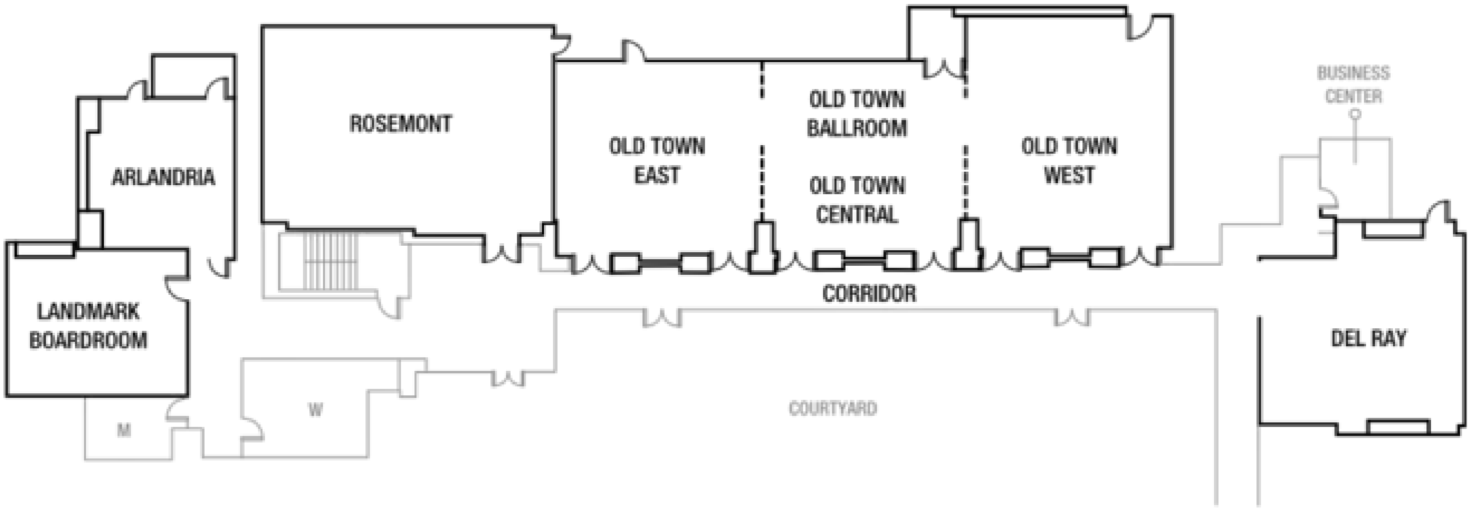
Poster Reception

Poster Reception Floor Plan



T1-100 Workforce Study: Community College Cybersecurity Alumni- Where Are They Now?	**T2-125** CyberCorps Scholarship for Service Program: The Expanding Role of Community Colleges	**T3-150** Community College Leadership Roles, Including the Impact of the NSA/ DHS CAE Program on Community Colleges
T4-175 CTE K-12 Pathways of Study in Cybersecurity: The Role of Community Colleges	**T5-200** National Trends of Community colleges Offering Bachelor's Degrees: What Are the Current and Future Impacts on the National Cyber Workforce?	**T6-225** The Successes and Challenges Faced by Community Colleges in Addressing the Evolving Cybersecurity Work Roles
T7-250 New Models for Cybersecurity Teaching and Training: The Case for National Action	**T8-275** The Challenges in Building Stronger Community College Cyber Articulation Agreements	**T9-300** The Achievements and Obstacles in Building a Diverse Cybersecurity Workforce
T10-325 An Examination of Community College and Government Partnerships	**T11-350** Innovations in Cybersecurity Classroom Practices: A Spotlight on Community Colleges	**T12-375** Evidence-Based Assessment: The Role of Extracurricular Activities in Preparing Students for the Cybersecurity Workforce
S1-100 Cloud Security Alliance	**S2-125** ISACA International	**S3-150** EC-Council | Academia
S4-175 Stanly Community College ASC | ITC	**S5-200** ISACA Los Angeles Chapter	**S6-225** Network Development Group
S7-250 US Bank	**S8-275** Cisco Networking Academy	**C1-100** National Cybersecurity Training & Education Center
C2-125 Center for Systems Security and Information Assurance	**C3-150** National Cyberwatch West	**I1-100** Building a Culturally Responsive Degree Program in Information Security
I2-125 Advanced Technological Education Coordination Network for Knowledge Sharing in Robotics/ Automation and Cybersecurity	**I3-150** CyberTraining: Implementation: Small: Using Problem-Based Learning for Vocational Training in cyberinfrastructure Security at Community Colleges	**I4-175** Cybersecurity Advanced Technological Education at a Tribal College

Venue Floor Plan



Nearby Restaurants

Fish Market Restaurant *Seafood restaurant - $$* 105 King St.	**Hen Quarter** *Southern restaurant - $$* 801 King St.	**Chop Shop Taco** *Mexican restaurant - $* 1008 Madison St.
Mia's Italian Kitchen *Italian restaurant - $$* 100 King St.	**Old House Cosmopolitan** *European restaurant - $$* 1024 Cameron St	**Chadwicks** *American restaurant - $* 203 Strand St
Landini Brothers Restaurant *Italian restaurant - $$$* 115 King St	**Blackwell Hitch** *American restaurant - $$* 5 Cameron St.	**Fontaine Caffee & Creperie** *French restaurant - $$* 119 S. Royal St.
The Warehouse *Fine Dining - $$* 214 King St	**Vola's Dockside Grill/Hi-Tide Lounge** *Seafood restaurant - $$* 101 N. Union St.	**Gadsby's Tavern Museum** *American restaurant- $$* 134 N Royal St
The Wharf *Seafood restaurant - $$* 119 King St	**Virtue Feed & Grain** *American Restaurant - $$* 106 S. Union St.	**TJ Stone's** *American restaurant - $$* 608 Montgomery St
La Madeleine *French restaurant- $$* 500 King St.	**District Taco** *Mexican restaurant - $* 701 S. Washington St	**Royal Restaurant** *Traditional American - $* 730 N. St. Asaph St.
Vaso's Mediterranean Bistro *Mediterranean restaurant - $$* 1118 King St	**Southside 815** *American restaurant - $$* 815 S. Washington St	**Blue & White Carryout** *Take out restaurant - $* 1024 Wythe St
The Majestic *New American restaurant - $$$* 911 King St	**Mason Social** *American restaurant - $$* 728 N. Henry	**Dos Amigos** *Tex Mex restaurant - $$* 535 E. Braddock Rd