



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]