C·O·E
CENTERS OF EXCELLENCE
Inform Connect Advance

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

CALIFORNIA ADVANCED SUPPLY CHAIN ANALYSIS & DIVERSIFICATION EFFORT
CASCADE

CALIFORNIA GOVERNOR'S OFFICE OF BUSINESS AND ECONOMIC DEVELOPMENT

TABLE OF CONTENTS

TABLE OF CONTENTS

ABOUT THE CASCADE PROGRAM

The California Cybersecurity Labor Market Analysis is one of 15 projects under the California Advanced Supply Chain Analysis & Diversification Effort (CASCADE).

CASCADE is an initiative funded by the U.S. Department of Defense, Office of Economic Adjustment (OEA), to bolster California's defense supply chain cybersecurity resilience, innovation capacity and diversification strategies, and to support the growth and sustainment of California's cybersecurity workforce through cybersecurity-related education curricula, training and apprenticeship programs. CASCADE is led by the California Governor's Office of Business and Economic Development (GO-Biz) and the California Governor's Office of Planning and Research (OPR). The CASCADE program includes 15 funded projects in partnership with government, industry, community, and academic institutions and is the most ambitious and comprehensive approach to addressing cybersecurity and the defense supply chain in California.

CASCADE Partner project activities will include cyber industry convenings, cyber provider mapping, cyber labor market research, supply chain mapping, supply chain outreach and resilience workshops, cyber physical security assessments, innovation and commercialization programs. The fundamentals of the projects will revolve around cybersecurity provider, defense supply chain and cyber workforce:

- Research and analysis,
- Education and outreach,
- Standards frameworks and best practices,
- Innovation, commercialization and diversification,
- Assistance and development programs.

REPORT DEVELOPMENT

Centers of Excellence for Labor Market Research, Economic and Workforce Development Program, California Community Colleges, www.coeccc.net

John Carrese, Michael Goss, Adele Hermann, Tina Ngo Bartel

The RP Group, Research and Planning for California Community Colleges, www.rpgroup.org

KC Greaney, Ph.D.

Davis Research LLC, www.davisresearch.com

David Fernandez

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.

EXECUTIVE SUMMARY

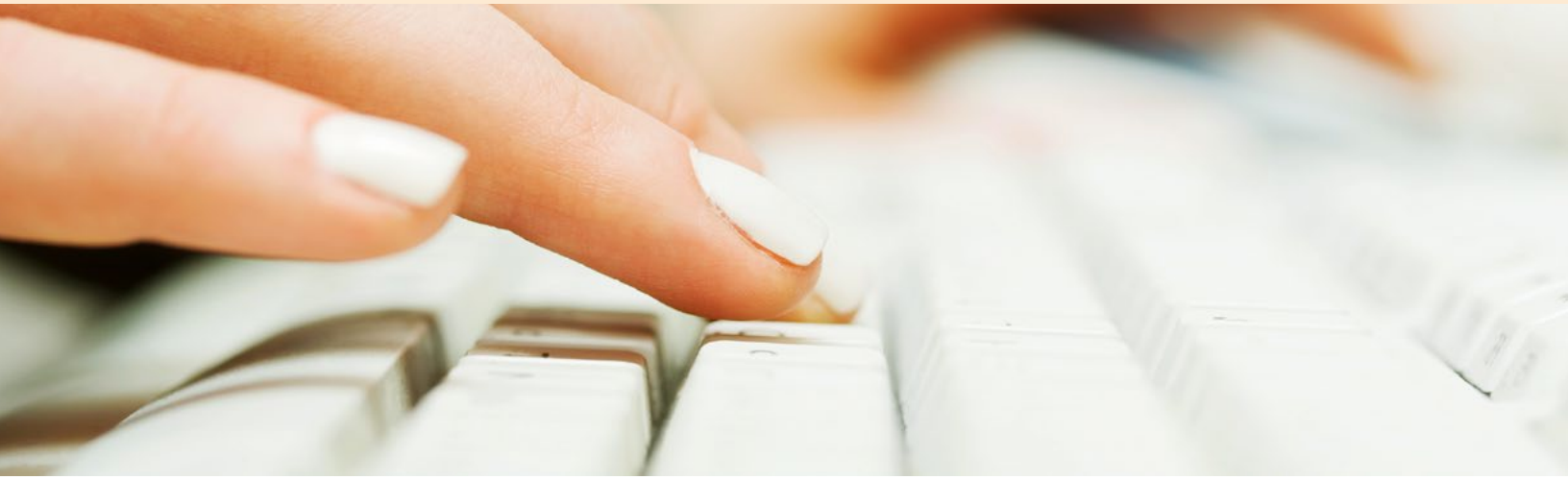
To address the statewide cybersecurity labor shortage, the California Community Colleges Centers of Excellence for Labor Market Research (COE) conducted a cybersecurity labor market analysis in 2018 as one of 15 CASCADE program activities. The study gathered information about workforce needs in California and the scope of training being provided by educational providers across the state.

