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

About the CASCADE Program 4

Report Development 4

Executive Summary 5

Introduction 6

Methodology 7

Section I: Industry Overview 9

- Rise of Ransomware 10
- Cybersecurity Skills Shortage 10
- Economic Implications 12
- Cybersecurity Workforce Preparation 13

Section II: Employer Survey and Workforce Demand Assessment 14

- Surveyed Employer Characteristics 14
- Workforce Demand for Nine Work Roles 18
- Workforce Challenges 21
- Candidate Challenges 27
- Security Certifications 33
- Importance of Cybersecurity Skills for IT/IS Work Roles 36
- Time Spent on Security/Cybersecurity Issues 38
- Education, Work Experience and Soft Skills 43

Section III: Educational Supply Assessment 44

- Cybersecurity Programs Assessment 44
- Program Awards 49
- Additional Programs and High School Enrollment 51

TABLE OF CONTENTS

Section IV: Survey of Educational Providers 55

Educational Provider Characteristics 55

Program Development 56

Cybersecurity Certifications 58

Soft Skills 59

Employer Involvement 60

Cybersecurity Certifications 61

Section V: Conclusion 62

Training Gap Analysis 62

Summary of Findings and Recommendations 63

Resources for Educators 67

Appendix A: California Cybersecurity Labor Market Survey Methodology 70

Appendix B: California Cybersecurity Labor Market Survey 73

Appendix C: Cybersecurity Labor Market Analysis Research Advisory Group Members 82

Appendix D: Work Role Profiles 83

Appendix E: Inventory of Cybersecurity Programs 96

Appendix F: Program Awards in Cybersecurity 109

Appendix G: Cybersecurity-related CIP (Classification of Instructional Programs) Codes 115

Appendix H: Postsecondary Cybersecurity Programming in California 122

Appendix I: Articulations Between Secondary and Postsecondary Programs 132

Appendix J: Cybersecurity Courses at California Public High Schools 139

Appendix K: Cybersecurity Education Programs Survey 140

Appendix L: References Cited 144

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

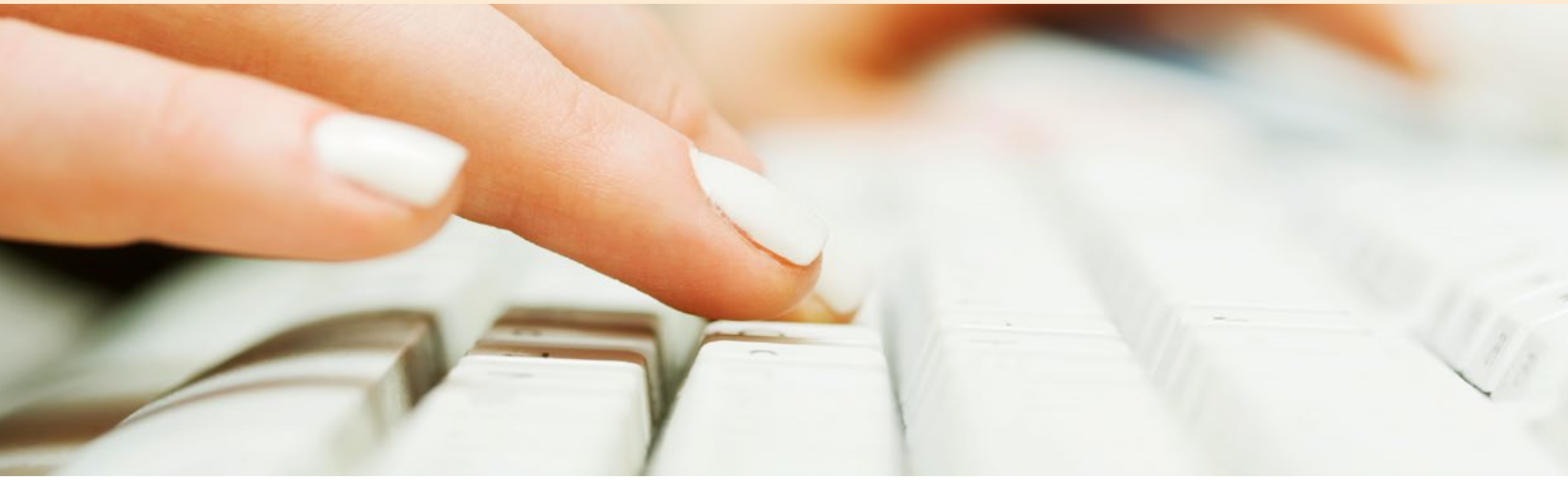
To address the statewide cybersecurity labor shortage, the California Community Colleges Centers of Excellence for Labor Market Research (COE) conducted a cybersecurity labor market analysis in 2018 as one of 15 CASCADE program activities. The study gathered information about workforce needs in California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

CYBERSECURITY SKILLS SHORTAGE

Cybersecurity Shortage by the Numbers

1.8 million jobs unfilled worldwide projected by **2022**

35,000 job openings in California, April 2017–March 2018

Cybersecurity job postings have **grown 3x** as fast as IT jobs

$75,000–$100,000 median cybersecurity salary

75% of organizations report understaffed security teams

There are typically not enough workers to fill cybersecurity job openings and these positions often take longer to fill than jobs in other industries.[19] In addition, the workforce gap is expected to worsen in coming years. The results from the 2017 Global Information Security Workforce Study (GISWS) by Frost & Sullivan estimates 1.8 million unfilled cybersecurity jobs globally by 2022, a 20% increase over the forecast made in 2015. The study found that two-thirds of businesses globally do not have enough cybersecurity workers in their organizations to meet the challenges they currently face.[20]

According to an article in Security Magazine, while security budgets are increasing, 59% of information security professionals report unfilled cyber/information security positions within their organizations.[21] As reported by Dark Reading, a separate study found that 75% of organizations report having understaffed security teams and experience difficulty in recruiting qualified job candidates; and nearly the same proportion report that AI and machine learning tools and services have exacerbated their staffing problems because more highly skilled workers are needed.[22]

A 2016 international report by McAfee and the Center for Strategic and International Studies found that the cybersecurity skills shortage does direct and measurable damage, according to 71% of respondents surveyed. According to the report, one in three respondents said a shortage of skills makes their organizations more desirable hacking targets, and one in four reported that "insufficient cybersecurity staff strength damaged their organization's reputation and led directly to the loss of proprietary data through cyberattack."[23]

Finding qualified workers to fill cybersecurity positions is a widespread challenge facing many employers across all industries.

[19] "Hack the Gap: Close the cybersecurity talent gap with interactive tools and data," CyberSeek, accessed May 18, 2018, https://www.cyberseek.org/index.html#about.

[20] "2017 Global Information Security Workforce Study," The Center for Cyber Safety and Education and Frost & Sullivan, 2017, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf.

[21] "Security Budgets Increasing, But Qualified Cybertalent Remains Hard to Find," Security Magazine, April 23, 2018, accessed May 18, 2017, https://www.securitymagazine.com/articles/88940-security-budgets-increasing-but-qualified-cybertalent-remains-hard-to-find.

[22] Erica Chickowski, "Automation exacerbates cybersecurity skills gap," Dark Reading, May 2, 2018, accessed May 18, 2018, https://www.darkreading.com/careers-and-people/automation-exacerbates-cybersecurity-skills-gap/d/d-id/1331697.

[23] "Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills," McAfee and the Center for Strategic and International Studies, 2016, accessed May 18, 2018, p. 4, https://www.mcafee.com/uk/resources/reports/rp-hacking-skills-shortage.pdf.

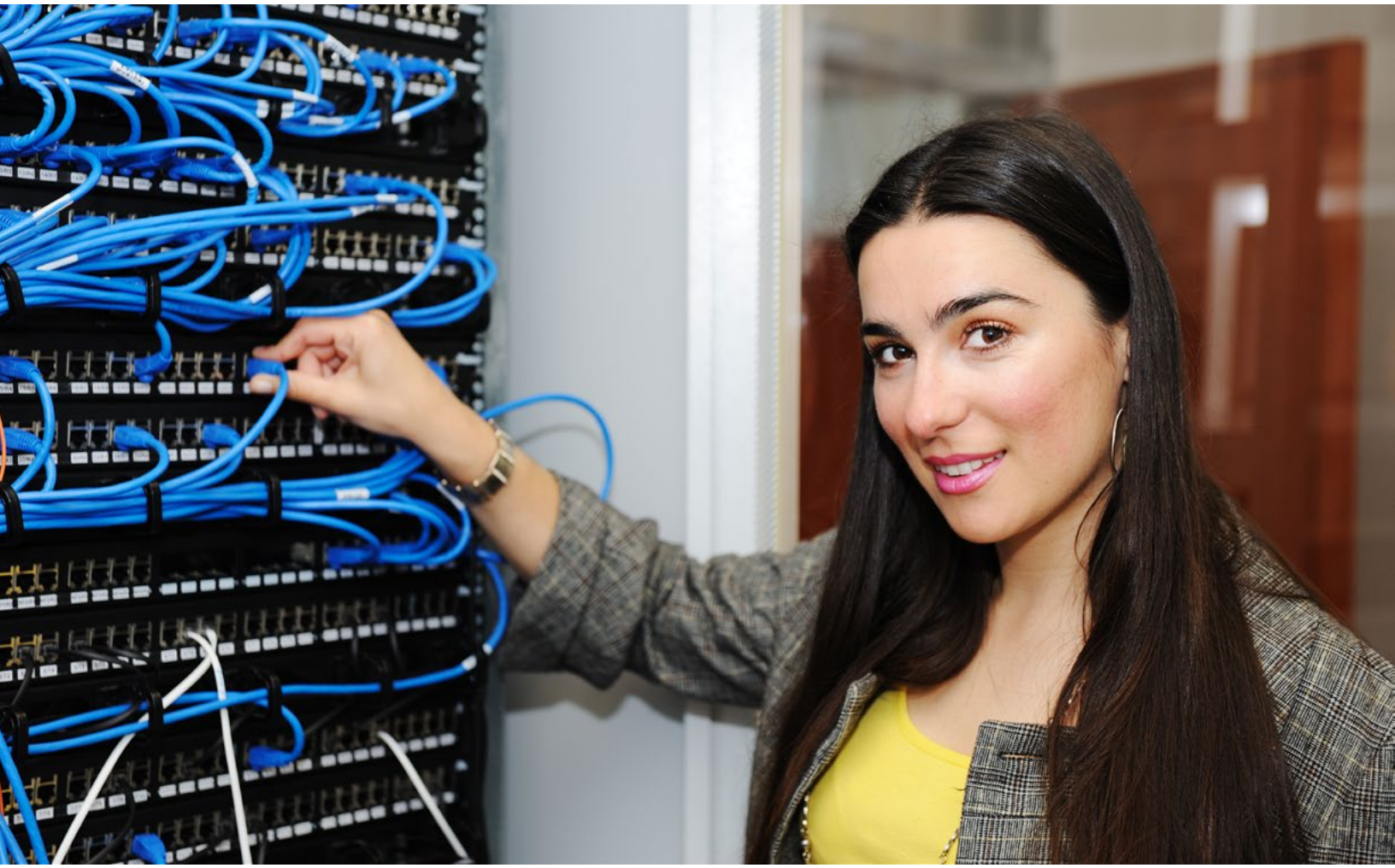
ECONOMIC IMPLICATIONS

According to a study by PwC, investors view cyber threats as the No. 1 threat to business, and think cybersecurity should be a top priority for building trust with customers.[24]

In addition, cyber threats to e-commerce are particularly a concern. Small businesses are big contributors to the economy, but many rely on e-commerce to generate revenue. Perhaps, most alarmingly, CNBC reported in July 2017 that roughly half of the 28 million small businesses in the United States had been breached by hackers, but only 2 percent of small-business owners surveyed viewed cyberattacks as their most critical issue.[25]

The magnitude of the international cybersecurity crisis was captured in this year's World Economic Forum's Global Risks Report. Cyber vulnerabilities ranked fourth in the list of the top five global risks. The soaring number of cyberattacks, particularly those resulting from WannaCry, as well as the number of businesses and institutions affected worldwide and the extreme cost of these attacks contributed to the ranking.

Most significantly, the larger implication of these attacks catapulted cyber vulnerabilities to the top of the list of world risks due the "growing trend of using cyberattacks to target critical infrastructures and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning."[26]



[24] "2018 Global Investor Survey: Anxious Optimism in a Complex World," PwC International Limited, p. 11 and p. 22, https://www.pwc.com/gx/en/ceo-survey/2018/deep-dives/pwc-global-investor-survey-2018.pdf.

[25] Chris Morris, "14 million businesses are at risk of a hacker threat," CNBC, July 25, 2017, accessed May 18, 2018, https://www.cnbc.com/2017/07/25/14-million-us-businesses-are-at-risk-of-a-hacker-threat.html.

[26] Ibid.

CYBERSECURITY WORKFORCE PREPARATION

Because the field of cybersecurity is new and still evolving, there is no standard curriculum nor consensus on standards for training. Cybersecurity studies and training can be included in basic computer courses, and can include specific training in topics such as computer and digital forensics, system vulnerability/penetration testing, system hardening, instruction detection and prevention, reverse malware engineering, and more.

In February 2013, then President Obama signed an executive order calling for a national set of standards, guidelines and practices to help organizations better protect themselves against cyber-attack, and the NICE Framework was developed. Other alternative frameworks are accepted in the field, and there is no consensus or standardization on what constitutes the canon of cybersecurity curriculum or training.

As there is no standardized cybersecurity curriculum, there is also no standard way for a cybersecurity professional to demonstrate qualifications. Various routes include: degrees and certificates issued by postsecondary institutions; industry certifications issued by vendors (e.g., CISCO, CompTIA, Oracle, Juniper/Junos); and other association/organization/governmental/quasi-governmental sponsored licenses, certifications and credentials. In addition, individuals who win cybersecurity contests are generally considered qualified for employment in the field.

The range in cybersecurity training is vast, from short-term, skills-based credentials to research doctoral degrees and postgraduate certifications. However, industry certifications may have become the de facto standardized measure of cybersecurity skills and competencies as there is no standardized curriculum nor standardized academic credentials. Although there is standardization within industry certification by individual security vendors, there is a lack of standardization across security vendors.

As there is no standardized cybersecurity curriculum, there is also no standard way for a cybersecurity professional to demonstrate qualifications.

According to a study by PwC, **investors view cyber threats as the No. 1 threat to business,** and think cybersecurity should be a top priority for building trust with customers.

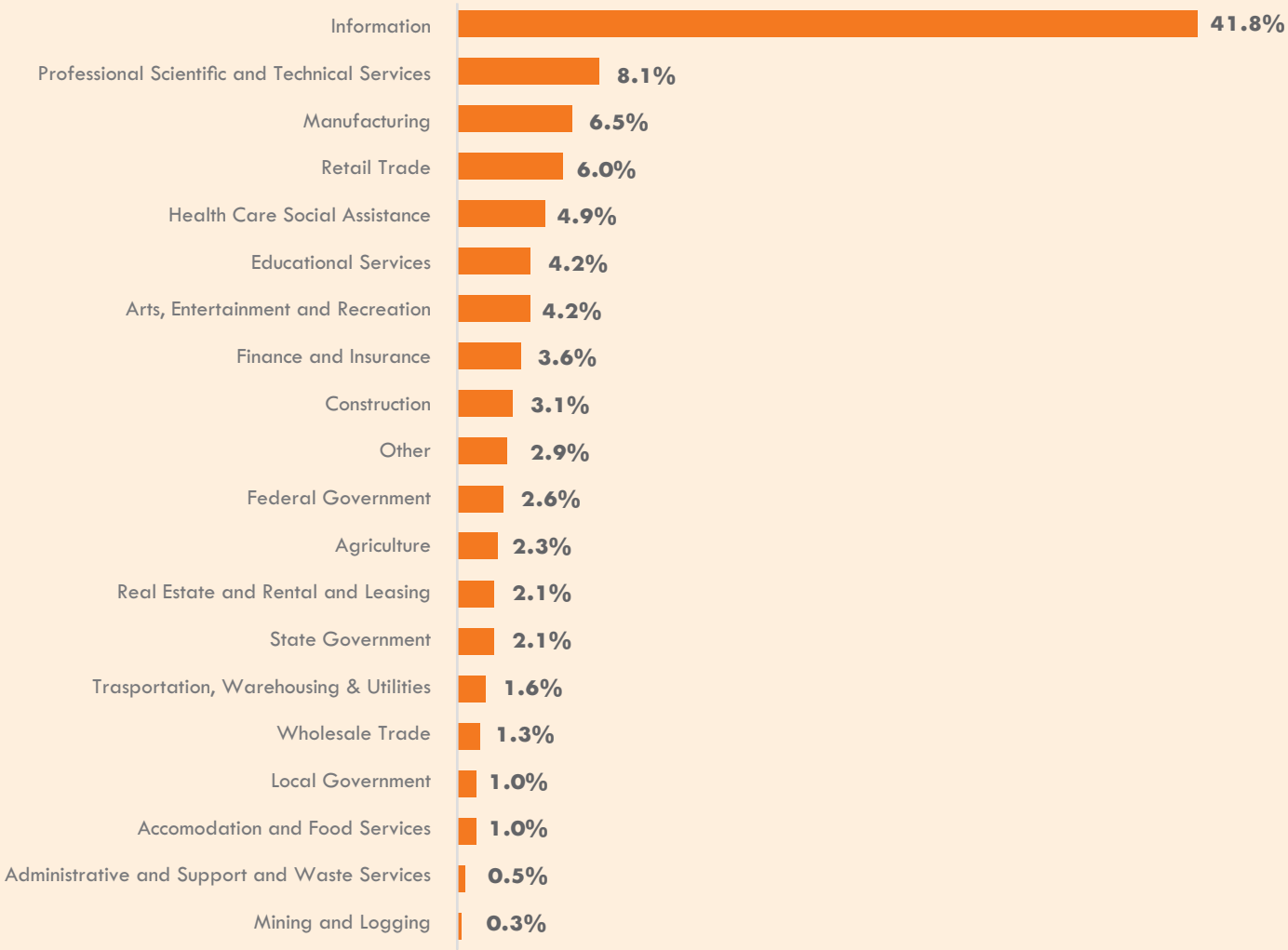
SECTION II: EMPLOYER SURVEY AND WORKFORCE DEMAND ASSESSMENT

SURVEYED EMPLOYER CHARACTERISTICS

Employer survey participants either employ cybersecurity workers or Information Technology/Information Systems (IT/IS) workers who require cybersecurity skills. Overall, there were 385 survey respondents. These survey participants were asked to identify the industry with which their business is most closely associated. About 42% of employers were associated with the information industry (Exhibit 1).

The information industry sector is composed of multiple sub-industries that include information technology, information systems, ISP providers, software publishers, telecommunications and data hosting businesses, all of which have high concentrations of IT/IS workers according to industry staffing patterns.

Exhibit 1. Industries associated with surveyed businesses (n-385)



SURVEYED EMPLOYER CHARACTERISTICS

Exhibit 2 shows the size of the 385 businesses surveyed, based on the number of permanent employees. Nearly 40% of respondents have fewer than 50 employees, while 21% of respondents have 1,000 employees or more, which is consistent with the larger size of businesses found in the information sector.

Exhibit 2. Size of surveyed business by number of employees (n=385)

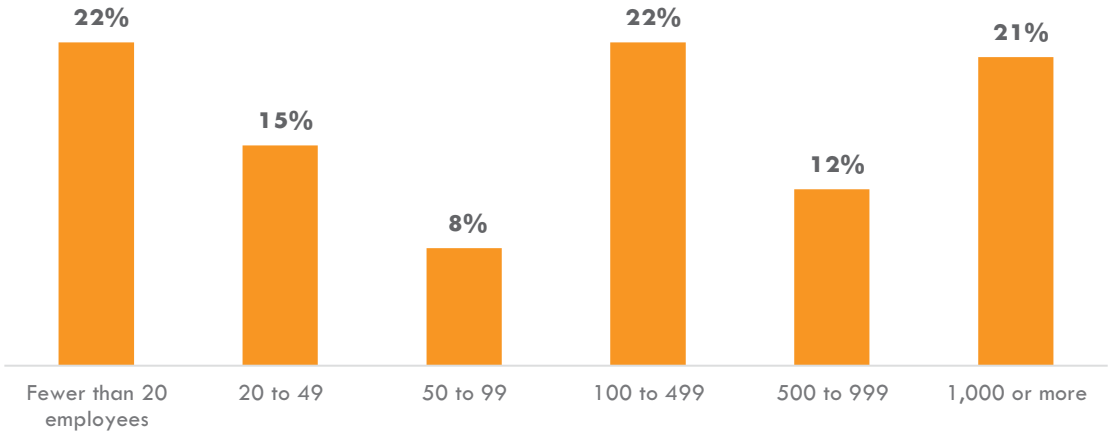
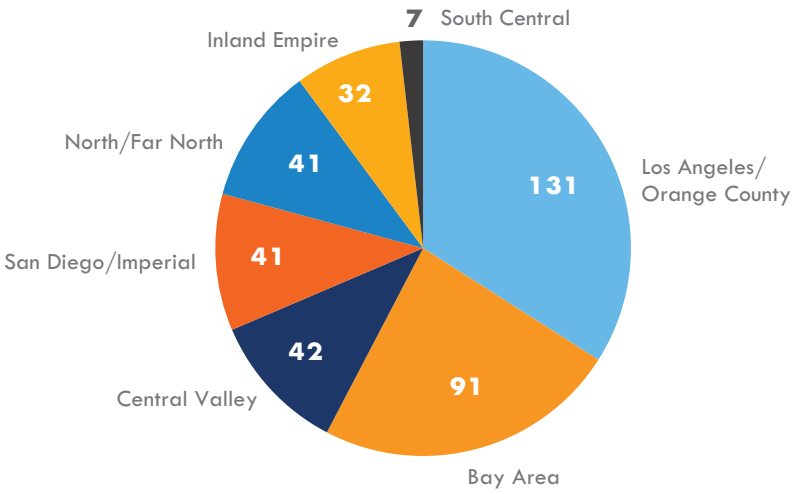


Exhibit 3 shows where the surveyed businesses are located by major geographic region in California. Of the businesses that participated in the survey, 34% were in Los Angeles and Orange counties, and 24% were in the Bay Area, which is consistent with these two regions having large concentrations of businesses that employ cybersecurity and IT/IS workers.

Exhibit 3. Surveyed businesses by region

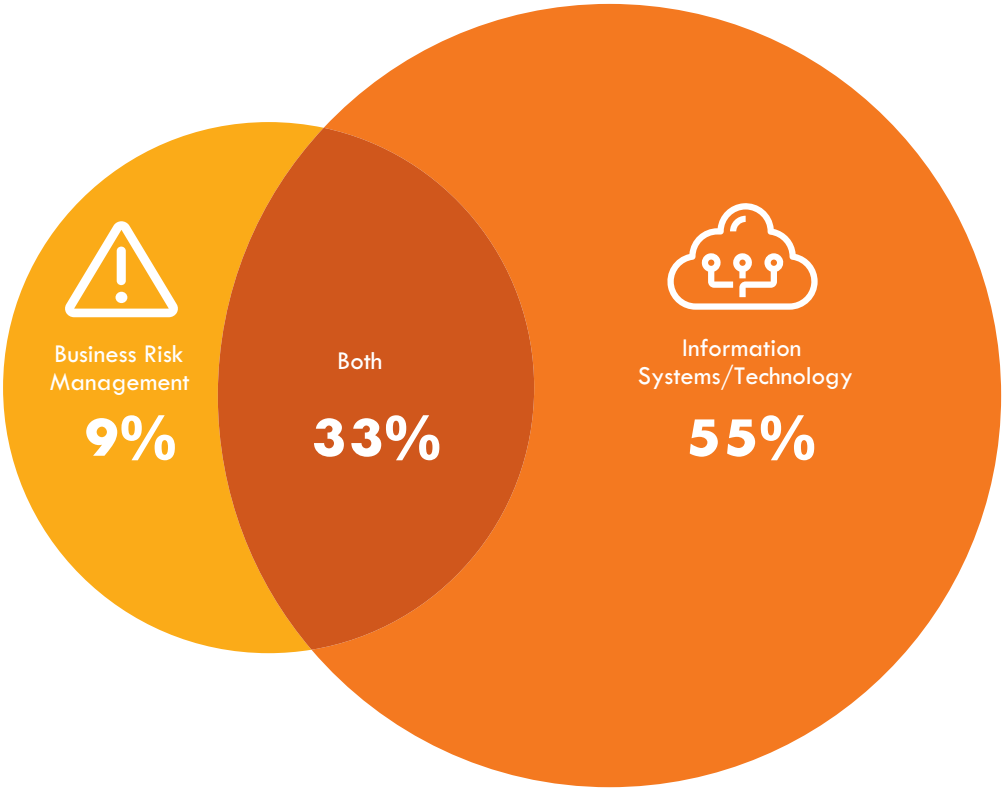


SURVEYED EMPLOYER CHARACTERISTICS

Respondents were asked if their business operates cybersecurity as an information systems or technology function, a business risk management function or both.

As shown in Exhibit 4, 55% of the businesses surveyed indicated they focus on cybersecurity as an information systems/technology function. Just over 33% of businesses operate cybersecurity as both an information systems/technology function and a business risk management function. Only about 9% of businesses operate cybersecurity as a business risk management function.

Exhibit 4. Distribution of surveyed firms in business risk management, IT/IS, or both



There are increasing concerns about whether businesses are sufficiently integrating cybersecurity into all aspects of their operations. To better understand how businesses/organizations are involved with cybersecurity, respondents were asked to indicate if their business is a creator/producer of cybersecurity products; a provider of cybersecurity products and/or services; a user of cybersecurity products and services; or has some other involvement with cybersecurity.

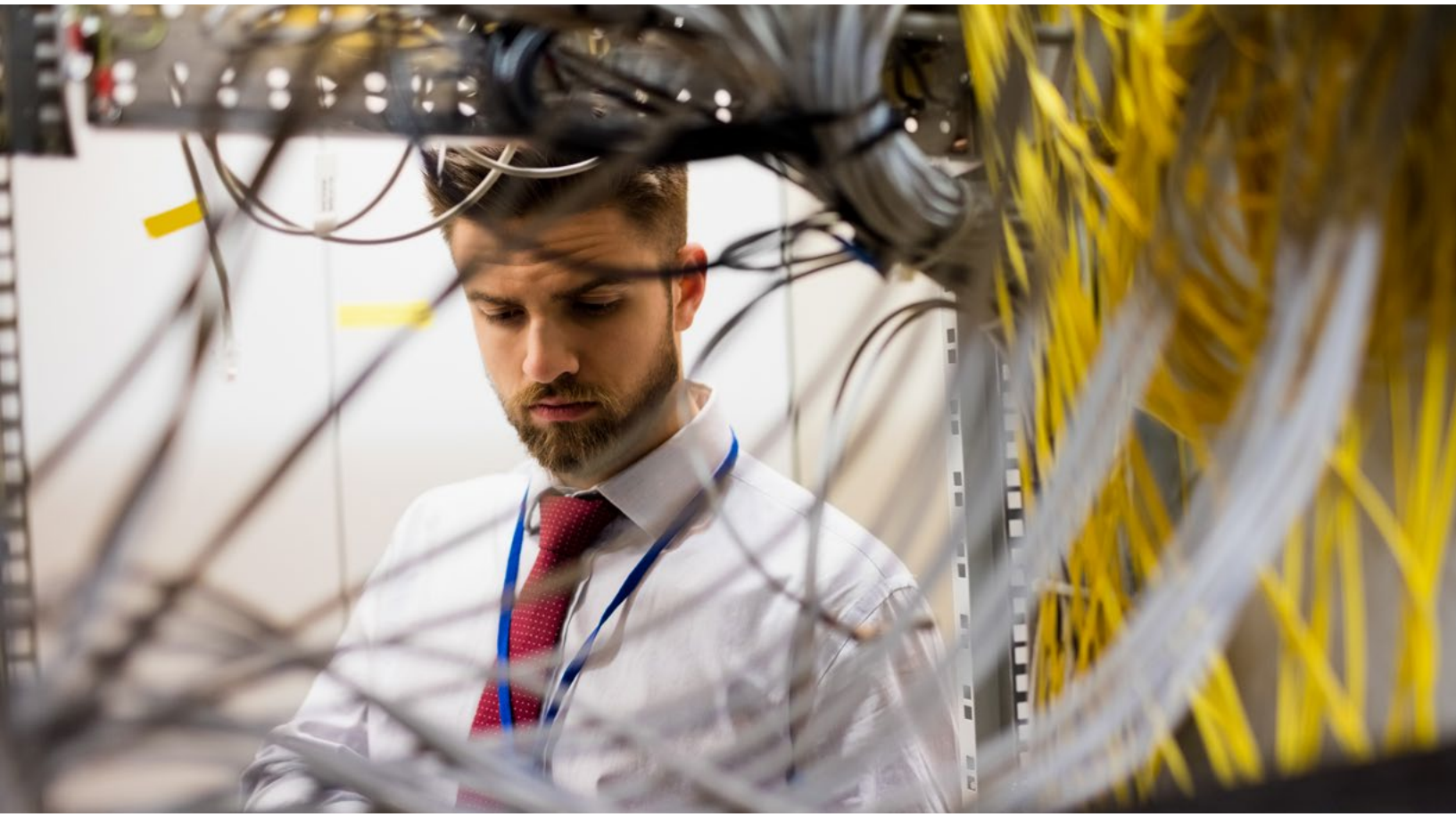
For this question, employers could choose more than one category, which resulted in a total of 530 responses for this question. As shown in Exhibit 5:

- 66% of respondents indicated they are a user of cybersecurity products and services.
- 43% of respondents indicated they are a provider of cybersecurity products and/or services (including management, testing, risk assessments and other services), and of this group 50% indicated that over half of their business focuses on this.
- 26% indicated they are a creator/producer of cybersecurity products, and of this group 57% indicated that over half of their business focuses on this.

SURVEYED EMPLOYER CHARACTERISTICS

To fulfill an important objective of this study, respondents were asked if their business is a defense contractor (including first, second, third, or fourth tier subcontractor) and 49% of businesses indicated they are a defense contractor. (Data for this sub-group of respondents is included in the next section of the report.) In addition, 43% of respondents indicated their business provides cybersecurity products and/or services to the defense industry (Exhibit 5).

Exhibit 5. How surveyed businesses are involved in cybersecurity (n=385)



WORKFORCE DEMAND FOR NINE WORK ROLES

Specialized Cybersecurity Work Roles

- Systems Security Analyst
- Cyber Defense Analyst
- Cyber Defense Infrastructure Support Specialist
- Vulnerability Assessment Analyst
- Cyber Defense Forensics Analyst

IT/IS Work Roles Requiring Cybersecurity Skills

- Technical Support Specialist
- Network Operations Specialist
- System Administrator
- Software Developer

This section of the report provides survey findings for the nine cybersecurity work roles selected for this study. The work roles include five specialized cybersecurity positions and four IT/IS positions that require cybersecurity skills.

Employers answered a series of questions about the nine work roles, providing information about a number of workforce-related issues and challenges.

Employers completed the survey for the work roles they employ at their business and for no more than three work roles, which kept the survey to a reasonable length of time. (Appendix D: Work Role Profiles contains detailed survey results for each work role.)

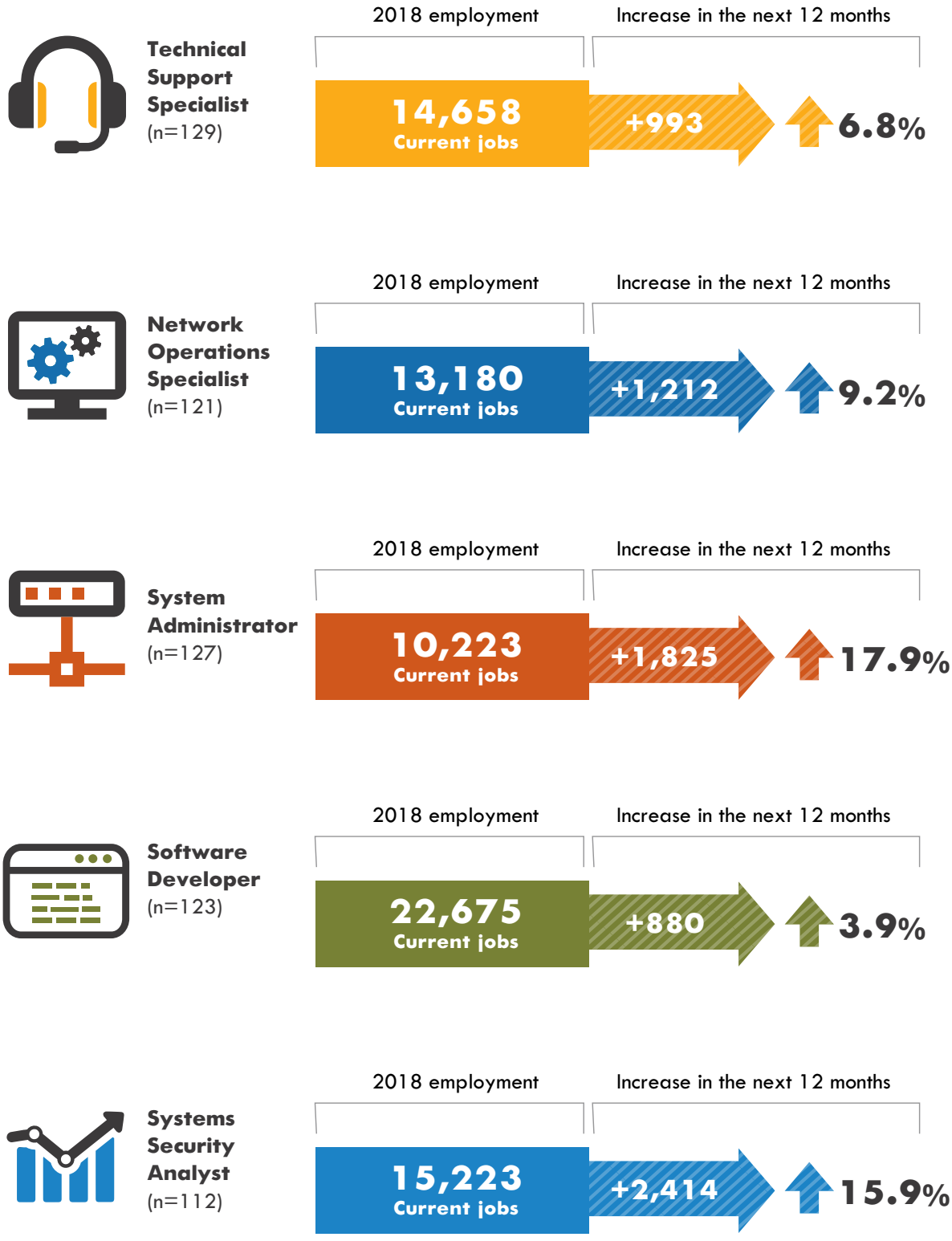
Exhibit 6 shows the current levels of combined permanent and temporary employment and the projected increase in permanent and temporary employment in 12 months, for each of the nine work roles. Notable findings include:

- **Software developer** is the largest work role, with current permanent and temporary employment totaling 22,675 positions.
- **Cyber defense forensic analyst** is the second largest work role with 21,293 positions.
- **System security analyst** is the work role projected to increase employment by the largest amount over the next 12 months, with an increase of 2,414 positions.
- **Cyber defense forensic analyst** is projected to have the second largest increase in the next 12 months, with 2,336 positions.
- **Cyber defense infrastructure support analyst** will have the largest percentage increase in permanent and temporary employment in 12 months, growing by 21.3% and adding 2,146 positions.
- **Systems administrator** is projected to increase employment by 17.9% in 12 months, adding 1,825 positions.

Across the nine work roles, when comparing defense contractors as a sub-group of all employers surveyed, the percentage increase in employment in 12 months is slightly higher. The range is 1% to 2% higher, depending on the work role.

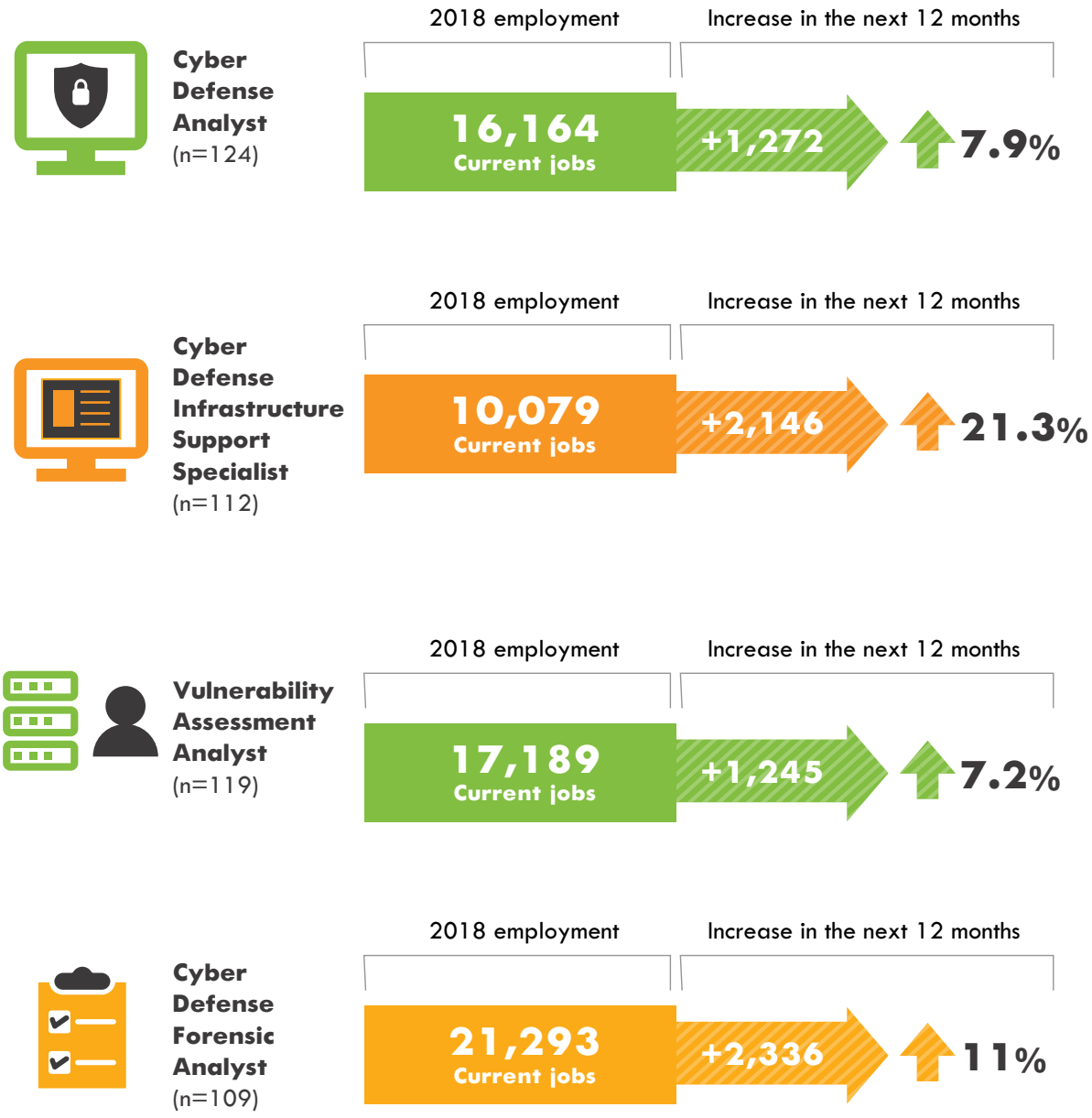
WORKFORCE DEMAND FOR NINE WORK ROLES

Exhibit 6. Current employment and projected occupational demand in 12 months for the nine work roles identified



WORKFORCE DEMAND FOR NINE WORK ROLES

Exhibit 6. Current employment and projected occupational demand in 12 months for the nine work roles identified (continued)



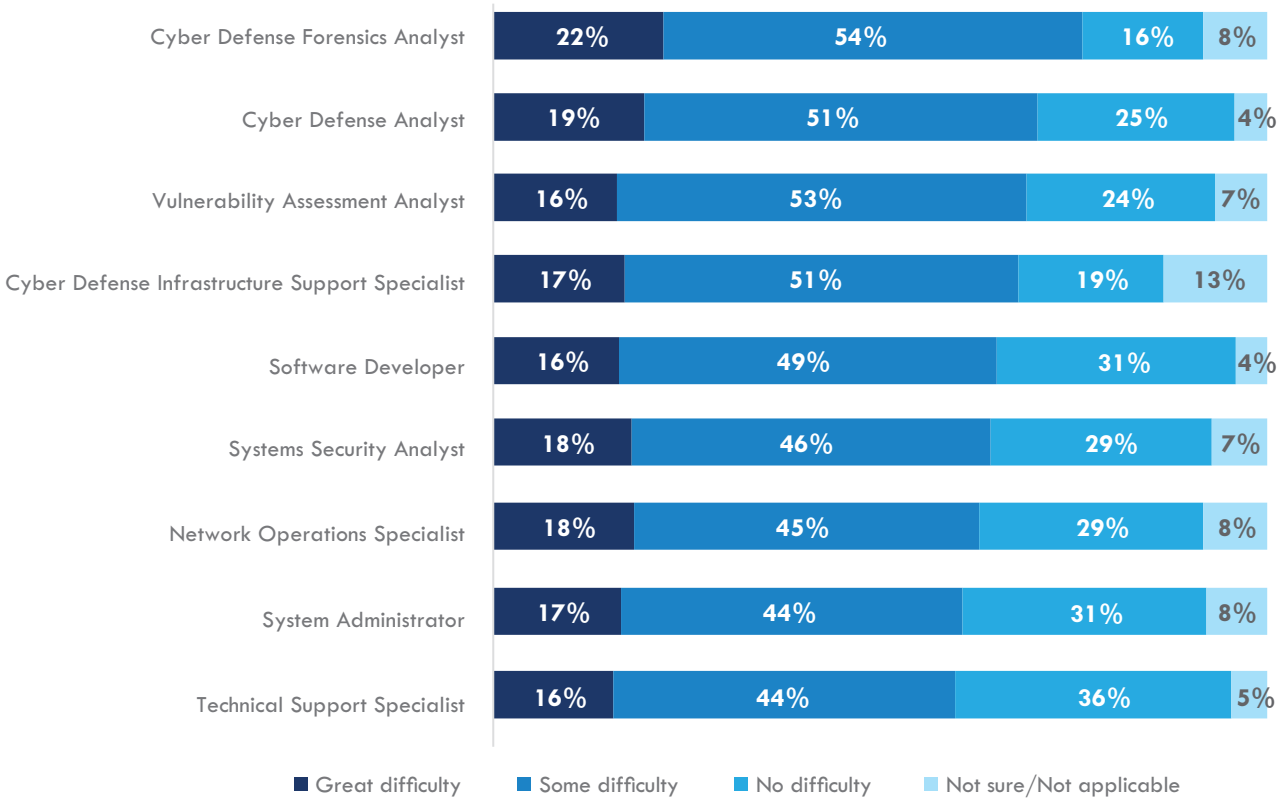
WORKFORCE CHALLENGES

Exhibit 7 displays the level of difficulty reported by employers in finding qualified cybersecurity workers in California. 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 finding the cybersecurity workers they need.

