CYBERSECURITY CERTIFICATIONS

Respondents were asked about challenges to the success of their cybersecurity programs. The biggest challenge was "staffing—finding instructors with practical experience/technical expertise," which was cited as an "extreme challenge" by 46% of respondents (Exhibit 40). Other extreme challenges include internships, curriculum, student employment, and equipment.

Exhibit 40. Challenges to the success of cybersecurity programs

Challenge	Not a Challenge	Somewhat/ Moderate Challenge	Extreme Challenge	Total
Staffing—finding instructors with practical experience/technical expertise	7.7%	46.2%	46.2%	52
Employer engagement—student internships	15.7%	47.1%	37.3%	51
Curriculum—keeping curriculum up-to-date with constantly evolving technologies	11.5%	57.7%	30.8%	52
Employer engagement—student/graduate employment	20.8%	52.1%	27.1%	48
Equipment—finding resources for new training equipment or soliciting donations for equipment	17.3%	55.8%	26.9%	52
Employer engagement—connecting employers to the program for advisory group functions	19.6%	58.8%	21.6%	51
Faculty development—providing access to professional development opportunities	21.2%	61.5%	17.3%	52
Facilities—adequate, workable space for this type of program	38.5%	46.2%	15.4%	52
Maintaining software licenses	34.7%	55.1%	10.2%	49

Other, provided in comment box:

4-year transferability

time to learn while dealing with lots and lots of Campus obligations such as peer faculty evals, committee obligations, and other non-pertinent duties

Marketing Courses

Motivating other instructors to teach current technology

Overburdened with academic work

SECTION V: CONCLUSION

TRAINING GAP ANALYSIS

The demand in California for cybersecurity workers and IT/IS workers requiring cybersecurity skills is large and growing larger according to survey data collected for this study, secondary data from CyberSeek.org, and recent workforce reports.

The data collected from a representative sample of California employers suggests strong growth over the next 12 months for cybersecurity jobs. Five cybersecurity-specific work roles range from 7% to 21% growth (an increase of about 9,400 positions) and four IT/IS work roles that require cybersecurity skills range from 4% to 18% growth (an increase of about 4,900 positions). Cyberseek.org estimated 35,275 online job listings from April 2017 through March 2018 as a separate measure of demand for cybersecurity-related jobs[30] in California.

There is an estimated annual supply of 15,720 candidates from accredited postsecondary institutions in California. However, an annual undersupply exists of approximately 19,500 cybersecurity workers in the state.

An assessment of California IPEDS reveals an estimated annual supply of 15,720 candidates potentially available to fill cybersecurity-related jobs from accredited postsecondary institutions in all three program categories established for this study: cybersecurity focused, includes aspects of cybersecurity, and likely includes cybersecurity. Supply from the two program categories most likely to be preparing qualified candidates—cybersecurity focused and includes aspects of cybersecurity—have an estimated annual supply of 3,200 candidates.

To make a state-level comparison of employer demand and education supply, the best available data sets for the entire state are utilized. On the demand side, the Cyberseek.org estimate of annual demand in the state for cybersecurity-related jobs of 35,275 can be compared to two different supply estimates.

In the first scenario, annual demand is compared to the annual supply of 15,720 candidates from all three program categories outlined above, who could potentially fill cybersecurity-related jobs. The result is an annual undersupply of approximately 19,500 workers for the cybersecurity labor market in the state. In the second scenario, annual demand is compared to the annual supply of 3,200 candidates from the two program categories—cybersecurity focused and includes aspects of cybersecurity—that are most likely to be preparing qualified candidates who could potentially fill cybersecurity-related jobs. The result is an annual undersupply of approximately 32,000 workers for the cybersecurity labor market in the state.