A statewide employer survey was conducted to collect data for nine of the most common cybersecurity occupations, using the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Additionally, as part of the study, primary and secondary data was collected on public and private postsecondary institutions offering cybersecurity related programs.

Based on employer responses, strong cybersecurity employment growth is expected over the next 12 months, ranging from 4% to 21% for the work roles studied, representing an increase of about 14,300 positions. In 2016, the most recent year of available data, 242 accredited postsecondary institutions in California offered 1,177 programs that were related to cybersecurity. However, only 3,200 awards were conferred in 2016 by programs that focused directly on cybersecurity or clearly included aspects of cybersecurity in their curriculum. California's educational institutions are not currently supplying enough qualified candidates to fill the thousands of cybersecurity job openings that exist.

Additional key findings:

- For all nine work roles, 60% or more of employers reported some or great difficulty finding qualified candidates. This demonstrates the significant challenge employers are facing hiring the cybersecurity workers they need.
- Across all nine work roles, the top three hiring challenges are: lack of qualified candidates in general, lack of relevant work experience, and lack of required technology skills.
- 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.
- For each of four IT/IS work roles, a majority of employers indicated that employees spend more than a quarter of their time on security/cybersecurity issues and that compared to 12 months ago the amount of time spent on security/cybersecurity issues had increased.
- The majority of cybersecurity-related programs are offered by public two-year (56%) and public four-year (16%) colleges, resulting in public colleges offering 72% of cybersecurity-related programs.
- 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.



INTRODUCTION

A major, persistent problem for businesses is a lack of a trained workforce to fill the growing needs of the cyber industry. A Cybersecurity Ventures study in 2016 projects there will be 1.5 million cybersecurity job openings worldwide by 2019.[1] This void in talent threatens the ability of defense suppliers to build cybersecurity resilience. Without employees with the right training, defense suppliers will continue to have difficulty adhering to NIST 800-171 guidelines on protecting controlled classified information in non-federal systems and organizations.

In response, in 2018, as one of the 15 CASCADE program activities, the California Community Colleges Centers of Excellence for Labor Market Research (COE) conducted a cybersecurity labor market analysis, including defense supply chain businesses. This study set out to develop a data-driven understanding of what the needs and capabilities of the cyber workforce in California are and determine the best targets for future education and training program growth. This report is organized into five sections: 1) industry overview; 2) employer survey findings and workforce needs based on the NICE Framework; 3) cybersecurity program inventory of postsecondary and secondary institutions; 4) findings from a survey of postsecondary educational providers; and 5) conclusions and recommendations.

The study had three main objectives:

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

To determine the scope of workforce needs, 385 California employers were surveyed. They were asked about current and projected employment, difficulty in hiring qualified candidates, in-demand skills, security certifications and a variety of other issues. In gathering information from employers, the survey incorporated nine work roles associated with common cybersecurity occupations identified in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.[2] About half of the employers surveyed were identified as defense contractors, and where possible, survey results for this cohort of respondents is highlighted in this report.

The COE also assessed the cybersecurity education supply in California, including cybersecurity education and training programs for workers potentially affected by changes in defense spending. The study gathered and analyzed data from the U.S. Department of Education on California's postsecondary institutions with cybersecurity-related programs. Data was also gathered on the pipeline of articulated programs between high schools/regional occupational centers (ROCPs) and postsecondary institutions to more fully assess California's capacity to meet cybersecurity workforce demand. In addition, a survey of cybersecurity education providers in the state was conducted to provide qualitative data on the spectrum of cybersecurity training being offered.

Finally, this study's findings are intended to bolster overall supply chain resiliency by helping employers and defense firms identify cybersecurity skills gaps and build capacity in cybersecurity workforce development. Moreover, this research is intended to assist potentially displaced defense workers in identifying cybersecurity job openings and training programs applicable to a variety of industries.

[1] "Cybersecurity Jobs Report 2018-2021," Cybersecurity Ventures and Herjavec Group, May 2017, https://cybersecurityventures.com/jobs/.

[2] NICE Cybersecurity Workforce Framework, December 12, 2017, accessed May 17, 2018, https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

METHODOLOGY

The labor market analysis conducted for this report includes both a workforce demand and educational supply assessment.

Employer Survey

To gather information from businesses about their cybersecurity workforce, the California Cybersecurity Labor Market Survey was conducted. The survey was completed by 385 California businesses that employ cybersecurity workers or Information Technology/ Information Systems (IT/IS) workers who require cybersecurity skills. The survey results provide data on current and projected employment, difficulty in hiring qualified candidates, importance of security certifications, in-demand technical and soft skills and other workforce-related issues.