Employers were asked about their difficulty hiring for specific work roles. Work roles with the greatest difficulty include:

- Cyber Defense Forensic Analysts—76% of employers reported some or great difficulty.
- Cyber Defense Analysts—70% of employers reported some or great difficulty.
- Vulnerability Assessment Analysts—69% of employers reported some or great difficulty.
- Cyber Defense Infrastructure Support Specialists—68% of employers reported some or great difficulty.

Exhibit 7. Percentage of employers reporting difficulty hiring for the nine identified work roles



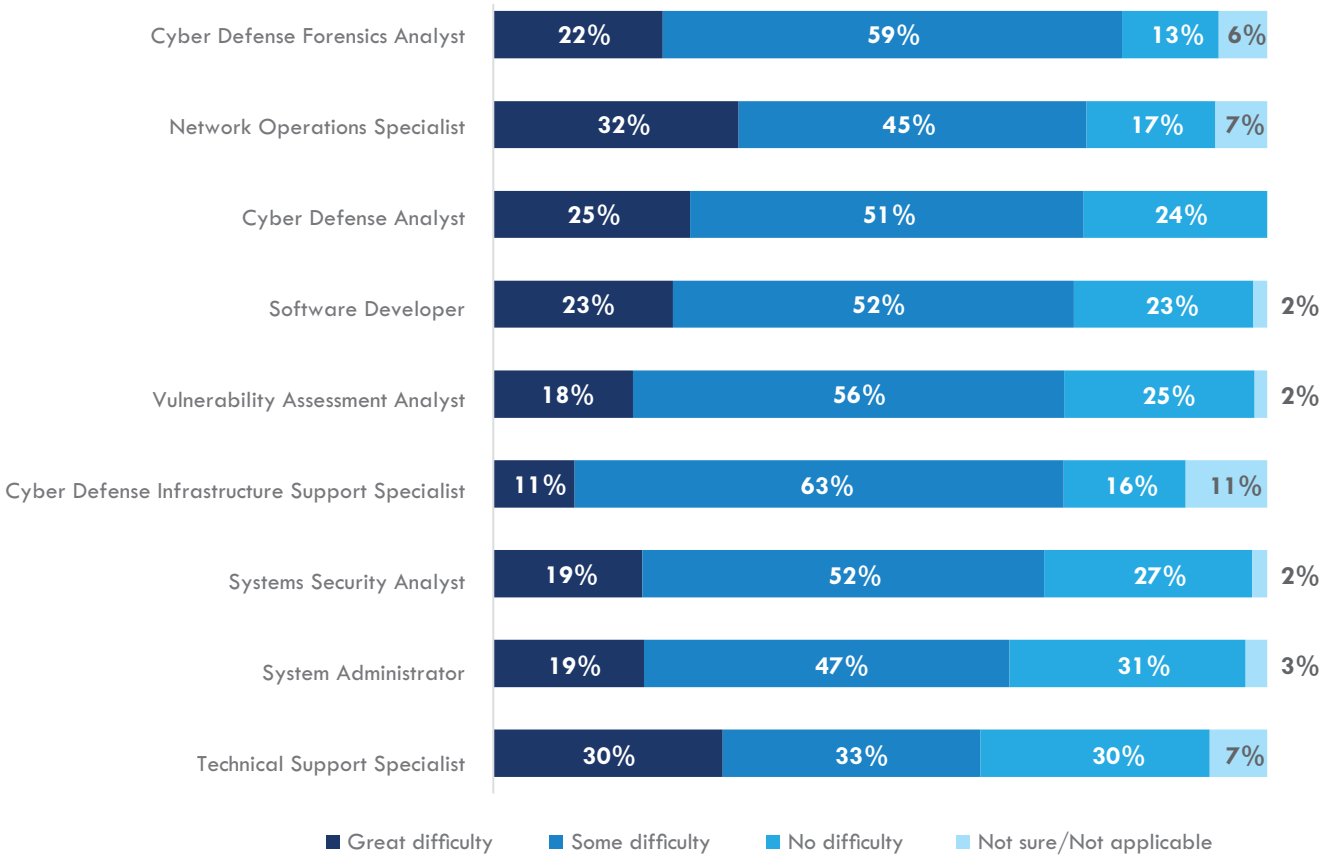
The percentage of defense contractors experiencing difficulty finding qualified candidates across the nine work roles is higher compared to all surveyed employers (Exhibit 8). The number of defense contractors who responded to this question ranges from 52 to 72 depending on the work role.

Work roles with the greatest difficulty reported by defense contractors include:

- Cyber Defense Forensics Analysts—81% of defense contractors reported some or great difficulty.
- Network Operations Specialists—77% of defense contractors reported some or great difficulty.
- Cyber Defense Analysts—76% of defense contractors reported some or great difficulty.
- Software Developers—75% of defense contractors reported some or great difficulty.

WORKFORCE CHALLENGES

Exhibit 8. Percentage of defense contractors reporting difficulty hiring for the nine identified work roles



For each work role, those employers who indicated they had some or great difficulty hiring qualified candidates, were asked how their business/organization responded to this workforce challenge. The number of employers who responded to this question ranged from 72 to 83, depending on the work role. Their responses are shown in the following subsections.

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.

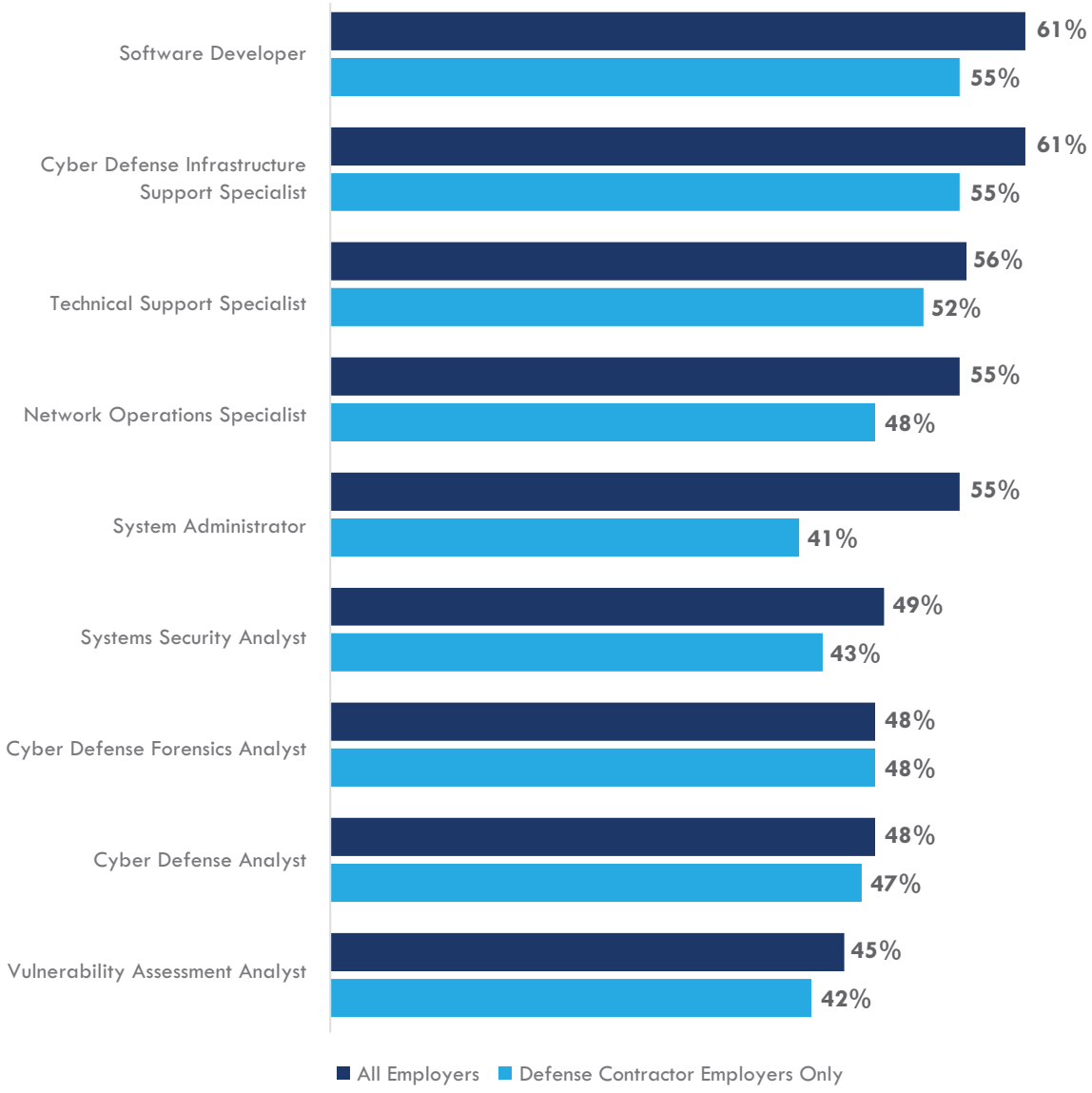
Defense contractors are also clearly using all three proactive strategies—increasing recruitment, increasing overtime with current employees, and increasing wages to attract candidates or retain current employees—to address their hiring challenges. The number of defense contractors who responded to this question ranged from 34 to 52, depending on the work role.

WORKFORCE CHALLENGES

Increased Recruitment

Increasing recruitment appears to be the preferred strategy used by employers (between 45% and 61% across all nine work roles) to address hiring challenges (Exhibit 9). Similarly, increasing recruitment efforts appears to be the most common strategy utilized by defense contractors across all nine work roles (between 41% and 55%) to address hiring challenges.

Exhibit 9. Increased recruitment effort, all employers and defense contractors

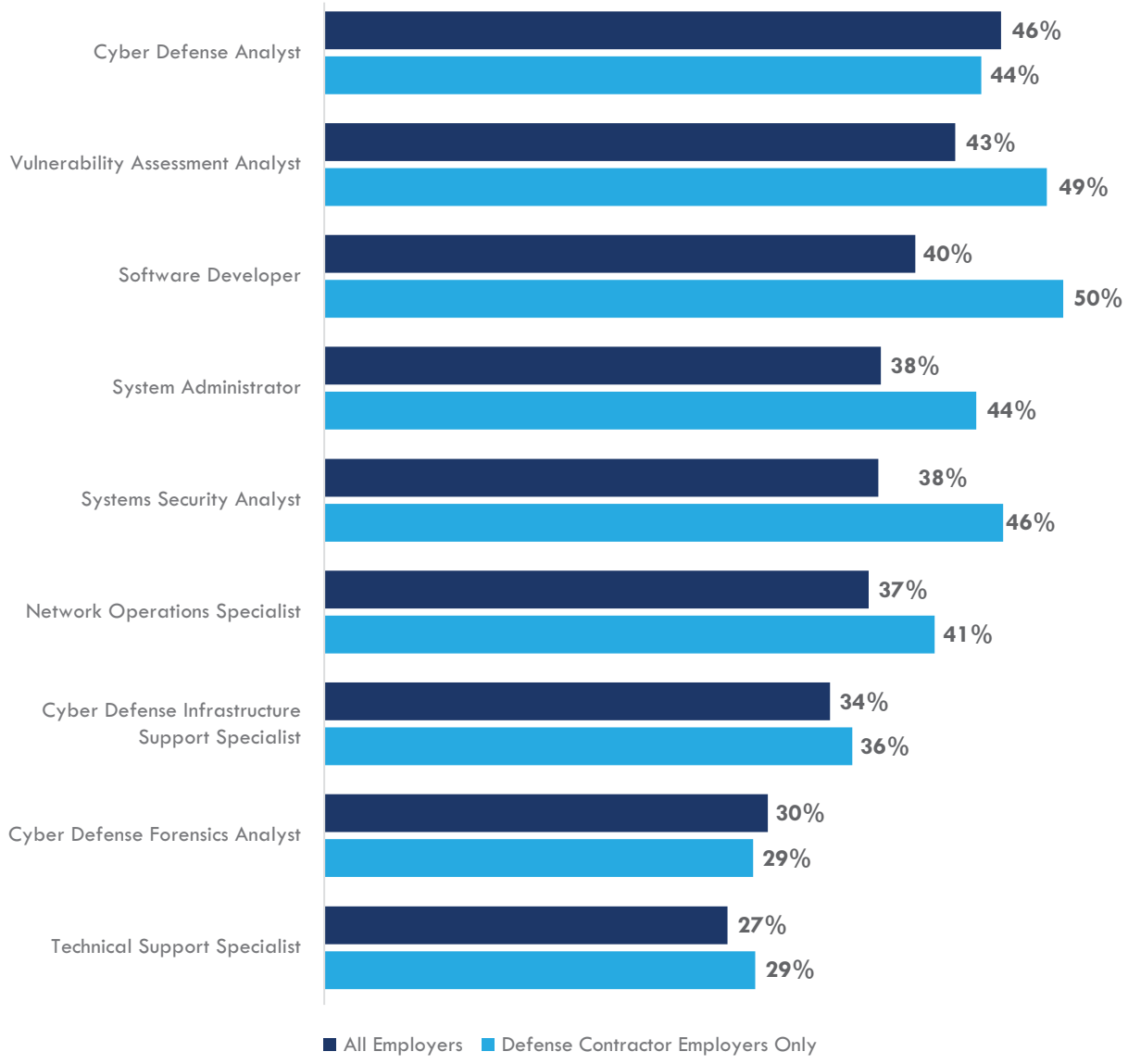


WORKFORCE CHALLENGES

Increased Wages

Increasing wages to attract candidates or retain current employees is used by employers and defense contractors as a retention strategy more for some work roles than others (Exhibit 10). For example, this strategy is not commonly used for cyber defense forensics analysts or technical support specialists. For seven of the nine work roles, defense contractors are utilizing this strategy more than employers in the overall sample.

Exhibit 10. Increased wages to attract candidates or retain current employees, all employers and defense contractors

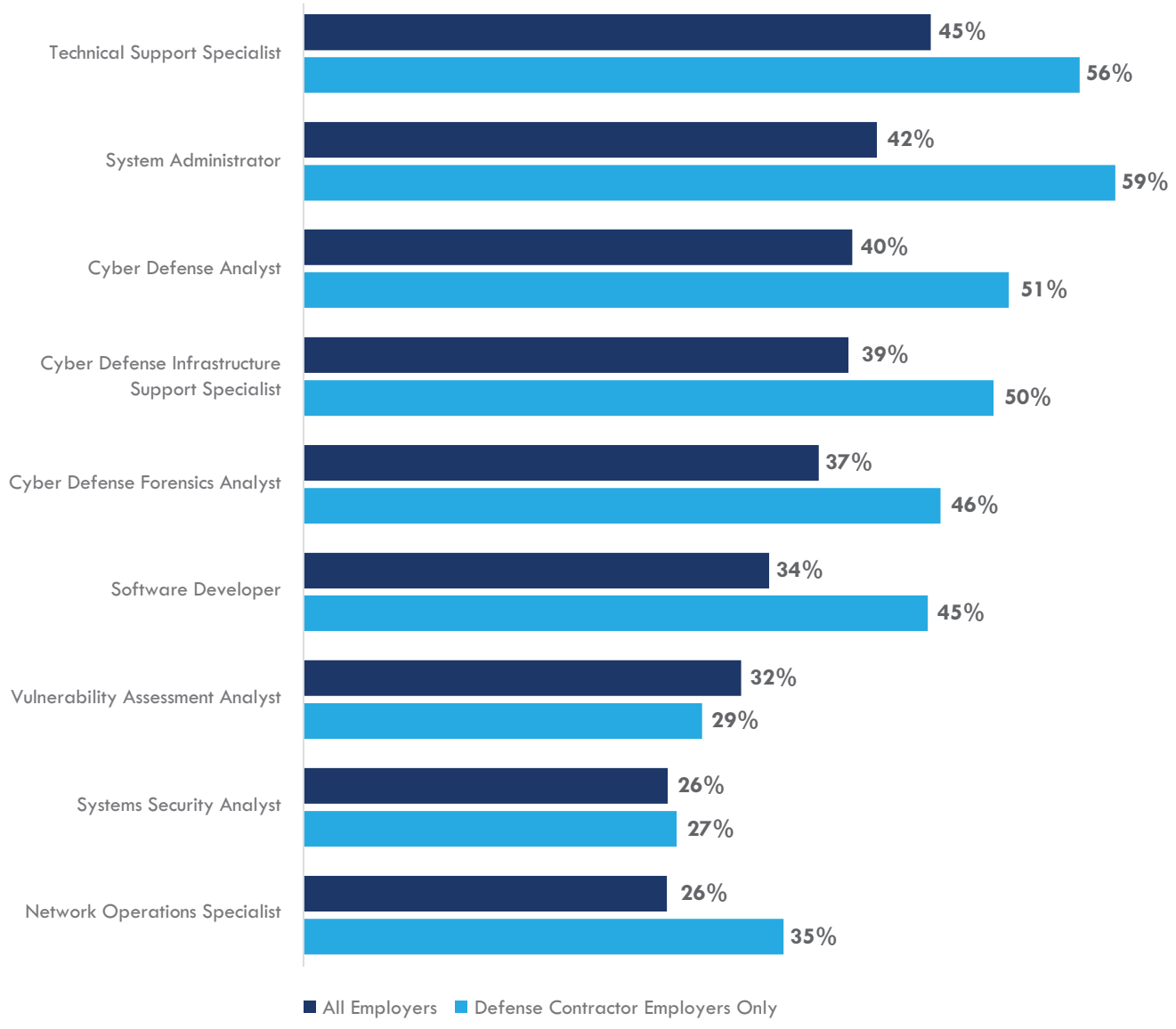


WORKFORCE CHALLENGES

Increased Overtime

As a strategy employers are using when facing hiring challenges, increased overtime for current employees to accommodate workload is roughly comparable to increased wages. Of all the work roles analyzed, increased overtime is more commonly used for technical support specialists and system administrators by employers and defense contractors (Exhibit 11). For eight of the nine work roles, defense contractors are utilizing this strategy more than employers in the overall sample.

Exhibit 11. Increased overtime for current employees to accommodate workload, all employers and defense contractors

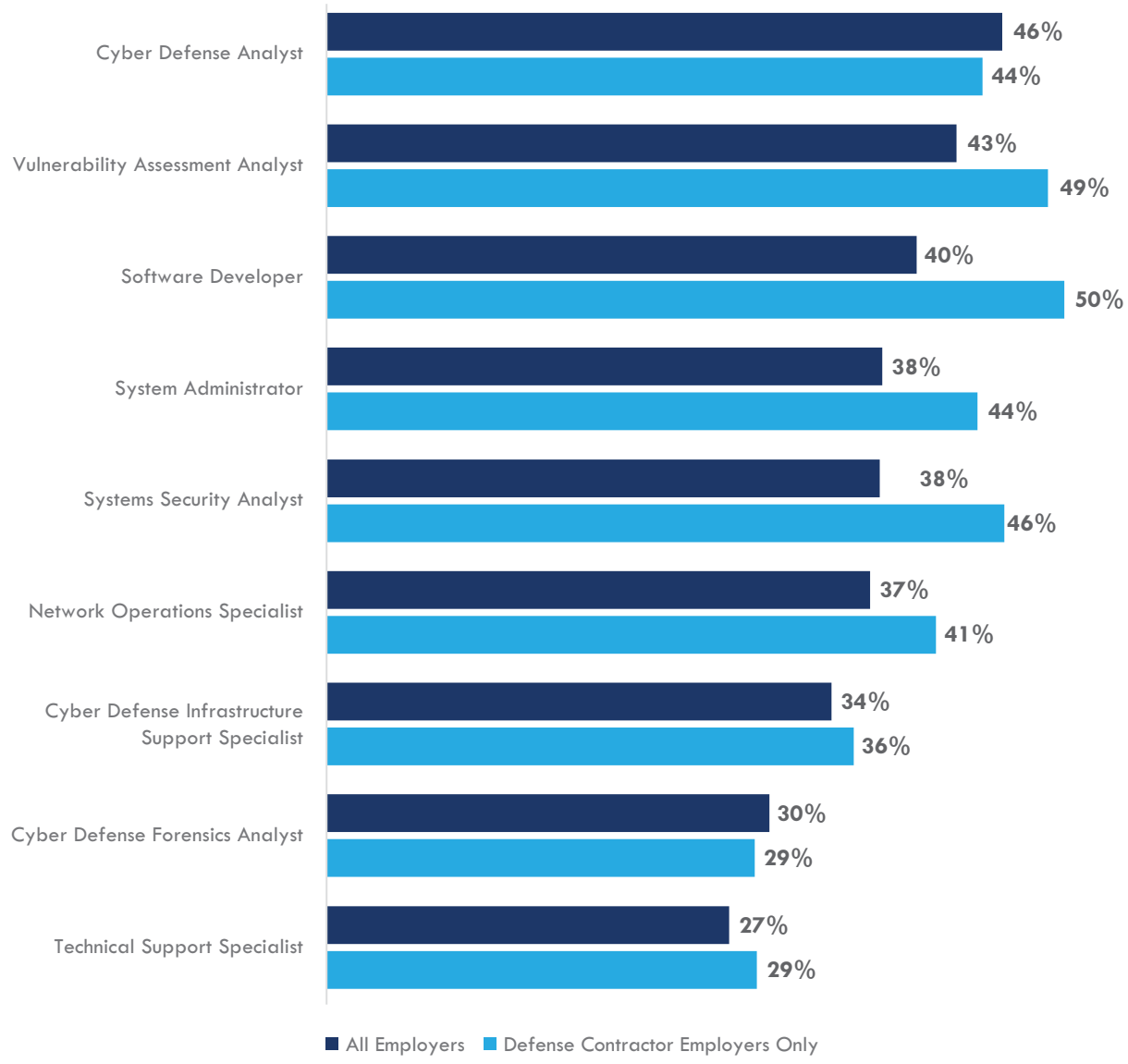


WORKFORCE CHALLENGES

Unfilled Positions

It is important to note that between 11% and 20% of employers, depending on the work role, indicated they did not fill the position when they could not find qualified candidates (Exhibit 12). Similar to all employers surveyed, between 12% and 19% of defense contractors (depending on the work role) are also not filling positions, when facing hiring challenges. This is a troubling sign regarding the shortage of cybersecurity workers in the labor market.

Exhibit 12. Positions left unfilled, all employers and defense contractors



CANDIDATE CHALLENGES

Five key issues or challenges were explored to better understand the range of workforce challenges employers face in finding qualified cybersecurity workers. The number of employers who responded to this question ranged from 72 to 83, depending on the work role.

Employers were asked if their business/organization was experiencing any of the following issues or challenges. They could select more than one option for the work role for which they were answering:

- Lack of qualified candidates with necessary security clearances,
- Candidates lack required educational attainment,
- Candidates lack relevant work experience,
- Candidates lack required technology skills, or
- Lack of qualified candidates in general.

On average, across all nine work roles, the top three issues or challenges businesses are facing related to hiring are:

1. Lack of qualified candidates in general,
2. Lack of relevant work experience, and
3. Lack of required technology skills.

The top work roles that **lack qualified candidates in general** are software developer (48%), vulnerability assessment analyst (43%), cyber defense analyst (42%), and system administrator (42%).

The top work roles for which **candidates lack relevant work experience** are cyber defense infrastructure support specialist(46%), technical support specialist (45%), and systems security analyst (42%).

The top work roles for which **candidates lack the required technology skills** are cyber defense infrastructure support analyst (49%), software developer (48%), and network operations specialist (41%).

This information was also collected from the defense contractors subgroup and the findings are displayed alongside the findings for all employers in Exhibits 13-17. The number of defense contractors who responded to this question ranged from 34 to 52, depending on the work role.

On average, across all nine work roles, the top three issues or challenges that defense contractors face when hiring are:

1. Candidates lack required technology skills,
2. Lack of qualified candidates with necessary security clearances, and
3. Lack of qualified candidates in general.

The top work roles for which **candidates lack the required technology skills** are cyber defense infrastructure support specialist (57%), software developer (45%), and network operations specialist (41%).

The top work roles that lack qualified candidates with the necessary security clearances are cyber defense infrastructure support specialist (52%), systems security analyst (49%), and software developer (40%).

The top work roles that lack qualified candidates in general are software developer (50%), system administrator (44%), and technical support specialist (44%).

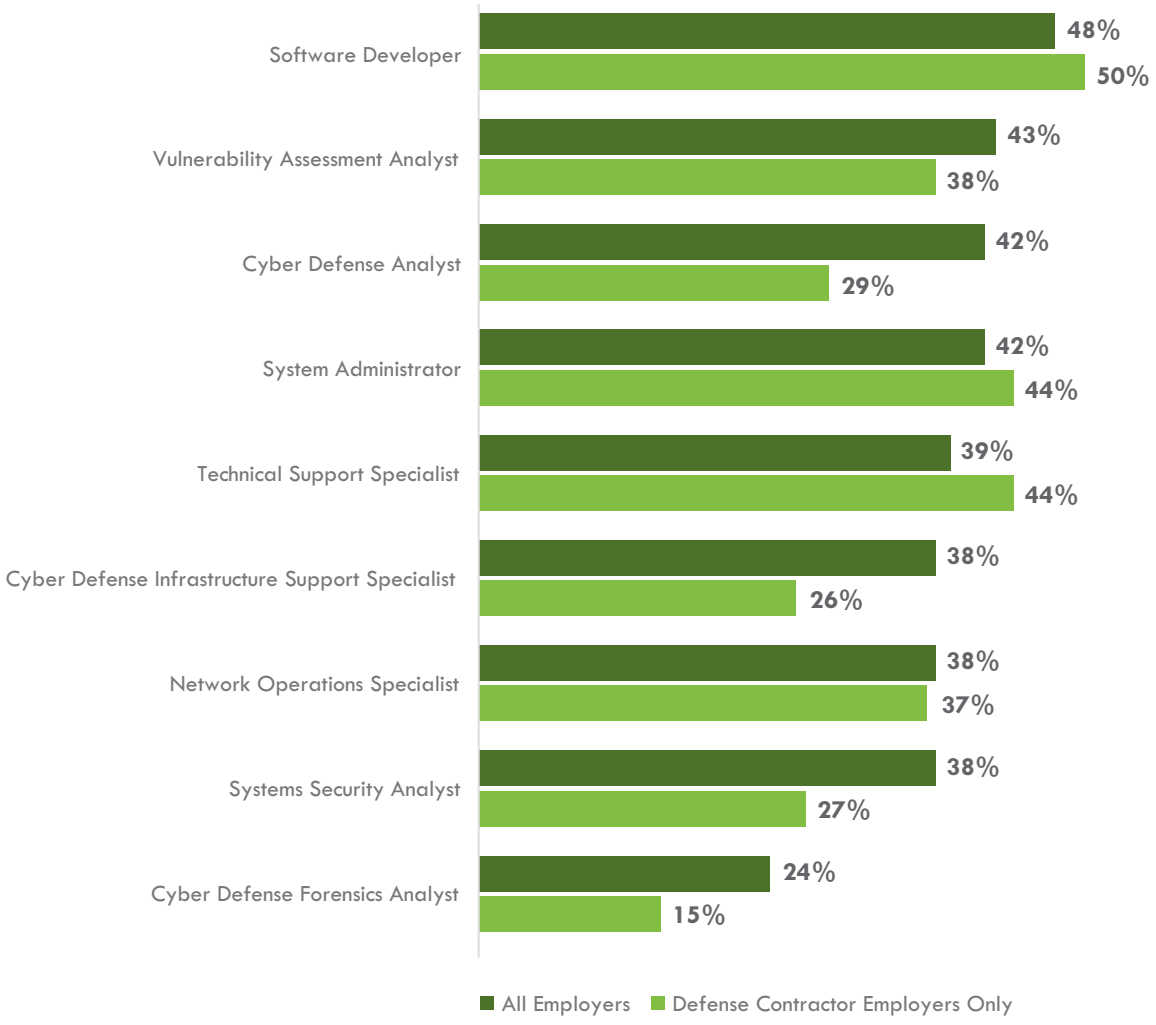
CANDIDATE CHALLENGES

Responses for two other issues or challenges also were collected from all employers and the defense contractors subgroup: "lack of qualified candidates with necessary security clearances" and "candidates lack required educational attainment" for all nine work roles. These responses are analyzed further in the following charts.

Lack of Qualified Candidates

Software developer was the top work role with a lack of qualified candidates reported by all employers and defense contractors (Exhibit 13). Employers in the overall sample also report a lack of vulnerability assessment analysts, while defense contractors report a lack of system administrators.

Exhibit 13. Lack of qualified candidates in general, all employers and defense contractors

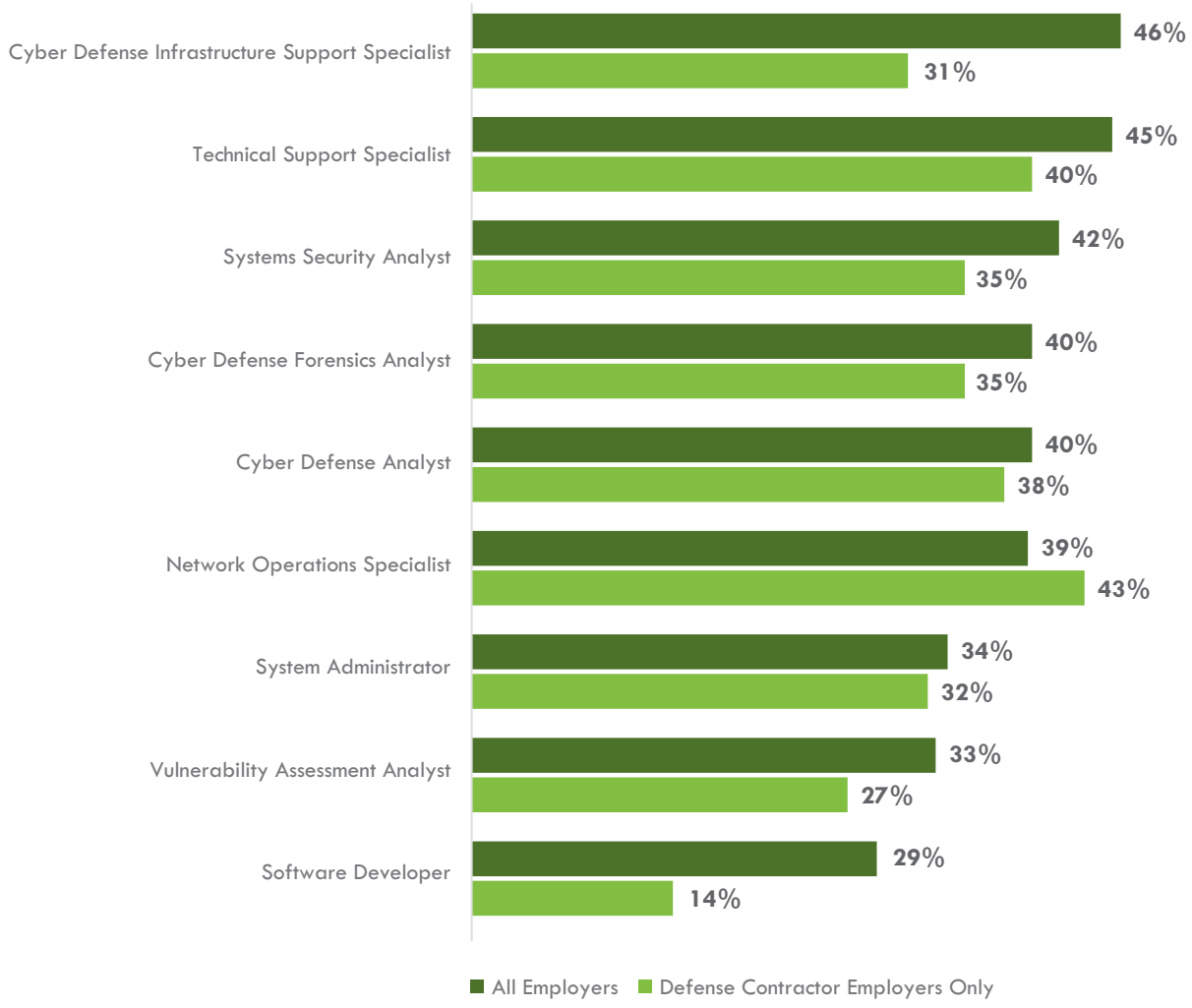


CANDIDATE CHALLENGES

Lack of Work Experience

The work roles for which job candidates lacked relevant work experience varied between all employers and defense contractors (Exhibit 14). All employers reported the top work role was cyber defense infrastructure support specialist, while defense contractors reported network operations specialist.

Exhibit 14. Lack of relevant work experience, all employers and defense contractors

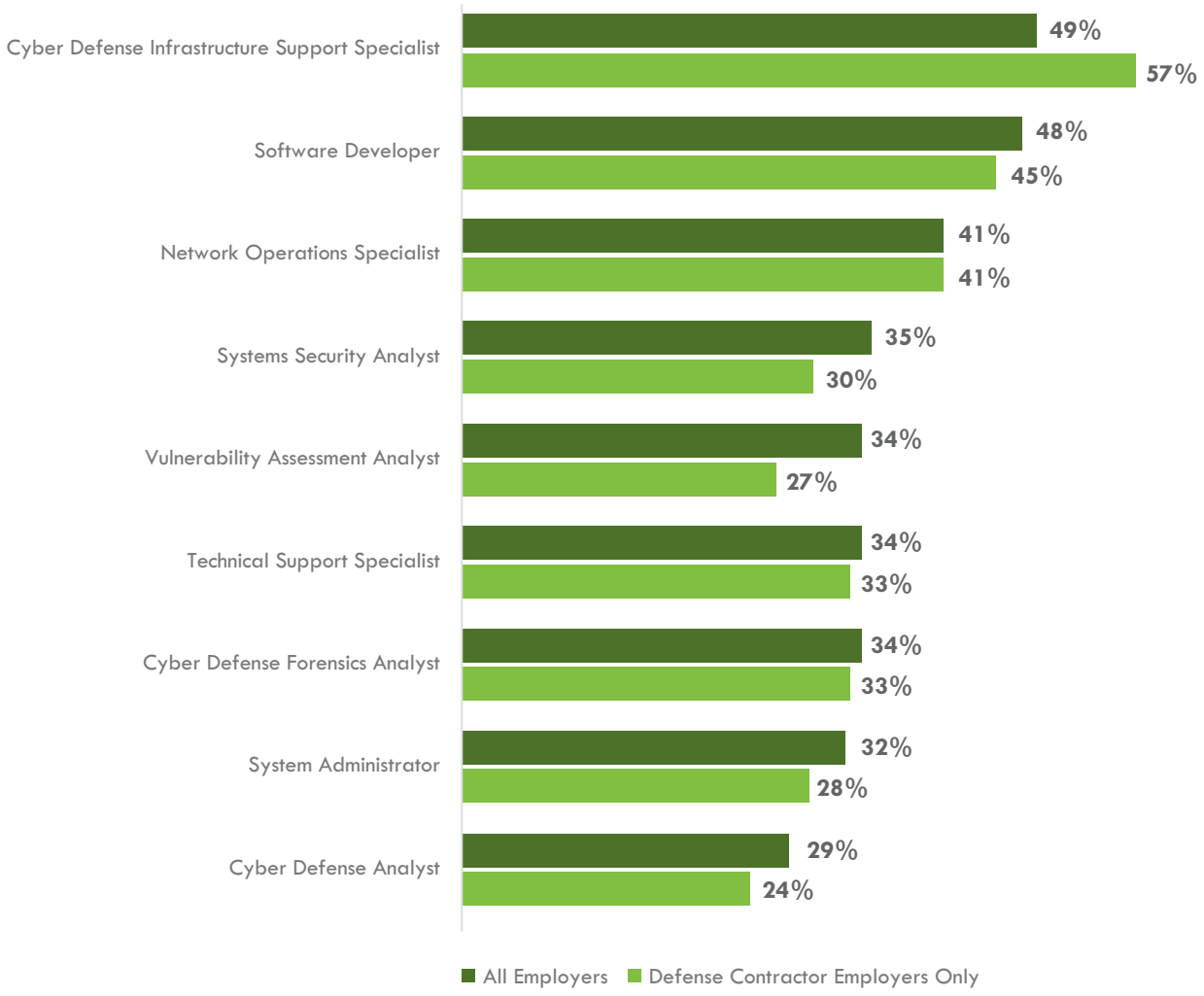


CANDIDATE CHALLENGES

Lack of Technology Skills

The top three work roles for which job candidates lack required technology skills are the same for all employers and defense contractors: cyber defense infrastructure support specialist, software developer and network operations specialist (Exhibit 15).

Exhibit 15. Lack of required technology skills, all employers and defense contractors



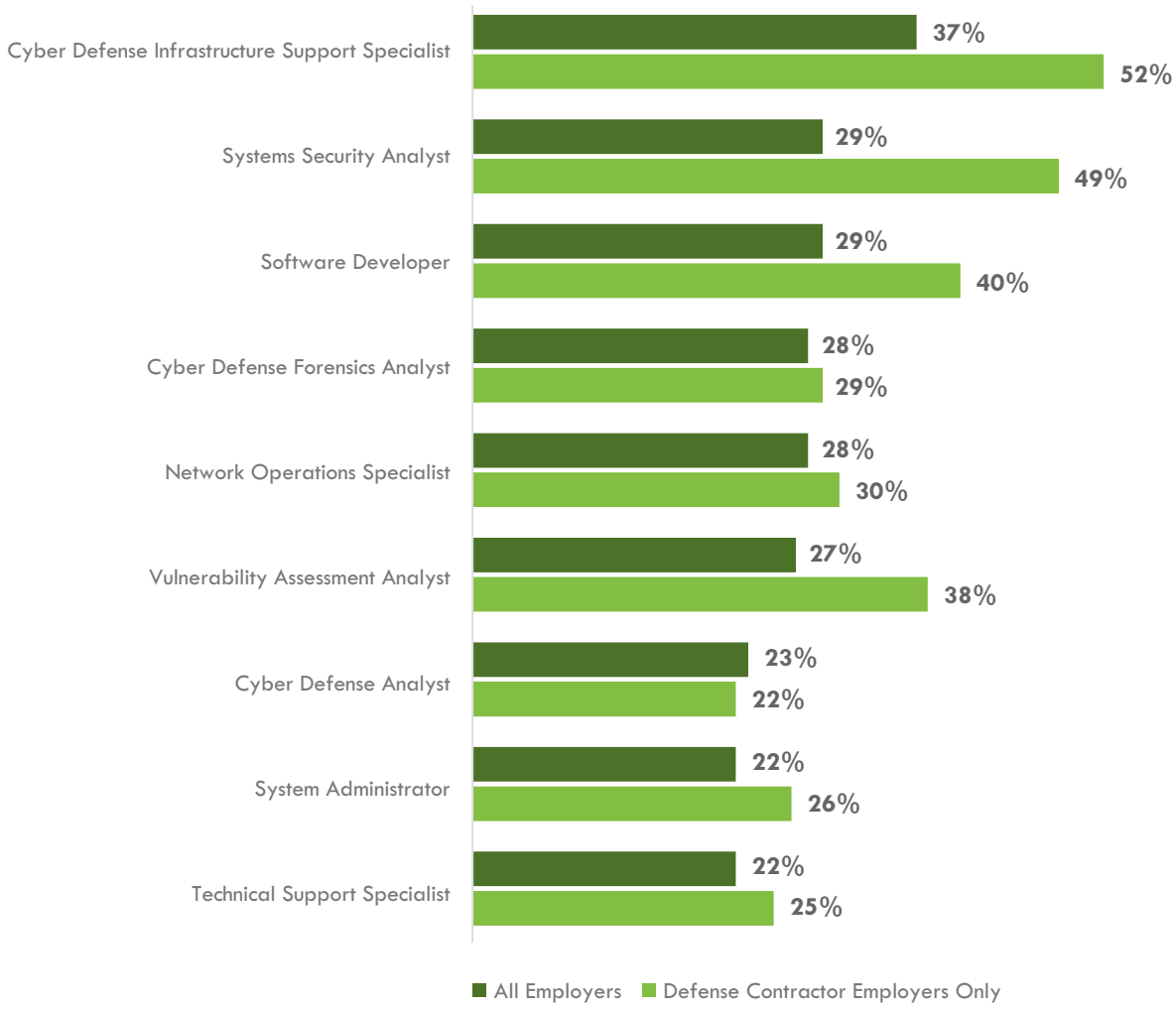
CANDIDATE CHALLENGES

Lack of Security Clearances

The top three work roles for which candidates lack necessary security clearances are the same for all employers and defense contractors: cyber defense infrastructure support specialist, systems security analyst and software developer (Exhibit 16).

Finding qualified candidates with the necessary security clearances is on average more of a challenge for defense contractors. For example, for systems security analysts the percentage of defense contractors reporting this challenge is 49%, which is 20% higher than employers in the overall sample.