This method is an approximation of the gap since there are many unknowns on the demand side, including, but not limited to, the accuracy of online job postings which are subject to employer data input errors, duplication and the effectiveness of the software utilized by online job posting vendors to collect these data. It is also important to note that not all available job openings are posted online. On the supply side there are also many unknowns, including, but not limited to, the unknown quantity of supply from other education and training providers not included in the IPEDS database of accredited postsecondary institutions and worker recruitment/relocation from outside California. Comprehensive data from all cybersecurity education and training providers is difficult to obtain due to the lack of a state or federal database that reports data for programs not accounted for in the IPEDS database.

[30] Includes workers in primary cybersecurity jobs—such as cybersecurity analysts—as well as workers in roles requiring cybersecurity-related skills and certifications.

TRAINING GAP ANALYSIS

Even with these data limitations, it seems highly likely that California's educational institutions are not currently supplying enough qualified candidates to fill the job openings that exist. Although the number of cybersecurity-related credentials awarded from accredited postsecondary institutions in California is increasing, the rate of growth is not enough to meet the demand employers have for cybersecurity workers.

In addition, Cyberseek.org data currently estimates about 85,290 workers in the California cybersecurity workforce. A comparison of the current cybersecurity workforce to the 35,275 cybersecurity job openings from the 12-month period of April 2017 through March 2018, shows there are 2.4 cybersecurity workers employed for every job opening. This ratio indicates a low supply of qualified cybersecurity workers in California compared to a national average across all industries of 6.5 workers for every job opening.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

A summary of findings from the demand-side analysis and educational supply analysis is outlined below.

Key Findings: California Cybersecurity Labor Market Survey

1. **There is projected growth for all nine work roles studied.**

   Over the next 12 months all nine work roles are projecting an increase in the combined number of permanent and temporary cybersecurity jobs of between 4% and 21% depending on the work role, resulting in an increase of about 9,400 specialized cybersecurity positions and about 4,900 IT/IS positions that require cybersecurity skills.

2. **A majority of employers are having difficulty finding qualified candidates.**

   For all nine work roles, 60% or more of employers reported some or great difficulty finding qualified candidates to hire, with defense contractors experiencing higher levels of difficulty.

   This demonstrates the significant challenge employers are facing finding the cybersecurity workers they need.

3. **Employers are responding to hiring challenges by increasing recruitment.**

   To address their hiring challenges, employers are clearly using proactive strategies—increasing recruitment, increasing overtime with current employees, and increasing wages to attract candidates or retain current employees. Increasing recruitment appears to be the preferred strategy used by employers, including defense contractors.

4. **Employers face multiple workforce issues or challenges.**

   On average, across all nine work roles, the top three issues or challenges related to hiring are: a) a lack of qualified candidates in general, b) candidates lack relevant work experience, and c) candidates lack required technology skills. For defense contractors, the top three issues or challenges are slightly different: a) candidates lack required technology skills, b) a lack of qualified candidates with necessary security clearances, and c) a lack of qualified candidates in general.

5. **Security certifications are important to employers when hiring.**

   For all nine work roles, 55% or more of employers reported that security certifications are important or very important when hiring and for seven of the work roles, 66% or more of employers reported this. By comparison, for all nine work roles, 75% or more of defense contractors reported that security certifications are important or very important when hiring, and for seven of the work roles, 80% or more of defense contractors reported this.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

6. **Information Technology/Information Systems (IT/IS) workers need skills related to cybersecurity in their work roles.**

   For all four IT/IS work roles, a high percentage of employers indicated that cybersecurity specific skills from the NICE Framework are important or very important. A very high percentage of defense contractors also rated the NICE Framework cybersecurity skills for the four work roles as important or very important. This provides validation of the cybersecurity specific skills outlined in the NICE Framework, for these four IT/IS work roles.

7. **IT/IS workers spend more than a quarter of their time on security/cybersecurity issues.**

   For each of the four IT/IS work roles, between 52% and 58% of employers indicated that employees spend more than a quarter of their time on security/cybersecurity issues. The percentage of defense contractors indicating that employees spend more than a quarter of their time on security/cybersecurity issues is higher by between 17% and 23%, depending on the work role, compared to employers in the overall sample.