To participate in the survey, employers met one of three eligibility criteria. They were either a defense contractor, including first, second, third, or fourth tier subcontractor; a firm operating in the cybersecurity sector with products and/or services with defense applications in California; or a firm with current or future projected shortages of cybersecurity workers or IT/IS workers that require cybersecurity skills. Appendix A contains a detailed methodology of how the survey was conducted. Appendix B includes the survey instrument.

The work roles studied were selected from the 52 work roles contained in the NICE Framework and met the criteria of being both common to businesses in California and ones for which postsecondary institutions in the state have the capacity to prepare students. Appendix D contains profiles for each of the nine work roles, including a definition of the role and detailed data from the survey.

The NICE Cybersecurity Workforce Framework (NICE Framework) was developed by the National Institute of Standards and Technology (NIST) to categorize and describe cybersecurity work. According to NIST, the NICE Framework can be applied in public, private and academic sectors and "establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed."

The survey was developed with input from a Cybersecurity Labor Market Analysis Research Advisory Group, formed and convened by the California Community Colleges Centers of Excellence for Labor Market Research for this research project. Appendix C has a list of the Research Advisory Group members.

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.[3]

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.[4]

[3] Department of Defense Instruction: Number 8500.01," Department of Defense Chief Information Officer, March 14, 2014, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf.

[4] "Department of Defense Directive: Number 8140.01," Department of Defense Chief Information Officer, updated July 21, 2017, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001_2015_dodd.pdf.

METHODOLOGY

Educational Supply Assessment and Survey

The COE also conducted an analysis of the supply of cybersecurity education programs in California and the capacity of educational providers to train the workforce in this critically important field.

The study's educational assessment objectives included:

1. Clarify which accredited, federally recognized postsecondary institutions currently provide education and training related to cybersecurity,
2. Document cybersecurity concentrations and program awards at such institutions, and
3. Document the pipeline of articulated programs between high schools/regional occupational center programs (ROCPs) and community colleges in order to more fully assess California's capacity to meet cybersecurity workforce demand.

Data was gathered from the U.S. Department of Education via the Integrated Postsecondary Education Data System (IPEDS), National Center for Educational Statistics on the education and training programs in California that prepare students for cybersecurity occupations. Information on high school career pathways was sourced from the California Statewide Pathways Project and the California State Department of Education.

To gather qualitative data on some of these cybersecurity-related programs, educators at public and private educational institutions across the state were surveyed about the programs and courses they offer to more fully assess the state's capacity to meet cybersecurity labor market demand. In total, 64 institutions responded to the survey. Appendix J contains the survey questions sent to educational institutions.

SECTION I: INDUSTRY OVERVIEW

The destruction wrought through malware, data breaches and the high-profile cyberattacks of Equifax, Target, and Yahoo have brought the need for increased cybersecurity to the public's attention.

In the case of Yahoo, the details of three billion users may have been breached, while hackers were able to gain access to 143 million customer accounts through Equifax.[5] In 2016, LinkedIn lost 167 million email and account password combinations.[6] Target's breach in 2013, which leaked 110 million people's account information, still ranks as one of the worst breaches in history.[7]

The list goes on with the Saks Fifth Avenue and Lord and Taylor hack, which occurred in April and resulted in the loss of credit card data belonging to 5 million customers.[8] Most recently, Twitter exposed user information through flawed security practices when an internal bug revealed user passwords in May, leading the company to notify its 330 million users of the breach.[9] Like Twitter, other tech companies have made internal security mistakes resulting in grave consequences.

In January, the security flaws dubbed "Meltdown" and "Spectre" were discovered in three billion computer chips, exposing sensitive information stored in computers, cell phones and tablets to hackers.[10] On every front, consumers' data seems to be under threat. Even apps backed by large banks, such as Zelle, have proved vulnerable to attack.[11]

Major Cyberbreaches

- **Yahoo, 3 billion users**
- **Twitter, 330 million users**
- **LinkedIn, 167 million email/password combinations**
- **Equifax, 143 million customers**
- **Target, 110 million accounts**
- **Saks Fifth Avenue/Lord & Taylor, 5 million customers**

[5] Matt Burgess, "That Yahoo data breach actually hit three billion accounts," Wired Magazine, October 4, 2017, http://www.wired.co.uk/article/hacks-data-breaches-2017.

[6] Robert Hackett, "LinkedIn Lost 167 Million Account Credentials in Data Breach," Fortune Magazine, May 18, 2016, http://fortune.com/2016/05/18/linkedin-data-breach-email-password/.

[7] Elizabeth Weise, "Equifax breach: Is it the biggest data breach?" USA Today, September 7, 2017, https://www.usatoday.com/story/tech/2017/09/07/nations-biggest-hacks-and-data-breaches-millions/644311001/.