Exhibit 16. Lack of candidates with necessary security clearances, all employers and defense contractors

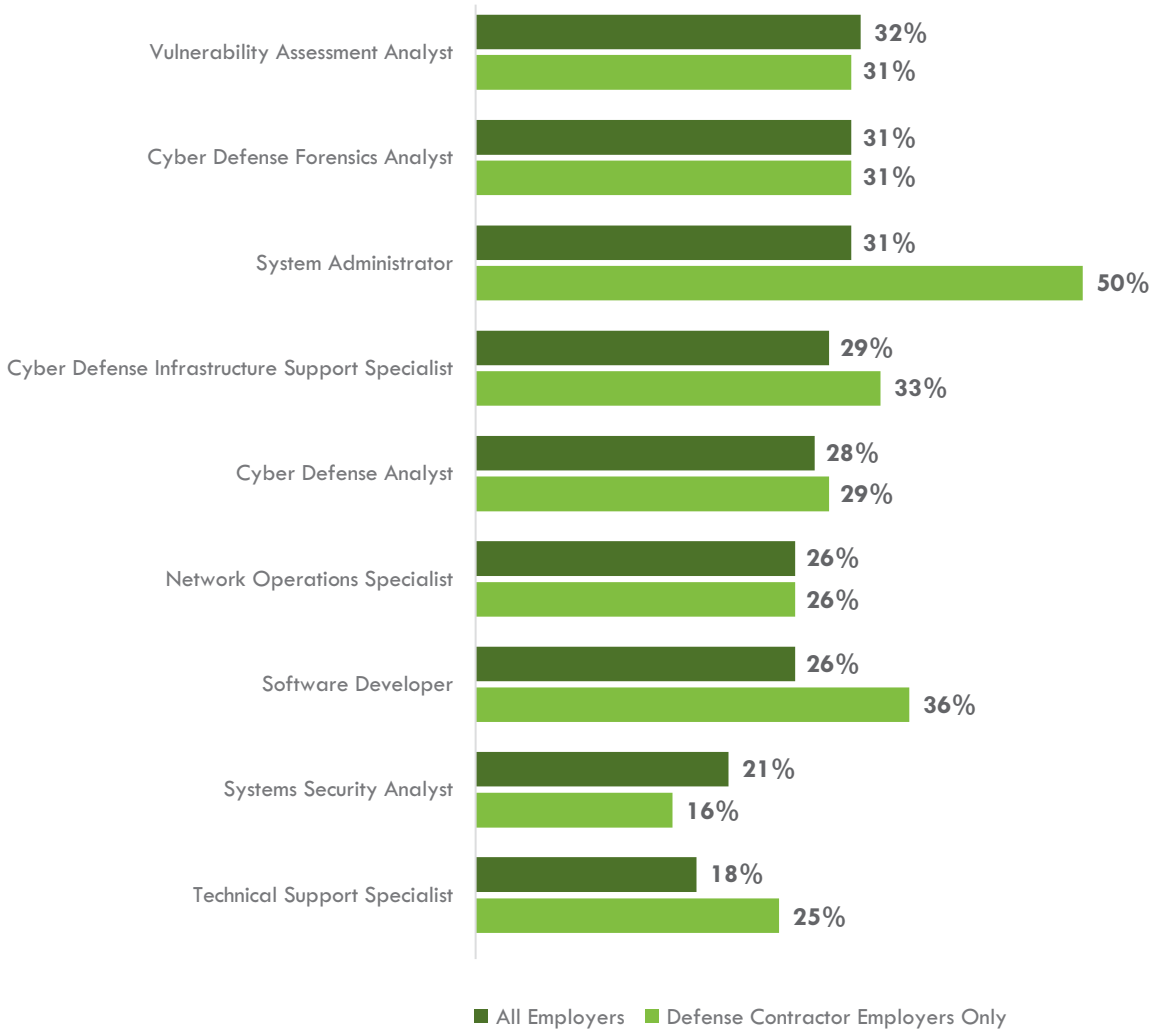


CANDIDATE CHALLENGES

Lack of Education

Defense contractors as a subgroup varied from employers in the overall sample in reporting which work roles lacked candidates with the required educational attainment (Exhibit 17). Vulnerability assessment analyst was the most common work role for all employers, while system administrator was the most common for defense contractors.

Exhibit 17. Lack of required educational attainment for work roles reported by all employers and defense contractors



SECURITY CERTIFICATIONS

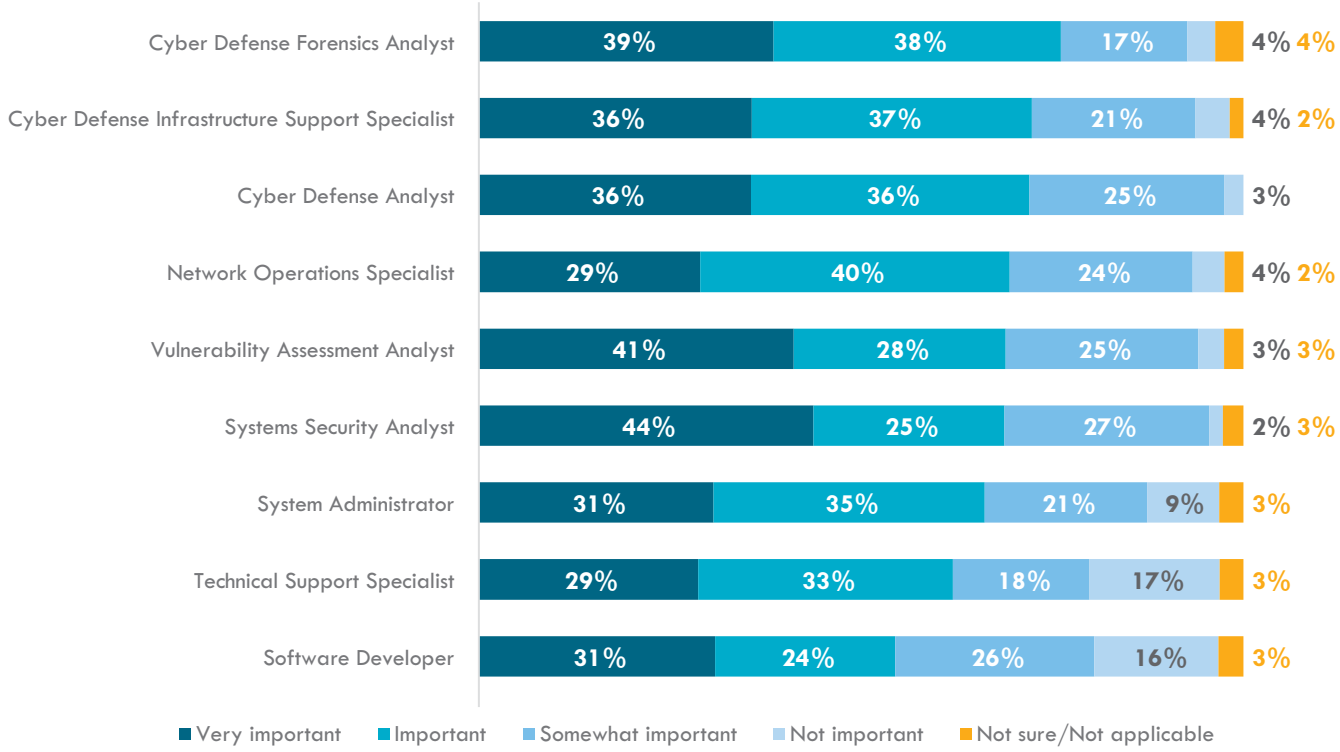
Employers were asked how important a security certification is when hiring for each of the nine work roles. The number of employers who responded to this question ranged from 109 to 129, depending on the work role.

For all nine work roles, 55% or more of employers reported that security certifications are important or very important when hiring (Exhibit 18). For seven of the nine work roles, 66% or more of employers reported that security certifications are important or very important when hiring.

Work roles for which employers reported security certifications are important include:

- 77% of employers reported that when hiring for cyber defense forensics analysts a security certification was important or very important.
- 73% of employers indicated that when hiring for cyber defense infrastructure support specialists a security certification was important or very important.
- 72% of employers reported that when hiring for cyber defense analysts a security certification was important or very important.

Exhibit 18. Level of importance of security certifications reported by employers for the nine work roles



SECURITY CERTIFICATIONS

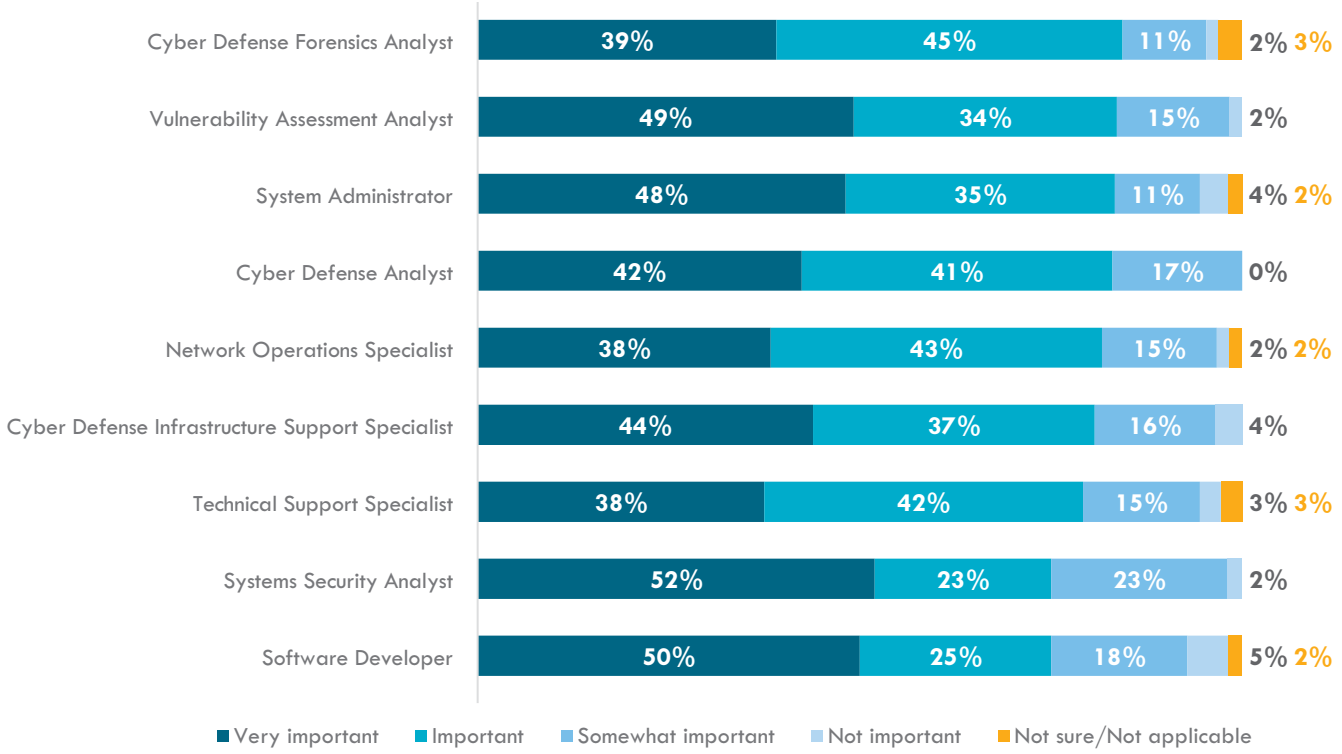
For all nine work roles, 75% or more of defense contractors reported that security certifications are important or very important when hiring (Exhibit 19). Security certifications appear to be more important to defense contractors than to the overall sample of employers who responded to this question. The number of defense contractors who responded to this question ranges from 52 to 72 depending on the work role.

For seven of the nine work roles, 80% or more of defense contractors reported that security certifications are important or very important when hiring.

Work roles for which defense contractors reported security certifications are important include:

- 84% of defense contractors reported that when hiring for cyber defense forensics analysts a security certification was important or very important.
- 83% of defense contractors indicated that when hiring for vulnerability assessment analysts a security certification was important or very important.
- 83% of defense contractors reported that when hiring for system administrators a security certification was important or very important.
- 83% of defense contractors reported that when hiring for cyber defense analysts a security certification was important or very important.

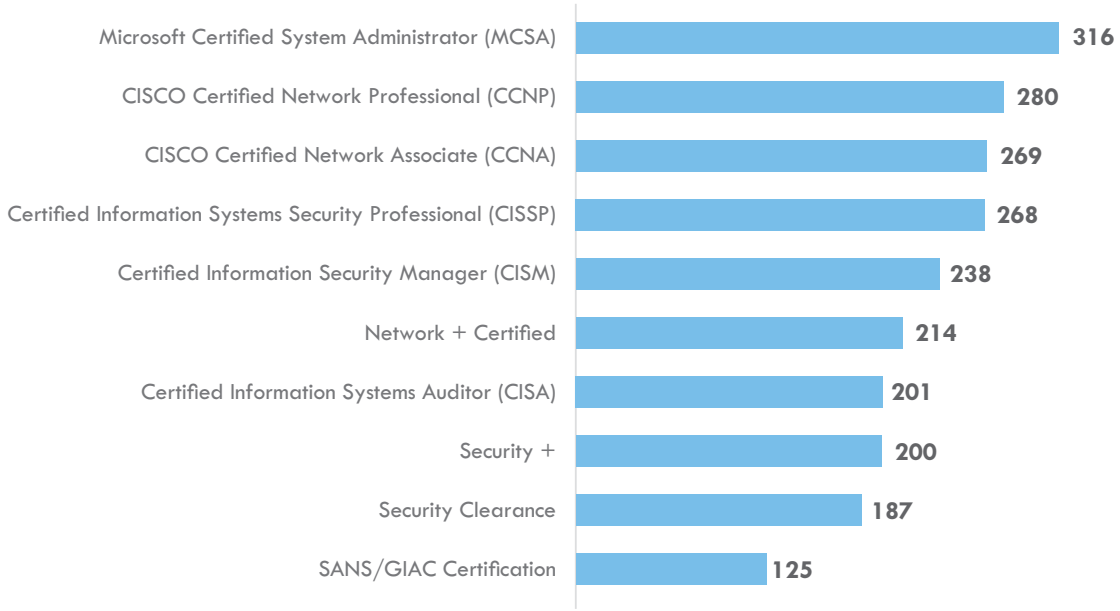
Exhibit 19. Level of importance of security certifications reported by defense contractors for the nine work roles



SECURITY CERTIFICATIONS

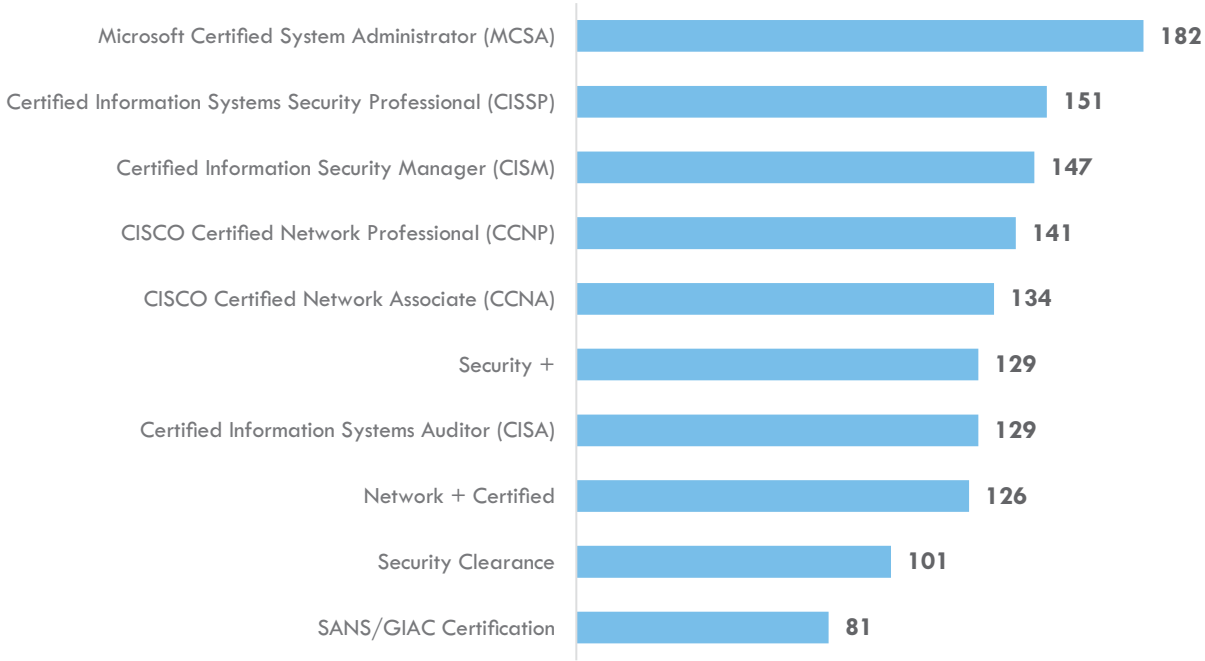
Respondents who answered that a security certification was important or very important were asked to select the certification(s) they prefer from a list of options; they could select all certifications that applied. Exhibit 20 shows the aggregate responses across all nine work roles. Results for the security certifications preferred for each work role are displayed in Appendix D in the work role profiles.

Exhibit 20. Security certifications preferred, all employers



Defense contractors who answered that a security certification was important or very important, were asked to select the certification(s) they prefer from a list of options; they could select all certifications that applied. Exhibit 21 shows the aggregate responses across all nine work roles reported by defense contractors.

Exhibit 21. Security certifications preferred, defense contractors



IMPORTANCE OF CYBERSECURITY SKILLS FOR IT/IS WORK ROLES

The high percentage of employers indicating these skills are important or very important provides validation of the skills in the NICE Framework.

Increasingly IT/IS workers need cybersecurity skills related to their work roles. Utilizing the NICE Framework, specific cybersecurity skills were identified from among the complete list of skills in the framework, for each of the following work roles: technical support specialist, network operations specialist, system administrator, and software developer.

Employers were asked to rate the importance of each cybersecurity specific skill for work roles they have at their business. The results below show the percentage of employers who indicated each skill was important or very important for the work role. The high percentage of California employers indicating these skills are important or very important provides validation of the cybersecurity specific skills outlined in the NICE Framework, for these four work roles.

Technical Support Specialist

Finding: For three of the four cybersecurity skills, 78% or more of employers indicated they are important or very important.

Skill: Accurately defining incidents, problems, and events in the trouble ticketing system. (84%)

Skill: Using the appropriate tools for repairing software, hardware, and peripheral equipment of a system. (83%)

Skill: Identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation. (78%)

Skill: Designing incident response for cloud service models. (67%)

Network Operations Specialist

Finding: For all six cybersecurity skills, 80% or more of employers indicated they are important or very important.

Skill: Protecting a network against malware (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters). (88%)

Skill: Configuring and utilizing network protection components (e.g., firewalls, VPNs, network intrusion detection systems). (88%)

Skill: Implementing, maintaining, and improving established network security practices. (86%)

Skill: Securing network communications. (85%)

Skill: Configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate). (83%)

Skill: Implementing and testing network infrastructure contingency and recovery plans. (80%)

IMPORTANCE OF CYBERSECURITY SKILLS FOR IT/IS WORK ROLES

Systems Administrator

Finding: For all four cybersecurity skills, 82% or more of employers indicated they are important or very important.

Skill: Accurately define incidents, problems, and events in the trouble ticketing system. (89%)

Skill: Applying cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (88%)

Skill: Configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware). (85%)

Skill: Establishing and maintaining automated security control assessments. (82%)

Software Developer

Finding: For five of the seven cybersecurity skills, 68% or more of employers indicated they are important or very important.

Skill: Applying cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (76%)

Skill: Developing and applying security system access controls. (70%)

Skill: Using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). (70%)

Skill: Secure test plan design (e.g., unit, integration, system, acceptance). (69%)

Skill: Designing countermeasures to identified security risks. (68%)

Skill: Discerning the protection needs (i.e., security controls) of information systems and networks. (64%)

Skill: Conducting vulnerability scans and recognizing vulnerabilities in security systems. (61%)

A very high percentage of defense contractors also rated the NICE Framework cybersecurity skills for the four work roles as important or very important. The number of defense contractors who responded to this question ranged from 52 to 72 depending on the work role.

Based on responses from defense contractors, key findings for each work role include:

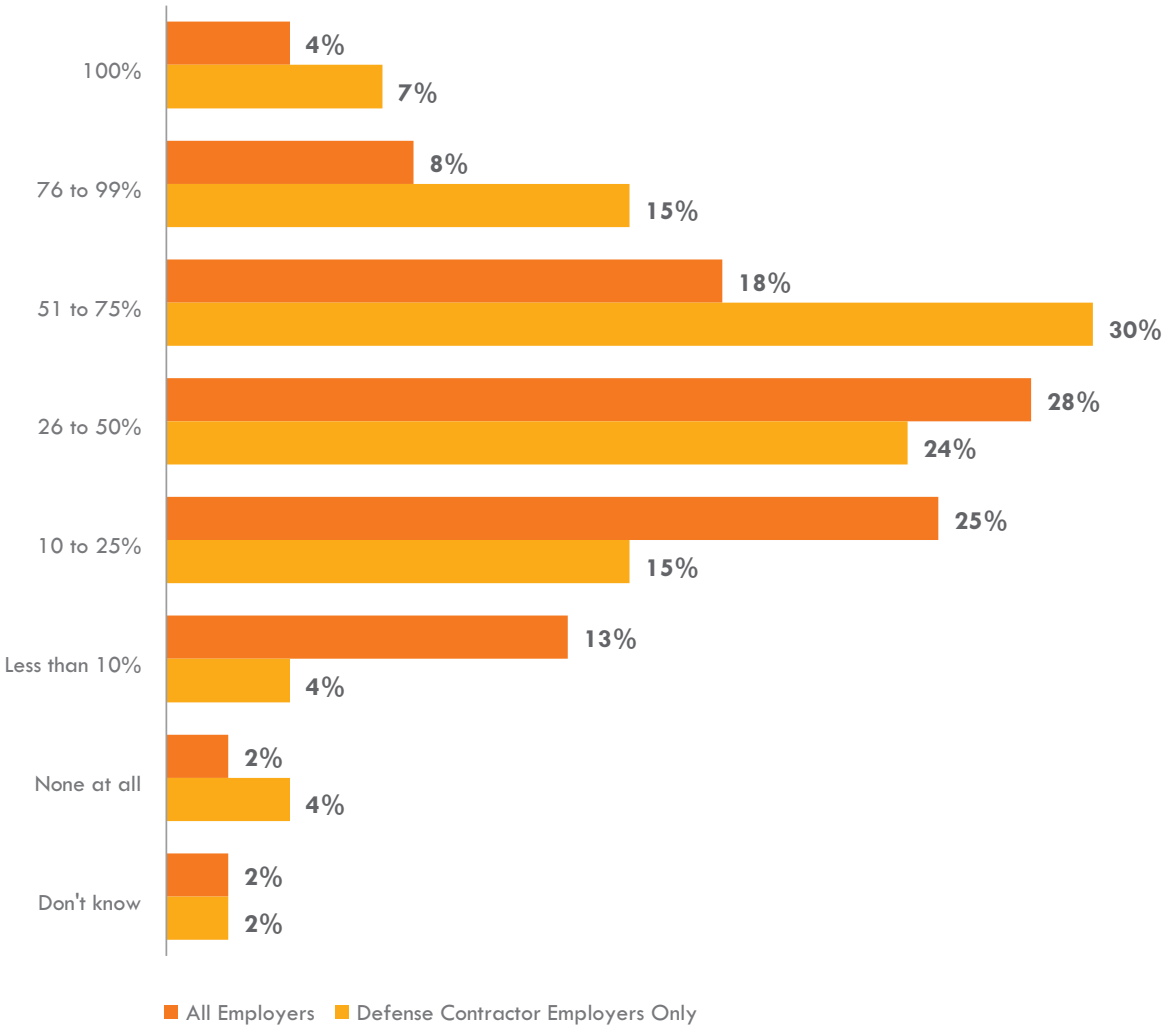
- Technical support specialist—For all four cybersecurity skills, 79% or more of defense contractors indicated they are important or very important.
- Network operations specialist—For all six cybersecurity skills, 82% or more of defense contractors indicated they are important or very important.
- Systems administrator—For all four cybersecurity skills, 80% or more of defense contractors indicated they are important or very important.
- Software developer—For all seven cybersecurity skills, 68% or more of defense contractors indicated they are important or very important.

TIME SPENT ON SECURITY/ CYBERSECURITY ISSUES

For the same four IT/IS work roles that require cybersecurity skills, employers were asked to document on average, the percentage of time (within the overall job duties) spent on security/cybersecurity issues. Compared to employers in the overall sample, 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.

Exhibit 22 shows that 58% of employers in the overall sample compared to 76% of defense contractors said that system administrators spend more than a quarter of their time on security/cybersecurity issues.

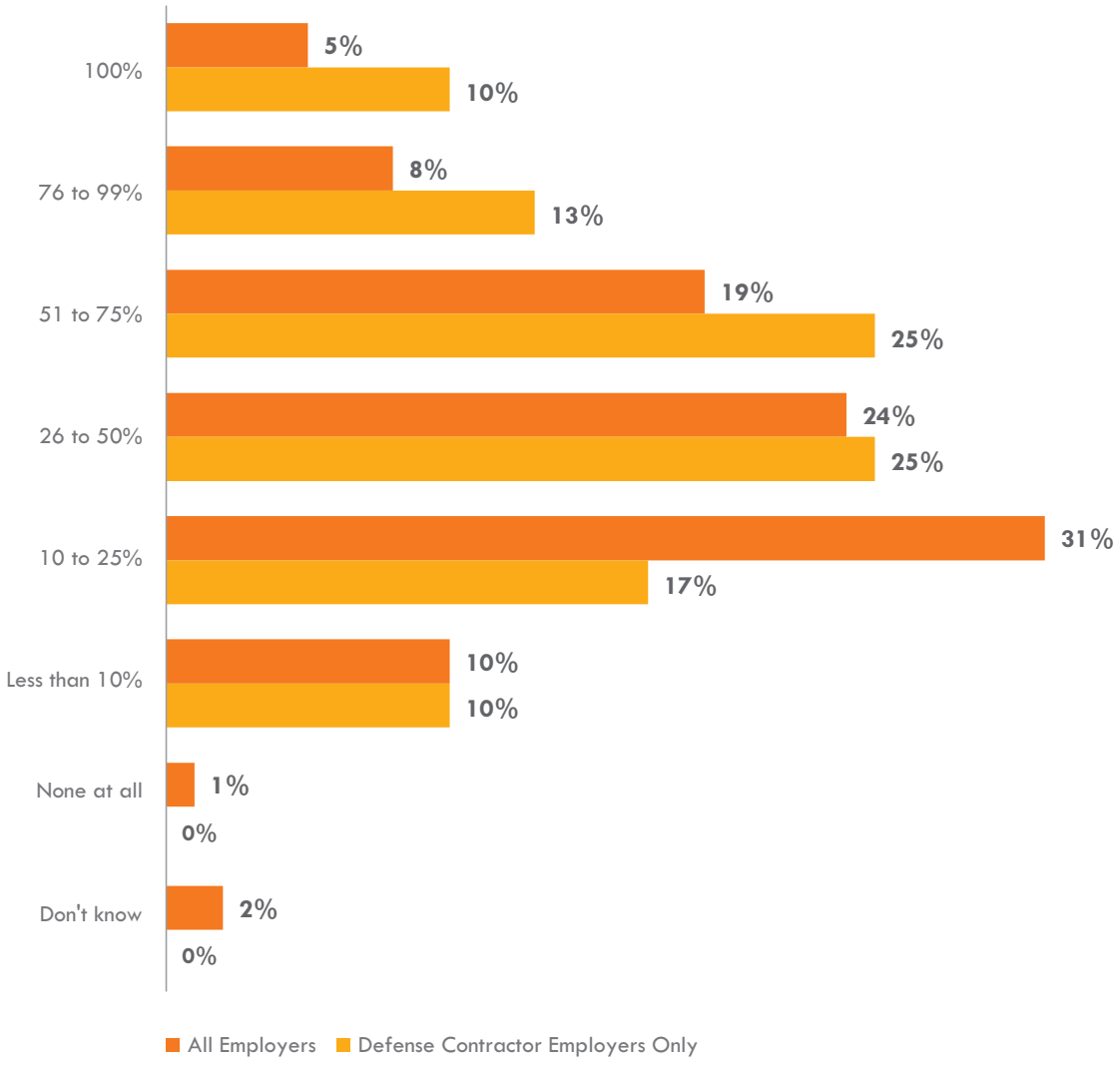
Exhibit 22. Percentage of time systems administrators spend on security/ cybersecurity issues, all employers and defense contractors



TIME SPENT ON SECURITY/ CYBERSECURITY ISSUES

Exhibit 23 shows 56% of all employers compared to 73% of defense contractors said that network operations specialists spend more than a quarter of their time on security/cybersecurity issues.

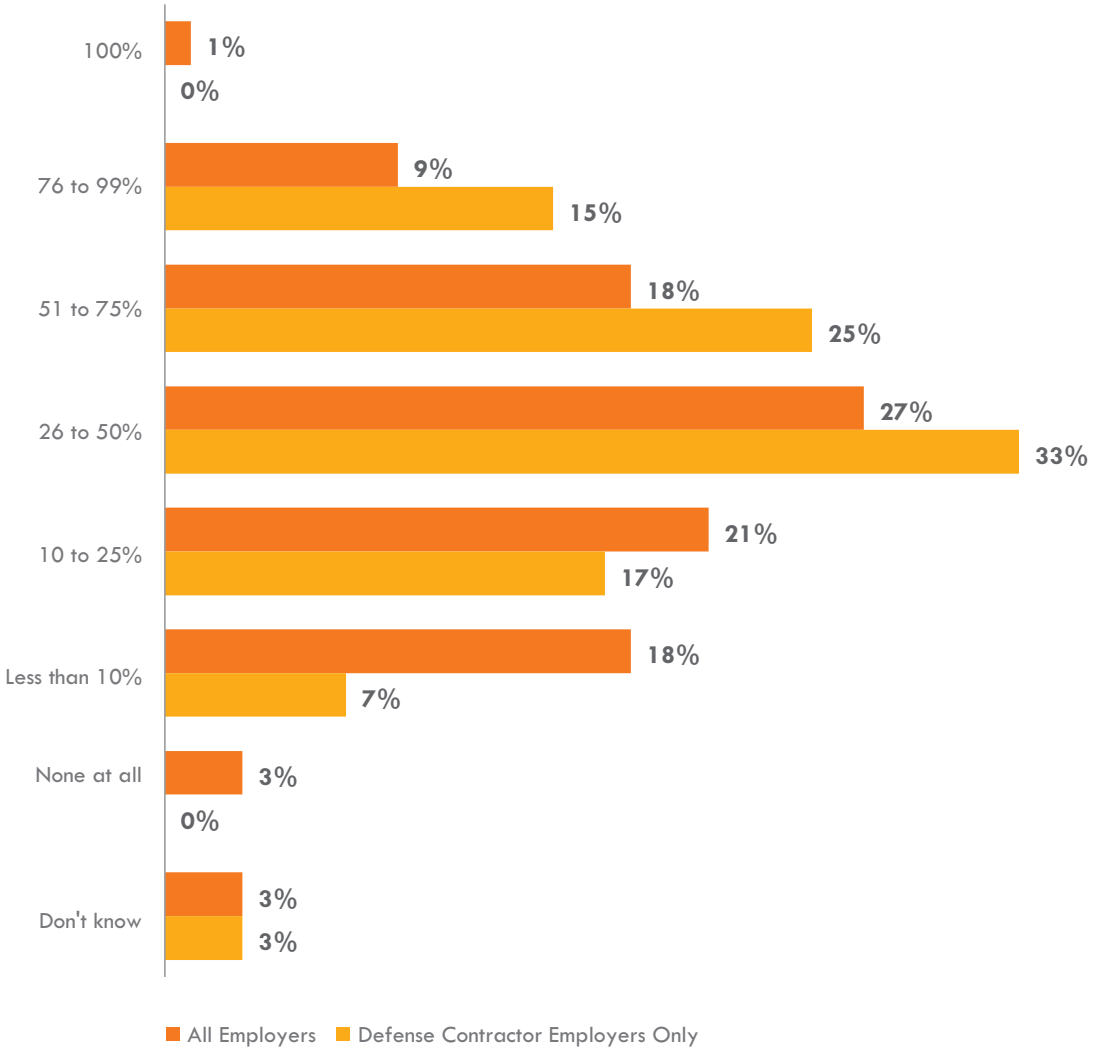
Exhibit 23. Percentage of time network operations specialists spend on security/ cybersecurity issues, all employers and defense contractors



TIME SPENT ON SECURITY/ CYBERSECURITY ISSUES

Exhibit 24 shows that 55% of employers compared to 73% of defense contractors said that technical support specialists spend more than a quarter of their time on security/cybersecurity issues.

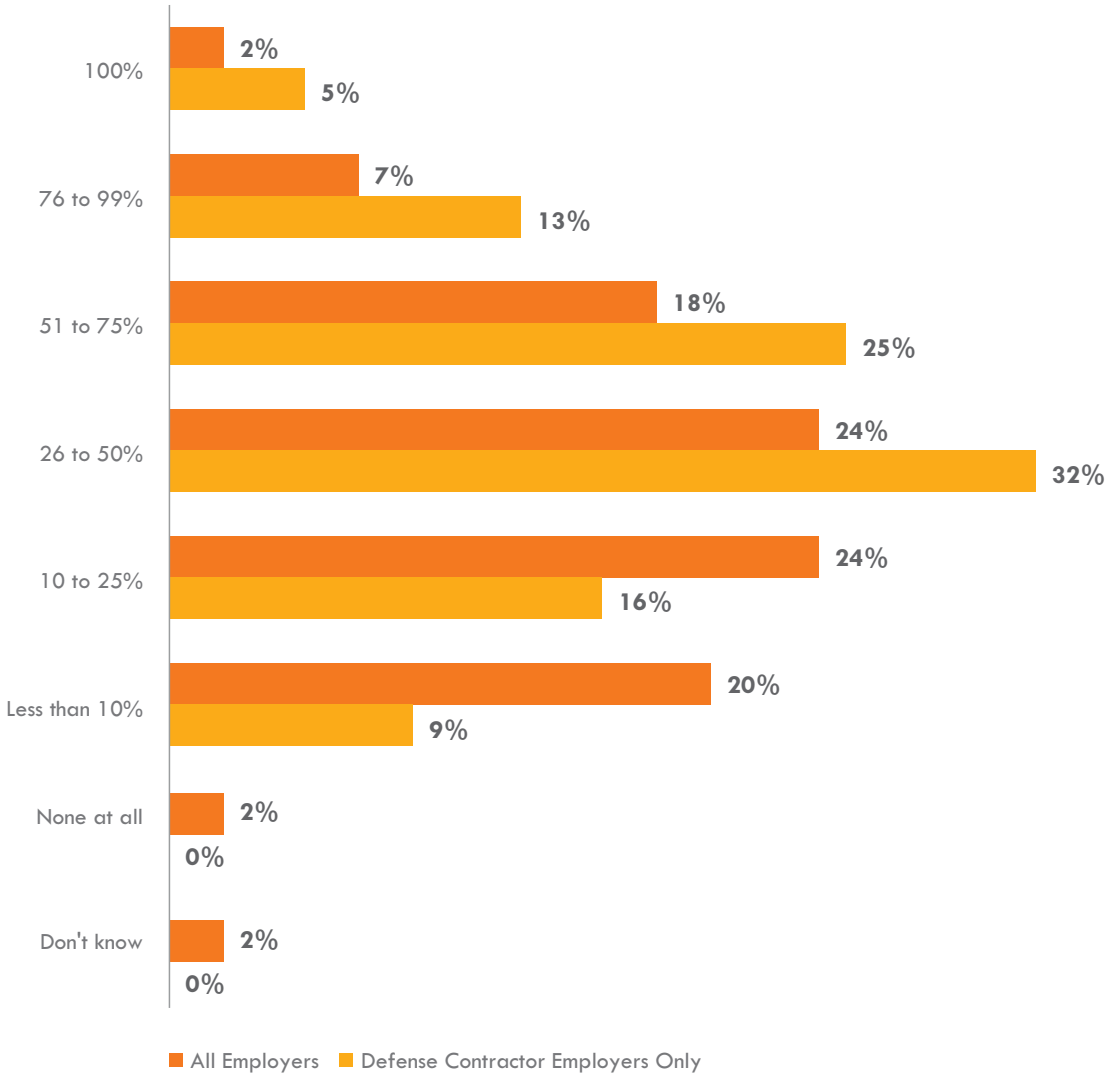
Exhibit 24. Percentage of time technical support specialists spend on security/ cybersecurity issues, all employers and defense contractors



TIME SPENT ON SECURITY/ CYBERSECURITY ISSUES

Exhibit 25 shows that 52% of employers compared to 75% of defense contractors said that software developers spend more than a quarter of their time on security/cybersecurity issues.

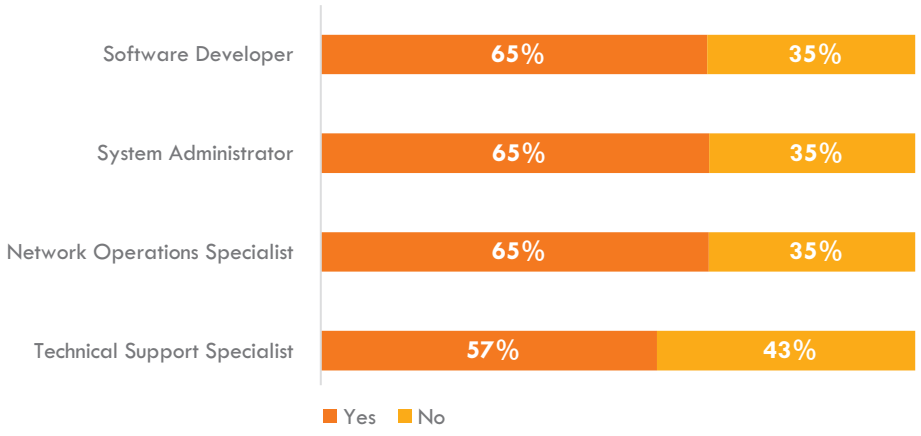
Exhibit 25. Percentage of time software developers spend on security/ cybersecurity issues, all employers and defense contractors



TIME SPENT ON SECURITY/ CYBERSECURITY ISSUES

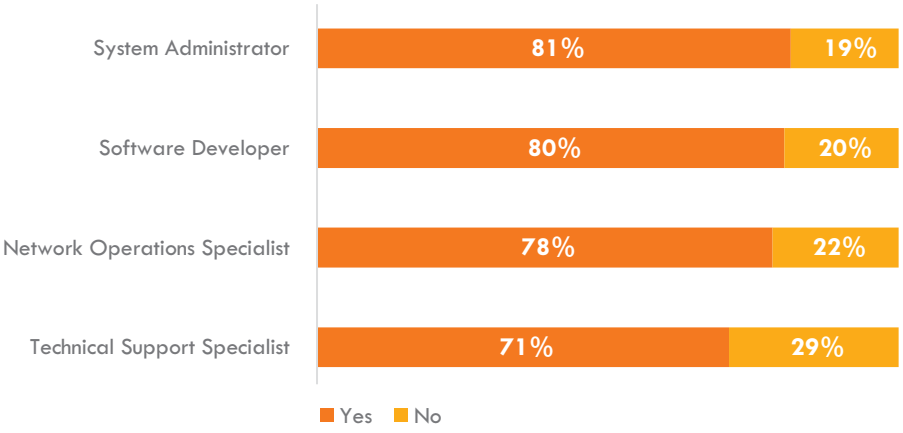
As a follow-up question, employers were asked if the percentage of time spent on security/cybersecurity issues for the four work roles had increased compared to 12 months ago. For three of the four work roles—network operations specialist, system administrator and software developer—65% of employers said the percentage of time spent on security/cybersecurity issues had increased compared to 12 months ago (Exhibit 26). By comparison, 57% of employers said that for technical support specialist the percentage of time had increased.

Exhibit 26. Increased time spent on security/cybersecurity issues compared to 12 months ago, all employers



There is a higher percentage of defense contractors who indicated that these four work roles are spending more time on security/cybersecurity issues compared to 12 months ago, than for employers in the overall sample (Exhibit 27). For all four work roles, 70% or more of defense contractors said the percentage of time spent on security issues had increased compared to 12 months ago. For system administrators and software developers, 80% or more of defense contractors said the percentage of time had increased compared to 12 months ago.

Exhibit 27. Increased time spent on security/cybersecurity issues compared to 12 months ago, defense contractors



EDUCATION, WORK EXPERIENCE AND SOFT SKILLS

For all nine work roles studied, employers were asked about the minimum level of education required for qualified candidates. For each of the nine work roles, 40% or more of employers selected a bachelor's degree as the minimum education level required. The percentages ranged from 40% for technical support specialists and vulnerability assessment analysts, to 58% for systems security analysts.

Employers were asked about the minimum prior work experience required for qualified candidates. For four work roles, the highest percentage of employers indicated one to two years of prior work experience when hiring for qualified candidates. One to two years of experience was preferred by 40% or more of employers for: technical support specialists, network operations specialists, vulnerability assessment analysts, and cyber defense forensics analysts.

