Regional Workforce Advisory Meeting Proceedings
Information & Communication Technologies: Cybersecurity
March 31st, 2022
Virtual - Zoom

Introduction

The Los Rios Community College District, in partnership with Valley Vision, and in collaboration with Sierra College and Yuba Community College District, invests Strong Workforce funding to organize and convene Regional Advisories. The objectives of the Regional Advisories are to build strong relationships between employers, educators, and workforce that:

- Provide timely information on skills gaps and workforce needs, informing partners on major industry trend information;
- Improve the efficiency of the advisory process for educators and employers;
- Reflect a regional view of workforce needs and assets;
- Provide opportunities for more systemic, ongoing engagement that includes workforce partners in key industry sectors.

Regional Advisory meetings help inform decisions on needed investments and enhancements for Career Education (CE) programs to help fill the growing demand for middle-skill positions. This meeting proceedings report includes key findings, best practices, and minutes from the Fall 2021 Regional Advisory meeting focused specifically on careers in Information and Communications Technologies.

Valley Vision supports a robust talent pipeline through our multiple 21st Century Workforce initiatives. We prepare our regional workforce for the future by addressing skills gaps, advancing research, aligning efforts and strengthening systems. Valley Vision's workforce efforts are supported by the Sacramento Employment and Training Agency (SETA), Golden Sierra Workforce Development Board (WDB), North Central Counties Consortium, Yolo WDB, City of Sacramento, local community college districts and others.

The Strong Workforce program provides Career Education opportunities to increase social mobility and fuels regional economies with skilled workers.

Key Findings

- Although 62% of positions require a bachelor's degree, certifications in combination with experience could allow applicants to attain jobs without needing baccalaureate education. The certifications that panelists placed the highest value on were CompTIA Security +, SANS, Python, and Microsoft Azure. Additional entry level opportunities were available through internships, apprenticeships, and contract work.

- Employers emphasized the preference for candidates to have hands-on experience which could be garnered through prior work history/work-based learning or even gaming, clubs or extracurricular activities engaging in cyber activities. Labor market analysis confirmed the value of experience indicating 35% of employers preferred applicants to have 3 to 5 years of prior experience.

- Cybersecurity and Cyber-enabled occupations provide high median wages at $96,347 annually with a respectable 5% job growth expectation and average almost 2,400 jobs annually. The fastest growing positions are Information Security Analysts at 18% and Software Developers and Software Quality Assurance Analysts and Testers with 12% expected growth.

- The National Institute of Standards and Technology (NIST) has a Workforce Framework for Cybersecurity Careers that details knowledge, skills, and abilities that are required for cybersecurity jobs. Additionally, employers stressed the need for soft/essential skills including communication, critical thinking, teamwork/collaboration, curiosity and continued learning.

- Despite initiatives, the cybersecurity industry still lacks significant diversity in gender, race, culture, ethnicity and experience. This can be remedied by bringing STEM programs into a wider range of K-12 schools, specifically those located in low-income communities. Additionally, early exposure to technology careers can broaden the workforce pipeline and ensure diverse populations have the opportunity to access these lucrative careers.

- The fast paced nature of the industry was highlighted including the challenge to develop and maintain relevant curriculum due to the industry changing so quickly. Panelists indicated that while generalists and specialists are needed, generalists who can receive specialty training on the job are also valuable. Additionally, employers were unanimous in appreciating applicants who express a passion/curiosity for continued learning in their field.

Meeting Proceedings

Welcome and Introduction

Markus Geissler, Professor of Computer Information Science at Cosumnes River College, began the Information and Communication Technologies Advisory with a warm welcome to all attendees. Geissler reminded attendees of the focus of regional advisories - to develop and maintain partnerships between educators and industry partners, encourage collaboration to inform current industry trends and development, and inform community college curriculum. Geissler then introduced the Keynote Speaker for this advisory, Nathaniel Le, Supervisory Special Agent of the Federal Bureau of Investigation. Nathaniel Le shared industry developments and information about IT cybersecurity and prevention and the Federal Bureau of Investigation's Cyber Strategy.