8. **IT/IS workers are spending more time on security/cybersecurity issues compared to 12 months ago.**

   For three of the four work roles—network operations specialist, system administrator and software developer—65% of employers said the percentage of time spent on security/cybersecurity issues had increased compared to 12 months ago. That number is slightly higher for defense contractors, with 70% or more reporting that the percentage of time spent on security issues had increased compared to 12 months ago, for all four work roles.

9. **A bachelor's degree is the minimum education level required by employers.**

   Employers selected a bachelor's degree as the minimum education level required, with 40% or more of employers indicating a bachelor's degree for all nine work roles.

10. **Problem solving is the most important soft skill for employers.**

    Problem solving emerged as the most important soft skill that employers want employees to have. It ranked as one of the top three soft skills important to employers, for all nine work roles.

Key Findings: California's Cybersecurity Education and Training Programs

1. **Cybersecurity training has a broad range.**

   Cybersecurity is a relatively new field, and currently there is no standardization of training nor credentialing. There is a broad range of training and education, from short-term intensive "boot camp" trainings to doctoral degrees, and a broad range of training providers, from accredited postsecondary institutions to for-profit training entities to specialized military training. Credentials range from industry certifications to university degrees. This trend is true in California as well as nationwide.

2. **The majority of programs at postsecondary institutions are not cybersecurity focused.**

   Overall, in California, there are 242 accredited postsecondary institutions that bestow awards in 1,177 programs of study related to cybersecurity. Of the 1,177 programs related to cybersecurity, only 5% are clearly cybersecurity focused, while 22% of programs are offered in the category of includes aspects of cybersecurity. The majority of the programs, 73%, are in the likely includes cybersecurity category. There are not enough programs in the state to produce the number of qualified candidates needed to fill specialized cybersecurity work roles, when only 5% are cybersecurity focused.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

3. **The number of awards from accredited postsecondary institutions in California is increasing, but not fast enough.**

   In the most recent five years for which data was available, there was a 29% increase in cybersecurity-focused awards (degrees and certificates) granted by California colleges and universities. There was also growth in cybersecurity-related awards in the same time period; however, this growth is not keeping pace with employer demand for cybersecurity workers.

4. **A majority of cybersecurity-related programs at postsecondary institutions appear to align with the "Operate and Maintain" category in the NICE Framework.**

   In a survey of postsecondary institutions with cybersecurity-related programs, nearly two-thirds of respondents indicated they offered programs that align with the "Operate and Maintain" category in the NICE Cybersecurity Workforce Framework.

5. **Problem solving is emphasized in cybersecurity-related education programs.**

   A survey of postsecondary institutions with cybersecurity-related programs indicated that problem solving is the soft skill most emphasized in cybersecurity coursework and training. Other highly emphasized soft skills are ethics, troubleshooting, and teamwork/collaboration.

6. **Participation on advisory boards is the most common way employers engage with cybersecurity-related education programs.**

   About two out of three postsecondary institutions indicated that participation on advisory boards is how employers engage with their cybersecurity-related education program. Other frequently cited employer engagement activities include provision of information about the industry and jobs, internships for students, and guest lectures.

7. **Cybersecurity-related education programs face staffing challenges.**

   The biggest challenge indicated by cybersecurity-related programs at California postsecondary institutions was "staffing—finding instructors with practical experience/technical expertise," which was cited as an "extreme challenge" by 46% of respondents.

8. **Cybersecurity courses are limited at the secondary level.**

   Public high schools in California offer pre-cybersecurity-related courses, but those courses are considered elective and account for less than 1% of high school enrollments. Recent efforts to promote occupations in cybersecurity with high school students have gone outside of the formal curriculum, in the form of CyberPatriot camps and the recently created California Cyberhub which aims to coordinate and promote cybersecurity training across secondary and postsecondary institutions.