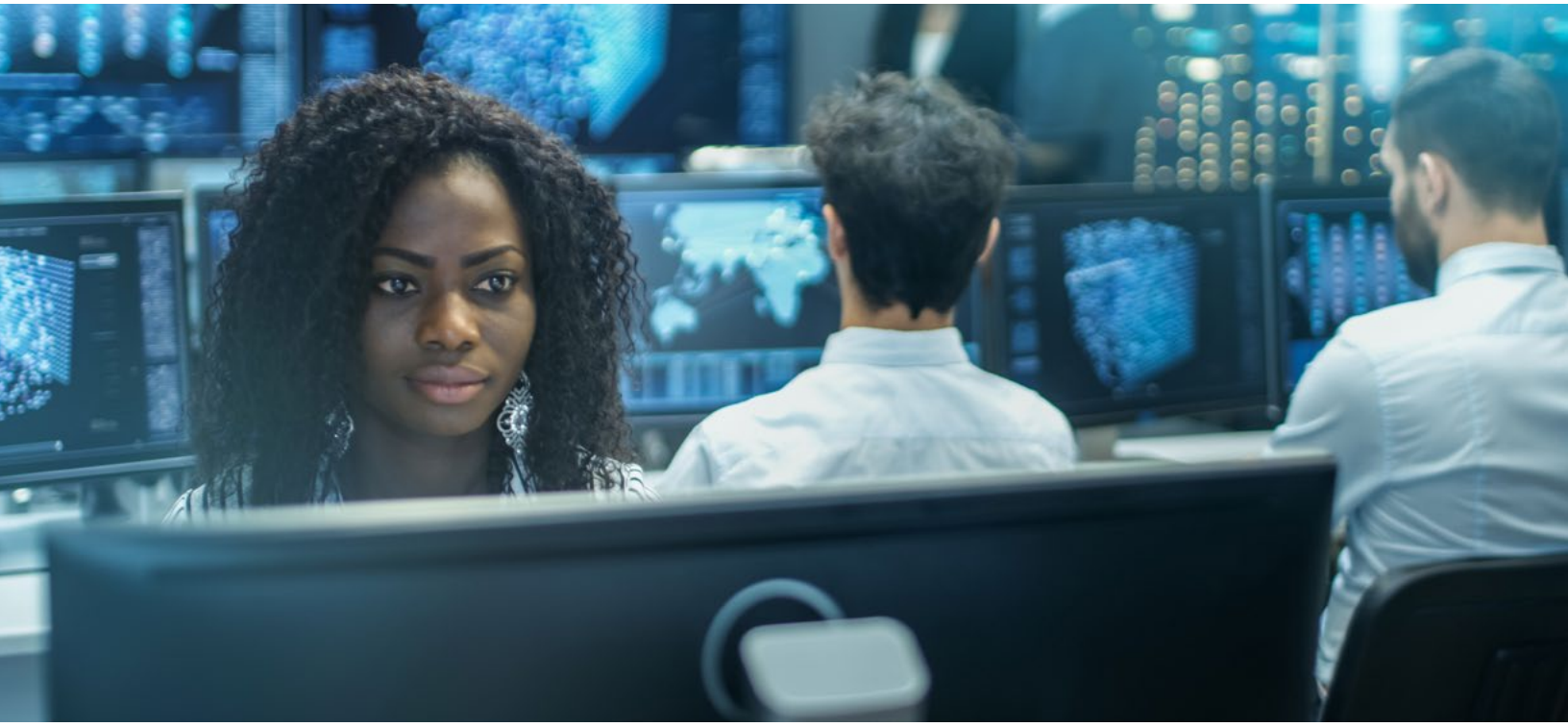
For the other five work roles, the highest percentage of employers indicated they preferred three to five years of prior work experience when hiring for qualified candidates. Three to five years of work experience was preferred by 39% or more of employers for: system administrator, software developer, systems security analyst, cyber defense analyst, and cyber defense infrastructure support specialist.

Employers were asked to select the top three soft skills most important for the work roles they employ. For all nine work roles, problem solving is one of the top three soft skills important to employers.

Several other soft skills topped the list:

- Troubleshooting is one of the top three soft skills for five of the nine work roles.
- Communication skills is one of the top three soft skills for four of the nine work roles.
- Teamwork/collaboration is one of the top three soft skills for four of the nine work roles.

Work role profiles in Appendix D have more details on education and work experience requirements as well as the top three soft skills for each work role.



SECTION III: EDUCATIONAL SUPPLY ASSESSMENT

CYBERSECURITY PROGRAMS ASSESSMENT

An assessment of the postsecondary educational supply of cybersecurity students in California was conducted to gauge whether educational training programs throughout the state are meeting workforce demand.

In order to access appropriate data from the Integrated Postsecondary Education Data System (IPEDS), National Center for Educational Statistics, it was first necessary to determine the list of Classification of Instructional Programs (CIP) codes relevant to cybersecurity training and education. CIP codes are used nationally to classify all postsecondary instructional programs, and the codes are determined by the U.S. Department of Education through the National Center for Education Statistics. The CIP codes used in this report were chosen based on programmatic focus on cybersecurity, or programs/curriculum likely to include elements of cybersecurity (Exhibit 28). The criteria used to identify cybersecurity CIP codes are:

1. **Cybersecurity Focused**—If both the CIP title and the description of the CIP code addressed cybersecurity, then a program was coded as "Cybersecurity Focused." Three CIP codes met the criteria. (See Exhibit 28.)
2. **Includes Aspects of Cybersecurity**—If the CIP title was related to cybersecurity and the description of the CIP code included aspects of cybersecurity (including phrases such as "information security," "cybersecurity," "data storage and security") then the program was coded as "Includes Aspects of Cybersecurity." Eleven CIP codes met these criteria.
3. **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, operational systems, networking, information systems, computer systems) then the program was coded as "Likely Includes Cybersecurity." Twenty CIP codes met these criteria.

Exhibit 28. Cybersecurity-related CIP codes and titles

Cybersecurity Focused	
11.1003	Computer and Information Systems Security/Information Assurance
29.0207	Cyber/Electronic Operations and Warfare
43.0116	Cyber/Computer Forensics and Counterterrorism
Includes Aspects of Cybersecurity	
11.0802	Data Modeling/Warehousing and Database Administration
11.0901	Computer Systems Networking and Telecommunications
11.1001	Network and System Administration/Administrator
11.1002	System, Networking, and LAN/WAN Management/Manager
11.1004	Web/Multimedia Management and Webmaster
15.1204	Computer Software Technology/Technician
43.0301	Homeland Security
43.0303	Critical Infrastructure Protection

continued

Exhibit 28. Cybersecurity-related CIP codes and titles (continued)

Includes Aspects of Cybersecurity (continued)	
52.1201	Management Information Systems, General
52.1206	Information Resources Management
52.2101	Telecommunications Management
Likely Includes Cybersecurity	
11.0101	Computer and Information Sciences, General
11.0102	Artificial Intelligence
11.0103	Information Technology
11.0104	Informatics
11.0199	Computer and Information Sciences, Other
11.0201	Computer Programming/Programmer, General
11.0202	Computer Programming, Specific Applications
11.0299	Computer Programming, Other
11.0401	Information Science/Studies
11.0501	Computer Systems Analysis/Analyst
11.0601	Data Entry/Microcomputer Applications, General
11.0701	Computer Science
11.0801	Web Page, Digital/Multimedia and Information Resources Design
11.0899	Computer Software and Media Applications, Other
11.1005	Information Technology Project Management
11.1006	Computer Support Specialist
11.1099	Computer/Information Technology Services Administration and Management, Other
11.9999	Computer and Information Sciences and Support Services, Other
15.1201	Computer Engineering Technology/Technician
15.1202	Computer Technology/Computer Systems Technology
15.1203	Computer Hardware Technology/Technician
15.1299	Computer Engineering Technologies/Technicians, Other

Note: Full descriptions of the above CIP codes are included in Appendix G of this report.

Cybersecurity Programs at Postsecondary Institutions

In 2016, there were 242 accredited postsecondary institutions in the state of California offering programs that either focused on or included cybersecurity. Also in 2016, the most recent year of available data, there were 1,177 programs related to cybersecurity at postsecondary institutions in California (Exhibit 29).

Of those, 61 were programs that were clearly "cybersecurity focused," and the majority of those were in the area of Computer and Information Systems Security (CIP 11.1003) rather than the newer emerging cybersecurity fields of Cyberwarfare (CIP 29.0207) or Homeland Security (CIP 43.0116). An additional 258 programs are offered in the category of "includes aspects of cybersecurity," and 858 in programs that "likely include cybersecurity."

CYBERSECURITY PROGRAMS ASSESSMENT

Of the 1,177 cybersecurity programs offered, 130 (11%) are taught exclusively online. Interestingly, cybersecurity-focused programs are more likely to be taught exclusively online than the cybersecurity-related programs. While data is not available to confirm, it is likely many programs might be offered partially online, or in a hybrid format.

Exhibit 29. Postsecondary cybersecurity-related programs offered in California

		Total Programs Offered	Total Programs Offered Exclusively Online	Percent of Programs Offered Exclusively Online
Cybersecurity Focused		**61**	**12**	**20%**
11.1003	Computer and Information Systems Security/Information Assurance	58	9	16%
29.0207	Cyber/Electronic Operations and Warfare	2	2	100%
43.0116	Cyber/Computer Forensics and Counterterrorism	1	1	100%
Includes Aspects of Cybersecurity		**258**	**32**	**12%**
11.0802	Data Modeling/Warehousing and Database Administration	23	4	17%
11.0901	Computer Systems Networking and Telecommunications	130	5	4%
11.1001	Network and System Administration/Administrator	14	6	43%
11.1002	System, Networking, and LAN/WAN Management/ Manager	2	0	0%
11.1004	Web/Multimedia Management and Webmaster	42	1	2%
15.1204	Computer Software Technology/Technician	1	0	0%
43.0301	Homeland Security	23	8	35%
43.0303	Critical Infrastructure Protection	1	0	0%
52.1201	Management Information Systems, General	13	3	23%
52.1206	Information Resources Management	5	2	40%
52.2101	Telecommunications Management	4	3	75%
Likely Includes Cybersecurity		**858**	**86**	**10%**
11.0101	Computer and Information Sciences, General	67	10	15%
11.0102	Artificial Intelligence	1	0	0%
11.0103	Information Technology	163	14	9%
11.0104	Informatics	3	1	33%
11.0199	Computer and Information Sciences, Other	7	0	0%
11.0201	Computer Programming/Programmer, General	124	12	10%
11.0202	Computer Programming, Specific Applications	2	1	50%
11.0299	Computer Programming, Other	1	0	0%
11.0401	Information Science/Studies	18	2	11%
11.0501	Computer Systems Analysis/Analyst	8	3	38%
11.0601	Data Entry/Microcomputer Applications, General	79	3	4%

continued

Exhibit 29. Postsecondary cybersecurity-related programs offered in California

(continued)

		Total Programs Offered	Total Programs Offered Exclusively Online	Percent of Programs Offered Exclusively Online
Likely Includes Cybersecurity		**858**	**86**	**10%**
11.0701	Computer Science	174	10	6%
11.0801	Web Page, Digital/Multimedia and Information Resources Design	109	15	14%
11.0899	Computer Software and Media Applications, Other	7	0	0%
11.1005	Information Technology Project Management	3	3	100%
11.1006	Computer Support Specialist	54	3	6%
11.1099	Computer/Information Technology Services Administration and Management, Other	8	4	50%
11.9999	Computer and Information Sciences and Support Services, Other	23	4	17%
15.1201	Computer Engineering Technology/Technician	2	1	50%
15.1202	Computer Technology/Computer Systems Technology	3	0	0%
15.1203	Computer Hardware Technology/Technician	1	0	0%
15.1299	Computer Engineering Technologies/Technicians, Other	1	0	0%
	Totals	**1,177**	**130**	**11%**

Source: National Center for Educational Statistics, IPEDS Data

For more detailed information, see Appendix E: Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California and Appendix F: Program Awards in Cybersecurity (and Closely Related Programs) at Postsecondary Institutions in California, Five-Year Trends.

There is diversity in the types of institutions providing cybersecurity programs, from non-degree granting institutions to two-year colleges and universities offering bachelor's degrees to doctoral degrees. Most cybersecurity programs reported to IPEDS (96%) are offered by degree-granting institutions (Exhibit 30). Within degree-granting institutions, the majority of cybersecurity-related programs are at public two-year (56%) and public four-year (16%) colleges, resulting in public colleges offering 72% of cybersecurity-related programs. Costs also vary by type of institution. Tuition and fees, and average net price of attendance are significantly lower at public colleges than at private colleges.

Exhibit 30. Postsecondary cybersecurity-related programs, by sector of institution and cost

	Total Programs Offered	Average Annual Tuition & Fees	Average Net Price of Attendance[27]
Degree-granting	**719**	**$7,448**	**$12,232**
Private for-profit, 2-year	25	$12,648	$15,736
Private for-profit, 4-year or above	61	$14,634	$21,698
Private not-for-profit, 4-year or above	95	$33,520	$29,374
Public, 2-year	420	$1,251	$8,024
Public, 4-year or above	118	$5,533	$9,412
Nondegree-granting, primarily postsecondary	**28**		**$18,813**
Private for-profit, 2-year	1		$23,210
Private for-profit, less-than 2-year	25		$19,244
Public, less-than 2-year	2		$13,173
Total/Overall Average	**747**	**$7,448**	**$12,408**

Source: National Center for Educational Statistics, IPEDS Data

Note: Data are from 2016, the most recent year available.

For more detailed information, see Appendix H: List of IPEDS-reporting Postsecondary Institutions Providing Cybersecurity Programming in California, with Institutional Characteristics.

Nine of the colleges and universities identified above have been designated a "National Center of Academic Excellence" in cyber defense, cyber operations, or research (related to cybersecurity) by the National Security Agency (NSA) and the Department of Homeland Security (DHS) through a joint program that recognizes and grants distinction to "schools that offer rigorous degree programs in information security."[28] (Colleges can receive more than one designation.)

The nine postsecondary institutions in California recognized as Centers of Academic Excellence are:

Cyber Defense

- California State Polytechnic University Pomona, Computer Information Systems Department
- California State University, Sacramento, Center for Information Assurance and Security
- California State University, San Bernardino, Cyber Security Center
- Coastline Community College, Cyber Security Center
- National University
- Naval Postgraduate School, Cyber Academic Group
- San Jose State University, Silicon Valley Big Data and Cybersecurity Center
- University of California, Davis, Computer Security Lab

Research

- Naval Postgraduate School, Cyber Academic Group
- University of California, Davis, Computer Security Lab
- University of California, Irvine, Secure Computing and Network Center

Cyber Operations

- Naval Postgraduate School, Cyber Academic Group

[27] In IPEDS, average institutional net price of attendance is generated by subtracting the average amount of federal, state/local government, or institutional grant and scholarship aid from the total cost of attendance. Total cost of attendance is the sum of published tuition and required fees (lower of in-district or in-state for public institutions), books and supplies, and the weighted average for room and board and other expenses.

[28] "National Centers of Academic Excellence in Cyber Education," National Security Agency, Central Security Service, October 31, 2016, accessed June 11, 2018, https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/.

PROGRAM AWARDS

While CIP codes classify instructional programs, program awards indicate the level of education and training associated with the programs. Awards range from certificates of less than one year to higher level certificates and degrees up to the doctoral level. Definitions of the different award levels are included in the notes of Appendix F: Program Awards in Cybersecurity (and Closely Related Programs) at Postsecondary Institutions in California, Five-Year Trends.

Overall, the number of cybersecurity-related awards increased between 2012 and 2016, rising from 12,227 awards to 15,721 awards in that time period, an increase of 29% (Exhibit 31). However, there were differences in growth by program, and by award levels.

Cybersecurity-focused program awards increased 80% between 2012 (452 awards) and 2016 (813 awards). This growth occurred mostly in awards of less than one academic year, associate degrees, post-baccalaureate certificates, and master's degrees. Bachelor's degree awards actually decreased in 2016 after peaking in 2015. It is interesting to note that no doctoral degrees were awarded in cybersecurity-focused programs during this time period.

Awards from programs in the category **"includes aspects of cybersecurity"** decreased 23% between 2012 (3,103 awards) and 2016 (2,401 awards). The decrease occurred across most award levels (most notably associate degrees and awards of less than two years). However, there was an increase in program awards for bachelor's, master's, and doctoral degrees.

Programs in the **"likely includes cybersecurity"** category increased awards 44% between 2012 (8,672 awards) and 2016 (12,507 awards). Most of this growth came in the associate, bachelor's, and master's degree categories. During the same time period, awards of at least one, but less than two academic years, decreased.

Because cybersecurity is an emerging field of study, it is possible that some of the fluctuations in program awards is due to the relatively new and emerging system for classifying these programs. Postsecondary institutions may not be current with the most recently added CIP codes to classify their cybersecurity-related programs. CIP code 43.0116 was recently created for Homeland Security, and only one program shows up with that CIP code in California in 2016, with no associated awards. Likely it is a new program that will take some years before students earn program awards. It is also likely that as curriculum and programs get updated, CIP codes will also be updated and newly added CIP codes can be considered.

Between 2012 and 2016, cybersecurity-related awards rose from 12,227 to 15,721, an increase of 29%.

PROGRAM AWARDS

Exhibit 31. Summary of cybersecurity (and closely related) awards from California postsecondary institutions, five-year trends

	2012	2013	2014	2015	2016	5-Year Total	5-Year Annual Average
Cybersecurity Focused	**452**	**499**	**788**	**922**	**813**	**3,474**	**695**
Award of less than 1 academic year	88	84	98	87	157	514	103
Award of at least 1 but less than 2 academic years	5	2	2	2	4	15	3
Associate degree	63	82	64	85	192	486	97
Bachelor's degree	195	217	399	450	132	1,393	279
Post-baccalaureate certificate	96	64	143	182	206	691	138
Master's degree	5	50	82	116	122	375	75
Includes Aspects of Cybersecurity	**3,103**	**3,637**	**3,457**	**3,293**	**2,401**	**15,891**	**3,178**
Award of less than 1 academic year	1,082	918	845	816	802	4,463	893
Award of at least 1 but less than 2 academic years	325	326	327	290	221	1,489	298
Associate degree	1,184	1,483	1,275	1,125	383	5,450	1,090
Bachelor's degree	289	548	649	619	568	2,673	535
Post-baccalaureate certificate	1	28	16	9	4	58	12
Master's degree	220	329	342	429	414	1,734	347
Doctoral degree - research/scholarship	2	5	3	5	9	24	5
Likely Includes Cybersecurity	**8,672**	**8,685**	**10,712**	**10,605**	**12,507**	**51,181**	**10,236**
Award of less than 1 academic year	1,270	1,281	2,417	1,728	1,448	8,144	1,629
Award of at least 1 but less than 2 academic years	1,064	775	745	425	412	3,421	684

Source: National Center for Educational Statistics, IPEDS Data

Note: For more detailed results, see Appendix F: Program Awards in Cybersecurity (and Closely Related Programs) at Postsecondary Institutions in California, Five-year Trends.

ADDITIONAL PROGRAMS AND HIGH SCHOOL ENROLLMENT

In addition to postsecondary institutions located in California that offer cybersecurity-related programs and training, there are many accredited and federally recognized institutions outside the state that offer online cybersecurity programs. Examples include Capella University, Kaplan University, Salem International University, University of Phoenix, Utica College, and Walden University.

There are many other providers of cybersecurity training outside of accredited, federally recognized postsecondary institutions, ranging from adult schools to university extensions. Some operate outside of established education institutions, such as "boot camps" and online industry sponsored training. In addition, entities outside of California provide online training that California residents can take. Some universities offer cybersecurity training through their extension or continuing education programs. Examples include UCLA Extension, UC Irvine Division of Continuing Education, California State University Fullerton University Extended Education, and Stanford University Online. These programs are generally fee-based and operate outside of the regular undergraduate or graduate university curriculum.

There are many providers of cybersecurity training outside of accredited, federally recognized postsecondary institutions, ranging from adult schools to university extensions.

The U.S. Military provides cybersecurity training, including at locations in California, such as the U.S. Navy Information Warfare Training Commands in San Diego and Monterey, the U.S. Army Reserve High Tech Regional Training Site in Sacramento, and the Marine Corps Communications and Electronics School in Twentynine Palms. In addition, some adult education schools offer entry-level cybersecurity training. These programs are provided through unified school districts in cities such as Sacramento, Chula Vista, San Diego, and Riverside. These programs are generally low cost compared to alternative cybersecurity training opportunities.

Industry Sponsored Programs

Many industry sponsored programs are offered through high schools or postsecondary institutions. Vendors partner with existing educational institutions to provide training leading to industry certification (which is bestowed by the vendor after students pass specific tests outside of the school or college). It is the role of the partner school/college to provide training to prepare students to pass the industry certification tests, and in exchange the educational institution often receives training materials and gifts of hardware and/or software from the vendor to support the training and promote their products and certifications.

There is no requirement to enroll in or pass a class to qualify for an industry certification. Individuals may be self-taught, may take free or for-pay online classes, may attend a "boot camp" or other short-term training, or any other strategy whereby they can gain the knowledge and competencies to pass the industry certification tests. There are dozens of cybersecurity training providers that are not affiliated with colleges or universities that provide training to prepare students to pass various industry certifications classes. Most if not all provide training online, and many have physical locations for face-to-face classes at various locations in California (including but not limited to the SANS Institute, Fast Lane, LearnQuest, Global Knowledge, ONLC Training Centers, TechData, INFOSEC Institute, Executrain). These training providers tend to be for-profit companies affiliated with one or more industry vendors, and the cost for training ranges from hundreds to thousands of dollars.

ADDITIONAL PROGRAMS AND HIGH SCHOOL ENROLLMENT

Secondary Institutions Programs

To gain a broader understanding of the spectrum of programs serving students, data was gathered on career pathways that exist between community colleges, secondary schools (high schools) and regional occupational center programs (ROCPs), including both formal articulation agreements and informal partnerships and collaborations. The California Statewide Pathways Project is the clearinghouse for formal articulation agreements between occupational courses and programs at high schools, ROCPs, and colleges. Cybersecurity falls under the career path "Information Technology," where there are five disciplines: CIS/Computer Programming, IT Web Design, Web Design, IT Applications, and CIS Cisco/A+. The last two could be considered introductory coursework leading to a cybersecurity career.

Articulation Agreements

There are 140 formal articulation agreements between high schools and colleges registered with the California Statewide Pathways Project, 69 in CIS Cisco/A+ and 71 in IT Applications (Exhibit 32). The majority of these agreements exist in the regional areas of the Inland Empire (Riverside and San Bernardino counties) and the LA/Orange County region (Los Angeles and Orange counties).

Exhibit 32. Formal articulation agreements between regional secondary and postsecondary cybersecurity-related programs

Region	CIS Cisco/A+	IT Applications	Subtotal
Bay Area	10	11	21
Central	4	2	6
Greater Sacramento	5	11	16
Inland Empire	28	28	56
LA/Orange	19	16	35
San Diego/Imperial	2	3	5
South Central	1	0	1
Far North	0	0	0
Total	**69**	**71**	**140**

Source: California Statewide Career Pathways

ADDITIONAL PROGRAMS AND HIGH SCHOOL ENROLLMENT

The colleges with formal articulation agreements with high schools are listed in Exhibit 33. A complete list that identifies the corresponding high schools and ROCPs can be found in Appendix I: Inventory of Formal Articulations between Regional Secondary and Postsecondary Cybersecurity-related Programs.

Exhibit 33. Articulation agreements between colleges and high schools

Bay	Central	Greater Sacramento	Inland Empire	LA/Orange	San Diego Imperial	South Central	Far North
San Jose City College	Bakersfield College	Sacramento City College	Chaffey College	Los Angeles Pierce College	Imperial Valley College	Moorpark College	Yuba College
Santa Rosa Junior College	College of the Sequoias	Folsom Lake College	College of the Desert	Mt. San Antonio College	Palomar College		
College of San Mateo		Woodland College	Crafton Hills College	Saddleback College	Southwestern College		
Evergreen Valley College			Mt. San Jacinto College	Coastline College			
Los Medanos College			Riverside CCD	Golden West College			
Mission College			San Bernardino Valley College	Rio Hondo College			
Ohlone College							
Skyline College							
Solano College							

While articulated programs exist between secondary and postsecondary schools, it appears enrollment is low at the high school level. At California public high schools, IT-related coursework is not a part of the core curriculum, and falls under the broad course subject area of "other" along with elective courses such as yearbook and life skills.

There are a few cybersecurity-related introductory courses in the public high school curriculum—two courses that can be identified as cybersecurity related and four that could be considered possibly pre-cybersecurity. These six courses are taught at 521 high schools, which represents approximately 15% of all public high schools in California. For a list of the courses and their descriptions, see Appendix J: List of Cybersecurity-related and Pre-cybersecurity Secondary Courses at California Public High Schools.

ADDITIONAL PROGRAMS AND HIGH SCHOOL ENROLLMENT

Cybersecurity High School Enrollment

High school enrollment in cybersecurity-related coursework totaled 1,901 in 2016-2017 (Exhibit 34). In the same year, pre-cybersecurity enrollment totaled 23,216 for a combined total of 25,117. As total high school enrollment reached nearly 2 million that year, cybersecurity-related and pre-cybersecurity courses comprised only 1% of those enrollments.

Exhibit 34. Enrollment in high school cybersecurity-related and pre-cybersecurity courses

Course Name	Course Code	Number of Schools	Courses Taught	Number of UC/ CSU Courses	Total Enrollment
Cybersecurity Related		**82**	**163**	**29**	**1,901**
Network Engineering	4604	55	107	17	1,643
Network Security	4646	27	56	12	258
Pre-Cybersecurity		**439**	**1199**	**422**	**23,216**
Database Design and SQL Programming	4631	8	11	8	222
Computer Repair and Support	4633	121	319	15	2,971
Exploring Computer Science	4634	284	821	353	18,741
CTE AP Computer Science A	4641	26	48	46	1,282
Total		**521**	**1362**	**451**	**25,117**

Source: California Department of Education

Note: Data are from 2016-2017, the most recent year available.

High school enrollment in cybersecurity-related and pre-cybersecurity courses is low, which indicates the formal articulation agreements may not function effectively to bring high school students into a cybersecurity pathway to further education and training, and ultimately employment. However, in addition to formal articulation agreements, many less formal and informal partnerships and collaborations exist with high schools.

There are many industry partnerships with high schools (CISCO, Oracle, CompTIA, Microsoft) that exist outside of formal articulation agreements with postsecondary institutions. Other programs, such as the CyberPatriot program, aim to create interest in cybersecurity among high school students. High schools may also have cybersecurity-related clubs on campus with the same aim.

The California Cyberhub is a recent development with the goal of coordinating cybersecurity training efforts in California to decrease duplication of effort and confusion. Started in 2017, the California Cyberhub is an interagency and interdepartmental collaborative including representation from K-12, California Community Colleges, California State Universities, CompTIA, Hewlett Packard, Amazon, Bust Buy, California Department of Technology, California Office of Emergency Service, Governor's Office, and others. This new organization sponsors faculty professional development and training, summer "Cyber Camps" for students, and competitions held throughout the state. The competitions have the goal of preparing students to participate in national CyberPatriot defense competitions. To date, over 100 middle and high school teams are registered on the Cyberhub website. The Cyberhub also promotes and provides links to free online CompTIA training in "IT Fundamentals."

[29] California Cyberhub, 2016, accessed June 11, 2018, https://ca-cyberhub.org/.

SECTION IV: SURVEY OF EDUCATIONAL PROVIDERS

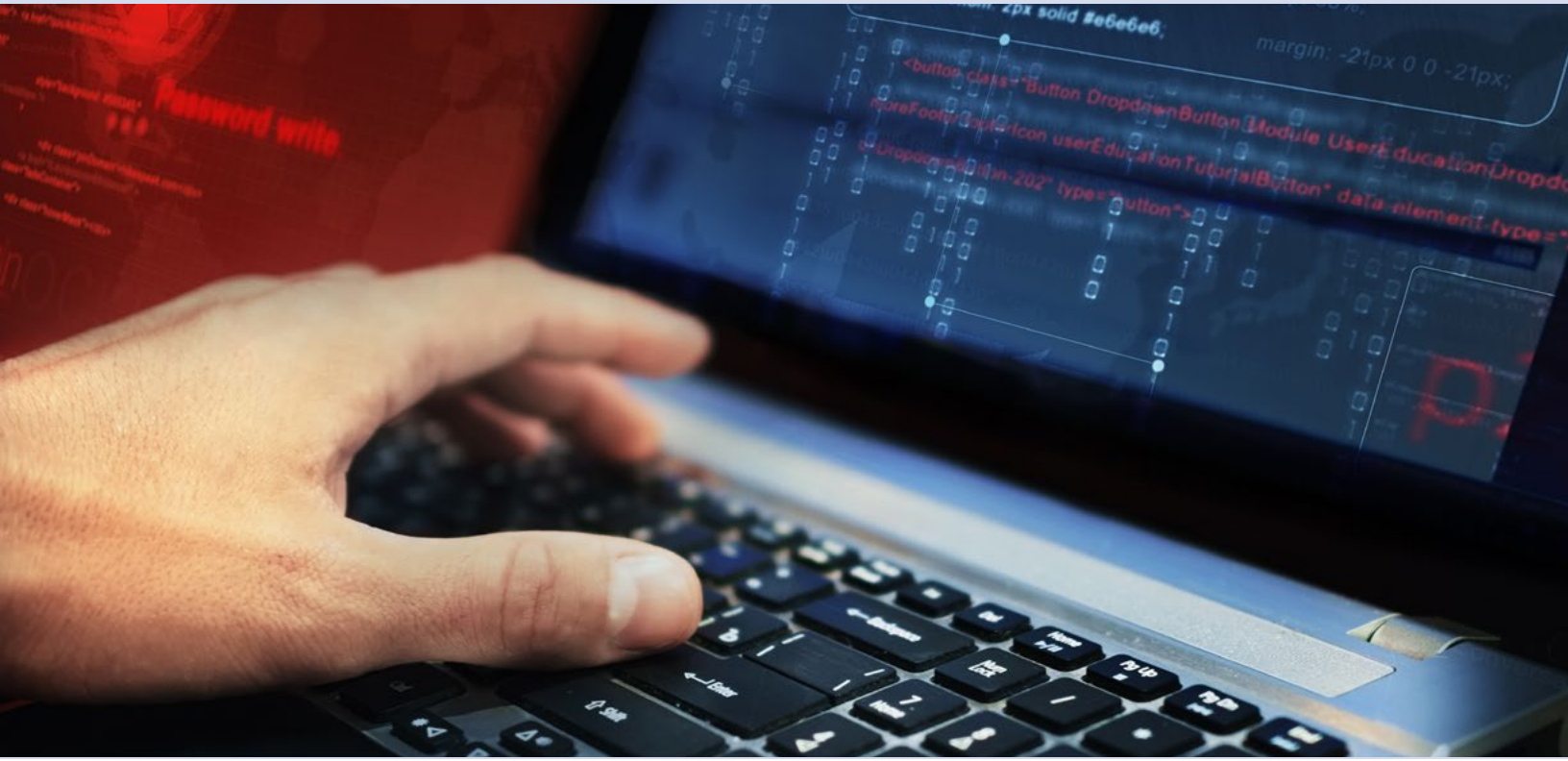
EDUCATIONAL PROVIDER CHARACTERISTICS

To glean additional information about cybersecurity programs offered by postsecondary institutions in California, a survey of postsecondary educational providers was conducted in spring 2018. Of the 242 institutions reporting to the U.S. Department of Education that they offer cybersecurity-related programs, 64 responded to the survey for an overall response rate of 26.4% (Exhibit 35). Seventy-five percent of responses were from community colleges, 24% were from four-year institutions and 1% was from a county office of education. Institutions with more focused cybersecurity programs were targeted for follow up, resulting in a higher response rate from that group. Survey feedback was received from 37.5% of programs characterized as "cybersecurity focused." Appendix K contains the survey questions sent to educational institutions.

Exhibit 35. Survey response rates by cybersecurity programming

	Number of Institutions with Programs*	Total Responses	Response Rate
Cybersecurity Focused	40	15	37.5%
Includes Cybersecurity	99	35	35.4%
Likely Includes Cybersecurity	233	63	27.0%
Unduplicated Overall Response Rate	**242**	**64**	**26.4%**

*There is duplication of institutions between cybersecurity program categories, as many institutions offer awards in multiple categories.



PROGRAM DEVELOPMENT

In utilizing the NICE Cybersecurity Framework, postsecondary institutions with cybersecurity-related programs were asked which of the seven NICE categories (interpreted here as program concentrations) were offered through their programs. Nearly two-thirds of respondents indicated they offered programs in "Operate and Maintain," while half have programs in "Protect and Defend" (Exhibit 36). Nearly half offer programs in "Investigate" and "Analyze," approximately one third in "Securely Provision," and one quarter offer programming in "Collect and Operate" and "Oversee and Govern."

Respondents also were asked whether they intended to develop programs in the NICE program concentration areas. Nearly half indicate they plan to develop programs in "Collect and Operate," which is the area where the fewest institutions report having programs in place. Conversely, one-fifth indicate they are considering developing programs in "Operate and Maintain," which is the concentration area with the highest proportion of respondents indicating they already have programs. Between a quarter and nearly a half of respondents indicated they do not have programs, and do not plan to develop programs, in the following concentration areas (listed in order of frequency of response): Oversee and Govern, Securely Provision, Collect and Operate, and Analyze.

Exhibit 36. Programmatic majors, concentrations, certificates or coursework/ training related to NICE Cybersecurity Workforce Framework

Program Concentration	Yes (program currently exists)	No (program does not exist; no plans to develop)	No, but we are considering developing one	Count
Securely Provision (includes: Risk Management; Software Development; Systems Architecture; Technology R&D; Systems Requirements Planning; Test and Evaluation; Systems Development)	31.2%	36.1%	32.8%	61
Operate and Maintain (includes: Data Administration; Knowledge Management; Customer Service and Technical Support; Network Services; Systems Administration; Systems Analyst)	63.9%	16.4%	19.7%	61
Oversee and Govern (includes: Legal Advice and Advocacy; Training, Education and Awareness; Cybersecurity Management; Strategic Planning and Policy; Executive Cyber Leadership; Program/Project Management and Acquisition)	24.6%	42.6%	32.8%	61
Protect and Defend (includes: Cyber Defense Analysis; Cyber Defense Infrastructure Support; Incident Response; Vulnerability Assessment and Management)	50.8%	13.1%	36.1%	61
Analyze (includes: Threat Analysis; Exploitation Analysis; All-Source Analysis; Targets; Language Analysis)	42.6%	24.6%	32.8%	61
Collect and Operate (includes: Collection Operations; Cyber Operational Planning; Cyber Operations)	26.2%	31.2%	42.6%	61
Investigate (includes: Cyber Investigation; Digital Forensics)	45.9%	14.8%	39.3%	61

PROGRAM DEVELOPMENT

Postsecondary institutions that indicated they were considering developing new cybersecurity programs were asked an open-ended question: What challenges are you facing as you consider adding/developing a new program or coursework/ training? The majority of responses fell into a few main categories: finding qualified instructors, curriculum development, budget, physical resources, and program marketing.

Here are a few illustrative quotes:

- Lack of qualified instructors. Lack of in-the-field-experienced instructors.
- Lack of space, talent and money.
- Funding for physical labs, funding for instructor training, program promotion.
- Small program minimally funded with limited time to complete curriculum development.
- Determining which coursework and training will result in a greater likelihood of our students finding employment.
- The lengthy curriculum approval process makes it difficult to respond quickly to industry and technology change.
- Marketing the program to the community to gain enrollment.

CYBERSECURITY CERTIFICATIONS

Because industry certifications are often required for job preparation, the survey asked postsecondary institutions which certifications are included in their cybersecurity-related programs. The majority of respondents prepare students for CompTIA Security+ and Security+ industry certifications (Exhibit 37). Other frequently cited industry certifications include: Certified Ethical Hacker, CISCO Certified Network Associate Security, and Microsoft Certified System Administrator.

Exhibit 37. Industry certifications for which cybersecurity programs train students

Certification	Number Responding	Percent
CompTIA Security +	41	64.1%
Security +	33	51.6%
Certified Ethical Hacker (CEH)	27	42.2%
CISCO Certificated Network Associate Security (CCNA-S)	20	31.3%
Microsoft Certified System Administrator (MCSA)	15	23.4%
Other, please specify (Note: see table footnote)	14	21.9%
CompTIA Cybersecurity Analyst (CySA+)	10	15.6%
CompTIA PenTest+	10	15.6%
Certified Information Systems Security Professional (CISSP)	9	14.1%
Cisco CCNA Cyber Ops	9	14.1%
Palo Alto Networks Firewall	8	12.5%
CISCO Certified Network Professional Security (CCNP-S)	4	6.3%
CompTIA Network+	4	6.3%
CompTIA Advanced Security Practitioner (CASP)	3	4.7%
Certified Information Systems Auditor (CISA)	2	3.1%
EC-Council Certified Security Analyst (ECSA)	2	3.1%
Offensive Security Certified Professional (OSCP)	2	3.1%
Department of Defense Directive 8140 (Security Clearance)	1	1.6%
SANS/GIAC Certification	1	1.6%
Certified Information Security Manager (CISM)	1	1.6%
Certified in Risk and Information Systems Control (CRISC)	1	1.6%
GIAC Penetration Tester (GPEN)	1	1.6%
Jupiter Networks Certification Program (JNCP) Junos Security Certification	1	1.6%
Palo Alto Networks Endpoint	0	0.0%

Note: The following certifications were identified in the "other" category:

CompTIA IT Fundamentals
Server+
Computer Hacking Forensic Investigator (CHFI)
ccsp, aws
IACIS, A+, CPCT, CFOT, CCENT
Computer Hacking Forensic Investigator(C|HFI), Systems Security Certified Practitioner (SSCP)
Cyber Program still under development and will include Python Security + Forensics + CyberLaw
FTK Computer Forensics – Certification ACE
Certified Network Forensic Investigator

SOFT SKILLS

Cybersecurity employers often consider soft skills when conducting hiring. The survey asked postsecondary institutions which soft skills were emphasized in their cybersecurity coursework and training. The most frequently cited soft skills include: problem solving, ethics, troubleshooting, teamwork/collaboration, and communication skills (Exhibit 38).

Exhibit 38. Soft skills emphasized in cybersecurity coursework and training

Soft Skill	% (out of 64 surveys)	Number of Responses
Problem solving	73.4%	47
Ethics	65.6%	42
Troubleshooting	60.9%	39
Teamwork/collaboration	60.9%	39
Communication skills	57.8%	37
Writing	46.9%	30
Planning	39.1%	25
Self-starter	31.3%	20
Enthusiasm	31.3%	20
Building effective relationships	26.6%	17
Quick learner	25.0%	16
Quality assurance and control	23.4%	15
Total		**347**

Note: Respondents were requested to "mark all that apply."
Other soft skills noted by respondents in comment box:
Research
Hands on activities
Proactive development of domain language skills
Networking with industry professionals
Documentation
Critical thinking skills

EMPLOYER INVOLVEMENT

Career education (CE) programs at postsecondary institutions generally include some form of employer involvement, with the intent of better aligning curriculum with workforce needs. The survey asked postsecondary institutions in California with cybersecurity-related programming how they involve employers in their programs.

Exhibit 39 shows the responses, including "other" comments, which are included below the table. The most common roles of employers are: participation on advisory board(s), provision of information about the industry and jobs, internships for students, and guest lectures.

Exhibit 39. Employer involvement in cybersecurity programs

Involvement	% (out of 64 surveys)	Count
Employers participate on my advisory board(s)	65.6%	42
Employers provide information about the industry and jobs	51.6%	33
Employers provide internships for my students	46.9%	30
Employers act as guest lecturers	42.2%	27
Employers offer facilities tours	37.5%	24
Employers donate equipment to my program	23.4%	15
Total		**171**

Other, provided in comment box:
Provide phone consultations
Sponsor club activities; provide promotional giveaways; provide scholarships to conferences
Potential employers provide feedback on our curriculum. We are looking to formalize an advisory board just for cyber security curriculum.
Support, participate and fund cyber security competitions

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

APPENDIX A: CALIFORNIA CYBERSECURITY LABOR MARKET SURVEY METHODOLOGY

Questionnaire Design

A questionnaire was designed with input from the California Cybersecurity Labor Market Study Research Advisory Committee, formed and convened by the COE for this research project. Prior to data collection, the questionnaire was reviewed and approved by the GO-Biz Leadership team, State and Federal Partners, as well as CASCADE (California Advanced Supply Chain & Diversification Effort) Industry Partners.

The survey utilized nine work roles associated with common cybersecurity occupations identified in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.[31] The nine work roles 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.

Of the nine cybersecurity work roles selected for this study, five were considered specialized cybersecurity work roles and the other four were considered information technology/information systems (IT/IS) work roles requiring cybersecurity skills. COE believed that it would be important to gather data for both work role groups, in order to better understand the range of workforce needs and challenges employers are facing related to finding qualified cybersecurity workers.

Specialized Cybersecurity Work Roles

1. Systems Security Analyst
2. Cyber Defense Analyst
3. Cyber Defense Infrastructure Support Specialist
4. Vulnerability Assessment Analyst
5. Cyber Defense Forensics Analyst

Information Technology/Information Systems (IT/IS) Work Roles Requiring Cybersecurity Skills

1. Technical Support Specialist
2. Network Operations Specialist
3. System Administrator
4. Software Developer

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

APPENDIX A: CALIFORNIA CYBERSECURITY LABOR MARKET SURVEY METHODOLOGY

Data Collection

Once the survey was finalized, Davis Research programmed the survey to collect the responses using a web questionnaire. Two recruitment strategies were utilized to drive respondents to the survey:

Phone Recruitment: Davis Research recruited respondents by telephone in accordance with the sampling plan specifications. Each potential respondent was screened for qualification criteria prior to being offered a survey link. The efforts included initial phone calls, reminder calls, email invites, and reminder emails. When a respondent only partially completed the survey, Davis Research sent reminders to those who started the survey, but hadn't finished it.

Online Campaign: An online survey link was created to inform potential participants about the project and encourage them to sign up to participate in the study. The GO-BIZ and CASCADE Partners forwarded the link to its networks.

Universe and Sample

To better understand who is employing the nine work roles selected for this study, firms across all major industry groups were sampled. Davis Research contacted a sample of firms in California based on the distribution of firms by industry NAICS code (North American Industry Classification System), as represented in the "% of Sample Ordered" column in the chart below. The chart also shows in the "Total %" column the distribution by industry of the 2,105 California businesses screened for this study. During the phone screening phase, Davis Research identified those businesses who employ cybersecurity workers or IT/IS workers who need cybersecurity skills to perform their job. These firms are in the "YES" column in the chart below and are categorized by major industry group.

Of the firms screened, 678 of the 2,105 firms (32%) qualified for the study. Of the 678 employers who qualified for the study, 385 completed the online survey and their data was analyzed for this report.

