SUMMARY & KEY FINDINGS

CYBERSECURITY:
LABOR MARKET ANALYSIS AND
STATEWIDE SURVEY RESULTS
FROM CALIFORNIA EMPLOYERS AND
POSTSECONDARY INSTITUTIONS

June 2018

Prepared by:
The California Community Colleges
Centers of Excellence for Labor Market Research
The California Community Colleges Centers of Excellence for Labor Market Research (COE) conducted a workforce demand study of 385 cybersecurity employers in 2018. The following summary highlights the findings for the nine cybersecurity jobs included in the study.

### IT/IS Jobs Requiring Cybersecurity Skills

Employers plan to add more than **4,900** information technology/information systems (IT/IS) jobs requiring cybersecurity skills over the next 12 months.

For each of the IT/IS work roles, the majority of employers said that employees spend more than a quarter of their time on security/cybersecurity issues.

48% of employers said there is a lack of qualified software developer candidates in general.

### Specialized Cybersecurity Jobs

Employers plan to add more than **9,400** specialized cybersecurity jobs over the next 12 months.

76% of employers reported some or great difficulty hiring cyber defense forensic analysts.

**Top 3 hiring challenges** for specialized cybersecurity jobs:

1. Lack of qualified candidates in general—vulnerability assessment analysts (43%)
2. Lack of relevant work experience—cyber defense infrastructure support specialists (46%)
3. Lack of required technology—cyber defense infrastructure support specialists (49%)
TRAINING GAP FINDINGS

It is highly likely that California’s educational institutions are not supplying enough qualified candidates to fill existing job openings. The number of cybersecurity-related credentials awarded from accredited postsecondary institutions in California is increasing; however, the rate of growth is not enough to meet the demand employers have for cybersecurity workers.

<table>
<thead>
<tr>
<th>Specialized cybersecurity jobs will increase</th>
<th>IT/IS jobs requiring cybersecurity skills will increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>7%–21%</td>
<td>4%–18%</td>
</tr>
<tr>
<td>Adding 9,413 workers</td>
<td>Adding 4,910 workers</td>
</tr>
<tr>
<td>60%</td>
<td>55%</td>
</tr>
<tr>
<td>or more reported difficulty finding qualified candidates</td>
<td>or more reported that security certifications are important or very important</td>
</tr>
</tbody>
</table>

Employers are responding to hiring challenges by:

- Increasing recruitment efforts
- Increasing overtime with current employees
- Increasing wages to attract or retain workers

Employers plan to add 14,300* cybersecurity jobs over the next 12 months

3,200 Awards conferred by California training programs that are cybersecurity focused or include aspects of cybersecurity

Potential training gap of 11,100* cybersecurity jobs

CyberSeek.org estimated 35,275 online job listings

For cybersecurity-related jobs in California from April 2017 to March 2018

* Based on the nine NICE Cybersecurity Workforce Framework work roles featured in the study.
RESOURCES FOR EDUCATORS

**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 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 are listed below:
- https://www.nsa.gov/resources/educators/
- https://niccs.us-cert.gov/formal-education

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

DHS’s workforce development tools and resources help organizations understand and act on their cybersecurity workforce needs.

**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 that features an interactive map and filters to search for courses offered in a local area.

**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. Curriculum resources include: curriculum guide, degree programs, certificates, technical courses, e-books, lab solution, competency-based curriculum.

**Cyberseek: Cybersecurity Career Pathway**
Website: https://www.cyberseek.org/pathway.html

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.

**California Cyberhub**
Website: https://ca-cyberhub.org/

California Cyberhub distills and catalogs best practices from cyber training and competitions in the state to provide concise resources for those wishing to adopt cyber training in their communities. Partners include K-12, public higher education, including the California Community Colleges, government, business, and the military.
The COE analyzed cybersecurity-related educational programs in California to assess the state’s capacity to meet employers’ workforce demand. The study identifies three different levels of cybersecurity programs and responses from 61 educators.

### Cybersecurity Focused:
If both the classified instructional program (CIP) title and the description addressed cybersecurity, then a program was coded as “Cybersecurity Focused.”

### Includes Aspects of Cybersecurity:
If the CIP title was related to cybersecurity and the description included aspects of cybersecurity, such as “information security.”

### Likely Includes Cybersecurity:
If the CIP title is in a field known to include cybersecurity as an important topic, such as computer and information science, and computer engineering and technology, and the CIP description included knowledge that is impacted by cybersecurity, such as “database administration.”

<table>
<thead>
<tr>
<th>Criteria</th>
<th>3 CIP titles met these criteria</th>
<th>11 CIP titles met these criteria</th>
<th>20 CIP titles met these criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>In California there are:</td>
<td>61 programs</td>
<td>258 programs</td>
<td>858 programs</td>
</tr>
<tr>
<td></td>
<td>813 awards</td>
<td>2,410 awards</td>
<td>12,507 awards</td>
</tr>
</tbody>
</table>

The number of cybersecurity-related awards conferred increased **29%** between 2012 and 2016.

**Postsecondary Cybersecurity Programs**
- **72%** Public postsecondary
- **56%** 2-year programs
- **28%** Private postsecondary
- **16%** 4-year programs

More than **64%** of surveyed postsecondary institutions prepare students for CompTIA Security+ certification.

More than **42%** of surveyed postsecondary institutions prepare students for the Certified Ethical Hacker (CEH) certification.

**Other Cybersecurity Training Providers**
- **521** High schools offer cybersecurity-related courses
- **25,117** High school enrollment in cybersecurity and pre-cybersecurity coursework

**Soft Skills**
- emphasized by postsecondary institutions

**Problem Solving**
- Teamwork/Collaboration

**Troubleshooting**
- Communication Skills

**Ethics**
For more information about the Cybersecurity: Labor Market Analysis and Statewide Survey results contact any of the following Centers of Excellence Directors:

**Bay Area Region**  
John Carrese  
📞 (415) 267-6544  
📧 jcarrese@ccsf.edu

**Inland Empire Region**  
Michael Goss  
📞 (909) 652-7754  
📧 michael.goss@chaffey.edu

**South Central Coast Region**  
Adele Hermann  
📞 (805) 553-4625  
📧 ahermann@vcccd.edu

**San Diego/Imperial Region**  
Tina Ngo Bartel  
📞 (760) 795-6889  
📧 tngobartel@miracosta.edu

This study was prepared under contract with the California Governor’s Office of Planning and Research with financial support from the U.S. Department of Defense, Office of Economic Adjustment. The content reflects the views of the California Community Colleges Centers of Excellence for Labor Market Research and does not necessarily reflect the views of the U.S. Department of Defense, Office of Economic Adjustment.