9. **Improved alignment and established pathways are needed between secondary and postsecondary educational institutions, and the workforce.**

   As pre-cybersecurity coursework is limited at high schools, there is not a well-established cybersecurity pathway leading into postsecondary coursework and the workforce. The alignment between postsecondary institutions and the workforce also seems limited, as degrees and certificates may not be valued by employers as much as skills attainment, which can be verified by industry certifications.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

> **"The NICE Framework provides employers, employees, educators, students, and training providers with a common language to define cybersecurity work. By defining the cybersecurity workforce and using standard terminology, academia and employers can synchronize education, recruitment, and development to establish a robust talent pipeline and sustain a highly qualified workforce."**
>
> NICE Framework Work Role Capability Indicators report, Draft NISTIR 8193, November 2017.

Recommendations

Education and training providers should expand capacity to prepare more students for the thousands of open specialized cybersecurity positions and IT/IS positions that require cybersecurity skills.

This report confirms and attempts to quantify the shortage of qualified workers ready to fill open cybersecurity positions in California's labor market. California's educational institutions can utilize this data to document the need to create new courses and programs or expand existing programs to prepare more qualified cybersecurity workers across the state. An encouraging sign from the qualitative survey of postsecondary institutions is that across the seven NICE program concentrations, between 20% and 43% of responding colleges and training institutions that currently do not have cybersecurity programs are interested in and/or anticipate creating such programming in the future.

Education and training providers should align their curriculum offerings with the NICE Cybersecurity Workforce Framework so students who complete programs have the requisite knowledge, skills and abilities for the work roles they are entering.

The challenge facing educational institutions is not only can they educate and train more students to fill the thousands of cybersecurity job openings in the state, but can they provide students with the skills that employers need to perform these jobs? Perhaps one of the main contributions of this report will be introducing education and training providers to the NICE Cybersecurity Workforce Framework. It establishes a taxonomy and common vocabulary that educators and employers can use to describe cybersecurity work, irrespective of where or for whom the work is performed.

As more education and training institutions align their curriculum with the knowledge, skills and abilities (KSAs) identified by the NICE Framework's work roles, they will be preparing their students to meet the requirements of employers, and students will be more likely to succeed in the workplace. Establishing this kind of clarity in terminology for this emerging field of study will help students and others interested in pursuing a cybersecurity career to understand all their options and pursue the right one for them. The work role profiles produced for each of the nine work roles studied provide a snapshot of what a qualified candidate looks like based on the sample of California employers surveyed. (See Appendix D.) A review of these profiles that include the technical and soft skills, education level, prior work experience, and security certifications that employers are seeking, is a good starting point for educators as they build curriculum and programs that prepare students to be qualified candidates for employment.

Employers should utilize the NICE Framework for creating job descriptions and designing workforce/professional development strategies.

Employers who are increasing the number of cybersecurity positions within their businesses, including IT/IS positions that require cybersecurity skills, have an opportunity to utilize the NICE Framework for creating job descriptions and workforce/professional development strategies to increase employee recruitment and retention efforts.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

The NICE Framework can play a major role in aligning employers and educators to address the cybersecurity workforce needs in California.

If a majority of both educators and employers in California adopt the NICE Framework in their respective roles, the result can be a more finely tuned cybersecurity labor market. Using the framework's cybersecurity workforce definitions and standard terminology, academia and employers can synchronize education, recruitment, and development to establish a robust talent pipeline and sustain a highly qualified workforce.

The NICE Framework can serve as the bridge to connect the education and business communities so students are prepared for the jobs that employers need to fill, and the training and education students receive aligns with employer job descriptions and hiring qualifications. It will be increasingly important to achieve this alignment if businesses are to achieve the security of their information technology and systems that is necessary.

RESOURCES FOR EDUCATORS

There is a wealth of information available to education and training providers as they develop new cybersecurity courses and programs or seek to enhance their existing programs to stay current and relevant as this field changes rapidly. Some important resources are listed below with their website and a brief description of what is provided by the organization.