NAICS	No	Yes	TOTAL	Total %	% of Sample Ordered
11 – Agriculture, Forestry, Fishing and Hunting	45	13	58	3%	3%
23 – Construction	75	17	92	4%	5%
31–33 – Manufacturing	165	36	201	10%	9%
42 – Wholesale Trade	56	19	75	4%	4%
44–45 – Retail Trade	123	42	165	8%	13%
48 – Transportation	39	9	48	2%	1%
51 – Information	140	230	370	18%	14%
52 – Finance and Insurance	103	33	136	6%	7%
53 – Real Estate and Rental and Leasing	50	14	64	3%	4%
54 – Professional, Scientific, and Technical Services	241	115	356	17%	12%
56 – Administrative and Support and Waste Management and Remediation Services	78	23	101	5%	7%
61 – Educational Services	26	16	42	2%	3%
62 – Health Care and Social Assistance	79	27	106	5%	5%
71 – Arts, Entertainment, and Recreation	64	23	87	4%	2%
72 – Accommodation and Food Services	37	14	51	2%	2%
81 – Other Services	86	20	106	5%	4%
92 – Public Administration	20	27	47	2%	4%
Total	**1,427**	**678**	**2,105**	**100%**	**100%**

APPENDIX B: CALIFORNIA CYBERSECURITY LABOR MARKET SURVEY

California Cybersecurity Labor Market Analysis (Cascade Project 2)

California Community Colleges, Center of Excellence for Labor Market Research

Screener Questions

State

Is your business/organization located in California?

1. Yes [CONTINUE]
2. Outside of CA [TERMINATE]

A. In what California county are you physically located?

1. Confirm CA County [CONTINUE]
2. Outside of CA [TERMINATE]

B. Do you employ Cybersecurity and/or Information Technology (IT)/Information Systems (IS) workers who require some level of cybersecurity skills?

1. Yes [CONTINUE TO D]
2. No [CONTINUE TO C]

Do you plan to hire any Cybersecurity and/or IT/IS workers in the next 12 months?

1. Yes [CONTINUE TO D]
2. No [TERMINATE]

C. Are you familiar with current employment numbers, work roles and hiring criteria for cybersecurity and/or IT/IS workers at your organization?

1. Yes [CONTINUE TO REST OF SURVEY]
2. No [TERMINATE]

Industry Demographic Questions

1. What industry is your firm most closely associated with? (Select only one)

- Mining and Logging
- Construction
- Manufacturing
- Agriculture
- Wholesale Trade
- Retail Trade
- Transportation, Warehousing & Utilities
- Information (including Information Technology, Information Systems, ISP providers, Software Publishers, Telecommunications, Cable, Motion Pictures, Newspapers, Data Hosting)
- Finance and Insurance
- Real Estate and Rental and Leasing
- Professional, Scientific and Technical Services (including Legal, Accounting, Tax Services, Design Services, Research and Development)
- Administrative and Support and Waste Services
- Educational Services

Workforce definitions to be provided to respondent in on-line version as they answer this question—via mouse-over and/or pop-up screen:

- **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.
- **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.

APPENDIX B: CALIFORNIA CYBERSECURITY LABOR MARKET SURVEY

(continued)

- Health Care and Social Assistance
- Arts, Entertainment and Recreation
- Accommodation and Food Services
- Federal Government
- State Government
- Local Government
- Other _____ (open ended response)

2. Does your business/organization operate cybersecurity as an information systems/technology function or a business risk management function?

1. Information Systems/Technology
2. Business Risk Management
3. Both
4. Other, please specify _____.

3. How is your business/organization involved with cybersecurity? (Select all that apply)

A. Creator/producer of cybersecurity products

B. Provider of cybersecurity products and/or services, including management, testing, risk assessments and other services

C. User of cybersecurity products and services

D. Other involvement with cybersecurity, please specify: _____

ASK IF Q3 = A

4. What percent of your business/organization is focused on creating/producing cybersecurity products?

A. Fewer than 10%
B. 10 to 25%
C. 26 to 50%
D. 51 to 75%
E. 76 to 99%
F. 100%

ASK IF Q3 = B

5. What percent of your business/organization is focused on providing cybersecurity products and/or services?

A. Fewer than 10%
B. 10 to 25%
C. 26 to 50%
D. 51 to 75%
E. 76 to 99%
F. 100%

ASK ALL

6. Is your business/organization a defense contractor (including first, second, third, fourth tier subcontractor)?

a. Yes b. No

7. Does your business/organization provide cybersecurity products and/or services to the defense industry?

a. Yes b. No

APPENDIX B: CALIFORNIA CYBERSECURITY LABOR MARKET SURVEY

Organization-Related Questions

8. **Including all full-time and part-time employees, how many permanent employees work at your location?**
   A. [RECORD #_____]

9. **If you currently have [TAKE Q8 #] full-time and part-time permanent employees at your business/organization location, how many more or less permanent employees do you expect to have at your location 12 months from now?**
   A. More [RECORD #_____]
   B. Less [RECORD #_____]
   C. [DON'T READ] Same number of permanent employees

[IF AMOUNT DIFFERS BY 10% OR MORE IN EITHER DIRECTION, ASK:]

To confirm, you currently have ____ permanent employees and you expect to have _____ (more/less) employees, for a total of ____ permanent employees 12 months from now.

Work Role Related Questions

10. **For the following set of questions, we would like for you to try to equate your business/organization's specific position titles with the more general work roles. The titles used in the survey may differ from the specific titles used in your organization. Please tell us if your business/organization employs, at your location, individuals in positions matching the following work roles:**

Here's the (first/next) one: _____ [READ/DISPLAY BRIEF DEFINITION OF WORK ROLE, THEN ASK]:

Do you have employees who fit this description at your business/organization?
   A. Yes [MOVE TO NEXT WORK ROLE]
   B. No [MOVE TO NEXT WORK ROLE; IF RESPONDENT SAYS "NO" TO ALL WORK ROLES, SKIP TO 25]

Work Roles that CA Employers will be asked about are from the NICE Cybersecurity Workforce Framework

Technical Support Specialist: provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (e.g., master incident management plan, when applicable).

Network Operations Specialist: plans, implements, and operates network services/systems, including hardware and virtual environments.

System Administrator: installs, configures, troubleshoots, and maintains hardware and software and administers system accounts.

Software Developer: develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Systems Security Analyst: responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

Cyber Defense Analyst: uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Cyber Defense Infrastructure Support Specialist: tests, implements, deploys, maintains, and administers the infrastructure hardware and software.

APPENDIX B: CALIFORNIA CYBERSECURITY LABOR MARKET SURVEY

Vulnerability Assessment Analyst: performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

Cyber Defense Forensics Analyst: analyzes digital evidence and investigates computer security incidents to derive information in support of system/network vulnerability mitigation.

Next, I'm going to ask you a few questions about the Work Roles you have at your business/organization.

[Respondent will answer questions 11-20 or questions 11-24 (depending on the Work Role), for a maximum of 3 Work Roles they currently employ. The 3 work roles selected will be randomly selected based on which roles have the least amount of ratings for the study]

11. For [INSERT WORK ROLE], how many individuals do you have at your business/organization who are currently employed in permanent positions or as temporary workers (e.g., contractors, independent contractors, consultants, non-permanent employees, contract workers, temporary staff, per project workers) either full-time or part-time?

	Permanent Positions	Temporary Workers	TOTAL
Work Role	### (3-digit number)	### (3-digit number)	

[CREATE INTERNAL CONTROL SO THAT TOTAL WORK ROLES (Q11) IS LESS THAN TOTAL (Q8)]

12. How many more or less employees or temporary workers (e.g., contractors, independent contractors, consultants, non-permanent employees, contract workers, temporary staff, per project workers) do you estimate will be employed either full-time or part-time as a [INSERT WORK ROLE], 12 months from now.

	Permanent Positions	Temporary Workers	TOTAL
Work Role	### (3-digit number)	### (3-digit number)	

[IF AMOUNT DIFFERS BY 10% OR MORE IN EITHER DIRECTION, ASK:] Just to confirm, you currently have ____ [INSERT WORK ROLE] and you expect to have _____ (more/less), for a total of ____ [INSERT WORK ROLE] 12 months from now.

13. Does your business/organization have no difficulty, some difficulty or great difficulty finding qualified candidates for [INSERT WORK ROLE]?

	No difficulty	Some difficulty	Great difficulty	DK/NA
Work Role	1	2	3	4

ASK IF Q13 = Some or Great Difficulty

14. When facing difficulty hiring qualified candidates for [INSERT WORK ROLE], how did your business/organization respond?

A. Did not fill the position
B. Increased recruitment effort
C. Increased overtime with current employees to accommodate workload
D. Increased wages to attract or retain current employees
E. NA/ DK
F. Other, please specify: _____

APPENDIX B: CALIFORNIA CYBERSECURITY LABOR MARKET SURVEY

15. What issues or challenges does your business/organization face in hiring for [INSERT WORK ROLE]? (Select all that apply)

A. Lack of qualified candidates with necessary security clearances
B. Candidates lack required educational attainment
C. Candidates lack relevant work experience
D. Candidates lack required technology skills
E. Lack of qualified candidates in general
F. Other, please specify: _____

16. What is the minimum education required for qualified candidates for [INSERT WORK ROLE]?

A. No formal educational credential
B. High school diploma or equivalent
C. Some college, no degree
D. Associate degree
E. Bachelor's degree
F. Master's degree or higher
G. DK/NA

17. What is the minimum prior work experience required for qualified candidates for [INSERT WORK ROLE].

A. None
B. Less than 1 year
C. 1 to 2 years
D. 3 to 5 years
E. 6 or more years

18. What are the top three soft skills that are most important for [INSERT WORK ROLE] (Select only 3)

A. Communication skills
B. Writing
C. Troubleshooting
D. Teamwork/collaboration
E. Ethics
F. Planning
G. Problem solving
H. Building effective relationships
I. Quality assurance and control
J. Self-starter
K. Enthusiasm
L. Quick learner
M. Bilingual
N. Other, please specify: _____

19. How important is a security certification when hiring for [INSERT WORK ROLE]?

1. Not important
2. Somewhat important
3. Important
4. Very important
5. DK/NA

ASK IF 19 = Important or Very Important

APPENDIX B: CALIFORNIA CYBERSECURITY LABOR MARKET SURVEY

20. For [INSERT WORK ROLE], which certifications are preferred? (Select all that apply)

A. Certified Information Systems Security Professional (CISSP)
B. CISCO Certified Network Associate (CCNA)
C. CISCO Certified Network Professional (CCNP)
D. Microsoft Certified System Administrator (MCSA)
E. Network + Certified
F. Security +
G. Security Clearance
H. SANS/GIAC Certification
I. Certified Information Systems Auditor (CISA)
J. Certified Information Security Manager (CISM)
K. Other, please specify: _____

*For Q. 21-24, only ask for the 4 occupations listed below that are **IS/IT Technician Work Roles from NICE Workforce Framework.***

1. Technical Support Specialist
2. Network Operations Specialist
3. Systems Administrator
4. Software Developer

21. On average, what percentage of time within the overall job duties for [INSERT WORK ROLE] are spent on security/cybersecurity issues?

A. None at all
B. Less than 10%
C. 10 to 25%
D. 26 to 50%
E. 51 to 75%
F. 76 to 99%
G. 100%
H. Don't know

22. On average, has the percentage of time spent by [INSERT WORK ROLE] on security/cybersecurity issues increased, compared to the percentage of time spent 12 months ago?

1.Yes
2. No (SKIP TO 24)

ASK IF Q22 = Yes

23. What was the increase in the percentage of time spent by [INSERT WORK ROLE] on security/cybersecurity issues?

A. Less than 10%
B. 10 to 25%
C. 26 to 50%
D. 51 to 75%
E. 76 to 99%
F. 100%
G. Don't know

APPENDIX B: CALIFORNIA CYBERSECURITY LABOR MARKET SURVEY

24. How important is it for [INSERT WORK ROLE] to possess each of the following cybersecurity skills to perform their job?

(Note: list of skills for each work role below is from NICE Cybersecurity Workforce Framework)

Technical Support Specialist (give definition here)

Skill 1: Identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.

1. Not important
2. Somewhat important
3. Important
4. Very important
5. DK/NA

Skill 2: Using the appropriate tools for repairing software, hardware, and peripheral equipment of a system. (Insert Scale)

Skill 3: Designing incident response for cloud service models. (Insert Scale)

Skill 4: Accurately defining incidents, problems, and events in the trouble ticketing system. (Insert Scale)

Network Operations Specialist (give definition here)

Skill 1: Implementing, maintaining, and improving established network security practices. (Insert Scale)

Skill 2: Securing network communications. (Insert Scale)

Skill 3: Protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters). (Insert Scale)

Skill 4: Configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems). (Insert Scale)

Skill 5: Implementing and testing network infrastructure contingency and recovery plans. (Insert Scale)

Skill 6: Configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate). (Insert Scale)

Systems Administrator (give definition here)

Skill 1: Configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware). (Insert Scale)

Skill 2: Accurately define incidents, problems, and events in the trouble ticketing system. (Insert Scale)

Skill 3: Applying cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (Insert Scale)

Skill 4: Establishing and maintaining automated security control assessments. (Insert Scale)

APPENDIX B: CALIFORNIA CYBERSECURITY LABOR MARKET SURVEY

Software Developer (give definition here)

Skill 1: Conducting vulnerability scans and recognizing vulnerabilities in security systems. (Insert Scale)

Skill 2: Designing countermeasures to identified security risks. (Insert Scale)

Skill 3: Developing and applying security system access controls. (Insert Scale)

Skill 4: Discerning the protection needs (i.e., security controls) of information systems and networks. (Insert Scale)

Skill 5: Secure test plan design (e. g. unit, integration, system, acceptance). (Insert Scale)

Skill 6: Using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). (Insert Scale)

Skill 7: Applying cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation). (Insert Scale)

Closing Questions

25. For which of the following would you like to be contacted by your region's education and training institutions? (i.e. community colleges, four year colleges, other education/training providers) (Check all that apply)

A. To arrange cybersecurity skills training for your current workers
B. To provide internship experiences and/or apprenticeships for students
C. To hire or recruit from education and training institutions
D. To advise education and training institutions on curriculum development
E. To provide scholarships for students
F. To speak to students about careers in cybersecurity
G. To provide job shadowing and/or host an industry tour/field trip for students
H. To fund a hackathon for students to participate in and compete for prizes
I. Other, please specify: _____
J. I am not interested in being contacted.

26. This survey is being led by the California Governor's Office of Business and Economic Development (GO-Biz) in partnership with the California Community Colleges, Center of Excellence for Labor Market Research. GO-Biz serves as California's single point of contact for economic development and job creation efforts, and provides free assistance to businesses in California such as site selection services, permit assistance, regulatory guidance, business expansion support, international trade development and general small business support.

Are you interested in receiving information on GO-Biz business assistance programs, or on business cybersecurity workshops, training and seminars led by Partners*?

Yes [CONTINUE TO F1]
No [SKIP TO CLOSING OF SURVEY]

APPENDIX B: CALIFORNIA CYBERSECURITY LABOR MARKET SURVEY

F1. California Governor's Office of Business and Economic Development (GO-Biz)
Link: http://www.business.ca.gov

Check any that you would like more information for:

- ❑ Site-selection services
- ❑ Permit assistance
- ❑ Regulatory guidance
- ❑ Business expansion support
- ❑ International trade development
- ❑ Small business and innovation support
- ❑ Cybersecurity
- ❑ Other, please specify: _____

CASCADE Partners*

Check any that you would like more information for:

❑ Cyber physical security for Manufacturers
Led by: California Manufacturing Technology Consulting (CMTC) Link: https://www.cmtc.com

❑ Defense supply chain resiliency seminars
Led by East San Diego County Economic Development Council Link: http://eastcountyedc.org

❑ Defense supply chain workshops
Led by California Community Colleges Small Business Sector Navigators Link: http://smallbusinesssector.net/

❑ Commercial, government, or international contracting 101 training
Led by California Community Colleges Small Business Sector Navigators Link: http://smallbusinesssector.net/

❑ Procurement opportunities workshops for underrepresented businesses Link:
Led by Nehemiah Community Foundation Link: https://nehemiahcorp.org/

❑ Entrepreneurial skills development training
Led by Cal State University San Bernardino, Inland Empire Center for Entrepreneurship (IECE) Link: http://iece.csusb.edu

*Partners as per the CASCADE U.S. Department of Defense grant. For additional CASCADE partner information, visit business.ca.gov/CASCADE.

ASK if Q25 A-I is selected OR Q26=YES

Please provide your contact information below:

Name: _____

Organization: _____

Email: _____

Phone: _____

APPENDIX C: CYBERSECURITY LABOR MARKET ANALYSIS RESEARCH ADVISORY GROUP MEMBERS

Advisory Group Members

Brian Hom
Cybersecurity Analyst
San Diego Supercomputer Center
UC San Diego

Lou Rabon
Founder and CEO
Cyber Defense Group
Los Angeles, CA

Stephen Monteros
Vice President
ConvergeOne
Ontario, CA

Steve Linthicum, JD, CISSP
Interim Project Director
Cybersecurity Apprenticeship Program
Coastline Community College

Richard Grotegut
Deputy Sector Navigator
Information and Communications Technologies
Bay Region Community Colleges

Barbara Sirotnik
Director
Institute of Applied Research and Policy Analysis
California State University, San Bernardino
CASCADE Supply Chain Mapping and Analysis Components
(Project #4)

Additional Cybersecurity Subject Matter Experts Supporting the Cybersecurity Labor Market Analysis:

Marian Merritt
Lead for Industry Engagement
National Initiative for Cybersecurity Education
National Institute of Standards and Technology

Bill Newhouse
Deputy Director
National Initiative for Cybersecurity Education
National Institute of Standards and Technology

Noel Kyle
Cybersecurity Education and Awareness Branch
U.S. Department of Homeland Security

APPENDIX D: WORK ROLE PROFILES

Technical Support Specialist - California, 2018

Provides technical support to customers who need assistance utilizing client level hardware and software in accordance with established or approved organizational process components. (i.e., Master Incident Management Plan, when applicable).

NICE Framework Category: Operate and Maintain

Specialty Area: Customer Service and Technical Support

Total Employer Survey Repsonses
129

Permanent jobs

10,369 Current jobs → **+351** (3% Increase in the next 12 months)

Temporary jobs

4,289 Current jobs → **+642** (15% Increase in the next 12 months)

84% of employers reported having the **Technical Support Specialist** work role

Employers said...

Education & Work Experience

40% Bachelor's degree

and

47% 1 to 2 years of experience

Soft Skills

44% Problem Solving

37% Troubleshooting

37% Communication Skills

Certifications

35% Microsoft Certified System Administrator (MCSA)

35% Certified Information Security Manager (CISM)

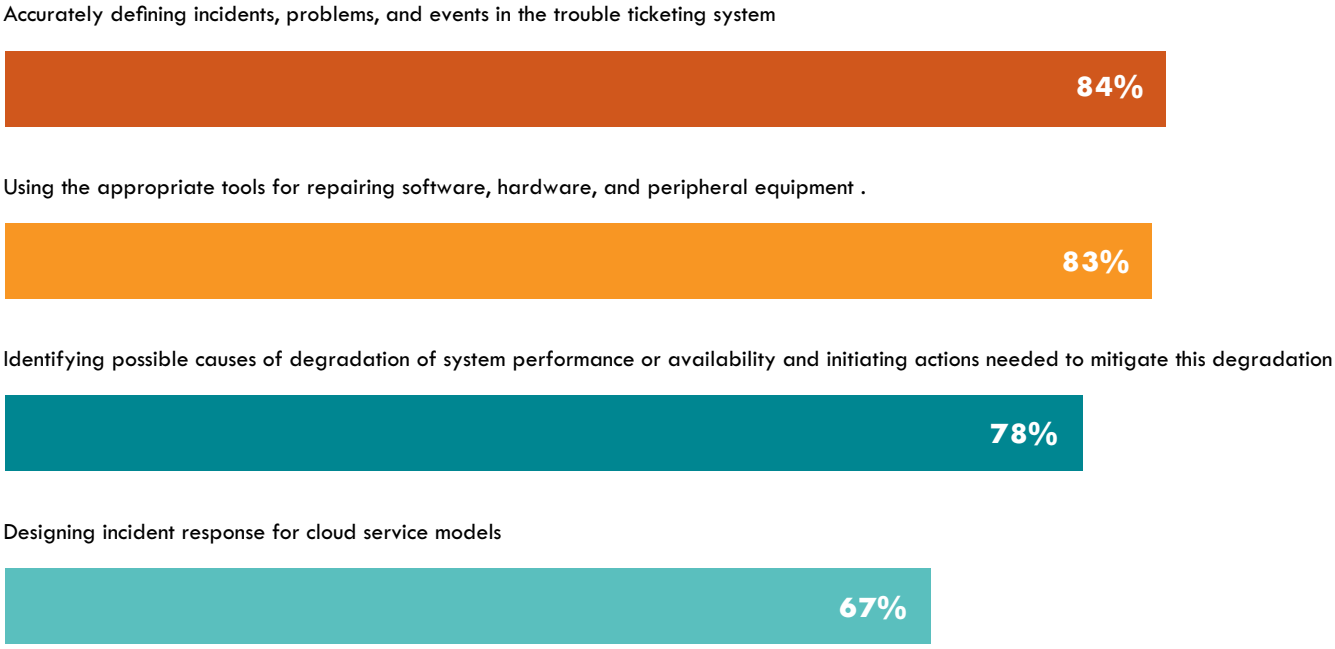
55% of Technical Support Specialists spend **more than a quarter of their time** on cybersecurity issues.

57% of employers said the amount of **time spent** on cybersecurity issues has increased compared to **12 months ago**.

APPENDIX D: WORK ROLE PROFILES

Cybersecurity skills Technical Support Specialist must possess to perform their job.

(combined percent of employers that said each skill was very important or important)



APPENDIX D: WORK ROLE PROFILES

Network Operations Specialist - California, 2018

Plans, implements, and operates network services/systems, including hardware and virtual environments.

NICE Framework Category: Operate and Maintain

Specialty Area: Network Services

Total Employer Survey Repsonses
121

Permanent jobs

8,848 Current jobs → **+848**

10% Increase in the next 12 months

Temporary jobs

4,332 Current jobs → **+364**

8% Increase in the next 12 months

81% of employers reported having the **Network Operations Specialist** work role

Employers said...

Education & Work Experience

51% Bachelor's degree

and

43% 1 to 2 years of experience

Soft Skills

52% Problem Solving

43% Troubleshooting

33% Teamwork/Collaboration

Certifications

51% Certified Network Professional (CCNP)

43% Certified Network Associate (CCNA)

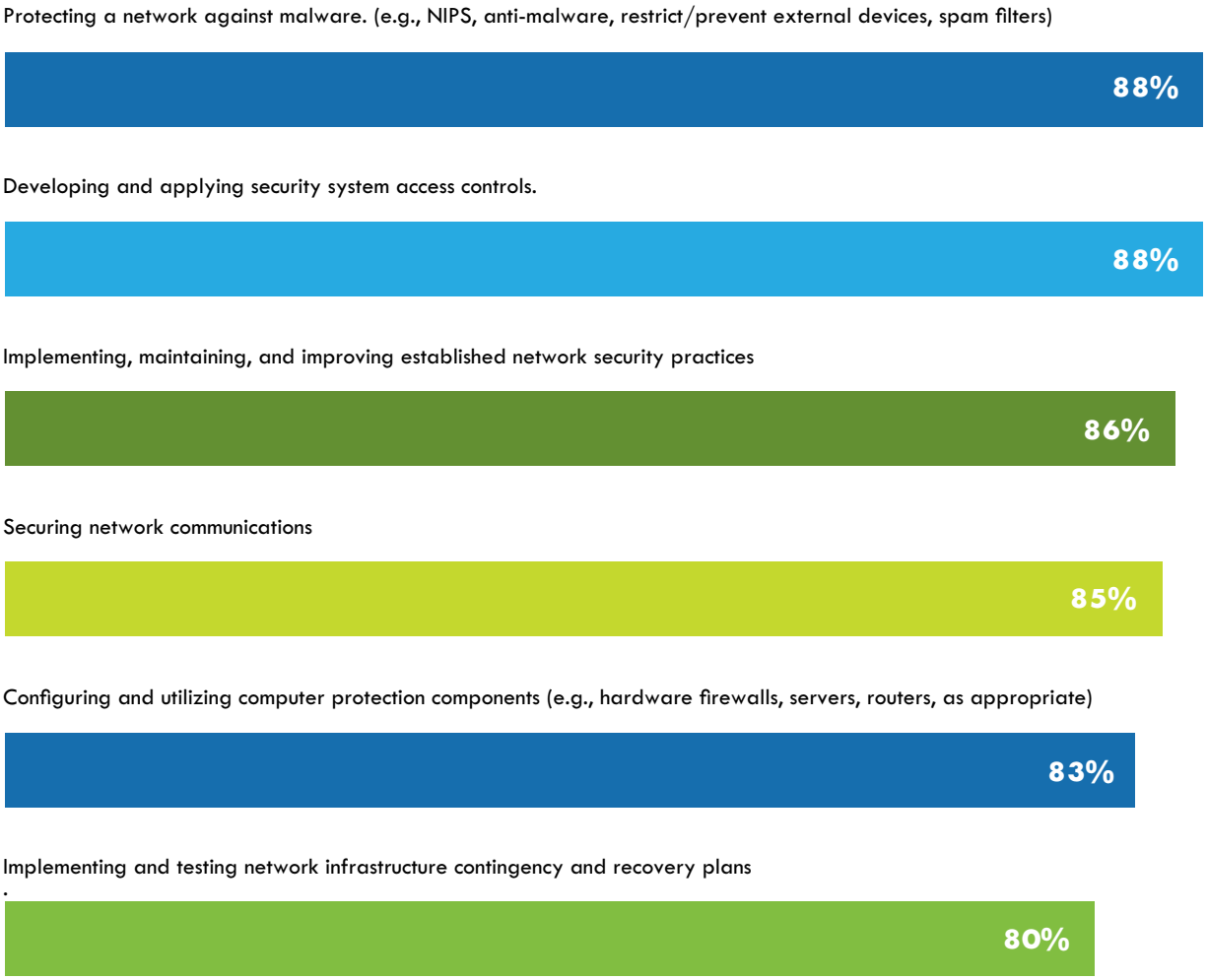
56% of Network Operations Specialists spend **more than a quarter of their time** on cybersecurity issues.

65% of employers said the amount of **time spent** on cybersecurity issues has increased compared to **12 months ago**.

APPENDIX D: WORK ROLE PROFILES

Cybersecurity skills Network Operations Specialist must possess to perform their job.

(combined percent of employers that said each skill was very important or important)



APPENDIX D: WORK ROLE PROFILES

System Administrator - California, 2018

Installs, configures, troubleshoots, and maintains hardware and software and administers system accounts.

NICE Framework Category: Operate and Maintain

Specialty Area: Systems Administration

Total Employer Survey Repsonses
127

Permanent jobs

7,627 Current jobs → **+1,128**

15% Increase in the next 12 months

Temporary jobs

2,596 Current jobs → **+697**

27% Increase in the next 12 months

89% of employers reported having the **System Administrator** work role

Employers said...

Education & Work Experience

44% Bachelor's degree

and

48% 1 to 2 years of experience

Soft Skills

52% Problem Solving

38% Troubleshooting

32% Communication Skills

Certifications

55% Microsoft Certified System Administrator (MCSA)

39% Certified InformationSecurity Manager (CISM)

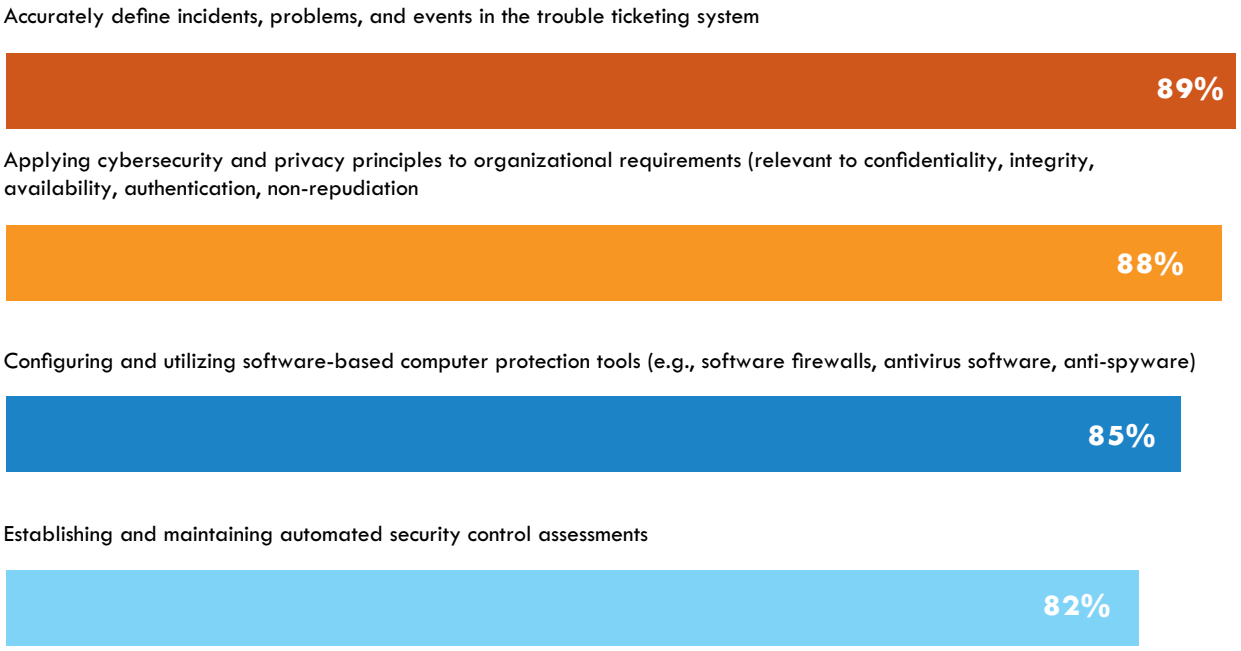
56% of System Administrators spend **more than a quarter of their time** on cybersecurity issues.

65% of employers said the amount of **time spent** on cybersecurity issues has increased compared to **12 months ago**.

APPENDIX D: WORK ROLE PROFILES

Cybersecurity skills System Administrator must possess to perform their job.

(combined percent of employers that said each skill was very important or important)



APPENDIX D: WORK ROLE PROFILES

Software Developer - California, 2018

Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

NICE Framework Category: Securely Provision

Specialty Area: Software Development

Total Employer Survey Repsonses
123

Permanent jobs

18,509 Current jobs → **+571** (3%) Increase in the next 12 months

Temporary jobs

4,166 Current jobs → **+309** (7%) Increase in the next 12 months

77% of employers reported having the **Software Developer** work role

Employers said...

Education & Work Experience

54% Bachelor's degree

and

42% 1 to 2 years of experience

Soft Skills

55% Problem Solving

41% Teamwork/Collaboration

Certifications

49% Microsoft Certified System Administrator (MCSA)

36% CISCO Certified Network Associate (CCNA)

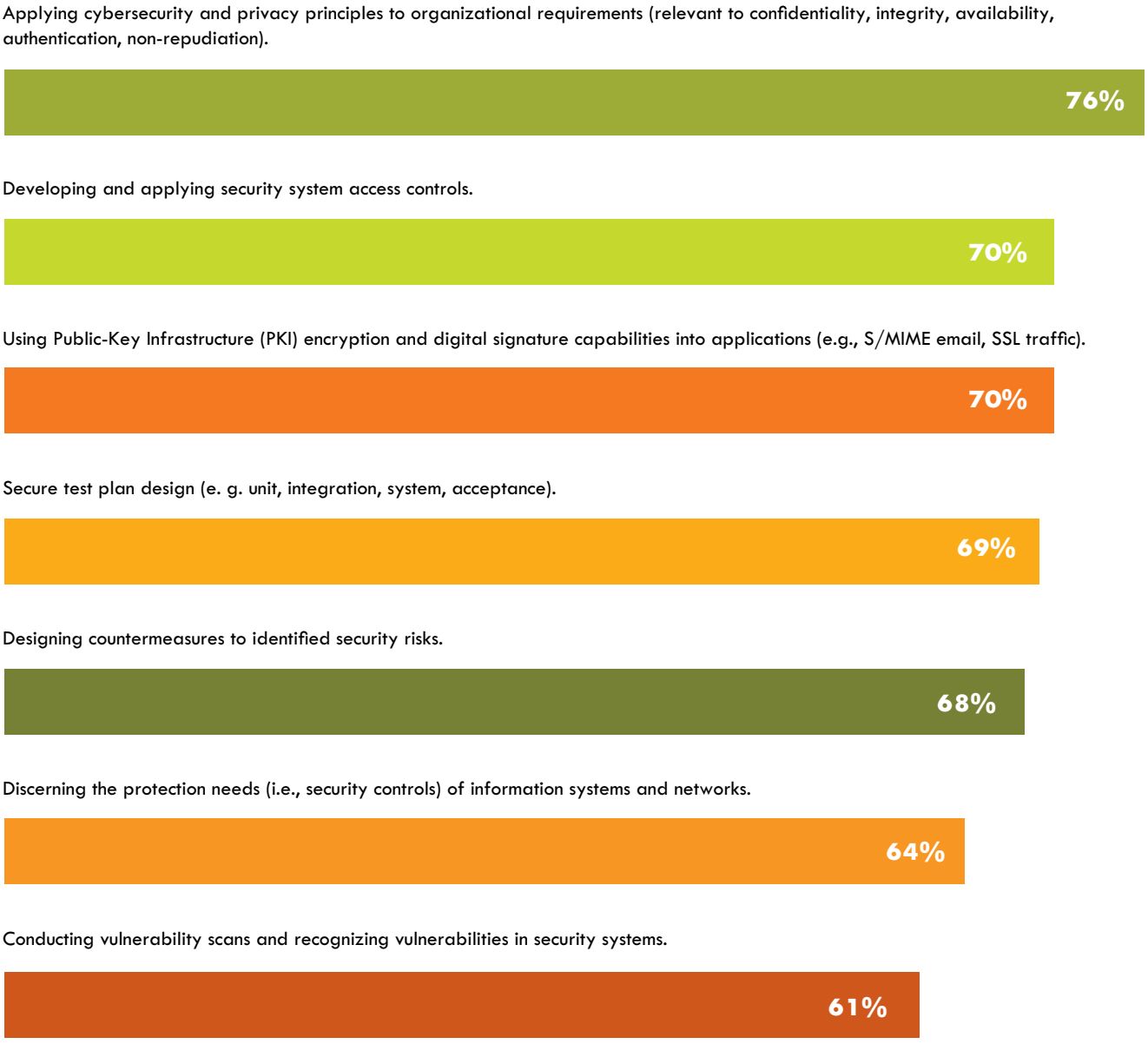
52% of Software Developers spend **more than a quarter of their time** on cybersecurity issues.

65% of employers said the amount of **time spent** on cybersecurity issues has increased compared to **12 months ago**.

APPENDIX D: WORK ROLE PROFILES

Cybersecurity skills Software Developer must possess to perform their job.

(combined percent of employers that said each skill was very important or im-portant)



APPENDIX D: WORK ROLE PROFILES

Systems Security Analyst - California, 2018

Responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

NICE Framework Category: Operate and Maintain

Specialty Area: Systems Analysis

Total Employer Survey Repsonses
112

Permanent jobs

11,082 Current jobs → **+1,679**

15% Increase in the next 12 months

Temporary jobs

4,141 Current jobs → **+735**

18% Increase in the next 12 months

77% of employers reported having the **System Security Analyst** work role

Employers said...

Education & Work Experience

58% Bachelor's degree

and

45% 3 to 5 years of experience

Soft Skills

46% Problem Solving

38% Teamwork/Collaboration

31% Quality Assurance & Control

Certifications

43% Certified Information Systems Secutiry Professional (CISSP)

42% CISCO Certified Network Associate (CCNA)

42% Microsoft Certified System Administrator (MCSA)

APPENDIX D: WORK ROLE PROFILES

Cyber Defense Analyst - California, 2018

Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

NICE Framework Category: Protect and Defend

Specialty Area: Cyber Defense Analysis

Total Employer Survey Repsonses
118

Permanent jobs

10,019 Current jobs → **+921** (9% Increase in the next 12 months)

Temporary jobs

6,145 Current jobs → **+350** (6% Increase in the next 12 months)

69% of employers reported having the **Cyber Defense Analyst** work role

Employers said...

Education & Work Experience

47% Bachelor's degree

and

44% 3 to 5 years of experience

Soft Skills

47% Problem Solving

44% Troubleshooting

Certifications

47% CISCO Certified Network Professional (CCNP)

41% Microsoft Certified System Administrator (MCSA)

40% CISCO Certified Network Associate (CCNA)

APPENDIX D: WORK ROLE PROFILES

Cyber Defense Infrastructure Support Specialist

- California, 2018

Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.

NICE Framework Category: Protect and Defend

Specialty Area: Cyber Defense Infrastructure Support

Total Employer Survey Repsonses
112

Permanent jobs

6,578 Current jobs → **+1,403** (**21%** Increase in the next 12 months)

Temporary jobs

3,501 Current jobs → **+743** (**21%** Increase in the next 12 months)

72% of employers reported having the **Cyber Defense Infrastructure Support Specialist** work role

Employers said...

Education & Work Experience

51% Bachelor's degree

and

39% 3 to 5 years of experience

Soft Skills

53% Problem Solving

45% Troubleshooting

39% Teamwork/Collaboration

Certifications

44% Certified Information Systems Security Professional (CISSP)

42% Microsoft Certified System Administrator (MCSA)

41% CISCO Certified Network Professional (CCNP)

APPENDIX D: WORK ROLE PROFILES

Vulnerability Assessment Analyst - California, 2018

Performs assessments of systems and networks within the network environmentor enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense.

NICE Framework Category: Protect and Defend

Specialty Area: Vulnerability Assessment and Management

Total Employer Survey Repsonses
119

Permanent jobs

13,477 Current jobs → **+824**

6% Increase in the next 12 months

Temporary jobs

3,712 Current jobs → **+421**

11% Increase in the next 12 months

66% of employers reported having the **Cyber Defense Infrastructure Support Specialist** work role

Employers said...

Education & Work Experience

40% Bachelor's degree

and

42% 1 to 2 years of experience

Soft Skills

46% Problem Solving

33% Communication Skills

Certifications

41% CISCO Certified Network Associate (CCNA)

40% Microsoft Certified System Administrator (MCSA)

40% Certified Information Systems Security Professional (CISSP)

APPENDIX D: WORK ROLE PROFILES

Cyber Defense Forensics Analyst - California, 2018

Analyzes digital evidence and investigates computer security incidents to derive information in support of system/network vulnerability mitigation.

NICE Framework Category: Investigate

Specialty Area: Digital Forensics

Total Employer Survey Repsonses
109

Permanent jobs

15,784 Current jobs → **+1,704** → **11%** Increase in the next 12 months

Temporary jobs

5,509 Current jobs → **+632** → **12%** Increase in the next 12 months

59% of employers reported having the **Cyber Defense Forensics Analyst** work role

Employers said...