[8] Vindu Goel and Rachel Abrams, "Card Data Stolen From 5 Million Saks and Lord & Taylor Customers," The New York Times, April 1, 2018, https://www.nytimes.com/2018/04/01/technology/saks-lord-taylor-credit-cards.html?rref=collection%2Ftimestopic%2FComputer%20Security%20(Cybersecurity)&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=6&pgtype=collection.

[9] Chaim Gartenberg, "Twitter advising all 330 million users to change passwords after bug exposed them in plain text," The Verge, May 3, 2018, accessed May 17, 2018, https://www.theverge.com/2018/5/3/17316684/twitter-password-bug-security-flaw-exposed-change-now.

[10] Martin Giles, "At Least Three Billion Computer Chips Have the Spectre Security Hole," MIT Technology Review, January 5, 2018, https://www.technologyreview.com/s/609891/at-least-3-billion-computer-chips-have-the-spectre-security-hole/.

[11] Stacy Cowley, "Zelle, the Banks' Answer to Venmo, Proves Vulnerable to Fraud," The New York Times, April 22, 2018, https://www.nytimes.com/2018/04/22/business/zelle-banks-fraud.html?rref=collection%2Ftimestopic%2FComputer%20Security%20(Cybersecurity)&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=5&pgtype=collection.

RISE OF RANSOMWARE

Ransomware Attacks

- **WannaCry**
- **SamSam**
- **NotPetya**
- **CrySis**
- **Locky**

News reports indicate that ransomware attacks are on the rise and have become a leading tool used by hackers to access vulnerable data. In fact, data breaches dropped in 2017 by nearly 25 percent as hackers switched to ransomware and destructive attacks that either destroy or lock data until the victim complies by paying a ransom.[12]

Notable attacks include the WannaCry ransomware worm which attacked Microsoft Windows operating systems around the world, and the SamSam ransomware attack, which crippled the city of Atlanta and is expected to cost the city $2.6 million in recovery efforts.[13]

In 2017, ransomware attacks increased by 415% from 2016, with WannaCry having a tremendous effect, representing 9 out of 10 ransomware detection reports.[14] And as Atlanta illustrates, cyberattacks can be expensive. In fact, half of all cyberattacks end up costing more than $500,000.[15]

Meanwhile, there is no comprehensive strategy to deal with the alarming number of cyberattacks being witnessed worldwide. However, in April 2018, 34 global technology and security companies, including Microsoft, Facebook and Cisco, formed the Cybersecurity Tech Accord, to defend against cyberattacks and the misuse of technology. The accord includes a commitment to working collectively to address threats and collaborate on cybersecurity.[16]

CYBERSECURITY SKILLS SHORTAGE

California had over 35,000 job openings from April 2017 to March 2018 for cybersecurity professionals, according to CyberSeek's Hack the Gap interactive map tool. According to data released by Burning Glass in 2015, job postings for cybersecurity openings have grown three times as fast as openings for IT jobs overall.[17]

The median salary for cybersecurity professionals in North America is $75,000-$100,000, with the highest salaries being earned in retail and consumer durables, according to a study by Exabeam.[18]

[12] "IBM X-Force Report: Fewer Records Breached in 2017," Security Magazine, April 4, 2018, https://www.securitymagazine.com/articles/88893-ibm-x-force-report-fewer-records-breached-in-2017.

[13] Zack Whittaker, "Atlanta projected to spend at least $2.6 million on ransomware recovery," ZDNet, April 23, 2018, accessed May 17, 2018, https://www.zdnet.com/article/atlanta-spent-at-least-two-million-on-ransomware-attack-recovery/.

[14] "The Changing State of Ransomware," F-Secure, May 2015, accessed May 17, 2018, p. 6 and p. 9, https://fsecurepressglobal.files.wordpress.com/2018/05/ransomware_report.pdf.

[15] "Nearly Half of All Cyberattacks Result in Damages over $500,000," Security Magazine, April 1, 2018, accessed May 23, 2018, https://www.securitymagazine.com/articles/88834-nearly-half-of-all-cyberattacks-result-in-damages-over-500000.

[16] "Signing pledge to fight cyberattacks, 34 leading companies promise equal protection for customers worldwide," Cybersecurity Tech Accord, April 17, 2018, accessed May 17, 2018, press release, https://cybertechaccord.org/.

[17] "Job Market Intelligence: Cybersecurity Jobs, 2015," Burning Glass, PowerPoint presentation, accessed May 18, 2018, https://www.burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf.

[18] "Exabeam 2018 Cyber Security Professionals salary and Job Report: Compensation, Job Satisfaction, Education, and Technology Outlook," Exabeam, May 2018, accessed May 23, 2018, p. 9, https://www.exabeam.com/wp-content/uploads/2018/05/EXA_Salary-Survey-Report_L1R7.pdf.