NICE Cybersecurity Workforce Framework

Website: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

The NICE Cybersecurity Workforce Framework (NICE Framework) is the blueprint to categorize, organize, and describe cybersecurity work. It was developed in partnership with the National Initiative for Cybersecurity Education (NICE), the Office of the Secretary of Defense, and Department of Homeland Security (DHS) to provide educators, students, employers, employees, training providers, and policy makers with a systematic and consistent way to organize the way we think and talk about cybersecurity work, and to identify the knowledge, skills, and abilities needed to perform cybersecurity tasks.

Department of Homeland Security (DHS)

DHS Education for Cybersecurity Careers

Website: https://www.dhs.gov/education-cybersecurity-careers

The cyber leaders of tomorrow are sitting in classrooms today. As cyber threats continue to evolve, the nation's protection against them relies on a steady stream of qualified cybersecurity professionals entering the workforce. The Department of Homeland Security (DHS) is committed to helping educate the nation's students in cybersecurity to develop a more resilient and capable cyber nation. Resources for academic institutions and teachers supported by DHS and outlined below:

- **Academic Institutions:** Colleges and universities interested in further developing their cyber-related degree programs can learn about becoming a National Center of Academic Excellence at https://www.nsa.gov/resources/educators/. Additionally, institutions can recruit the best and the brightest by offering scholarship and job placement assistance through participating in the CyberCorps® Scholarship for Service (SFS) program at https://www.sfs.opm.gov/StudFAQ.aspx?#num36
- **Teachers:** Teachers can learn about professional development opportunities at https://niccs.us-cert.gov/formal-education and information they can use to motivate and educate students of all ages to consider cyber careers. Teachers can also access free lesson plans at the website above.

RESOURCES FOR EDUCATORS

DHS Cybersecurity Workforce Development Resources
Website: https://www.dhs.gov/cybersecurity-workforce-development-resources

To develop a more resilient and capable cyber nation, we must have a highly-skilled cybersecurity workforce across industry and government. The Department of Homeland Security (DHS) is committed to helping organizations build a comprehensive cybersecurity professional capability. DHS's workforce development tools and resources help organizations understand and act on their cybersecurity workforce needs and answer questions such as:

- What is the current state of my employee's cyber capabilities?
- What gaps do we need to fill?
- What kinds of cybersecurity workers do we need to hire?
- How can I keep and grow my cybersecurity staff?

Effective cybersecurity workforce development helps organizations more efficiently and effectively recruit qualified cybersecurity professionals, and to provide this critical workforce with clear job descriptions and development opportunities. DHS has a resource to help organizations get—and keep—the right cybersecurity staff: The *Cybersecurity Workforce Development Toolkit,* which can be downloaded at:
https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit

The Toolkit helps organizations understand their cybersecurity workforce and staffing needs, and includes things like templates to create cybersecurity career paths, and resources to recruit and retain top cybersecurity talent.

DHS Training for Current and Aspiring Cybersecurity Professionals
Website: https://www.dhs.gov/training-cybersecurity-careers

DHS offers multiple training and education resources, including an extensive Training Catalog, which can be found at: https://www.dhs.gov/training-cybersecurity-careers that features an interactive map and filters to search for courses offered in a local area. The Training Catalog maps cybersecurity courses to Specialty Areas in the NICE Cybersecurity Workforce Framework.

Cybersecurity professionals and those entering cybersecurity careers can quickly identify the courses they need to advance within their specialty area or to transfer skills.

The Training Catalog organizes more than 2,000 courses provided by organizations across the cybersecurity industry. A broad range of courses are offered to meet the needs of anyone interested in training, including:

- Current cybersecurity professionals who want to update their skills and advance their career.
- Students who are looking to enter the cybersecurity field; and
- Professionals in a related field (including veterans) who would like to change careers.

National CyberWatch Center

Website: https://www.nationalcyberwatch.org/programs-resources/curriculum/

Funded by the National Science Foundation's Advanced Technological Education program, the National CyberWatch Center, located at Prince George's Community College in Maryland, has model cybersecurity curricula available, including multiple degree and certificate programs. The Center continues to update and create model Information Security curricula, which supports the growth of cybersecurity education nationally, including complete courses for degrees and multiple certificates. Curriculum resources include:

RESOURCES FOR EDUCATORS

Curriculum Guide: National CyberWatch's Information Security Curricula Guide: A Complete Solution for Higher Education Institutions.