Education & Work Experience

48% Bachelor's degree

and

40% 1 to 2 years of experience

Soft Skills

38% Problem Solving

30% Comminication Skills

Certifications

48% Microsoft Certified System Administrator (MCSA

40% Certified Information Systems Security Professional (CISSP))

37% CISCO Certified Network Professional (CCNP)

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Cybersecurity Focused		**27**	**5**	**16**	**0**	**4**	**0**	**7**	**2**	**0**	**61**
City College of San Francisco	Bay Area	1	0	1	0	0	0	0	0	0	2
College of San Mateo	Bay Area	1	1	1	0	0	0	0	0	0	3
Contra Costa College	Bay Area	1	0	0	0	0	0	0	0	0	1
Foothill College	Bay Area	1	0	0	0	0	0	0	0	0	1
Fresno City College	Bay Area	1	0	0	0	0	0	0	0	0	1
Gavilan College	Bay Area	1	0	1	0	0	0	0	0	0	2
Los Medanos College	Bay Area	1	1	1	0	0	0	0	0	0	3
Naval Postgraduate School	Bay Area	0	0	0	0	0	0	2	2	0	4
Ohlone College	Bay Area	1	0	0	0	0	0	0	0	0	1
University of San Francisco	Bay Area	0	0	0	0	0	0	1	0	0	1
Mt San Jacinto Community College District	Inland Empire/ Desert Region	1	0	0	0	0	0	0	0	0	1
Azusa Pacific University	Los Angeles/Orange County	0	0	0	0	1	0	0	0	0	1
Charter College-Canyon Country	Los Angeles/Orange County	0	1	0	0	0	0	0	0	0	1
Citrus College	Los Angeles/Orange County	1	0	0	0	0	0	0	0	0	1
Coastline Community College	Los Angeles/Orange County	1	0	1	0	0	0	0	0	0	2
Cypress College	Los Angeles/Orange County	1	0	0	0	0	0	0	0	0	1
Learnet Academy Inc	Los Angeles/Orange County	1	0	0	0	0	0	0	0	0	1
Long Beach City College	Los Angeles/Orange County	1	0	0	0	0	0	0	0	0	1
Mt San Antonio College	Los Angeles/Orange County	0	0	1	0	0	0	0	0	0	1
Mt Sierra College	Los Angeles/Orange County	0	0	0	0	1	0	0	0	0	1
Santa Ana College	Los Angeles/Orange County	1	0	0	0	0	0	0	0	0	1
University of Southern California	Los Angeles/Orange County	0	0	0	0	0	0	1	0	0	1
West Los Angeles College	Los Angeles/Orange County	1	0	0	0	0	0	0	0	0	1
California Miramar University	San Diego/Imperial	1	0	0	0	0	0	0	0	0	1
Coleman University	San Diego/Imperial	0	0	1	0	1	0	0	0	0	2
Imperial Valley College	San Diego/Imperial	1	0	1	0	0	0	0	0	0	2
National University	San Diego/Imperial	0	0	0	0	0	0	1	0	0	1
San Diego City College	San Diego/Imperial	1	0	1	0	0	0	0	0	0	2
Southwestern College	San Diego/Imperial	1	1	1	0	0	0	0	0	0	3
University of San Diego	San Diego/Imperial	0	0	0	0	0	0	2	0	0	2
Cuesta College	South Central Coast	0	1	1	0	0	0	0	0	0	2
Santa Barbara City College	South Central Coast	0	0	1	0	0	0	0	0	0	1
Columbia College	Central California	1	0	0	0	0	0	0	0	0	1
American River College	Far North	1	0	1	0	0	0	0	0	0	2
Asher College	Far North	1	0	0	0	0	0	0	0	0	1
Cosumnes River College	Far North	1	0	1	0	0	0	0	0	0	2

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016) (continued)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Cybersecurity Focused (continued)											
Sacramento City College	Far North	1	0	1	0	0	0	0	0	0	2
Shasta College	Far North	1	0	0	0	0	0	0	0	0	1
Sierra College	Far North	1	0	1	0	0	0	0	0	0	2
University of Phoenix - California	N/A	0	0	0	0	1	0	0	0	0	1
Includes Aspects of Cybersecurity		**105**	**41**	**66**	**0**	**20**	**0**	**19**	**5**	**2**	**258**
Berkeley City College	Bay Area	1	0	0	0	0	0	0	0	0	1
California State University-East Bay	Bay Area	0	0	0	0	0	0	1	0	0	1
City College of San Francisco	Bay Area	2	0	0	0	0	0	0	0	0	2
Cogswell College	Bay Area	0	0	0	0	1	0	0	0	0	1
College of Marin	Bay Area	0	0	1	0	0	0	0	0	0	1
College of San Mateo	Bay Area	0	0	1	0	0	0	0	0	0	1
Contra Costa College	Bay Area	2	0	1	0	0	0	0	0	0	3
De Anza College	Bay Area	2	2	2	0	0	0	0	0	0	6
Diablo Valley College	Bay Area	1	1	1	0	0	0	0	0	0	3
Foothill College	Bay Area	1	0	3	0	0	0	0	0	0	4
Fresno City College	Bay Area	2	1	2	0	0	0	0	0	0	5
Gavilan College	Bay Area	1	0	1	0	0	0	0	0	0	2
Golden Gate University-San Francisco	Bay Area	1	0	0	0	1	0	1	0	0	3
Las Positas College	Bay Area	1	0	1	0	0	0	0	0	0	2
Los Medanos College	Bay Area	1	1	1	0	0	0	0	0	0	3
Merritt College	Bay Area	1	0	0	0	0	0	0	0	0	1
Mission College	Bay Area	2	1	1	0	0	0	0	0	0	4
Naval Postgraduate School	Bay Area	0	0	0	0	0	0	2	2	0	4
Ohlone College	Bay Area	2	1	1	0	0	0	0	0	0	4
San Jose City College	Bay Area	2	1	2	0	0	0	0	0	0	5
Santa Clara University	Bay Area	0	0	0	0	1	0	0	0	0	1
Santa Rosa Junior College	Bay Area	2	1	0	0	0	0	0	0	0	3
Skyline College	Bay Area	0	1	1	0	0	0	0	0	0	2
Solano Community College	Bay Area	0	1	1	0	0	0	0	0	0	2
University of San Francisco	Bay Area	0	0	0	0	1	0	1	0	0	2
Chaffey College	Inland Empire/ Desert Region	2	1	0	0	0	0	0	0	0	3
Moreno Valley College	Inland Empire/ Desert Region	1	0	0	0	0	0	0	0	0	1
Mt San Jacinto Community College District	Inland Empire/ Desert Region	2	2	0	0	0	0	0	0	0	4
Norco College	Inland Empire/ Desert Region	1	0	0	0	0	0	0	0	0	1

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016) (continued)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Includes Aspects of Cybersecurity (continued)											
Riverside City College	Inland Empire/ Desert Region	3	0	0	0	0	0	0	0	0	3
University of Redlands	Inland Empire/ Desert Region	0	1	0	0	0	0	0	0	0	1
ABCO Technology	Los Angeles/ Orange County	3	0	0	0	0	0	0	0	0	3
Advanced Computing Institute	Los Angeles/ Orange County	0	0	1	0	0	0	0	0	0	1
Brand College	Los Angeles/ Orange County	2	0	0	0	0	0	0	0	0	2
California Career School	Los Angeles/ Orange County	1	0	0	0	0	0	0	0	0	1
California Intercontinental University	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	1	2
Cerritos College	Los Angeles/ Orange County	1	0	1	0	0	0	0	0	0	2
Citrus College	Los Angeles/ Orange County	1	0	1	0	0	0	0	0	0	2
Coastline Community College	Los Angeles/ Orange County	2	0	2	0	0	0	0	0	0	4
Cypress College	Los Angeles/ Orange County	2	0	0	0	0	0	0	0	0	2
East Los Angeles College	Los Angeles/ Orange County	1	0	0	0	0	0	0	0	0	1
Fullerton College	Los Angeles/ Orange County	1	0	0	0	0	0	0	0	0	1
Glendale Community College	Los Angeles/ Orange County	2	0	1	0	0	0	0	0	0	3
Irvine Valley College	Los Angeles/ Orange County	1	0	1	0	0	0	0	0	0	2
Long Beach City College	Los Angeles/ Orange County	3	1	2	0	0	0	0	0	0	6
Los Angeles City College	Los Angeles/ Orange County	3	0	0	0	0	0	0	0	0	3
Los Angeles Pierce College	Los Angeles/ Orange County	2	0	1	0	0	0	0	0	0	3
Loyola Marymount University	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
Mt San Antonio College	Los Angeles/ Orange County	1	0	2	0	0	0	0	0	0	3
Mt Sierra College	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
PCI College	Los Angeles/ Orange County	1	0	0	0	0	0	0	0	0	1
Pepperdine University	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
Saddleback College	Los Angeles/ Orange County	2	0	1	0	0	0	0	0	0	3

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016) (continued)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Includes Aspects of Cybersecurity (continued)											
Santa Ana College	Los Angeles/ Orange County	2	0	0	0	0	0	0	0	0	2
Santa Monica College	Los Angeles/ Orange County	0	1	1	0	0	0	0	0	0	2
Trident University International	Los Angeles/ Orange County	0	0	0	0	0	0	1	1	0	2
University of California-Irvine	Los Angeles/ Orange County	0	0	0	0	1	0	1	0	1	3
University of Southern California	Los Angeles/ Orange County	0	0	0	0	0	0	2	0	0	2
Vanguard University of Southern California	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
West Los Angeles College	Los Angeles/ Orange County	2	2	2	0	0	0	0	0	0	6
Ashford University	San Diego/Imperial	0	0	0	0	1	0	0	0	0	1
California Miramar University	San Diego/Imperial	1	0	0	0	0	0	0	0	0	1
Coleman University	San Diego/Imperial	0	0	1	0	1	0	1	0	0	3
Cuyamaca College	San Diego/Imperial	0	1	1	0	0	0	0	0	0	2
Grossmont College	San Diego/Imperial	3	3	3	0	0	0	0	0	0	9
MiraCosta College	San Diego/Imperial	1	1	2	0	0	0	0	0	0	4
National University	San Diego/Imperial	1	0	0	0	2	0	4	0	0	7
Palomar College	San Diego/Imperial	2	1	2	0	0	0	0	0	0	5
Point Loma Nazarene University	San Diego/Imperial	0	0	0	0	1	0	0	0	0	1
San Diego City College	San Diego/Imperial	1	0	0	0	0	0	0	0	0	1
Southwestern College	San Diego/Imperial	1	1	1	0	0	0	0	0	0	3
Allan Hancock College	South Central Coast	1	0	1	0	0	0	0	0	0	2
Antelope Valley College	South Central Coast	1	1	1	0	0	0	0	0	0	3
California Lutheran University	South Central Coast	0	0	0	0	0	0	2	0	0	2
College of the Canyons	South Central Coast	1	1	1	0	0	0	0	0	0	3
Cuesta College	South Central Coast	1	0	0	0	0	0	0	0	0	1
Laurus College	South Central Coast	1	0	0	0	0	0	0	0	0	1
Moorpark College	South Central Coast	1	1	1	0	0	0	0	0	0	3
Oxnard College	South Central Coast	1	1	1	0	0	0	0	0	0	3
Santa Barbara City College	South Central Coast	0	1	1	0	0	0	0	0	0	2
Ventura Adult and Continuing Education	South Central Coast	0	2	0	0	0	0	0	0	0	2
Modesto Junior College	Central California	1	0	0	0	0	0	0	0	0	1
Reedley College	Central California	1	0	1	0	0	0	0	0	0	2
San Joaquin Delta College	Central California	1	0	1	0	0	0	0	0	0	2
West Hills College-Lemoore	Central California	1	0	0	0	0	0	0	0	0	1

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016) (continued)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Includes Aspects of Cybersecurity (continued)											
American River College	Far North	3	0	2	0	0	0	0	0	0	5
Asher College	Far North	1	2	2	0	0	0	0	0	0	5
College of the Redwoods	Far North	0	1	1	0	0	0	0	0	0	2
Cosumnes River College	Far North	2	0	1	0	0	0	0	0	0	3
Folsom Lake College	Far North	2	0	0	0	0	0	0	0	0	2
MTI College	Far North	1	0	1	0	0	0	0	0	0	2
Sacramento City College	Far North	2	3	1	0	0	0	0	0	0	6
Shasta College	Far North	2	1	1	0	0	0	0	0	0	4
Sierra College	Far North	1	0	1	0	0	0	0	0	0	2
Yuba College	Far North	1	0	0	0	0	0	0	0	0	1
Computer Training Academy	N/A	1	0	0	0	0	0	0	0	0	1
DeVry University-California	N/A	0	0	1	0	1	0	2	2	0	6
Institute of Technology	N/A	0	1	0	0	0	0	0	0	0	1
University of Phoenix-California	N/A	2	0	1	0	4	0	1	0	0	8
Likely Includes Cybersecurity		**229**	**126**	**272**	**2**	**137**	**1**	**65**	**8**	**18**	**858**
Academy of Art University	Bay Area	0	0	1	1	2	0	1	1	0	6
Argosy University-San Francisco Bay Area	Bay Area	0	0	1	0	1	0	0	0	0	2
Argosy University-The Art Institute of California-San Francisco	Bay Area	0	1	1	0	1	0	0	0	0	3
Argosy University-The Art Institute of California-Silicon Valley	Bay Area	0	1	1	0	1	0	0	0	0	3
Berkeley City College	Bay Area	2	1	3	0	0	0	0	0	0	6
Cabrillo College	Bay Area	3	3	4	0	0	0	0	0	0	10
California State University-East Bay	Bay Area	0	0	0	0	1	0	1	0	0	2
California State University-Monterey Bay	Bay Area	0	0	0	0	2	0	0	0	0	2
Canada College	Bay Area	1	0	1	0	0	0	0	0	0	2
Chabot College	Bay Area	1	0	4	0	0	0	0	0	0	5
City College of San Francisco	Bay Area	4	0	2	0	0	0	0	0	0	6
Cogswell College	Bay Area	0	0	0	0	1	0	0	0	0	1
College of Alameda	Bay Area	1	0	1	0	0	0	0	0	0	2
College of Marin	Bay Area	2	0	2	0	0	0	0	0	0	4
College of San Mateo	Bay Area	1	1	3	0	0	0	0	0	0	5
Contra Costa College	Bay Area	2	0	2	0	0	0	0	0	0	4
De Anza College	Bay Area	3	3	4	0	0	0	0	0	0	10
Diablo Valley College	Bay Area	3	1	3	0	0	0	0	0	0	7

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016) (continued)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Likely Includes Cybersecurity (continued)											
Evergreen Valley College	Bay Area	0	0	1	0	0	0	0	0	0	1
Foothill College	Bay Area	1	0	4	0	0	0	0	0	0	5
Fresno City College	Bay Area	2	0	1	0	0	0	0	0	0	3
Gavilan College	Bay Area	2	0	3	0	0	0	0	0	0	5
Golden Gate University-San Francisco	Bay Area	1	0	0	0	2	0	2	1	0	6
Hartnell College	Bay Area	0	2	2	0	0	0	0	0	0	4
Holy Names University	Bay Area	0	0	0	0	2	0	0	0	0	2
International Technological University	Bay Area	0	0	0	0	0	0	1	0	0	1
Laney College	Bay Area	0	1	1	0	0	0	0	0	0	2
Las Positas College	Bay Area	2	0	3	0	0	0	0	0	0	5
Los Medanos College	Bay Area	1	1	1	0	0	0	0	0	0	3
Merritt College	Bay Area	1	0	1	0	0	0	0	0	0	2
Mills College	Bay Area	0	0	0	0	1	0	1	1	0	3
Mission College	Bay Area	1	0	2	0	0	0	0	0	0	3
Monterey Peninsula College	Bay Area	2	2	3	0	0	0	0	0	0	7
Napa Valley College	Bay Area	1	2	1	0	0	0	0	0	0	4
Naval Postgraduate School	Bay Area	0	0	0	0	0	0	4	1	2	7
Notre Dame de Namur University	Bay Area	0	0	0	0	1	0	1	0	0	2
Ohlone College	Bay Area	5	1	3	0	0	0	0	0	0	9
Pacific Union College	Bay Area	0	0	0	0	2	0	0	0	0	2
San Francisco State University	Bay Area	0	0	0	0	1	0	1	0	0	2
San Jose City College	Bay Area	2	2	3	0	0	0	0	0	0	7
San Jose State University	Bay Area	0	0	0	0	1	0	1	0	0	2
Santa Clara University	Bay Area	0	0	0	0	1	0	1	0	0	2
Santa Rosa Junior College	Bay Area	5	1	1	0	0	0	0	0	0	7
Skyline College	Bay Area	2	0	2	0	0	0	0	0	0	4
Solano Community College	Bay Area	1	1	2	0	0	0	0	0	0	4
Sonoma State University	Bay Area	0	0	0	0	1	0	0	0	0	1
Stanford University	Bay Area	0	0	0	0	1	0	1	0	1	3
University of California-Berkeley	Bay Area	0	0	0	0	1	0	2	0	2	5
University of California-San Francisco	Bay Area	0	0	0	0	0	0	1	0	1	2
University of California-Santa Cruz	Bay Area	0	0	0	0	5	0	1	0	1	7
University of San Francisco	Bay Area	0	0	0	0	2	0	3	0	0	5
West Valley College	Bay Area	2	0	4	0	0	0	0	0	0	6

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016) (continued)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Likely Includes Cybersecurity (continued)											
Argosy University-Inland Empire	Inland Empire/ Desert Region	0	0	1	0	1	0	0	0	0	2
Argosy University-The Art Institute of California-Inland Empire	Inland Empire/ Desert Region	0	1	0	0	1	0	0	0	0	2
Barstow Community College	Inland Empire/ Desert Region	1	0	1	0	0	0	0	0	0	2
California Baptist University	Inland Empire/ Desert Region	0	0	0	0	2	0	0	0	0	2
California State University-San Bernardino	Inland Empire/ Desert Region	0	0	0	0	2	0	1	0	0	3
Chaffey College	Inland Empire/ Desert Region	2	2	3	0	0	0	0	0	0	7
College of the Desert	Inland Empire/ Desert Region	0	1	2	0	0	0	0	0	0	3
Copper Mountain Community College	Inland Empire/ Desert Region	0	3	3	0	0	0	0	0	0	6
Crafton Hills College	Inland Empire/ Desert Region	2	0	2	0	0	0	0	0	0	4
La Sierra University	Inland Empire/ Desert Region	0	0	0	0	1	0	0	0	0	1
Mayfield College	Inland Empire/ Desert Region	1	0	0	0	0	0	0	0	0	1
Milan Institute-Palm Desert	Inland Empire/ Desert Region	0	1	0	0	0	0	0	0	0	1
Moreno Valley College	Inland Empire/ Desert Region	2	1	3	0	0	0	0	0	0	6
Mt San Jacinto Community College District	Inland Empire/ Desert Region	3	2	2	0	0	0	0	0	0	7
Norco College	Inland Empire/ Desert Region	3	2	3	0	0	0	0	0	0	8
Palo Verde College	Inland Empire/ Desert Region	3	0	1	0	0	0	0	0	0	4
Riverside City College	Inland Empire/ Desert Region	3	1	3	0	0	0	0	0	0	7
San Bernardino Valley College	Inland Empire/ Desert Region	3	1	1	0	0	0	0	0	0	5
University of California-Riverside	Inland Empire/ Desert Region	0	0	0	0	2	0	1	0	1	4
University of Redlands	Inland Empire/ Desert Region	0	0	0	0	2	0	1	0	0	3
Victor Valley College	Inland Empire/ Desert Region	1	0	1	0	0	0	0	0	0	2
ABCO Technology	Los Angeles/ Orange County	2	0	0	0	0	0	0	0	0	2
Advanced Computing Institute	Los Angeles/ Orange County	2	1	2	0	0	0	0	0	0	5
Allied American University	Los Angeles/ Orange County	3	0	1	0	1	0	0	0	0	5

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016) (continued)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Likely Includes Cybersecurity (continued)											
Argosy University-Los Angeles	Los Angeles/ Orange County	0	0	1	0	1	0	0	0	0	2
Argosy University-Orange County	Los Angeles/ Orange County	0	0	1	0	1	0	0	0	0	2
Argosy University-The Art Institute of California-Hollywood	Los Angeles/ Orange County	0	1	1	0	1	0	0	0	0	3
Argosy University-The Art Institute of California-Los Angeles	Los Angeles/ Orange County	0	1	1	0	1	0	0	0	0	3
Argosy University-The Art Institute of California-Orange County	Los Angeles/ Orange County	0	1	1	0	1	0	0	0	0	3
Art Center College of Design	Los Angeles/ Orange County	0	0	0	0	1	0	1	0	0	2
Azusa Pacific University	Los Angeles/ Orange County	0	0	0	0	1	0	1	0	0	2
Bethesda University	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
Biola University	Los Angeles/ Orange County	0	0	0	0	2	0	0	0	0	2
Brand College	Los Angeles/ Orange County	6	1	0	0	0	0	0	0	0	7
Brandman University	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
California Institute of Technology	Los Angeles/ Orange County	0	0	0	0	1	0	1	0	1	3
California Intercontinental University	Los Angeles/ Orange County	0	0	1	0	1	0	0	0	0	2
California State Polytechnic University-Pomona	Los Angeles/ Orange County	0	0	0	0	1	0	1	0	0	2
California State University-Dominguez Hills	Los Angeles/ Orange County	0	0	0	0	2	0	1	0	0	3
California State University-Fullerton	Los Angeles/ Orange County	0	0	0	0	1	0	2	0	0	3
California State University-Long Beach	Los Angeles/ Orange County	0	0	0	0	2	0	1	0	0	3
California State University-Los Angeles	Los Angeles/ Orange County	0	0	0	0	3	0	2	1	0	6
California State University-Northridge	Los Angeles/ Orange County	0	0	0	0	4	0	1	0	0	5
California University of Management and Sciences	Los Angeles/ Orange County	0	0	0	0	0	0	1	0	0	1
Cerritos College	Los Angeles/ Orange County	0	3	4	0	0	0	0	0	0	7
Chapman University	Los Angeles/ Orange County	0	0	0	0	2	0	1	0	0	3

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016) (continued)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Likely Includes Cybersecurity (continued)											
Claremont Graduate University	Los Angeles/ Orange County	0	0	0	0	0	0	1	1	1	3
Claremont McKenna College	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
Coastline Community College	Los Angeles/ Orange County	3	1	0	0	0	0	0	0	0	4
Cypress College	Los Angeles/ Orange County	5	1	3	0	0	0	0	0	0	9
East Los Angeles College	Los Angeles/ Orange County	3	0	1	0	0	0	0	0	0	4
East San Gabriel Valley Regional Occupational Program	Los Angeles/ Orange County	1	0	1	0	0	0	0	0	0	2
El Camino College-Compton Center	Los Angeles/ Orange County	0	0	1	0	0	0	0	0	0	1
El Camino Community College District	Los Angeles/ Orange County	2	2	2	0	0	0	0	0	0	6
Empire College	Los Angeles/ Orange County	0	1	1	0	0	0	0	0	0	2
Fremont College	Los Angeles/ Orange County	0	0	1	0	0	0	0	0	0	1
Fullerton College	Los Angeles/ Orange County	0	1	2	0	0	0	0	0	0	3
Glendale Community College	Los Angeles/ Orange County	2	3	3	0	0	0	0	0	0	8
Golden West College	Los Angeles/ Orange County	1	0	1	0	0	0	0	0	0	2
Harvey Mudd College	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
Irvine Valley College	Los Angeles/ Orange County	3	0	4	0	0	0	0	0	0	7
Learnet Academy Inc	Los Angeles/ Orange County	2	0	0	0	0	0	0	0	0	2
Long Beach City College	Los Angeles/ Orange County	3	3	3	0	0	0	0	0	0	9
Los Angeles City College	Los Angeles/ Orange County	1	1	2	0	0	0	0	0	0	4
Los Angeles Harbor College	Los Angeles/ Orange County	0	1	2	0	0	0	0	0	0	3
Los Angeles Mission College	Los Angeles/ Orange County	1	2	1	0	0	0	0	0	0	4
Los Angeles Pierce College	Los Angeles/ Orange County	3	0	1	0	0	0	0	0	0	4
Los Angeles Southwest College	Los Angeles/ Orange County	1	0	3	0	0	0	0	0	0	4
Los Angeles Trade Technical College	Los Angeles/ Orange County	0	1	1	0	0	0	0	0	0	2
Los Angeles Valley College	Los Angeles/ Orange County	2	1	1	0	0	0	0	0	0	4

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016) (continued)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Likely Includes Cybersecurity (continued)											
Loyola Marymount University	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
Mount Saint Mary's University	Los Angeles/ Orange County	0	0	1	0	0	0	0	0	0	1
Mt San Antonio College	Los Angeles/ Orange County	5	0	2	0	0	0	0	0	0	7
Mt Sierra College	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
Occidental College	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
Orange Coast College	Los Angeles/ Orange County	0	2	2	0	0	0	0	0	0	4
Pacific States University	Los Angeles/ Orange County	0	0	0	0	1	0	1	0	0	2
Palladium Technical Academy	Los Angeles/ Orange County	0	1	0	0	0	0	0	0	0	1
Pasadena City College	Los Angeles/ Orange County	3	0	3	1	0	0	0	0	0	7
Pepperdine University	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
Pitzer College	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
Pomona College	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
Rio Hondo College	Los Angeles/ Orange County	1	1	1	0	0	0	0	0	0	3
Saddleback College	Los Angeles/ Orange County	3	0	4	0	0	0	0	0	0	7
Santa Ana College	Los Angeles/ Orange County	5	2	2	0	0	0	0	0	0	9
Santa Monica College	Los Angeles/ Orange County	0	3	3	0	0	0	0	0	0	6
Santiago Canyon College	Los Angeles/ Orange County	3	0	2	0	0	0	0	0	0	5
Scripps College	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
Southern California Institute of Technology	Los Angeles/ Orange County	0	1	0	0	1	0	0	0	0	2
Stanbridge College	Los Angeles/ Orange County	1	0	1	0	1	0	0	0	0	3
The Master's University and Seminary	Los Angeles/ Orange County	0	0	0	0	2	0	0	0	0	2
Trident University International	Los Angeles/ Orange County	0	0	0	0	2	0	1	1	0	4
Unitek College	Los Angeles/ Orange County	1	0	0	0	0	0	0	0	0	1
University of California-Irvine	Los Angeles/ Orange County	0	0	0	0	3	0	2	0	2	7
University of California-Los Angeles	Los Angeles/ Orange County	0	0	0	0	1	0	2	0	2	5

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016) (continued)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Likely Includes Cybersecurity (continued)											
University of La Verne	Los Angeles/ Orange County	0	0	0	0	1	0	0	0	0	1
University of Southern California	Los Angeles/ Orange County	0	0	0	0	1	0	3	1	1	6
University of the People	Los Angeles/ Orange County	0	0	1	0	1	0	0	0	0	2
University of the West	Los Angeles/ Orange County	0	0	0	0	0	0	1	0	0	1
West Los Angeles College	Los Angeles/ Orange County	1	1	1	0	0	0	0	0	0	3
Advanced Training Associates	San Diego/Imperial	1	0	1	0	0	0	0	0	0	2
Argosy University-San Diego	San Diego/Imperial	0	0	1	0	1	0	0	0	0	2
Argosy University-The Art Institute of California-San Diego	San Diego/Imperial	0	1	0	0	1	0	0	0	0	2
Ashford University	San Diego/Imperial	0	0	0	0	1	0	0	0	0	1
Associated Technical College-San Diego	San Diego/Imperial	1	0	0	0	0	0	0	0	0	1
California College San Diego	San Diego/Imperial	0	0	4	0	3	0	0	0	0	7
California State University-San Marcos	San Diego/Imperial	0	0	0	0	1	0	1	0	0	2
Coleman University	San Diego/Imperial	0	0	3	0	3	0	0	0	0	6
Cuyamaca College	San Diego/Imperial	2	1	1	0	0	0	0	0	0	4
Grossmont College	San Diego/Imperial	1	2	2	0	0	0	0	0	0	5
Imperial Valley College	San Diego/Imperial	2	0	3	0	0	0	0	0	0	5
MediaTech Institute-Oceanside	San Diego/Imperial	0	2	0	0	0	0	0	0	0	2
MiraCosta College	San Diego/Imperial	5	0	3	0	0	0	0	0	0	8
National University	San Diego/Imperial	1	0	0	0	2	0	2	0	0	5
Palomar College	San Diego/Imperial	2	3	3	0	0	0	0	0	0	8
Platt College-San Diego	San Diego/Imperial	1	1	0	0	0	0	0	0	0	2
Point Loma Nazarene University	San Diego/Imperial	0	0	0	0	1	0	0	0	0	1
San Diego City College	San Diego/Imperial	3	1	1	0	0	0	0	0	0	5
San Diego Mesa College	San Diego/Imperial	3	1	2	0	0	0	0	0	0	6
San Diego Miramar College	San Diego/Imperial	2	1	1	0	0	0	0	0	0	4
San Diego State University	San Diego/Imperial	0	0	0	0	2	0	2	0	0	4
Southwestern College	San Diego/Imperial	5	3	7	0	0	0	0	0	0	15
University of California-San Diego	San Diego/Imperial	0	0	0	0	1	0	2	0	1	4
University of San Diego	San Diego/Imperial	0	0	0	0	1	0	0	0	0	1
Allan Hancock College	South Central Coast	1	0	2	0	0	0	0	0	0	3

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016) (continued)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Likely Includes Cybersecurity (continued)											
Antelope Valley College	South Central Coast	0	3	3	0	0	0	0	0	0	6
California Lutheran University	South Central Coast	0	0	0	0	2	1	1	0	0	4
California Polytechnic State University-San Luis Obispo	South Central Coast	0	0	0	0	1	0	1	0	0	2
California State University-Channel Islands	South Central Coast	0	0	0	0	2	0	1	0	0	3
College of the Canyons	South Central Coast	1	0	1	0	0	0	0	0	0	2
Cuesta College	South Central Coast	1	0	2	0	0	0	0	0	0	3
Laurus College	South Central Coast	1	1	2	0	0	0	0	0	0	4
Moorpark College	South Central Coast	1	1	2	0	0	0	0	0	0	4
Oxnard College	South Central Coast	0	1	1	0	0	0	0	0	0	2
Santa Barbara Business College-Ventura	South Central Coast	0	0	1	0	0	0	0	0	0	1
Santa Barbara City College	South Central Coast	0	1	2	0	0	0	0	0	0	3
University of California-Santa Barbara	South Central Coast	0	0	0	0	1	0	1	0	1	3
Westmont College	South Central Coast	0	0	0	0	1	0	0	0	0	1
Bakersfield College	Central California	0	3	3	0	0	0	0	0	0	6
California State University-Bakersfield	Central California	0	0	0	0	1	0	0	0	0	1
California State University-Fresno	Central California	0	0	0	0	1	0	1	0	0	2
California State University-Stanislaus	Central California	0	0	0	0	3	0	0	0	0	3
Cerro Coso Community College	Central California	1	2	3	0	0	0	0	0	0	6
Clovis Community College	Central California	1	0	2	0	0	0	0	0	0	3
College of the Sequoias	Central California	1	2	1	0	0	0	0	0	0	4
Columbia College	Central California	2	1	1	0	0	0	0	0	0	4
Merced College	Central California	0	0	2	0	0	0	0	0	0	2
Milan Institute-Visalia	Central California	0	1	0	0	0	0	0	0	0	1
Modesto Junior College	Central California	2	0	1	0	0	0	0	0	0	3
MTI Business College Inc	Central California	0	1	0	0	0	0	0	0	0	1
Porterville College	Central California	1	1	1	0	0	0	0	0	0	3
Reedley College	Central California	3	0	2	0	0	0	0	0	0	5
San Joaquin Delta College	Central California	2	1	2	0	0	0	0	0	0	5
San Joaquin Valley College-Visalia	Central California	0	1	2	0	0	0	0	0	0	3
Santa Barbara Business College-Bakersfield	Central California	0	0	2	0	0	0	0	0	0	2
Taft College	Central California	2	0	0	0	0	0	0	0	0	2
University of the Pacific	Central California	0	0	0	0	1	0	0	0	0	1

APPENDIX E: INVENTORY OF CYBERSECURITY PROGRAMS

Inventory of Cybersecurity (and Closely Related) Programs at Postsecondary Institutions in California, by Region (2016) (continued)

Educational Institution	Region	Award of less than 1 academic year	Award of at least 1 but less than 2 academic years	Associate degree	Award of 2 but less than 4 academic years	Bachelor's degree	Post-master's certificate	Master's degree	Post-baccalaureate certificate	Doctor's degree -- research/ scholarship	Grand Total
Likely Includes Cybersecurity (continued)											
West Hills College-Coalinga	Central California	1	0	1	0	0	0	0	0	0	2
West Hills College-Lemoore	Central California	1	0	1	0	0	0	0	0	0	2
American River College	Far North	4	1	4	0	0	0	0	0	0	9
Argosy University-The Art Institute of California-Sacramento	Far North	0	1	1	0	1	0	0	0	0	3
Asher College	Far North	0	2	2	0	0	0	0	0	0	4
Butte College	Far North	2	1	3	0	0	0	0	0	0	6
California State University-Chico	Far North	0	0	0	0	2	0	1	0	0	3
California State University-Sacramento	Far North	0	0	0	0	1	0	1	0	0	2
College of the Siskiyous	Far North	0	0	1	0	0	0	0	0	0	1
Cosumnes River College	Far North	6	1	2	0	0	0	0	0	0	9
Feather River Community College District	Far North	0	1	1	0	0	0	0	0	0	2
Folsom Lake College	Far North	3	0	1	0	0	0	0	0	0	4
Humboldt State University	Far North	0	0	0	0	2	0	0	0	0	2
Lake Tahoe Community College	Far North	1	1	1	0	0	0	0	0	0	3
Mendocino College	Far North	1	0	2	0	0	0	0	0	0	3
MTI College	Far North	2	1	0	0	0	0	0	0	0	3
Sacramento City College	Far North	4	5	4	0	0	0	0	0	0	13
Shasta College	Far North	0	0	1	0	0	0	0	0	0	1
Sierra College	Far North	4	0	6	0	0	0	0	0	0	10
University of California-Davis	Far North	0	0	0	0	1	0	1	0	1	3
Yuba College	Far North	1	0	2	0	0	0	0	0	0	3
Computer Training Academy	N/A	2	0	0	0	0	0	0	0	0	2
DeVry University-California	N/A	0	0	1	0	3	0	0	0	0	4
University of Phoenix - California	N/A	1	0	1	0	4	0	1	0	0	7
Grand Total		**361**	**172**	**354**	**2**	**161**	**1**	**91**	**15**	**20**	**1177**

Source: National Center for Educational Statistics, IPEDS data
Note: Data are from 2016, the most recent year available

APPENDIX F: PROGRAM AWARDS IN CYBERSECURITY

Program Awards in Cybersecurity (and Closely Related Programs) at Postsecondary Institutions in California, Five-Year Trends

	2012	2013	2014	2015	2016	5-Year Total
Focused on Cybersecurity	**452**	**499**	**788**	**922**	**813**	**3,474**
Computer and Information Systems Security/ Information Assurance	356	482	707	815	694	3,054
Associate degree	63	82	64	85	192	486
Award of at least 1 but less than 2 academic years	5	2	2	2	4	15
Award of less than 1 academic year	88	84	98	87	157	514
Bachelor's degree	195	217	399	450	132	1,393
Master's degree	5	50	73	106	100	334
Postbaccalaureate certificate		47	71	85	109	312
Cyber/Computer Forensics and Counterterrorism					0	0
Master's degree					0	0
Cyber/Electronic Operations and Warfare	96	17	81	107	119	420
Master's degree			9	10	22	41
Postbaccalaureate certificate	96	17	72	97	97	379
Includes Cybersecurity	**3,103**	**3,637**	**3,457**	**3,293**	**2,401**	**15,891**
Computer Software Technology/Technician	0	0	0	0	3	3
Award of at least 1 but less than 2 academic years	0	0	0	0		0
Bachelor's degree					3	3
Computer Systems Networking and Telecommunications	1,764	1,919	1,414	1,383	1,314	7,794
Associate degree	983	1005	475	383	321	3,167
Award of at least 1 but less than 2 academic years	289	218	231	224	167	1,129
Award of less than 1 academic year	376	418	462	517	566	2,339
Bachelor's degree	76	192	190	203	191	852
Doctor's degree – research/scholarship	2	5	3	3	3	16
Master's degree	38	73	48	52	66	277
Postbaccalaureate certificate		8	5	1	0	14
Critical Infrastructure Protection	92	86	99	78	97	452
Master's degree	91	86	99	78	97	451
Postbaccalaureate certificate	1					1
Data Modeling/Warehousing and Database Administration	36	31	42	60	97	266
Associate degree	7	2	5	13	14	41
Award of at least 1 but less than 2 academic years		2	0	2	8	12
Award of less than 1 academic year	29	27	26	27	28	137
Bachelor's degree			8	12	7	27
Master's degree		0	3	6	40	49
Homeland Security	658	522	396	245	150	1,971
Associate degree	178	190	116	77	11	572
Award of at least 1 but less than 2 academic years	1	2	2	1	0	6
Award of less than 1 academic year	466	286	204	108	51	1,115
Bachelor's degree		28	53	47	54	182
Master's degree	13	16	21	12	33	95
Postbaccalaureate certificate		0	0	0	1	1

APPENDIX F: PROGRAM AWARDS IN CYBERSECURITY

Program Awards in Cybersecurity (and Closely Related Programs) at Postsecondary Institutions in California, Five-Year Trends (continued)

	2012	2013	2014	2015	2016	5-Year Total
Includes Cybersecurity (continued)						
Information Resources Management	76	83	100	207	79	545
Bachelor's degree	22	22	39	37	37	157
Doctor's degree – research/scholarship				2	6	8
Master's degree	54	61	61	168	36	380
Management Information Systems, General	154	373	408	407	398	1,740
Award of less than 1 academic year		0	0	0	0	0
Bachelor's degree	137	278	305	302	269	1,291
Master's degree	17	88	98	102	126	431
Postbaccalaureate certificate		7	5	3	3	18
Network and System Administration/Administrator	122	177	176	177	146	798
Associate degree	11	17	42	31	29	130
Award of at least 1 but less than 2 academic years	31	25	34	30	33	153
Award of less than 1 academic year	26	95	41	92	68	322
Bachelor's degree	54	27	45	11	1	138
Master's degree			8	8	15	31
Postbaccalaureate certificate		13	6	5	0	24
System, Networking, and LAN/WAN Management/ Manager	123	347	704	629	23	1,826
Associate degree	0	257	625	613		1,495
Award of at least 1 but less than 2 academic years		70	50	16		136
Award of less than 1 academic year	123	20	29		23	195
Telecommunications Management	1	2	0	0	0	3
Award of less than 1 academic year		2	0	0	0	2
Bachelor's degree	0	0	0	0	0	0
Master's degree	1	0	0	0	0	1
Web/Multimedia Management and Webmaster	77	97	118	107	94	493
Associate degree	5	12	12	8	8	45
Award of at least 1 but less than 2 academic years	4	9	10	17	13	53
Award of less than 1 academic year	62	70	83	72	66	353
Bachelor's degree		1	9	7	6	23
Master's degree	6	5	4	3	1	19
Likely Includes Cybersecurity	**8,672**	**8,685**	**10,712**	**10,605**	**12,507**	**51,181**
Artificial Intelligence	10	3	6	12	11	42
Master's degree	10	3	6	12	11	42
Computer and Information Sciences and Support Services, Other	309	247	137	75	62	830
Associate degree	2	0	0	0	0	2
Award of at least 1 but less than 2 academic years	1	6	3	2	3	15
Award of less than 1 academic year	256	214	117	53	49	689
Bachelor's degree	40	18	9	11	4	82
Doctor's degree – research/scholarship	4	5	6	5	3	23
Master's degree	6	4	2	4	3	19

APPENDIX F: PROGRAM AWARDS IN CYBERSECURITY

Program Awards in Cybersecurity (and Closely Related Programs) at Postsecondary Institutions in California, Five-Year Trends (continued)

	2012	2013	2014	2015	2016	5-Year Total
Likely Includes Cybersecurity (continued)						
Computer and Information Sciences, General	422	416	528	499	507	2,372
Associate degree	32	21	27	43	81	204
Award of at least 1 but less than 2 academic years	17	6	18	2	16	59
Award of less than 1 academic year	122	142	225	197	116	802
Bachelor's degree	179	140	146	167	190	822
Doctor's degree – research/scholarship	23	28	14	8	13	86
Master's degree	48	79	98	82	91	398
Postbaccalaureate certificate	1	0	0	0	0	1
Computer and Information Sciences, Other	38	57	271	151	150	667
Award of less than 1 academic year		5	195	41	4	245
Bachelor's degree	38	52	76	110	130	406
Master's degree					16	16
Postbaccalaureate certificate					0	0
Computer Engineering Technologies/Technicians, Other					0	0
Award of less than 1 academic year					0	0
Computer Engineering Technology/Technician	4	29	32	24	21	110
Bachelor's degree	4	29	32	24	21	110
Computer Hardware Technology/Technician				4	0	4
Award of less than 1 academic year				4	0	4
Computer Programming, Other		10	56	52	48	166
Award of less than 1 academic year		10	56	52	48	166
Computer Programming, Specific Applications		4	1	7	6	18
Bachelor's degree				0	0	0
Master's degree		4	1	7	6	18
Computer Programming/Programmer, General	519	574	864	804	964	3,725
Associate degree	172	225	236	222	298	1,153
Award of at least 1 but less than 2 academic years	105	74	91	72	109	451
Award of at least 2 but less than 4 academic years	1					1
Award of less than 1 academic year	219	244	480	430	475	1,848
Bachelor's degree	22	31	57	80	82	272
Computer Science	4,094	4,197	4,958	5,800	7,428	26,477
Associate degree	132	164	241	294	450	1281
Award of at least 1 but less than 2 academic years	2	5	3	6	5	21
Award of less than 1 academic year	13	59	88	63	31	254
Bachelor's degree	1,796	2,097	2,789	3,289	4,270	14,241
Doctor's degree – research/scholarship	196	229	256	230	187	1,098
Master's degree	1,955	1,643	1,581	1,918	2,485	9,582
Computer Software and Media Applications, Other	37	32	41	114	82	306
Associate degree	4	24	28	20	8	84
Award of at least 1 but less than 2 academic years	33	5	1	0	1	40
Award of less than 1 academic year			0	59	45	104

APPENDIX F: PROGRAM AWARDS IN CYBERSECURITY

Program Awards in Cybersecurity (and Closely Related Programs) at Postsecondary Institutions in California, Five-Year Trends (continued)

	2012	2013	2014	2015	2016	5-Year Total
Likely Includes Cybersecurity (continued)						
Computer Software and Media Applications, Other (continued)						
Bachelor's degree	0	3	12	16	13	44
Master's degree				19	15	34
Computer Support Specialist	428	428	450	430	424	2,160
Associate degree	84	72	77	84	127	444
Award of at least 1 but less than 2 academic years	113	115	95	143	106	572
Award of less than 1 academic year	231	241	276	203	191	1,142
Bachelor's degree			2			2
Computer Systems Analysis/Analyst	3	110	245	202	204	764
Associate degree	1	2	3	1	2	9
Award of at least 1 but less than 2 academic years					1	1
Award of less than 1 academic year	2	4	91	82	90	269
Bachelor's degree		104	151	119	111	485
Computer Technology/Computer Systems Technology	828	457	402	89	114	1,890
Associate degree		2	2	1		5
Award of at least 1 but less than 2 academic years	710	387	275			1,372
Award of less than 1 academic year	118	68	125	88	114	513
Computer/Information Technology Services Administration and Management, Other	103	100	472	181	88	944
Associate degree	0	0	10	5	5	20
Award of at least 1 but less than 2 academic years	0	1	1			2
Award of at least 2 but less than 4 academic years	1					1
Award of less than 1 academic year	21	36	399	98	10	564
Bachelor's degree	40	32	27	57	59	215
Master's degree	39	28	32	21	14	134
Postbaccalaureate certificate	2	3	3	0	0	8
Informatics	39	29	37	49	89	243
Bachelor's degree	39	29	37	48	68	221
Master's degree			0	1	21	22
Information Science/Studies	172	136	179	113	276	876
Bachelor's degree	33	18	55	8	56	170
Doctor's degree – research/scholarship	20	10	7	15	15	67
Master's degree	119	108	117	90	205	639
Postbaccalaureate certificate	0	0	0	0	0	0
Information Technology	1,064	1,122	1,196	1,225	1,304	5,911
Associate degree	259	286	329	334	322	1,530
Award of at least 1 but less than 2 academic years	45	80	85	83	94	387
Award of less than 1 academic year	116	146	272	268	200	1,002
Bachelor's degree	452	438	356	378	363	1,987
Master's degree	192	172	142	150	319	975
Postbaccalaureate certificate			12	12	5	29
Post-master's certificate					1	1

APPENDIX F: PROGRAM AWARDS IN CYBERSECURITY

Program Awards in Cybersecurity (and Closely Related Programs) at Postsecondary Institutions in California, Five-Year Trends (continued)

	2012	2013	2014	2015	2016	5-Year Total
Likely Includes Cybersecurity (continued)						
Information Technology Project Management	1	57	74	72	78	282
Award of less than 1 academic year		0	0	1	2	3
Bachelor's degree	1	52	71	68	75	267
Master's degree		5	3	2	1	11
Postbaccalaureate certificate				1		1
Web Page, Digital/Multimedia and Information Resources Design	601	677	763	702	651	3,394
Associate degree	85	170	168	148	111	682
Award of at least 1 but less than 2 academic years	38	96	173	117	77	501
Award of at least 2 but less than 4 academic years	0		0	0	0	0
Award of less than 1 academic year	172	112	93	89	73	539
Bachelor's degree	237	217	257	259	286	1,256
Master's degree	69	82	72	89	104	416
Postbaccalaureate certificate					0	0
Grand Total	**12,227**	**12,821**	**14,957**	**14,820**	**15,721**	**70,546**

Source: National Center for Educational Statistics, IPEDS Data

IPEDS Award levels

The eleven award levels under which completions can be reported are:

1. Postsecondary award, certificate, or diploma of (less than 1 academic year)
   - Less than 900 contact or clock hours
   - Less than 30 SEMESTER or TRIMESTER credit hours, or
   - Less than 45 QUARTER credit hours
2. Postsecondary award, certificate, or diploma of (at least 1 but less than 2 academic years)
   - At least 900, but less than 1800 contact or clock hours, or
   - At least 30, but less than 60 SEMESTER OR TRIMESTER HOURS
   - At least 45, but less than 90 QUARTER HOURS
3. Associate degree
   - An award that normally requires at least 2 but less than 4 years of full-time equivalent college work
4. Postsecondary award, certificate, or diploma of (at least 2 but less than 4 academic years)
   - 1800 or more contact or clock hours, or
   - 60 or more SEMESTER OR TRIMESTER credit hours, or
   - 90 or more QUARTER credit hours

APPENDIX F: PROGRAM AWARDS IN CYBERSECURITY

5. Bachelor's degree
    - An award (baccalaureate or equivalent degree, as determined by the Secretary, U.S. Department of Education) that normally requires at least 4 but not more than 5 years of full-time equivalent college-level work. This includes all bachelor's degrees conferred in a 5-year cooperative (work-study) program. A cooperative plan provides for alternate class attendance and employment in business, industry, or government; thus, it allows students to combine actual work experience with their college studies. Also includes bachelor's degrees in which the normal 4 years of work are completed in 3 years.
6. Postbaccalaureate certificate
    - An award that requires completion of an organized program of study beyond the bachelor's. It is designed for persons who have completed a baccalaureate degree, but does not meet the requirements of a master's degree.
7. Master's degree
    - An award that requires the successful completion of a program of study of at least the full-time equivalent of 1 but not more than 2 academic years of work beyond the bachelor's degree.
8. Post-master's certificate
    - An award that requires completion of an organized program beyond the master's degree, but does not meet the requirements of academic degrees at the doctor's level.
9. Doctor's degree – research/scholarship
    - A Ph.D. or other doctor's degree that requires advanced work beyond the master's level, including the preparation and defense of a dissertation based on original research, or the planning and execution of an original project demonstrating substantial artistic or scholarly achievement.
10. Doctor's degree – professional practice
    - A doctor's degree that is conferred upon completion of a program providing the knowledge and skills for the recognition, credential, or license required for professional practice. The degree is awarded after a period of study such that the total time to the degree, including both pre-professional and professional preparation, equals at least six full-time equivalent academic years.
11. Doctor's degree – other
    - A doctor's degree that does not meet the definition of a doctor's degree—research/scholarship or a doctor's degree—professional practice.

