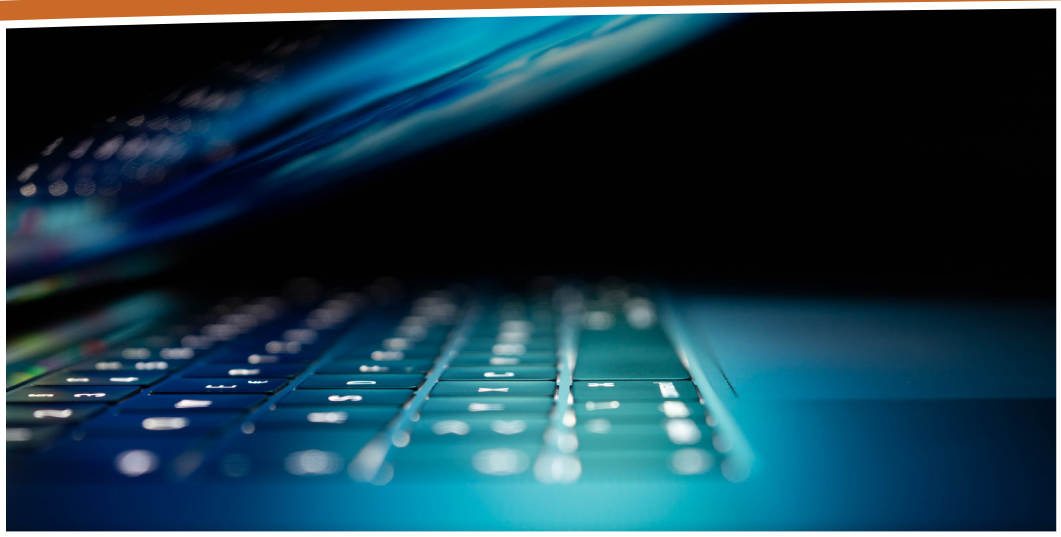
TRAINING TOMORROW'S CYBERSECURITY WORKFORCE

Download this **Document**

One Pager

Briefing held: **MARCH 2023**

For more details about this briefing: ccst.us/expert-briefings



SUMMARY

- The cybersecurity workforce is facing a shortage of trained professionals as we become more computer-reliant, data-driven, and network-based society.
- Academic, educational, and workforce systems are working together to implement novel training to meet the ever-increasing demand for cybersecurity professionals.

Cybersecurity Workforce has Reached Critical Demand

The demand for cybersecurity workers is exceeding the supply and is intensifying as a result of increased numbers of cyberattacks. The COVID-19 pandemic severely impacted the global cyber threat landscape due to the large and sudden shift to teleworking. This shift resulted in large security vulnerabilities which leave organizations, institutions, and companies susceptible to increased security exposures. Additionally, increased reliance on networks, cloud-based, data-driven work requires protection.

The Need for Cybersecurity in a Technology-Driven World

In a modern and data-driven society with increased cybersecurity risks, a skilled and qualified cybersecurity workforce is needed to fill in the various jobs in the sector. Coordinated efforts in education, training, and workforce development are needed to support the development of cybersecurity specialists and professionals to meet the ever-increasing demand of the cybersecurity workforce.

Alongside a trained cybersecurity workforce, cyber hygiene is important to implement to create an aware and informed user base. Despite known risks, threats, and vulnerabilities, there exists a dangerous shortage of cybersecurity professionals in the workforce. California alone has reached a critical point with over 72,000 vacancies and job growth projections predicted to be 28% through 2026. Currently, the demand for cybersecurity professionals far exceeds the supply of a qualified workforce.

Preparing for the Workforce Through Collaborations

New ways to increase the preparedness of students to pursue careers in cybersecurity are needed to address the growing concern on how to keep up with the pace of tech and

STRONGER WITH SCIENCE FOR 35 YEARS

CCST CALIFORNIA COUNCIL ON SCIENCE & TECHNOLOGY

CCST Disaster Resilience Initiative: Ongoing, complex, and intersecting disasters—including climate change, extreme heat, power outages, and the COVID-19 pandemic—are radically disrupting the ways in which Californians live and work. CCST is committed to delivering science and technology advice to improve our resilience to disasters, reduce harm, and improve the lives of all Californians.