Degree Programs: Based on input from industry, labor market demand research, and over 10 years of Information Security content development experience, the National CyberWatch Center degree programs help prepare students for the in-demand jobs of the knowledge economy.

Certificates: These specialized and stackable certificates allow students to earn multiple academic certificates while pursuing their associate degree and to earn industry credentials by sitting for industry-recognized professional certification exams.

Technical Courses: The technical courses in the National CyberWatch Center degree and certificate programs align to various industry-recognized professional certifications, federal and national standards, job roles, and provide hands-on experiences required in today's competitive marketplace.

E-Books: The National CyberWatch Center, in conjunction with Jones & Bartlett Learning, have produced a series of e-Books. Instructors can request an access code by sending an email to: info@nationalcyberwatch.org

Lab Solution: National CyberWatch Center and Infosec Learning have partnered to develop a Complete Cloud-Based Lab Solution.

Competency-Based Curriculum: Competency-based objectives, principles, and techniques target increased cybersecurity capability maturity of the entrant and incumbent Information Technology workforce.

California Community Colleges, IT Technician Pathway – Cybersecurity Specialist

Website: https://ict-dm.net/ittp
Pathway Graphic: https://ict-dm.net/images/itp/toolkit/ITTP_Specializations_all_toprint.pdf

The California Community Colleges IT Technician Pathway (ITTP) provides a clear roadmap for gaining the key elements of career success: 1) Technical Training, 2) Industry Certifications, and 3) Work Experience. As students progress through the pathway, additional training and certification, lead to higher skilled and better paying jobs.

Cyberseek: Cybersecurity Career Pathway

Website: https://www.cyberseek.org/pathway.html

There are many opportunities for workers to start and advance their careers within cybersecurity. This interactive career pathway shows key jobs within cybersecurity, common transition opportunities between them, and detailed information about the salaries, credentials, and skill sets associated with each role.

APPENDIX A: CALIFORNIA CYBERSECURITY LABOR MARKET SURVEY METHODOLOGY

The California Community Colleges Centers of Excellence for Labor Market Research (COE) and Davis Research conducted an online, employer-demand survey of California businesses about their cybersecurity workforce needs. In total, 385 businesses completed the survey to achieve a 95% confidence level (+/- 5% margin of error). Employers met at least one of the following criteria to participate in the demand side survey:

1. Be a prime defense contractor or first, second, third, or fourth tier subcontractor.
2. Be a firm operating in the cybersecurity sector with products with defense applications in California.
3. Be a firm with current or future projected shortages of cybersecurity workers or IT/IS workers that require cybersecurity skills.

Method	Web survey with online and telephone recruitment
Population	About 2,105 California businesses
Sample	385 businesses in California who employ cybersecurity workers or information technology/information systems (IT/IS) workers who require cybersecurity skills
Field dates	February 20, 2018 to April 24, 2018

Research Objectives

Prior to beginning the project, the COE and California Governor's Office of Business and Economic Development (GO-Biz) agreed upon the following research objectives for the study:

- To gather cybersecurity labor market data and training provider information in order to enhance the cybersecurity resilience of California's defense supply chain, which will in turn support supply chain modernization, diversification and sustainability efforts.
- To gather labor market and other workforce data from California employers that will project demand for cybersecurity workers and the skills these workers need.
- To gather data on the training and education programs in California that prepare students for cybersecurity occupations in order to more fully assess California's capacity to meet cybersecurity workforce demand.

For purposes of this survey, the cybersecurity workforce was defined as follows:

- Cybersecurity workforce: Personnel who secure, defend, and preserve data, networks, netcentric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities.

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

- Cyberspace IT workforce: Personnel who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize portfolio investments; architect, engineer, acquire, implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information.

http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001_2015_dodd.pdf