Definitions for each of these award levels can be found in the IPEDS Glossary:
https://surveys.nces.ed.gov/ipeds/VisGlossaryAll.aspx

APPENDIX G: CYBERSECURITY-RELATED CIP (CLASSIFICATION OF INSTRUCTIONAL PROGRAMS) CODES

National Center for Education Statistics
Classification of Instructional Programs – 2010

Key for Cybersecurity Program Focus:

- Cybersecurity Focused
- Includes Aspects of Cybersecurity

Otherwise = Likely Includes Cybersecurity

CIP Codes Relevant to Cybersecurity

11 Computer And Information Sciences and Support Services.

Instructional programs that focus on the computer and information sciences and prepare individuals for various occupations in information technology and computer operations fields.

11.0101 Computer and Information Sciences, General.
A general program that focuses on computing, computer science, and information science and systems. Such programs are undifferentiated as to title and content and are not to be confused with specific programs in computer science, information science, or related support services.

11.0102 Artificial Intelligence.
A program that focuses on the symbolic inference, representation, and simulation by computers and software of human learning and reasoning processes and capabilities, and the computer modeling of human motor control and motion. Includes instruction in computing theory, cybernetics, human factors, natural language processing, and applicable aspects of engineering, technology, and specific end-use applications.
See also: 14.4201 - Mechatronics, Robotics, and Automation Engineering.

11.0103 Information Technology.
A program that focuses on the design of technological information systems, including computing systems, as solutions to business and research data and communications support needs. Includes instruction in the principles of computer hardware and software components, algorithms, databases, telecommunications, user tactics, application testing, and human interface design.

11.0104 Informatics.
A program that focuses on computer systems from a user-centered perspective and studies the structure, behavior and interactions of natural and artificial systems that store, process and communicate information. Includes instruction in information sciences, human computer interaction, information system analysis and design, telecommunications structure and information architecture and management.
Examples:
- Social Informatics
See also: 26.1103 - Bioinformatics., 51.2706 - Medical Informatics.

11.0199 Computer and Information Sciences, Other.
Any instructional program in computer science not listed above.

11.0201 Computer Programming/Programmer, General.
A program that focuses on the general writing and implementation of generic and customized programs to drive operating systems and that generally prepares individuals to apply the methods and procedures of software design and programming to software installation and maintenance. Includes instruction in software design, low- and high-level languages and program writing; program customization and linking; prototype testing; troubleshooting; and related aspects of operating systems and networks.

APPENDIX G: CYBERSECURITY-RELATED CIP (CLASSIFICATION OF INSTRUCTIONAL PROGRAMS) CODES

11.0202 Computer Programming, Specific Applications.
A program that prepares individuals to apply the knowledge and skills of general computer programming to the solution of specific operational problems and customization requirements presented by individual software users and organizational users. Includes training in specific types of software and its installation and maintenance.

11.0203 Computer Programming, Vendor/Product Certification.
A program that prepares individuals to fulfill the requirements set by vendors for professional qualification as certified installation, customization, and maintenance engineers for specific software products and/or processes. Includes training in specific vendor-supported software products and their installation and maintenance.

11.0299 Computer Programming, Other.
Any instructional program in computer programming not listed above.

11.0401 Information Science/Studies.
A program that focuses on the theory, organization, and process of information collection, transmission, and utilization in traditional and electronic forms. Includes instruction in information classification and organization; information storage and processing; transmission, transfer, and signaling; communications and networking; systems planning and design; human interfacing and use analysis; database development; information policy analysis; and related aspects of hardware, software, economics, social factors, and capacity.
See also: 25.0101 - Library and Information Science., 52.1201 - Management Information Systems, General.

11.0501 Computer Systems Analysis/Analyst.
A program that prepares individuals to apply programming and systems analysis principles to the selection, implementation, and troubleshooting of customized computer and software installations across the life cycle. Includes instruction in computer hardware and software; compilation, composition, execution, and operating systems; low- and high-level languages and language programming; programming and debugging techniques; installation and maintenance testing and documentation; process and data flow analysis; user needs analysis and documentation; cost-benefit analysis; and specification design.
See also: 14.2701 - Systems Engineering.

11.0701 Computer Science.
A program that focuses on computer theory, computing problems and solutions, and the design of computer systems and user interfaces from a scientific perspective. Includes instruction in the principles of computational science, computer development and programming, and applications to a variety of end-use situations.
See also: 14.0901 - Computer Engineering, General.

11.0801 Web Page, Digital/Multimedia and Information Resources Design.
A program that prepares individuals to apply HTML, XML, JavaScript, graphics applications, and other authoring tools to the design, editing, and publishing (launching) of documents, images, graphics, sound, and multimedia products on the World Wide Web. Includes instruction in Internet theory, web page standards and policies, elements of web page design, user interfaces, vector tools, special effects, interactive and multimedia components, search engines, navigation, morphing, e-commerce tools, and emerging web technologies.

APPENDIX G: CYBERSECURITY-RELATED CIP (CLASSIFICATION OF INSTRUCTIONAL PROGRAMS) CODES

11.0802 Data Modeling/Warehousing and Database Administration.
A program that prepares individuals to design and manage the construction of databases and related software programs and applications, including the linking of individual data sets to create complex searchable databases (warehousing) and the use of analytical search tools (mining). Includes instruction in database theory, logic, and semantics; operational and warehouse modeling; dimensionality; attributes and hierarchies; data definition; technical architecture; access and security design; integration; formatting and extraction; data delivery; index design; implementation problems; planning and budgeting; and client and networking issues.

11.0899 Computer Software and Media Applications, Other.
Any instructional program in computer software and media applications not listed above.

11.0901 Computer Systems Networking and Telecommunications.
A program that focuses on the design, implementation, and management of linked systems of computers, peripherals, and associated software to maximize efficiency and productivity, and that prepares individuals to function as network specialists and managers at various levels. Includes instruction in operating systems and applications; systems design and analysis; networking theory and solutions; types of networks; network management and control; network and flow optimization; security; configuring; and troubleshooting.
Examples:
- Computer Systems Telecommunications
- Computer Systems Networking

11.1001 Network and System Administration/Administrator.
A program that prepares individuals to manage the computer operations and control the system configurations emanating from a specific site or network hub. Includes instruction in computer hardware and software and applications; local area (LAN) and wide area (WAN) networking; principles of information systems security; disk space and traffic load monitoring; data backup; resource allocation; and setup and takedown procedures.
Examples:
- Network Administration

11.1002 System, Networking, and LAN/WAN Management/Manager.
A program that prepares individuals to oversee and regulate the computer system and performance requirements of an entire organization or network of satellite users. Includes instruction in performance balancing; redundancy; local area (LAN) and wide area (WAN) network management; system migration and upgrading; outage control; problem diagnosis and troubleshooting; and system maintenance, budgeting, and management.

11.1003 Computer and Information Systems Security/Information Assurance.
A program that prepares individuals to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation and maintenance of security devices, systems, and procedures. Includes instruction in computer architecture, programming, and systems analysis; networking; telecommunications; cryptography; security system design; applicable law and regulations; risk assessment and policy analysis; contingency planning; user access issues; investigation techniques; and troubleshooting.
Examples:
- Information Assurance
- IT Security
- Internet Security
- Network Security
- Information Systems Security
See also: 43.0116 - Cyber/Computer Forensics and Counterterrorism.

11.1004 Web/Multimedia Management and Webmaster.
A program that prepares individuals to develop and maintain web servers and the hosted web pages at one or a group of web sites, and to function as designated webmasters. Includes instruction in computer systems and networks, server installation and maintenance, web page design and editing, information resources management, web policy and procedures, Internet applications of information systems security, user interfacing and usability research, and relevant management and communications skills.
Examples:
- Website Development
- Web Development
- Webmaster

11.1005 Information Technology Project Management.
A program that prepares individuals to design, develop, and manage information technology projects in a variety of companies and organizations. Includes instruction in principles of project management, risk management, procurement and contract management, information security management, software management, organizational principles and behavior, communications, quality assurance, financial analysis, leadership, and team effectiveness.
See also: 52.0211 - Project Management.

11.1006 Computer Support Specialist.
A program that prepares individuals to provide technical assistance, support, and advice to computer users to help troubleshoot software and hardware problems. Includes instruction in computer concepts, information systems, networking, operating systems, computer hardware, the Internet, software applications, help desk concepts and problem solving, and principles of customer service.
Examples:
- Technical Support Specialist
- Help Desk Specialist
- IT Support Specialist

11.1099 Computer/Information Technology Services Administration and Management, Other.
Any instructional program in computer/information technology services administration and management not listed above.
See also: 51.0706 - Health Information/Medical Records Administration/Administrator.

11.9999 Computer and Information Sciences and Support Services, Other.
Any instructional program in computer and information sciences and support services not listed above.

---

15 Engineering Technologies and Engineering-Related Fields.

Instructional programs that prepare individuals to apply basic engineering principles and technical skills in support of engineering and related projects or to prepare for engineering-related fields.

15.1201 Computer Engineering Technology/Technician.
A program that prepares individuals to apply basic engineering principles and technical skills in support of computer engineers engaged in designing and developing computer systems and installations. Includes instruction in computer electronics and programming, prototype development and testing, systems installation and testing, solid state and microminiature circuitry, peripheral equipment, and report preparation.

APPENDIX G: CYBERSECURITY-RELATED CIP (CLASSIFICATION OF INSTRUCTIONAL PROGRAMS) CODES

15.1202 Computer Technology/Computer Systems Technology.
A program that prepares individuals to apply basic engineering principles and technical skills in support of professionals who use computer systems. Includes instruction in basic computer design and architecture, programming, problems of specific computer applications, component and system maintenance and inspection procedures, hardware and software problem diagnosis and repair, and report preparation.

See also: 47.0104 - Computer Installation and Repair Technology/Technician.

15.1203 Computer Hardware Technology/Technician.
A program that prepares individuals to apply basic engineering principles and technical skills to support engineers in designing computer hardware and peripheral systems. Includes instruction in computer systems design, computer architecture, computer electronics, processors, peripherals, testing equipment, and computer manufacturing processes.

15.1204 Computer Software Technology/Technician.
A program that prepares individuals to apply basic engineering principles and technical skills to support engineers in developing, implementing, and evaluating computer software and program applications. Includes instruction in computer programming, programming languages, databases, user interfaces, networking and warehousing, encryption and security, software testing and evaluation, and customization.

15.1299 Computer Engineering Technologies/Technicians, Other.
Any instructional program in computer engineering technologies not listed above.

---

29 Military Technologies and Applied Sciences.

Instructional programs that prepare individuals in specialized and advanced subject matter for the armed services and related national security organizations, including intelligence operations, military applied sciences, and military technologies.

29.0207 Cyber/Electronic Operations and Warfare.
A program that focuses on the technological and operation aspects of information warfare, including cyber attack and cyber defense. Includes instruction in computer and network security, cryptography, computer forensics, systems security engineering, software applications, threat and vulnerability assessment, wireless networks and satellite communications, tactical and strategic planning, legal and ethical issues, and cyber warfare systems development and acquisition.
Examples:
- Cyberspace Operations
- Electronic Warfare
- Information Warfare

APPENDIX G: CYBERSECURITY-RELATED CIP (CLASSIFICATION OF INSTRUCTIONAL PROGRAMS) CODES

43 Homeland Security, Law Enforcement, Firefighting and Related Protective Services.

Instructional programs that focus on the principles and procedures for providing homeland security, police, fire, and other safety services and managing penal institutions. Note: this series is titled "Security and Protective Services" in the Canadian CIP.

43.0116 Cyber/Computer Forensics and Counterterrorism.
A program focusing on the principles and techniques used to identify, search, seize and analyze digital media and to conduct cyber investigations against criminal and terrorist activity. Includes instruction in computer boot processes and drives, jumper setting, file access and reconstruction, hacking, network systems, cryptography, programming, investigative techniques, forensic imagery, web-based investigation methods, cyberterrorism, and applicable laws and administrative procedures.
Examples:
- Internet Investigation
See also: 11.1003 - Computer and Information Systems Security/Information Assurance.

43.0301 Homeland Security.
A program focusing on security policy, planning and operations dedicated to the protection of U.S. territory, assets, infrastructure, institutions and citizens from external threats. Includes instruction in national security policy, government relations, intelligence, law enforcement, security technology, communications and information technology, homeland security planning and operations, disaster planning and applications to specific threat scenarios.

43.0303 Critical Infrastructure Protection.
A program focusing on the design, planning and management of systems and procedures for protecting critical national physical and cyber infrastructure from external threats, including terrorism. Includes instruction in homeland security policy, critical infrastructure policy, information security, matrix vulnerability assessment, threat assessment, physical security, personnel security, operational security, contingency planning, case analyses of specific industries and systems, redundancy planning, emergency and disaster planning, security systems, and intelligence operations.

---

52 Business, Management, Marketing, and Related Support Services.

Instructional programs that prepare individuals to perform managerial, technical support, and applied research functions related to the operation of commercial and non-profit enterprises and the buying and selling of goods and services.

52.1201 Management Information Systems, General.
A program that generally prepares individuals to provide and manage data systems and related facilities for processing and retrieving internal business information; select systems and train personnel; and respond to external data requests. Includes instruction in cost and accounting information systems, management control systems, personnel information systems, data storage and security, business systems networking, report preparation, computer facilities and equipment operation and maintenance, operator supervision and training, and management information systems policy and planning.
See also: 11.0401 - Information Science/Studies.

APPENDIX G: CYBERSECURITY-RELATED CIP (CLASSIFICATION OF INSTRUCTIONAL PROGRAMS) CODES

52.1206 Information Resources Management.
A program that prepares individuals to apply principles of information technology, computer systems management, and business operations to the planning, management, and evaluation of information services in organizations. Includes instruction in telecommunications, systems planning and integration, information policy, information security, contracting and purchasing, budgeting, information technology, operations management, human resources, communications skills, and applicable law and regulations.
Examples:
- Information Management
- Chief Information Officer Training

52.2101 Telecommunications Management.
A program that prepares individuals to apply business skills to design, implement, and manage the voice, video, and data networking systems of organizations. Includes instruction in telecommunications concepts and technologies, network operations and management, wireless communications and mobile computing, cybersecurity, regulation and public policy, business practices and management, and written and oral communications.

For a full listing of the universe of 2010 CIP Codes, visit the National Center for Educational Statistics, Resources Page, CIP Codes: https://nces.ed.gov/ipeds/cipcode/resources.aspx?y=55

APPENDIX H: POSTSECONDARY CYBERSECURITY PROGRAMMING IN CALIFORNIA

List of IPEDS-reporting Postsecondary Institutions Providing Cybersecurity Programming in California, with Institutional Characteristics, by Region

Institution Name	ZIP Code Location	Enrollment	Sector	Degree/ nondegree (D/ND)†	Tuition & Fees	Net Price‡
Bay Area						
Academy of Art University	94105	10,000 - 19,999	Private for-profit, 4-year or above	D	$20,340	$29,301
Argosy University-San Francisco Bay Area	94501	Under 1,000	Private for-profit, 4-year or above	D	$13,560	
Argosy University-The Art Institute of California-San Francisco	94102-4908	Under 1,000	Private for-profit, 4-year or above	D	$18,744	$22,560
Argosy University-The Art Institute of California-Silicon Valley	94086	Under 1,000	Private for-profit, 4-year or above	D		
Berkeley City College	94704	5,000 - 9,999	Public, 2-year	D	$1,156	$8,908
Cabrillo College	95003	10,000 - 19,999	Public, 2-year	D	$1,376	$10,228
California State University-East Bay	94542	10,000 - 19,999	Public, 4-year or above	D	$6,564	$10,758
California State University-Monterey Bay	93955-8001	5,000 - 9,999	Public, 4-year or above	D	$6,119	$11,390
Canada College	94061-1099	5,000 - 9,999	Public, 2-year	D	$1,344	$5,441
Chabot College	94545	10,000 - 19,999	Public, 2-year	D	$1,138	$6,877
City College of San Francisco	94112-1898	20,000 and above	Public, 2-year	D	$1,598	$5,466
Cogswell College	95134	Under 1,000	Private for-profit, 4-year or above	D	$16,640	$23,304
College of Alameda	94501	5,000 - 9,999	Public, 2-year	D	$1,156	$7,071
College of Marin	94904-2590	5,000 - 9,999	Public, 2-year	D	$1,488	$9,717
College of San Mateo	94402-3784	5,000 - 9,999	Public, 2-year	D	$1,324	$4,494
Contra Costa College	94806-3195	5,000 - 9,999	Public, 2-year	D	$1,298	$8,366
De Anza College	95014	20,000 and above	Public, 2-year	D	$1,542	$6,544
Diablo Valley College	94523	10,000 - 19,999	Public, 2-year	D	$1,298	$7,055
Evergreen Valley College	95135-1598	5,000 - 9,999	Public, 2-year	D	$1,338	$11,694
Foothill College	94022	10,000 - 19,999	Public, 4-year or above	D	$1,551	$6,281
Fresno City College	93741	20,000 and above	Public, 2-year	D	$1,142	$4,002
Gavilan College	95020	5,000 - 9,999	Public, 2-year	D	$1,246	$7,016
Golden Gate University-San Francisco	94105-2968	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$14,640	
Hartnell College	93901	10,000 - 19,999	Public, 2-year	D	$1,420	$10,815
Holy Names University	94619-1699	Under 1,000	Private not-for-profit, 4-year or above	D	$35,666	$21,464
International Technological University	95134	1,000 - 4,999	Private not-for-profit, 4-year or above	D		
Laney College	94607	10,000 - 19,999	Public, 2-year	D	$1,156	$9,709
Las Positas College	94551-7650	5,000 - 9,999	Public, 2-year	D	$1,138	$6,593
Los Medanos College	94565	5,000 - 9,999	Public, 2-year	D	$1,298	$6,614
Merritt College	94619-3196	5,000 - 9,999	Public, 2-year	D	$1,156	$10,741

APPENDIX H: POSTSECONDARY CYBERSECURITY PROGRAMMING IN CALIFORNIA

List of IPEDS-reporting Postsecondary Institutions Providing Cybersecurity Programming in California, with Institutional Characteristics, by Region (continued)

Institution Name	ZIP Code Location	Enrollment	Sector	Degree/ nondegree (D/ND)†	Tuition & Fees	Net Price‡
Bay Area (continued)						
Mills College	94613	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$44,258	$27,647
Mission College	95054-1897	5,000 - 9,999	Public, 2-year	D	$1,174	$10,004
Monterey Peninsula College	93940-4799	5,000 - 9,999	Public, 2-year	D	$1,174	$6,081
Napa Valley College	94558-6236	5,000 - 9,999	Public, 2-year	D	$1,142	$13,067
Naval Postgraduate School	93943	1,000 - 4,999	Public, 4-year or above	D		
Notre Dame de Namur University	94002-1908	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$32,608	$28,873
Ohlone College	94539-0390	5,000 - 9,999	Public, 2-year	D	$1,162	$12,792
Pacific Union College	94508-9707	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$29,064	$24,555
San Francisco State University	94132	20,000 and above	Public, 4-year or above	D	$6,476	$13,250
San Jose City College	95128-2798	5,000 - 9,999	Public, 2-year	D	$1,338	$11,410
San Jose State University	95192-0001	20,000 and above	Public, 4-year or above	D	$7,378	$13,777
Santa Clara University	95053	5,000 - 9,999	Private not-for-profit, 4-year or above	D	$45,300	$37,657
Santa Rosa Junior College	95401-4395	20,000 and above	Public, 2-year	D	$1,318	$8,989
Skyline College	94066-1698	5,000 - 9,999	Public, 4-year or above	D	$1,447	$4,251
Solano Community College	94534-3197	5,000 - 9,999	Public, 2-year	D	$1,416	$7,978
Sonoma State University	94928-3609	5,000 - 9,999	Public, 4-year or above	D	$7,330	$16,204
Stanford University	94305	10,000 - 19,999	Private not-for-profit, 4-year or above	D	$46,320	$16,695
University of California-Berkeley	94720	20,000 and above	Public, 4-year or above	D	$13,431	$17,160
University of California-San Francisco	94143-0244	1,000 - 4,999	Public, 4-year or above	D		
University of California-Santa Cruz	95064-1011	10,000 - 19,999	Public, 4-year or above	D	$13,461	$16,261
University of San Francisco	94117-1080	10,000 - 19,999	Private not-for-profit, 4-year or above	D	$42,634	$35,054
West Valley College	95070-5698	5,000 - 9,999	Public, 2-year	D	$1,186	$10,047
Central California						
Bakersfield College	93305-1299	20,000 and above	Public, 4-year or above	D	$1,326	$4,409
California State University-Bakersfield	93311-1099	5,000 - 9,999	Public, 4-year or above	D	$6,811	$6,143

APPENDIX H: POSTSECONDARY CYBERSECURITY PROGRAMMING IN CALIFORNIA

List of IPEDS-reporting Postsecondary Institutions Providing Cybersecurity Programming in California, with Institutional Characteristics, by Region (continued)

Institution Name	ZIP Code Location	Enrollment	Sector	Degree/ nondegree (D/ND)†	Tuition & Fees	Net Price‡
Central California (continued)						
California State University-Fresno	93740	20,000 and above	Public, 4-year or above	D	$6,311	$6,177
California State University-Stanislaus	95382-0299	5,000 - 9,999	Public, 4-year or above	D	$6,704	$7,557
Cerro Coso Community College	93555-9571	5,000 - 9,999	Public, 2-year	D	$1,290	$6,661
Clovis Community College	93730	5,000 - 9,999	Public, 2-year	D	$1,304	$8,024
College of the Sequoias	93277-2214	10,000 - 19,999	Public, 2-year	D	$1,388	$2,868
Columbia College	95370	1,000 - 4,999	Public, 2-year	D	$1,162	$7,790
Merced College	95348-2898	10,000 - 19,999	Public, 2-year	D	$1,141	$9,842
Milan Institute-Visalia	93277	Under 1,000	Private for-profit, less-than 2-year	ND		$20,666
Modesto Junior College	95350-5800	10,000 - 19,999	Public, 4-year or above	D	$1,162	$10,068
MTI Business College Inc	95207-4349	Under 1,000	Private for-profit, less-than 2-year	ND		$17,967
Porterville College	93257	1,000 - 4,999	Public, 2-year	D	$1,322	$3,456
Reedley College	93654	10,000 - 19,999	Public, 2-year	D	$1,324	$4,534
San Joaquin Delta College	95207	10,000 - 19,999	Public, 2-year	D	$1,104	$10,579
San Joaquin Valley College-Visalia	93291-9283	5,000 - 9,999	Private for-profit, 2-year	D		$18,733
Santa Barbara Business College-Bakersfield	93309	Under 1,000	Private for-profit, 4-year or above	D	$13,619	$12,586
Taft College	93268	5,000 - 9,999	Public, 2-year	D	$1,134	$7,374
University of the Pacific	95211-0197	5,000 - 9,999	Private not-for-profit, 4-year or above	D	$42,934	$33,794
West Hills College-Coalinga	93210	1,000 - 4,999	Public, 2-year	D	$1,380	$8,411
West Hills College-Lemoore	93245	1,000 - 4,999	Public, 2-year	D	$1,380	$10,291
Far North						
American River College	95841-4286	20,000 and above	Public, 2-year	D	$1,104	$8,829
Argosy University-The Art Institute of California-Sacramento	95833	Under 1,000	Private for-profit, 4-year or above	D	$18,744	$23,065
Asher College	95825	Under 1,000	Private for-profit, 2-year	D		$18,286
Butte College	95965-8399	10,000 - 19,999	Public, 2-year	D	$1,364	$5,921
California State University-Chico	95929-0150	10,000 - 19,999	Public, 4-year or above	D	$7,022	$13,645
California State University-Sacramento	95819-2694	20,000 and above	Public, 4-year or above	D	$6,872	$9,127
College of the Redwoods	95501-9300	1,000 - 4,999	Public, 2-year	D	$1,182	$5,514
College of the Siskiyous	96094-2899	1,000 - 4,999	Public, 2-year	D	$1,154	$8,565
Cosumnes River College	95823-5799	10,000 - 19,999	Public, 2-year	D	$1,104	$10,022
Feather River Community College District	95971-9124	1,000 - 4,999	Public, 4-year or above	D	$1,461	$12,225
Folsom Lake College	95630	5,000 - 9,999	Public, 2-year	D	$1,104	$10,480

APPENDIX H: POSTSECONDARY CYBERSECURITY PROGRAMMING IN CALIFORNIA

List of IPEDS-reporting Postsecondary Institutions Providing Cybersecurity Programming in California, with Institutional Characteristics, by Region (continued)

Institution Name	ZIP Code Location	Enrollment	Sector	Degree/ nondegree (D/ND)†	Tuition & Fees	Net Price‡
Far North (continued)						
Humboldt State University	95521-8299	5,000 - 9,999	Public, 4-year or above	D	$7,195	$13,147
Lake Tahoe Community College	96150	1,000 - 4,999	Public, 2-year	D	$1,224	$8,453
Mendocino College	95482	1,000 - 4,999	Public, 2-year	D	$1,422	$9,120
MTI College	95841-9817	Under 1,000	Private for-profit, 2-year	D		$16,836
Sacramento City College	95822-1386	20,000 and above	Public, 2-year	D	$1,104	$10,107
Shasta College	96003	5,000 - 9,999	Public, 4-year or above	D	$1,183	$7,537
Sierra College	95677-3397	10,000 - 19,999	Public, 2-year	D	$1,142	$8,215
University of California-Davis	95616-8678	20,000 and above	Public, 4-year or above	D	$13,951	$16,039
Yuba College	95901	5,000 - 9,999	Public, 2-year	D	$1,144	$5,948
Inland Empire/Desert Region						
Argosy University-Inland Empire	91761	Under 1,000	Private for-profit, 4-year or above	D	$13,560	$21,132
Argosy University-The Art Institute of California-Inland Empire	92408-2800	1,000 - 4,999	Private for-profit, 4-year or above	D	$18,744	$21,426
Barstow Community College	92311	1,000 - 4,999	Public, 2-year	D	$1,104	$9,312
California Baptist University	92504-3297	5,000 - 9,999	Private not-for-profit, 4-year or above	D	$30,384	$25,875
California State University-San Bernardino	92407-2397	20,000 and above	Public, 4-year or above	D	$6,577	$6,444
Chaffey College	91737-3002	20,000 and above	Public, 2-year	D	$1,153	$10,306
College of the Desert	92260	10,000 - 19,999	Public, 2-year	D	$1,326	$9,484
Copper Mountain Community College	92252	1,000 - 4,999	Public, 2-year	D	$1,108	$8,543
Crafton Hills College	92339-1799	5,000 - 9,999	Public, 2-year	D	$1,142	$13,506
La Sierra University	92515-8247	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$30,471	$23,414
Mayfield College	92234	Under 1,000	Private for-profit, 2-year	D	$12,648	$21,354
Milan Institute-Palm Desert	92211	Under 1,000	Private for-profit, less-than 2-year	ND		$18,710
Moreno Valley College	92551	5,000 - 9,999	Public, 2-year	D	$1,416	$8,043
Mt San Jacinto Community College District	92583-2399	10,000 - 19,999	Public, 2-year	D	$1,386	$6,783
Norco College	92860	5,000 - 9,999	Public, 2-year	D	$1,416	$7,337
Palo Verde College	92225	1,000 - 4,999	Public, 2-year	D	$1,288	$11,681
Riverside City College	92506	10,000 - 19,999	Public, 2-year	D	$1,426	$7,670
San Bernardino Valley College	92410-2798	10,000 - 19,999	Public, 2-year	D	$1,238	$8,887
University of California-Riverside	92521	20,000 and above	Public, 4-year or above	D	$13,527	$12,841

APPENDIX H: POSTSECONDARY CYBERSECURITY PROGRAMMING IN CALIFORNIA

List of IPEDS-reporting Postsecondary Institutions Providing Cybersecurity Programming in California, with Institutional Characteristics, by Region (continued)

Institution Name	ZIP Code Location	Enrollment	Sector	Degree/ nondegree (D/ND)†	Tuition & Fees	Net Price‡
Inland Empire/Desert Region (continued)						
University of Redlands	92373-0999	5,000 - 9,999	Private not-for-profit, 4-year or above	D	$44,900	$34,200
Victor Valley College	92395-5850	10,000 - 19,999	Public, 2-year	D	$1,114	$9,195
Los Angeles/Orange County						
ABCO Technology	90045-1551	Under 1,000	Private for-profit, less-than 2-year	ND		$14,917
Advanced Computing Institute	90010-3911	Under 1,000	Private for-profit, 2-year	D		$10,210
Allied American University	92653-1337	Under 1,000	Private for-profit, 4-year or above	D		$18,359
Argosy University-Los Angeles	90045	Under 1,000	Private for-profit, 4-year or above	D	$13,560	$21,327
Argosy University-Orange County	92868	Under 1,000	Private for-profit, 4-year or above	D	$13,560	$25,040
Argosy University-The Art Institute of California-Hollywood	91601	1,000 - 4,999	Private for-profit, 4-year or above	D	$18,744	$28,044
Argosy University-The Art Institute of California-Los Angeles	90405-3035	Under 1,000	Private for-profit, 4-year or above	D		
Argosy University-The Art Institute of California-Orange County	92704	Under 1,000	Private for-profit, 4-year or above	D	$18,744	$23,872
Art Center College of Design	91103	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$39,230	$43,814
Azusa Pacific University	91702-7000	10,000 - 19,999	Private not-for-profit, 4-year or above	D	$34,754	$28,506
Bethesda University	92801	Under 1,000	Private not-for-profit, 4-year or above	D	$6,174	$10,012
Biola University	90639-0001	5,000 - 9,999	Private not-for-profit, 4-year or above	D	$34,498	$32,273
Brand College	91203	Under 1,000	Private for-profit, less-than 2-year	ND		
Brandman University	92618	5,000 - 9,999	Private not-for-profit, 4-year or above	D	$12,240	
California Career School	92805	Under 1,000	Private for-profit, less-than 2-year	ND		$5,548
California Institute of Technology	91125	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$45,390	$26,839
California Intercontinental University	92614-5636	Under 1,000	Private for-profit, 4-year or above	D	$8,690	
California State Polytechnic University-Pomona	91768	20,000 and above	Public, 4-year or above	D	$7,016	$12,598
California State University-Dominguez Hills	90747-0005	10,000 - 19,999	Public, 4-year or above	D	$6,213	$3,297

APPENDIX H: POSTSECONDARY CYBERSECURITY PROGRAMMING IN CALIFORNIA

List of IPEDS-reporting Postsecondary Institutions Providing Cybersecurity Programming in California, with Institutional Characteristics, by Region (continued)

Institution Name	ZIP Code Location	Enrollment	Sector	Degree/ nondegree (D/ND)†	Tuition & Fees	Net Price‡
Los Angeles/Orange County (continued)						
California State University-Fullerton	92831-3599	20,000 and above	Public, 4-year or above	D	$6,437	$8,170
California State University-Long Beach	90840-0115	20,000 and above	Public, 4-year or above	D	$6,452	$9,867
California State University-Los Angeles	90032-8506	20,000 and above	Public, 4-year or above	D	$6,355	$3,933
California State University-Northridge	91330	20,000 and above	Public, 4-year or above	D	$6,569	$6,574
California University of Management and Sciences	92801	Under 1,000	Private not-for-profit, 4-year or above	D	$9,570	
Cerritos College	90650-6298	20,000 and above	Public, 2-year	D	$1,346	$10,579
Chapman University	92866	5,000 - 9,999	Private not-for-profit, 4-year or above	D	$47,260	$40,709
Charter College-Canyon Country	91351	Under 1,000	Private for-profit, 4-year or above	D	$17,336	
Citrus College	91741-1899	10,000 - 19,999	Public, 2-year	D	$1,174	$4,051
Claremont Graduate University	91711-6160	1,000 - 4,999	Private not-for-profit, 4-year or above	D		
Claremont McKenna College	91711-6400	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$49,045	$30,527
Coastline Community College	92708-2597	10,000 - 19,999	Public, 2-year	D	$1,136	$17,760
Cypress College	90630-5897	10,000 - 19,999	Public, 2-year	D	$1,138	$8,102
East Los Angeles College	91754-6099	20,000 and above	Public, 2-year	D	$1,222	$9,024
East San Gabriel Valley Regional Occupational Program	91790	Under 1,000	Public, 2-year	D		$15,466
El Camino College-Compton Center	90221-5393	5,000 - 9,999	Public, 2-year	D	$1,142	$9,841
El Camino Community College District	90506	20,000 and above	Public, 2-year	D	$1,142	$10,569
Empire College	95403-2126	Under 1,000	Private for-profit, 4-year or above	D		$15,821
Fremont College	90703	Under 1,000	Private for-profit, 4-year or above	D		$21,542
Fullerton College	92832-2095	20,000 and above	Public, 2-year	D	$1,138	$7,001
Glendale Community College	91208-2894	10,000 - 19,999	Public, 2-year	D	$1,175	$3,799
Golden West College	92647-2710	10,000 - 19,999	Public, 2-year	D	$1,176	$9,846
Harvey Mudd College	91711	Under 1,000	Private not-for-profit, 4-year or above	D	$50,649	$35,460
Irvine Valley College	92618-0301	10,000 - 19,999	Public, 2-year	D	$1,326	$7,515
Learnet Academy Inc	90020	Under 1,000	Private for-profit, 2-year	D		
Long Beach City College	90808-1706	20,000 and above	Public, 2-year	D	$1,182	$5,467
Los Angeles City College	90029	10,000 - 19,999	Public, 2-year	D	$1,198	$7,470

APPENDIX H: POSTSECONDARY CYBERSECURITY PROGRAMMING IN CALIFORNIA

List of IPEDS-reporting Postsecondary Institutions Providing Cybersecurity Programming in California, with Institutional Characteristics, by Region (continued)

Institution Name	ZIP Code Location	Enrollment	Sector	Degree/ nondegree (D/ND)†	Tuition & Fees	Net Price‡
Los Angeles/Orange County (continued)						
Los Angeles Harbor College	90744-2397	5,000 - 9,999	Public, 2-year	D	$1,198	$11,120
Los Angeles Mission College	91342-3200	10,000 - 19,999	Public, 2-year	D	$1,198	$9,425
Los Angeles Pierce College	91371-0002	20,000 and above	Public, 2-year	D	$1,198	$9,980
Los Angeles Southwest College	90047-4899	5,000 - 9,999	Public, 2-year	D	$1,198	$7,338
Los Angeles Trade Technical College	90015-4181	10,000 - 19,999	Public, 2-year	D	$1,198	$7,330
Los Angeles Valley College	91401-4096	10,000 - 19,999	Public, 2-year	D	$1,198	$9,684
Loyola Marymount University	90045-2659	5,000 - 9,999	Private not-for-profit, 4-year or above	D	$42,795	$40,946
Mount Saint Mary's University	90049-1599	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$35,944	$27,134
Mt San Antonio College	91789-1399	20,000 and above	Public, 2-year	D	$1,348	$4,555
Mt Sierra College	91016	Under 1,000	Private for-profit, 4-year or above	D	$15,588	$21,513
Occidental College	90041-3392	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$49,248	$31,990
Orange Coast College	92626	20,000 and above	Public, 2-year	D	$1,184	$10,515
Pacific States University	90010	Under 1,000	Private not-for-profit, 4-year or above	D	$16,005	
Palladium Technical Academy	91780	Under 1,000	Private for-profit, less-than 2-year	ND		$18,385
Pasadena City College	91106-2003	20,000 and above	Public, 2-year	D	$1,152	$6,780
PCI College	90703	Under 1,000	Private for-profit, 2-year	ND		$23,210
Pepperdine University	90263	5,000 - 9,999	Private not-for-profit, 4-year or above	D	$48,342	$39,637
Pitzer College	91711-6101	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$48,670	$25,521
Pomona College	91711-6319	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$47,620	$18,140
Rio Hondo College	90601-1616	10,000 - 19,999	Public, 4-year or above	D	$1,360	$7,420
Saddleback College	92692-3635	10,000 - 19,999	Public, 2-year	D	$1,326	$9,145
Santa Ana College	92706-3398	20,000 and above	Public, 4-year or above	D	$1,142	$5,912
Santa Monica College	90405-1628	20,000 and above	Public, 4-year or above	D	$1,136	$7,016
Santiago Canyon College	92869-4512	10,000 - 19,999	Public, 2-year	D	$1,142	$5,703
Scripps College	91711-3905	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$49,152	$37,860

APPENDIX H: POSTSECONDARY CYBERSECURITY PROGRAMMING IN CALIFORNIA

List of IPEDS-reporting Postsecondary Institutions Providing Cybersecurity Programming in California, with Institutional Characteristics, by Region (continued)

Institution Name	ZIP Code Location	Enrollment	Sector	Degree/ nondegree (D/ND)†	Tuition & Fees	Net Price‡
Los Angeles/Orange County (continued)						
Southern California Institute of Technology	92801-3758	Under 1,000	Private for-profit, 4-year or above	D	$17,235	$24,026
Stanbridge College	92612	1,000 - 4,999	Private for-profit, 4-year or above	D		$25,027
The Master's University and Seminary	91321-1200	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$30,920	$26,650
Trident University International	90630-5041	5,000 - 9,999	Private for-profit, 4-year or above	D	$9,000	$13,175
Unitek College	94538	1,000 - 4,999	Private for-profit, 4-year or above	D	$32,685	$42,096
University of California-Irvine	92697	20,000 and above	Public, 4-year or above	D	$13,252	$13,780
University of California-Los Angeles	90095-1405	20,000 and above	Public, 4-year or above	D	$12,763	$14,236
University of La Verne	91750-4401	5,000 - 9,999	Private not-for-profit, 4-year or above	D	$38,560	$22,284
University of Southern California	90089	20,000 and above	Private not-for-profit, 4-year or above	D	$50,210	$32,932
University of the People	91101	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$1,000	$2,138
University of the West	91770	Under 1,000	Private not-for-profit, 4-year or above	D	$10,656	$12,474
Vanguard University of Southern California	92626	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$30,050	$21,827
West Los Angeles College	90230-3519	10,000 - 19,999	Public, 4-year or above	D	$1,198	$8,643
San Diego/Imperial						
Advanced Training Associates	92020	Under 1,000	Private for-profit, 2-year	D		$12,810
Argosy University-San Diego	92108	Under 1,000	Private for-profit, 4-year or above	D	$13,560	$20,749
Argosy University-The Art Institute of California-San Diego	92108-4423	1,000 - 4,999	Private for-profit, 4-year or above	D	$18,744	$24,168
Ashford University	92123	20,000 and above	Private for-profit, 4-year or above	D	$10,720	$18,235
Associated Technical College-San Diego	92101	Under 1,000	Private for-profit, less-than 2-year	ND		$21,763
California College San Diego	92069-2971	Under 1,000	Private not-for-profit, 4-year or above	D	$16,968	$25,215
California Miramar University	92108	Under 1,000	Private for-profit, 4-year or above	D	$8,240	$20,960

APPENDIX H: POSTSECONDARY CYBERSECURITY PROGRAMMING IN CALIFORNIA

List of IPEDS-reporting Postsecondary Institutions Providing Cybersecurity Programming in California, with Institutional Characteristics, by Region (continued)

Institution Name	ZIP Code Location	Enrollment	Sector	Degree/ nondegree (D/ND)†	Tuition & Fees	Net Price‡
San Diego/Imperial (continued)						
California State University-San Marcos	92096-0001	10,000 - 19,999	Public, 4-year or above	D	$7,269	$8,985
Coleman University	92123-1506	Under 1,000	Private not-for-profit, 4-year or above	D	$20,725	$25,619
Cuyamaca College	92019	5,000 - 9,999	Public, 2-year	D	$1,388	$5,474
Grossmont College	92020-1799	10,000 - 19,999	Public, 2-year	D	$1,388	$2,953
Imperial Valley College	92251-0158	5,000 - 9,999	Public, 2-year	D	$1,365	$4,605
MediaTech Institute-Oceanside	92054-5116	Under 1,000	Private for-profit, less-than 2-year	ND		$22,176
MiraCosta College	92056-3899	10,000 - 19,999	Public, 2-year	D	$1,152	$5,743
National University	92037-1011	10,000 - 19,999	Private not-for-profit, 4-year or above	D	$12,744	$22,377
Palomar College	92069-1487	20,000 and above	Public, 2-year	D	$1,338	$5,137
Platt College-San Diego	92115-3919	Under 1,000	Private for-profit, 4-year or above	D	$23,250	$35,949
Point Loma Nazarene University	92106-2899	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$32,400	$29,954
San Diego City College	92101-4787	10,000 - 19,999	Public, 2-year	D	$1,142	$6,358
San Diego Mesa College	92111-4998	20,000 and above	Public, 4-year or above	D	$1,142	$7,567
San Diego Miramar College	92126-2999	10,000 - 19,999	Public, 2-year	D	$1,142	$6,850
San Diego State University	92182	20,000 and above	Public, 4-year or above	D	$6,976	$14,344
Southwestern College	91910-7299	10,000 - 19,999	Public, 2-year	D	$1,336	$5,652
University of California-San Diego	92093	20,000 and above	Public, 4-year or above	D	$13,530	$14,770
University of San Diego	92110-2492	5,000 - 9,999	Private not-for-profit, 4-year or above	D	$44,586	$38,596
South Central Coast						
Allan Hancock College	93454-6399	10,000 - 19,999	Public, 2-year	D	$1,346	$5,387
Antelope Valley College	93536-5426	10,000 - 19,999	Public, 4-year or above	D	$1,104	$4,646
California Lutheran University	91360-2787	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$38,430	$29,038
California Polytechnic State University-San Luis Obispo	93407	20,000 and above	Public, 4-year or above	D	$9,001	$18,530
California State University-Channel Islands	93012	5,000 - 9,999	Public, 4-year or above	D	$6,547	$14,461
College of the Canyons	91355-1899	10,000 - 19,999	Public, 2-year	D	$1,154	$6,680
Cuesta College	93403-8106	10,000 - 19,999	Public, 2-year	D	$1,234	$10,342

APPENDIX H: POSTSECONDARY CYBERSECURITY PROGRAMMING IN CALIFORNIA

List of IPEDS-reporting Postsecondary Institutions Providing Cybersecurity Programming in California, with Institutional Characteristics, by Region (continued)

Institution Name	ZIP Code Location	Enrollment	Sector	Degree/ nondegree (D/ND)†	Tuition & Fees	Net Price‡
South Central Coast (continued)						
Laurus College	93401	1,000 - 4,999	Private for-profit, 2-year	D		$13,098
Moorpark College	93021-1695	10,000 - 19,999	Public, 2-year	D	$1,388	$4,223
Oxnard College	93033-6699	5,000 - 9,999	Public, 2-year	D	$1,388	$2,997
Santa Barbara Business College-Ventura	93003	Under 1,000	Private for-profit, 4-year or above	D	$13,619	$16,554
Santa Barbara City College	93109-2394	10,000 - 19,999	Public, 2-year	D	$1,374	$10,984
University of California-Santa Barbara	93106	20,000 and above	Public, 4-year or above	D	$13,968	$15,149
Ventura Adult and Continuing Education	93003-0000	Under 1,000	Public, less-than 2-year	ND		$13,173
Westmont College	93108-1089	1,000 - 4,999	Private not-for-profit, 4-year or above	D	$41,360	$34,974
Region N/A						
Computer Training Academy	92507	Under 1,000	Private for-profit, less-than 2-year	ND		$28,640
DeVry University-California	91768	1,000 - 4,999	Private for-profit, 4-year or above	D	$19,568	$27,224
Institute of Technology	93612	1,000 - 4,999	Private for-profit, 2-year	D		$24,000
University of Phoenix-California	92626	10,000 - 19,999	Private for-profit, 4-year or above	D	$9,818	$18,059

† Degree-granting status: D is Degree-granting; ND is Nondegree-granting, primarily postsecondary.