SELECT EXPERTS

The following experts can advise on cybersecurity workforce development:

JOHN HANAFEE (Moderator)
Advisory Services Program Chief,
California Information Security Office
California Dept. of Technology
john.hanafee@state.ca.gov

KAYVAN CHINICHIAN
Senior Director of Development
California Cybersecurity Institute
Cal Poly, San Luis Obispo
kchinich@calpoly.edu

EXPERTISE: DATABASE MANAGEMENT, BRANDING AND IDENTITY, NONPROFIT ADMINISTRATION, IRANIAN POLITICS, INTERNATIONAL AFFAIRS, FOREIGN POLICY, POLITICAL/SOCIAL MOVEMENTS

TONY COULSON PHD
Professor
CSU San Bernardino
tcoulson@caecommunity.org

EXPERTISE: GLOBALLY RECOGNIZED CYBERSECURITY EXPERT ON MANAGEMENT INFORMATION SYSTEMS, LEADS THE CAE COMMUNITY CYBERSECURITY EDUCATION

MARKUS GEISSLER PHD
Professor, Computer Information Science
Cosumnes River College
geisslerm@gmail.com

EXPERTISE: PROFESSOR OF COMPUTER INFORMATION SCIENCE WITH A DEMONSTRATED HISTORY OF WORKING IN THE HIGHER EDUCATION INDUSTRY

DONNA WOODS
Instructor, Cyber Academic Pathway
Moreno Valley Unified School District
dwoods@mvusd.net

EXPERTISE: EDUCATOR, WORKSHOP FACILITATOR IN KNOWLEDGE IN THE INFORMATION TECHNOLOGY AND CYBER SERVICES INDUSTRY

CCST CONTACTS:

Brie.Lindsey@ccst.us
Director, Science Services

Sarah.Brady@ccst.us
Deputy Director

related challenges of protecting computers, data, and networks.

The need to supplement the cybersecurity workforce is being addressed by the **California Cybersecurity Task Force (CCTF)** co-chaired by the California Governor's Office of Emergency Service (CalOES) and California Department of Technology (CDT).

The Workforce Development and Education Subcommittee of the CCTF is working to implement the **California Cybersecurity Career Education Pipeline Project** involving K-12 educational systems, community colleges, and universities. The pipeline project develops the framework through **15 recommendations** to implement a plan to prepare 50,000 entry-level professionals in California between 2020-30.

A Look at the Pipeline Recommendations:

Non-traditional educational pathways to strengthen the workforce

Coordinated efforts and linkages between different levels of education are necessary for cybersecurity education and workforce development. To facilitate seamless transitions, educational and training roadmaps provide a guided perspective for different workforce sectors including academia, industry, and government.

Training the workforce within the K-12 education space

(Pipeline Recommendation #2)

K-12 education must have accessible, standardized, and comprehensive cybersecurity programs that include curriculum, courses, extracurricular activities, and professional development. One example recommended by the pipeline project is creating an industry-recognized standardized certification program with all levels of cybersecurity background available online to relieve local education agencies of financial burden. Another is to integrate cybersecurity coursework with "A-G" graduation requirements.

Two- and four-year degree level programs

(Pipeline Recommendation #3)

Development and implementation of cybersecurity transfer programs between community colleges and universities is crucial for students to seamlessly transition into the next level of education.

California community colleges, California State Universities, and Universities of California partner together to create Associate Transfer Degree (ADT) programs by standardizing and coordination program and course design to facilitate the 2-year to 4-year transition.

Graduate programs: master's and doctoral level programs

(Pipeline Recommendation #4)

Cybersecurity training at the Master's and Doctoral levels is also crucial to consider in the career preparedness and workforce pipeline. Entry-level cybersecurity jobs do not require advanced degrees; however, graduate training in cybersecurity is crucial to advance research, teaching, and training in all cybersecurity fields.

New instructors, educators, and researchers are needed to advance the dynamic landscape of cybersecurity knowledge and training. Efforts to retain women in cybersecurity and historically underrepresented backgrounds in cybersecurity are especially important to diversify the training workforce.

Professional certification and training

(Pipeline Recommendation #5)

Aligning cybersecurity education and training with workforce development and professional certification have been increasing over the years but more is needed. Aligning human resources job classification listings with certificate training objectives is still needed. Placing graduating students from different exit points of education into professional cybersecurity entry-level positions is the ultimate goal.