‡ Average Net Price of Attendance

APPENDIX I: ARTICULATIONS BETWEEN SECONDARY AND POSTSECONDARY PROGRAMS

Inventory of Formal Articulations between Regional Secondary and Postsecondary Cybersecurity-related Programs by Region

Secondary School	Post-Secondary School	Region	Discipline	Date	Template Title/ Agreement Title
San Mateo County Office of Education, ROP	College of San Mateo	Bay Area	IT Applications	4/16/12	Introduction to Computer Information Systems/Applications
East Side Union HSD	Evergreen Valley College	Bay Area	IT Applications	9/9/11	Introduction to Computer Information Systems/Applications
Antioch High	Los Medanos College	Bay Area	IT Applications	2/24/17	Introduction to Computer Information Systems/Applications
Pittsburg High	Los Medanos College	Bay Area	IT Applications	7/4/05	Introduction to Computer Information Systems/Applications
Milpitas High	Mission College	Bay Area	IT Applications	4/28/10	Introduction to Computer Information Systems/Applications
Santa Clara Adult Ed	Mission College	Bay Area	IT Applications	3/19/10	Introduction to Computer Information Systems/Applications
Wilson High	Mission College	Bay Area	IT Applications	3/20/10	Introduction to Computer Information Systems/Applications
Eden Area ROP	Ohlone College	Bay Area	CIS Cisco/A+	4/10/17	Cisco Networking Academy: Discovery I Networking for Home and Small Business
Mission Valley ROP	Ohlone College	Bay Area	CIS Cisco/A+	4/10/17	A+ IT Essentials
Mission Valley ROP	Ohlone College	Bay Area	CIS Cisco/A+	1/1/09	Cisco Networking Academy: Discovery I Networking for Home and Small Business
East Side Union HSD	San Jose City College	Bay Area	IT Applications	5/13/13	Introduction to Computer Information Systems/Applications
Healdsburg High	Santa Rosa Junior College	Bay Area	CIS Cisco/A+	5/12/10	A+ IT Essentials
Healdsburg High	Santa Rosa Junior College	Bay Area	CIS Cisco/A+	5/13/10	Cisco Networking Academy: Discovery I Networking for Home and Small Business
Middletown High	Santa Rosa Junior College	Bay Area	CIS Cisco/A+	5/12/10	A+ IT Essentials
Middletown High	Santa Rosa Junior College	Bay Area	CIS Cisco/A+	4/1/10	Cisco Networking Academy: Discovery II: Working at a Small-to-Medium Business or ISP
Santa Rosa High	Santa Rosa Junior College	Bay Area	CIS Cisco/A+	5/26/10	A+ IT Essentials
Santa Rosa High	Santa Rosa Junior College	Bay Area	CIS Cisco/A+	5/26/10	Cisco Networking Academy: Discovery I Networking for Home and Small Business
Goodwill Industries	Skyline College	Bay Area	CIS Cisco/A+	4/1/10	A+ IT Essentials
Benicia High	Solano College	Bay Area	IT Applications	11/19/14	Introduction to Computer Information Systems/Applications
Sem Yeto High	Solano College	Bay Area	IT Applications	2/27/13	Introduction to Computer Information Systems/Applications
Vanden High	Solano College	Bay Area	IT Applications	3/5/13	Introduction to Computer Information Systems/Applications
Bakersfield Adult School	Bakersfield College	Central California	IT Applications	4/30/15	Introduction to Computer Information Systems/Applications

APPENDIX I: ARTICULATIONS BETWEEN SECONDARY AND POSTSECONDARY PROGRAMS

Inventory of Formal Articulations between Regional Secondary and Postsecondary Cybersecurity-related Programs by Region (continued)

Secondary School	Post-Secondary School	Region	Discipline	Date	Template Title/ Agreement Title
Cesar E. Chavez High	Bakersfield College	Central California	IT Applications	4/30/14	Introduction to Computer Information Systems/Applications
Golden West High	College of the Sequoias	Central California	CIS Cisco/A+	4/28/09	A+ IT Essentials
Granite Hills High	College of the Sequoias	Central California	CIS Cisco/A+	4/28/09	A+ IT Essentials
Porterville High	College of the Sequoias	Central California	CIS Cisco/A+	4/28/09	Cisco Networking Academy: Discovery I Networking for Home and Small Business
Porterville High	College of the Sequoias	Central California	CIS Cisco/A+	4/28/09	Network +
Colusa Community Learning Center	Woodland College	Far North	IT Applications	12/16/10	Introduction to Computer Information Systems/Applications
Maxwell High	Woodland College	Far North	IT Applications	3/15/11	Introduction to Computer Information Systems/Applications
Sutter County One Stop	Woodland College	Far North	IT Applications	3/15/11	Introduction to Computer Information Systems/Applications
Woodland High	Woodland College	Far North	IT Applications	11/29/12	Introduction to Computer Information Systems/Applications
Faith Christian High	Yuba College	Far North	IT Applications	4/6/11	Introduction to Computer Information Systems/Applications
Middletown High	Yuba College	Far North	IT Applications	3/28/11	Introduction to Computer Information Systems/Applications
Sutter County One Stop	Yuba College	Far North	IT Applications	4/7/11	Introduction to Computer Information Systems/Applications
Cordova High	Folsom Lake College	Greater Sacramento	IT Applications	3/6/14	Introduction to Computer Information Systems/Applications
Folsom High	Folsom Lake College	Greater Sacramento	IT Applications	11/17/15	Introduction to Computer Information Systems/Applications
Sheldon High	Folsom Lake College	Greater Sacramento	IT Applications	4/27/17	Introduction to Computer Information Systems/Applications
Davis Senior High	Sacramento City College	Greater Sacramento	CIS Cisco/A+	3/10/15	A+ IT Essentials
Davis Senior High	Sacramento City College	Greater Sacramento	CIS Cisco/A+	3/18/13	Cisco Networking Academy: Discovery I Networking for Home and Small Business
Davis Senior High	Sacramento City College	Greater Sacramento	CIS Cisco/A+	10/6/16	Cisco Networking Academy: Exploration I: Network Fundamentals
Pioneer High	Sacramento City College	Greater Sacramento	CIS Cisco/A+	3/24/17	A+ IT Essentials
Pioneer High	Sacramento City College	Greater Sacramento	CIS Cisco/A+	4/9/13	Cisco Networking Academy: Discovery I Networking for Home and Small Business
Sacramento New Technology High	Sacramento City College	Greater Sacramento	IT Applications	10/6/16	Introduction to Computer Information Systems/Applications
A. B. Miller High	Chaffey College	Inland Empire/ Desert	IT Applications	11/6/14	Introduction to Computer Information Systems/Applications

APPENDIX I: ARTICULATIONS BETWEEN SECONDARY AND POSTSECONDARY PROGRAMS

Inventory of Formal Articulations between Regional Secondary and Postsecondary Cybersecurity-related Programs by Region (continued)

Secondary School	Post-Secondary School	Region	Discipline	Date	Template Title/ Agreement Title
Alta Loma High	Chaffey College	Inland Empire/ Desert	CIS Cisco/A+	11/6/14	A+ IT Essentials
Alta Loma High	Chaffey College	Inland Empire/ Desert	IT Applications	11/7/14	Introduction to Computer Information Systems/Applications
Baldy View ROP Alta Career Technical Center	Chaffey College	Inland Empire/ Desert	CIS Cisco/A+	3/3/15	A+ IT Essentials
Baldy View ROP Career Training Center	Chaffey College	Inland Empire/ Desert	CIS Cisco/A+	4/9/18	A+ IT Essentials
Birch High	Chaffey College	Inland Empire/ Desert	CIS Cisco/A+	11/14/14	A+ IT Essentials
Birch High	Chaffey College	Inland Empire/ Desert	IT Applications	11/6/14	Introduction to Computer Information Systems/Applications
Chaffey High	Chaffey College	Inland Empire/ Desert	IT Applications	11/7/14	Introduction to Computer Information Systems/Applications
Citrus High	Chaffey College	Inland Empire/ Desert	IT Applications	11/6/14	Introduction to Computer Information Systems/Applications
Colony High	Chaffey College	Inland Empire/ Desert	IT Applications	11/7/14	Introduction to Computer Information Systems/Applications
Etiwanda High	Chaffey College	Inland Empire/ Desert	IT Applications	11/7/14	Introduction to Computer Information Systems/Applications
Fontana High	Chaffey College	Inland Empire/ Desert	IT Applications	11/6/14	Introduction to Computer Information Systems/Applications
Henry J. Kaiser High	Chaffey College	Inland Empire/ Desert	IT Applications	11/6/14	Introduction to Computer Information Systems/Applications
Jurupa Hills High	Chaffey College	Inland Empire/ Desert	IT Applications	11/6/14	Introduction to Computer Information Systems/Applications
Los Osos High	Chaffey College	Inland Empire/ Desert	IT Applications	11/7/14	Introduction to Computer Information Systems/Applications
Montclair High	Chaffey College	Inland Empire/ Desert	IT Applications	11/7/14	Introduction to Computer Information Systems/Applications
Ontario High	Chaffey College	Inland Empire/ Desert	CIS Cisco/A+	11/6/14	A+ IT Essentials
Ontario High	Chaffey College	Inland Empire/ Desert	IT Applications	5/1/17	Introduction to Computer Information Systems/Applications
Pacific High	Chaffey College	Inland Empire/ Desert	CIS Cisco/A+	11/14/14	A+ IT Essentials
Rancho Cucamonga High	Chaffey College	Inland Empire/ Desert	IT Applications	11/7/14	Introduction to Computer Information Systems/Applications
Redlands East Valley High	Chaffey College	Inland Empire/ Desert	CIS Cisco/A+	2/12/15	Cisco Networking Academy: Discovery I Networking for Home and Small Business
Redlands East Valley High	Chaffey College	Inland Empire/ Desert	CIS Cisco/A+	2/12/15	Cisco Networking Academy: Discovery II: Working at a Small-to-Medium Business or ISP
Redlands Senior High	Chaffey College	Inland Empire/ Desert	CIS Cisco/A+	2/12/15	Cisco Networking Academy: Discovery I Networking for Home and Small Business

APPENDIX I: ARTICULATIONS BETWEEN SECONDARY AND POSTSECONDARY PROGRAMS

Inventory of Formal Articulations between Regional Secondary and Postsecondary Cybersecurity-related Programs by Region (continued)

Secondary School	Post-Secondary School	Region	Discipline	Date	Template Title/ Agreement Title
Redlands Senior High	Chaffey College	Inland Empire/ Desert	CIS Cisco/A+	2/12/15	Cisco Networking Academy: Discovery II: Working at a Small-to-Medium Business or ISP
Summit High	Chaffey College	Inland Empire/ Desert	CIS Cisco/A+	11/14/14	A+ IT Essentials
Summit High	Chaffey College	Inland Empire/ Desert	IT Applications	11/6/14	Introduction to Computer Information Systems/Applications
Twentynine Palms High	Chaffey College	Inland Empire/ Desert	CIS Cisco/A+	11/14/14	A+ IT Essentials
Upland High	Chaffey College	Inland Empire/ Desert	IT Applications	12/17/14	Introduction to Computer Information Systems/Applications
Valley View High	Chaffey College	Inland Empire/ Desert	IT Applications	11/7/14	Introduction to Computer Information Systems/Applications
Coachella Valley High	College of the Desert	Inland Empire/ Desert	IT Applications	3/30/12	Introduction to Computer Information Systems/Applications
La Familia Continuation High	College of the Desert	Inland Empire/ Desert	IT Applications	3/30/12	Introduction to Computer Information Systems/Applications
Palo Verde High	College of the Desert	Inland Empire/ Desert	IT Applications	6/21/12	Introduction to Computer Information Systems/Applications
Colton-Redlands-Yucaipa ROP	Crafton Hills College	Inland Empire/ Desert	CIS Cisco/A+	1/30/15	Cisco Networking Academy: Discovery I Networking for Home and Small Business
Colton-Redlands-Yucaipa ROP	Crafton Hills College	Inland Empire/ Desert	CIS Cisco/A+	5/6/13	Cisco Networking Academy: Discovery II: Working at a Small-to-Medium Business or ISP
Colton-Redlands-Yucaipa ROP	Crafton Hills College	Inland Empire/ Desert	CIS Cisco/A+	6/2/09	Cisco Networking Academy: Exploration I: Network Fundamentals
San Bernardino City USD	Crafton Hills College	Inland Empire/ Desert	CIS Cisco/A+	3/16/10	Cisco Networking Academy: Discovery I Networking for Home and Small Business
San Bernardino City USD	Crafton Hills College	Inland Empire/ Desert	CIS Cisco/A+	3/16/10	Cisco Networking Academy: Discovery II: Working at a Small-to-Medium Business or ISP
San Bernardino City USD	Crafton Hills College	Inland Empire/ Desert	CIS Cisco/A+	6/15/14	Cisco Networking Academy: Exploration I: Network Fundamentals
San Bernardino County ROP	Crafton Hills College	Inland Empire/ Desert	CIS Cisco/A+	5/5/09	A+ IT Essentials
Brawley High	Imperial Valley College	Inland Empire/ Desert	IT Applications	7/5/05	Introduction to Computer Information Systems/Applications
Central Union High	Imperial Valley College	Inland Empire/ Desert	IT Applications	7/5/05	Introduction to Computer Information Systems/Applications
Holtville High	Imperial Valley College	Inland Empire/ Desert	IT Applications	7/5/05	Introduction to Computer Information Systems/Applications
San Pasqual High	Imperial Valley College	Inland Empire/ Desert	IT Applications	7/5/05	Introduction to Computer Information Systems/Applications
Southwest High	Imperial Valley College	Inland Empire/ Desert	IT Applications	7/5/05	Introduction to Computer Information Systems/Applications

APPENDIX I: ARTICULATIONS BETWEEN SECONDARY AND POSTSECONDARY PROGRAMS

Inventory of Formal Articulations between Regional Secondary and Postsecondary Cybersecurity-related Programs by Region (continued)

Secondary School	Post-Secondary School	Region	Discipline	Date	Template Title/ Agreement Title
Lake Elsinore USD	Mt. San Jacinto College	Inland Empire/ Desert	IT Applications	2/21/13	Introduction to Computer Information Systems/Applications
Perris UHSD	Mt. San Jacinto College	Inland Empire/ Desert	IT Applications	2/21/13	Introduction to Computer Information Systems/Applications
Colton-Redlands-Yucaipa ROP	Riverside CCD	Inland Empire/ Desert	CIS Cisco/A+	6/2/11	Cisco Networking Academy: Exploration I: Network Fundamentals
Riverside USD	Riverside CCD	Inland Empire/ Desert	CIS Cisco/A+	6/2/11	Cisco Networking Academy: Discovery I Networking for Home and Small Business
Riverside USD	Riverside CCD	Inland Empire/ Desert	CIS Cisco/A+	6/2/11	Cisco Networking Academy: Discovery II: Working at a Small-to-Medium Business or ISP
San Bernardino City USD	Riverside CCD	Inland Empire/ Desert	CIS Cisco/A+	6/2/11	Cisco Networking Academy: Exploration I: Network Fundamentals
Val Verde USD	Riverside CCD	Inland Empire/ Desert	CIS Cisco/A+	6/2/11	Cisco Networking Academy: Exploration I: Network Fundamentals
San Bernardino County ROP	San Bernardino Valley College	Inland Empire/ Desert	CIS Cisco/A+	5/5/09	A+ IT Essentials
San Bernardino County ROP	San Bernardino Valley College	Inland Empire/ Desert	CIS Cisco/A+	3/16/10	Cisco Networking Academy: Discovery I Networking for Home and Small Business
San Bernardino County ROP	San Bernardino Valley College	Inland Empire/ Desert	CIS Cisco/A+	5/4/09	Cisco Networking Academy: Discovery II: Working at a Small-to-Medium Business or ISP
San Bernardino County ROP	San Bernardino Valley College	Inland Empire/ Desert	CIS Cisco/A+	3/16/10	Cisco Networking Academy: Exploration I: Network Fundamentals
San Bernardino County ROP	San Bernardino Valley College	Inland Empire/ Desert	IT Applications	3/5/09	Introduction to Computer Information Systems/Applications
Central County Occupational Center	Coastline College	Los Angeles/ Orange County	CIS Cisco/A+	5/1/14	A+ IT Essentials
Central County ROP	Coastline College	Los Angeles/ Orange County	CIS Cisco/A+	5/1/14	A+ IT Essentials
Central County ROP	Coastline College	Los Angeles/ Orange County	CIS Cisco/A+	5/1/14	Network +
Central County ROP	Coastline College	Los Angeles/ Orange County	IT Applications	4/23/10	Introduction to Computer Information Systems/Applications
Central Orange County CTEP	Coastline College	Los Angeles/ Orange County	CIS Cisco/A+	5/6/16	A+ IT Essentials
Central Orange County CTEP	Coastline College	Los Angeles/ Orange County	CIS Cisco/A+	5/6/16	Network +
Central Orange County CTEP	Coastline College	Los Angeles/ Orange County	IT Applications	5/6/16	Introduction to Computer Information Systems/Applications
Coastline ROP	Coastline College	Los Angeles/ Orange County	CIS Cisco/A+	4/23/10	A+ IT Essentials
Garden Grove Unified School District	Coastline College	Los Angeles/ Orange County	CIS Cisco/A+	4/23/10	Network +

APPENDIX I: ARTICULATIONS BETWEEN SECONDARY AND POSTSECONDARY PROGRAMS

Inventory of Formal Articulations between Regional Secondary and Postsecondary Cybersecurity-related Programs by Region (continued)

Secondary School	Post-Secondary School	Region	Discipline	Date	Template Title/ Agreement Title
Garden Grove Unified School District	Coastline College	Los Angeles/ Orange County	IT Applications	4/23/10	Introduction to Computer Information Systems/Applications
Huntington Beach Adult School	Coastline College	Los Angeles/ Orange County	CIS Cisco/A+	5/6/16	A+ IT Essentials
Huntington Beach Adult School	Coastline College	Los Angeles/ Orange County	CIS Cisco/A+	5/6/16	Cisco Networking Academy: Discovery I Networking for Home and Small Business
North Orange County ROP	Coastline College	Los Angeles/ Orange County	IT Applications	1/0/00	Introduction to Computer Information Systems/Applications
Valencia High	Coastline College	Los Angeles/ Orange County	CIS Cisco/A+	5/21/09	A+ IT Essentials
Central County ROP	Golden West College	Los Angeles/ Orange County	IT Applications	7/5/05	Introduction to Computer Information Systems/Applications
Coast Union High	Golden West College	Los Angeles/ Orange County	IT Applications	4/1/12	Introduction to Computer Information Systems/Applications
Coastline ROP	Golden West College	Los Angeles/ Orange County	IT Applications	7/5/05	Introduction to Computer Information Systems/Applications
El Toro High	Golden West College	Los Angeles/ Orange County	IT Applications	7/5/05	Introduction to Computer Information Systems/Applications
Laguna Hills High	Golden West College	Los Angeles/ Orange County	IT Applications	7/5/05	Introduction to Computer Information Systems/Applications
Marina High	Golden West College	Los Angeles/ Orange County	IT Applications	7/5/05	Introduction to Computer Information Systems/Applications
North Orange County ROP	Golden West College	Los Angeles/ Orange County	IT Applications	7/5/05	Introduction to Computer Information Systems/Applications
Calabasas High	Los Angeles Pierce College	Los Angeles/ Orange County	CIS Cisco/A+	11/17/10	Cisco Networking Academy: Discovery I Networking for Home and Small Business
Baldwin Park Adult and Continuing Education	Mt. San Antonio College	Los Angeles/ Orange County	CIS Cisco/A+	10/16/13	A+ IT Essentials
Baldy View ROP Career Training Center	Mt. San Antonio College	Los Angeles/ Orange County	CIS Cisco/A+	2/26/16	A+ IT Essentials
East San Gabriel Valley ROP	Mt. San Antonio College	Los Angeles/ Orange County	CIS Cisco/A+	1/15/15	A+ IT Essentials
Tri-C Adult Education	Mt. San Antonio College	Los Angeles/ Orange County	CIS Cisco/A+	1/0/00	A+ IT Essentials
Santa Fe High	Rio Hondo College	Los Angeles/ Orange County	IT Applications	11/19/12	Introduction to Computer Information Systems/Applications
Capistrano-Laguna Beach ROP	Saddleback College	Los Angeles/ Orange County	CIS Cisco/A+	7/5/05	A+ IT Essentials
Coastline ROP	Saddleback College	Los Angeles/ Orange County	CIS Cisco/A+	7/8/05	A+ IT Essentials
Coastline ROP	Saddleback College	Los Angeles/ Orange County	IT Applications	4/17/13	Introduction to Computer Information Systems/Applications
College and Career Advantage	Saddleback College	Los Angeles/ Orange County	CIS Cisco/A+	7/8/05	A+ IT Essentials

APPENDIX I: ARTICULATIONS BETWEEN SECONDARY AND POSTSECONDARY PROGRAMS

Inventory of Formal Articulations between Regional Secondary and Postsecondary Cybersecurity-related Programs by Region (continued)

Secondary School	Post-Secondary School	Region	Discipline	Date	Template Title/ Agreement Title
Laguna Hills High	Saddleback College	Los Angeles/ Orange County	IT Applications	4/25/17	Introduction to Computer Information Systems/Applications
New Vista School Tech Academy	Saddleback College	Los Angeles/ Orange County	IT Applications	4/25/17	Introduction to Computer Information Systems/Applications
Saddleback Valley USD	Saddleback College	Los Angeles/ Orange County	IT Applications	4/17/13	Introduction to Computer Information Systems/Applications
South Coast ROP	Saddleback College	Los Angeles/ Orange County	CIS Cisco/A+	7/8/05	A+ IT Essentials
Del Norte High	Palomar College	San Diego/ Imperial	IT Applications	3/10/10	Introduction to Computer Information Systems/Applications
Escondido Charter High	Palomar College	San Diego/ Imperial	IT Applications	11/5/10	Introduction to Computer Information Systems/Applications
Rancho Bernardo High	Palomar College	San Diego/ Imperial	IT Applications	5/18/10	Introduction to Computer Information Systems/Applications
Sweetwater Union HSD CTE Division of Adult Ed	Southwestern College	San Diego/ Imperial	CIS Cisco/A+	11/25/08	A+ IT Essentials
Sweetwater Union HSD CTE Division of Adult Ed	Southwestern College	San Diego/ Imperial	CIS Cisco/A+	11/25/08	Network +
Moorpark High	Moorpark College	South Central	CIS Cisco/A+	5/1/08	A+ IT Essentials

Source: California Statewide Career Pathways (www.statepathways.org)

APPENDIX J: CYBERSECURITY COURSES AT CALIFORNIA PUBLIC HIGH SCHOOLS

List of Cybersecurity-related and Pre-cybersecurity Secondary Courses at California Public High Schools

Course Number	Course Title	Course Description
4604	Network Engineering	This course prepares students for jobs as network technicians and helps them develop skills required for computer technicians provides a basic overview of routing and remote access, addressing, and security. It also familiarizes students with servers that provide email services, web space, and authenticated access. Students learn about the soft skills required for help desk and customer service positions, and help them prepare for industry certification exams. Students perform a great deal of hands-on work on routers, switches, and firewalls as they learn to design, build, and maintain data networks using with some of the most powerful enterprise network technologies of the day. The course covers some of the most powerful technologies used on enterprise networks including wireless networks, virtual LANs (VLANs), Spanning-Tree Protocol (STP), traffic management with access control lists (ACLs), dynamic routing, and wide area network (WAN) technologies. Course titles may also include: Network Design, Installation & Engineering; Introduction to Networking.
4631	Database Design and SQL Programming	This two-part course teaches data modeling and Structured Query Language (SQL). In the database design curriculum, students learn to analyze complex business scenarios and create a data model, a conceptual representation of an organization's information. In the database programming with SQL curriculum, students implement their database design by creating a physical database using SQL, the industry-standard database programming language. Upon completion of this course, students have the opportunity to take an exam to earn the industry certification Oracle Database SQL Certified Expert.
4633	Computer Repair and Support	This course will explore workplace safety, customer relations, and help ticket documentation. Students will also learn various computer operating systems such as Linus, computer maintenance, electrical measurements and energy conservation, basic troubleshooting, and virus protection. Students will also be introduced to various devices such as tablets, laptops and mobile devices; and, network architecture and internet technologies, as well as careers in the IT industry. This course will prepare students for internships working at a helpdesk, or in a computer repair shop. Course titles may also include: Information Technology Essentials; Computer Service Technology.
4634	Exploring Computer Science	This course provides students with foundational knowledge of computer science. Students will explore topics of human computer interaction, problem solving, web design, computer programming, data modeling, and robotics. Throughout the course, students will understand the algorithmic underpinnings of computer applications and gain technical expertise using computational tools. Course titles may also include: Introduction to Computer Science A; Computer Principles.
4641	CTE AP Computer Science A	Taught by a Career Technical Education (CTE) authorized teacher, CTE Computer Science A emphasizes object oriented programming methodology with a concentration on problem solving and algorithm development and is meant to be the equivalent of a first semester college level course in Computer Science. It also includes the study of data structures, design, and abstraction, but these topics are not covered to the extent that they are in Computer Science AB.
4646	Network Security	This course provides an in-depth study of Network Security fundamentals and provides a comprehensive overview of network security, including computer forensics. Students will gain the knowledge and skills required to identify risk and participate in risk mitigation activities; provide infrastructure, application, operational, and information security; apply security controls to maintain confidentiality, integrity, and availability; identify appropriate technologies and products; and operate with an awareness of applicable policies, laws, and regulations.

Source: California Department of Education, CALPADS Code Sets

APPENDIX K: CYBERSECURITY EDUCATION PROGRAMS SURVEY

Part I: Institution

Q1. Please choose the category that best describes your institution:

California Community College

Other higher education institution, including Colleges and Universities

Q2. Please choose the name of college you represent:

▼Allan Hancock College (1) ... Yuba College (181)

Q2A. Please choose the name of your organization:

▼Cal Poly Pomona (1) ... Westmont College (146)

Q3. This survey is designed to collect information on cybersecurity programs and coursework/training offered at postsecondary institutions in California. We want to make sure we are reaching the right person in your institution with the knowledge regarding cybersecurity offerings to respond to this survey. Are you the best person at your institution to answer these questions?

Yes

No

Q4. (If No to Q3) Please tell us who the best person is at your institution to respond to questions about cybersecurity in the curriculum.

Name: _____

Email: _____

Phone: _____

APPENDIX K: CYBERSECURITY EDUCATION PROGRAMS SURVEY

Part II: Program Information

Q5. Does your college currently offer *programs* (majors, concentrations, or certificates) or *coursework/training* related to the following topics? (Note: these categories are from the NICE Cybersecurity Workforce Framework)

	Yes (program currently exists)	**No** (program does not exist; no plans to develop)	**No** (but we are considering adding/ developing)
Securely Provision (includes: Risk Management; Software Development; Systems Architecture; Technology R&D; Systems Requirements Planning; Test and Evaluation; Systems Development)			
Operate and Maintain (includes: Data Administration; Knowledge Management; Customer Service and Technical Support; Network Services; Systems Administration; Systems Analyst)			
Oversee and Govern (includes: Legal Advice and Advocacy; Training, Education and Awareness; Cybersecurity Management; Strategic Planning and Policy; Executive Cyber Leadership; Program/Project Management and Acquisition)			
Protect and Defend (includes: Cyber Defense Analysis; Cyber Defense Infrastructure Support; Incident Response; Vulnerability Assessment and Management)			
Analyze (includes: Threat Analysis; Exploitation Analysis; All-Source Analysis; Targets; Language Analysis)			
Collect and Operate (includes: Collection Operations; Cyber Operational Planning; Cyber Operations)			
Investigate (includes: Cyber Investigation; Digital Forensics)			

Q6. What challenges are you facing as you consider adding/developing a new program or coursework/training?

Q7. Do your cybersecurity programs or coursework/training prepare students for any of the following specific industry certifications? (Mark all that apply)

- ❑ Certified Information Systems Security Professional (CISSP)
- ❑ CISCO Certificated Network Associate Security (CCNA-S)
- ❑ CISCO Certified Network Professional Security (CCNP-S)
- ❑ Microsoft Certified System Administrator (MCSA)
- ❑ Security +
- ❑ Department of Defense Directive 8140 (Security Clearance)
- ❑ SANS/GIAC Certification
- ❑ Certified Information Systems Auditor (CISA)
- ❑ Certified Information Security Manager (CISM)
- ❑ Certified in Risk and Information Systems Control (CRISC)
- ❑ CompTIA Security +
- ❑ CompTIA Cybersecurity Analyst (CySA+)
- ❑ CompTIA PenTest+
- ❑ CompTIA Advanced Security Practitioner (CASP)
- ❑ Cisco CCNA Cyber Ops
- [❑ Certified Ethical Hacker (CEH)

- ❑ EC-Council Certified Security Analyst (ECSA)
- ❑ GIAC Penetration Tester (GPEN)
- ❑ Offensive Security Certified Professional (OSCP)
- ❑ Palo Alto Networks Firewall
- ❑ Palo Alto Networks Endpoint
- ❑ Jupiter Networks Certification Program (JNCP) Junos Security Certification
- ❑ Other, please specify: _____
- ❑ None of the above

Q8. Which soft skills are covered the most thoroughly in your cybersecurity coursework/training? (Mark all that apply)

- ❑ Communication skills
- ❑ Writing
- ❑ Troubleshooting
- ❑ Teamwork/collaboration
- ❑ Ethics
- ❑ Planning
- ❑ Problem solving
- ❑ Building effective relationships
- ❑ Quality assurance and control
- ❑ Self-starter
- ❑ Enthusiasm
- ❑ Quick learner
- ❑ Other, please specify: _____

Q9. How have employers been involved in your program in the past year? (Mark all that apply)

❑ Employers participate on my advisory board(s). If so, please indicate how many employers:

_____

❑ Employers provide internships for my students. If so, please indicate how many employers participate:

_____

❑ Employers donate equipment to my program. If so please indicate how many employers:

_____

❑ Employers act as guest lecturers. If so please indicate how many employers:

_____

❑ Employers provide information about the industry and jobs. If so please indicate how many employers:

_____

❑ Employers offer facilities tours. If so please indicate how many employers:

_____

❑ Other:

_____

❑ None of the above

APPENDIX K: CYBERSECURITY EDUCATION PROGRAMS SURVEY

Q10. How much of a challenge do the following issues present to the success of your program?

	Not a challenge	Somewhat/ Moderate challenge	Extreme challenge
Facilities—adequate, workable space for this type of program			
Staffing—finding instructors with practical experience/technical expertise			
Faculty development—providing access to professional development opportunities			
Curriculum—keeping curriculum up-to-date with constantly evolving technologies			
Equipment—finding resources for new training equipment or soliciting donations for equipment			
Employer engagement—connecting employers to the program for advisory group functions			
Employer engagement—student internships			
Employer engagement—student/graduate employment			
Maintaining Software Licenses			
Other, please specify: _____			

Q11. Does your program have dedicated computer labs for cybersecurity coursework/trainings?

- ❑ Yes
- ❑ No

Q12. Does your program have dedicated virtual computer labs for cybersecurity coursework/trainings?

- ❑ Yes
- ❑ No

Thank you very much for your important feedback!

APPENDIX L: REFERENCES CITED

"2018 Global Investor Survey: Anxious Optimism in a Complex World." PwC International Limited, 2018, p. 11 and p. 22. https://www.pwc.com/gx/en/ceo-survey/2018/deep-dives/pwc-global-investor-survey-2018.pdf.

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

California Cyberhub, 2016. https://ca-cyberhub.org/.

"The Changing State of Ransomware." F-Secure, May 2015. https://fsecurepressglobal.files.wordpress.com/2018/05/ransomware_report.pdf.

Chickowski, Erica. "Automation exacerbates cybersecurity skills gap." Dark Reading, May 2, 2018, accessed May 18, 2018. https://www.darkreading.com/careers-and-people/automation-exacerbates-cybersecurity-skills-gap/d/d-id/1331697.

Cowley, Stacy. "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.

Cuthbertson, Anthony. "Ransomware attacks reach 250 percent in 2017, hitting U.S. hardest." Newsweek, May 23, 2017. http://www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034.

"Cyber Security in San Diego: An Economic and Industry Assessment." San Diego Economic Development Corporation, March 2014.

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

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

"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.

"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.

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

Gartenberg, Chaim. "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.

Giles, Martin. "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/.

Goel, Vindu 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.

Hackett, Robert. "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/.

APPENDIX L: REFERENCES CITED

"Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills." McAfee and the Center for Strategic and International Studies, 2016. https://www.mcafee.com/uk/resources/reports/rp-hacking-skills-shortage.pdf.

"Hack the Gap: Close the cybersecurity talent gap with interactive tools and data." CyberSeek, accessed May 18, 2018. https://www.cyberseek.org/index.html#about.

"IBM X-Force Report: Fewer Records Breached in 2017." Security Magazine, April 4, 2018, accessed May 18, 2018. https://www.securitymagazine.com/articles/88893-ibm-x-force-report-fewer-records-breached-in-2017.

"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.

Morris, Chris. "14 million businesses are at risk of a hacker threat." CNBC, July 25, 2017, accessed May 18, 2018. https://www.cnbc.com/2017/07/25/14-million-us-businesses-are-at-risk-of-a-hacker-threat.html.

"National Centers of Academic Excellence in Cyber Education," National Security Agency, Central Security Service, October 31, 2016, accessed June 11, 2018, https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/.

"Nearly Half of All Cyberattacks Result in Damages over $500,000," Security Magazine, April 1, 2018, accessed May 18, 2018. https://www.securitymagazine.com/articles/88834-nearly-half-of-all-cyberattacks-result-in-damages-over-500000.

Newhouse, William, Stephanie Keith, Benjamin Scribner, and Greg Witte. "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework." National Institute of Standards and Technology, U.S. Department of Commerce, August 2017.

NICE Cybersecurity Workforce Framework, December 12, 2017. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework.

"Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision Making." Committee on Professionalizing the Nation's Cybersecurity Workforce: Criteria for Future Decision-Making, National Research Council of the National Academies, (Washington, DC: The National Academies Press), 2013.

Rio Hondo College. "Rio Hondo College to train cybersecurity technicians, professionals to meet rapidly growing industry need," press release, November 14, 2017. https://www.riohondo.edu/marketing/rio-hondo-college-to-train-cybersecurity-technicians-professionals-to-meet-rapidly-growing-industry-need/

"Security Budgets Increasing, But Qualified Cybertalent Remains Hard to Find." Security Magazine, April 23, 2018, accessed May 18, 2017. https://www.securitymagazine.com/articles/88940-security-budgets-increasing-but-qualified-cybertalent-remains-hard-to-find.

Stein, Daniel, Benjamin Scribner, Noel Kyle, William Newhouse, Clarence Williams, and Baris Yakim. "National Initiative for Cybersecurity Education (NICE) Work Role Capability Indicators." National Institute of Standards and Technology, U.S. Department of Commerce, November 2017.

Vickers, Jenny. "Cybersecurity takes center stage." Business Facilities, April 16, 2018. https://businessfacilities.com/2018/04/cybersecurity-takes-center-stage/.

Weise, Elizabeth. "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/.

Williams, Jamie. "The Worst Law in Technology Strikes Again: 2017 in Review." Electronic Frontier Foundation, December 29, 2017, accessed May 23, 2018. https://www.eff.org/deeplinks/2017/12/worst-law-technology-strikes-again-2017-review.

Whittaker, Zack. "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/.

MORE ABOUT THE CENTERS OF EXCELLENCE

The Centers of Excellence (COE) for Labor Market Research deliver regional workforce research and technical expertise to California Community Colleges for program decision making and resource development. This information has proven valuable to colleges in beginning, revising, or updating economic development and Career Education (CE) programs, strengthening grant applications, assisting in the accreditation process, and in supporting strategic planning efforts.

The Centers of Excellence Initiative is funded in part by the Chancellor's Office, California Community Colleges, Economic and Workforce Development Program. The Centers aspire to be the leading source of regional workforce information and insight for California Community Colleges. More information about the Centers of Excellence is available at **www.coeccc.net**.

For more information on this study, contact:

John Carrese,
Director, Center of Excellence
for Labor Market Research
San Francisco Bay Region
Hosted at City College of San Francisco
(415)452-5529
jcarrese@ccsf.edu

Important Disclaimer

All representations included in this report have been produced from primary research and/or secondary review of publicly and/or privately available data and/or research reports. Efforts have been made to qualify and validate the accuracy of the data and the reported findings; however, neither the Centers of Excellence, COE host District, nor California Community Colleges Chancellor's Office are responsible for applications or decisions made by recipient community colleges or their representatives based upon components or recommendations contained in this study.

© 2018 California Community Colleges Chancellor's Office Economic and Workforce Development Program

Please consider the environment before printing.
This document is designed for double-sided printing.

C·O·E
CENTERS OF EXCELLENCE
Inform Connect Advance