ICT Labor Market and Insights

Ebony Benzing, Research Manager at the California Community Colleges' North/Far North Center of Excellence, provided the labor market analysis for attendees. Benzing presented an overview of the cybersecurity job landscape of the Greater Sacramento region by looking at traditional labor market demand and projections, analyzing job posting data, skill analysis and postsecondary education supply of cybersecurity-related programs across the seven county Greater Sacramento region.

Traditional Labor Market Demand

Job posting data from EMSI/Burning Glass projected that from 2020 to 2025, the average job growth for cybersecurity is 5%; there were nearly 32,000 cybersecurity jobs in 2020 and these positions are expected to grow up to 33,688 jobs in 2025. Reports on the median annual wage for these cybersecurity careers is $96,347. There are an estimated 2,700 job openings anticipated each year for the next 5 years.

Cybersecurity Occupations Data

Benzing noted that while the traditional cyber security occupation is Information Cybersecurity Analyst, there are several cyber-enabled positions which include some cyber tasks. The labor market information presented includes both cybersecurity and cyber-enabled occupations as detailed in Figure 1.

Cybersecurity and Cyber-enabled occupations provide high median wages at $96,347 ($46 per hour) with a respectable overall 5% job growth expectation. About two-thirds of the regional cybersecurity workforce is concentrated in the following occupations: Computer User Support Specialists, Software Developers, and Software Quality Assurance Analysts and Testers (QA). Both Software Developers and Information Security Analysts are occupations demonstrating faster than average growth at 12% and 18% respectively.

Figure 1: Cybersecurity Occupations & Wages

Cybersecurity Occupations (w/ wages)

			2020 -2025 Change	2020 -2025 % Change	2020 –2025 Annual Openings	Avg. Hourly Earnings	Median Typical Entry Level Education	
Computer User Support Specialists	12,237	12,322	85	1%	945	$42.88	Some college, no degree	
Software Developers and Software Quality Assurance Analysts and Testers	8,090	9,093	1,003	12%	812	$57.01	Bachelor's degree	
Computer Occupations, All Other	4,023	4,198	175	4%	335	$39.60	Bachelor's degree	
Computer Systems Analysts	3,143	3,296	153	5%	255	$50.73	Bachelor's degree	
Network and Computer Systems Administrators	1,646	1,728	82	5%	126	$44.64	Bachelor's degree	
Detectives and Criminal Investigators	1,518	1,562	44	3%	120	$49.00	High school diploma or equivalent	
Computer Network Support Specialists	914	970	56	6%	80	$34.85	Associate's degree	
Database Administrators and Architects	717	762	46	6%	62	$54.76	Bachelor's degree	
Computer Network Architects	685	713	28	4%	48	$56.17	Bachelor's degree	
Information Security Analysts	514	607	92	18%	58	$55.07	Bachelor's degree	
North (Greater Sacramento)Totals	**33,488**	**35,251**	**1,763**	**5%**	**2,840**	**--**	**--**	

Note: Detectives and Criminal Investigators were excluded from the traditional LMI section of this presentation (slides 6 and8).

Benzing utilized two methods to collect job posting data based on trends for the last year (from April 2021 - 2022), which cover the seven county Sacramento region. For the first method, she focused on the 10 occupations that were highlighted in the traditional labor demand data section as a whole, and then she applied a filter within the 10 occupations that had skills with cybersecurity, utilizing keywords such as “authentication”, “network security”, “phishing”, “threat intelligence” and more. Industries with the most cybersecurity-related postings (25%) fall within the Professional Scientific and Technical Services industry, which includes business-related functions such as consulting, engineering and design. Finance and Insurance positions made up 11% of postings, followed by Manufacturing at 7%, Public Administration/Government at 4%, Educational Services at 4%, and Information and Utilities both at 3% of postings. Top regional employers of Cybersecurity-related jobs are Accenture, Deloitte, Pacific Gas & Electric Company, and Intel.

Figure 2: Cybersecurity Skills Cluster and Occupations

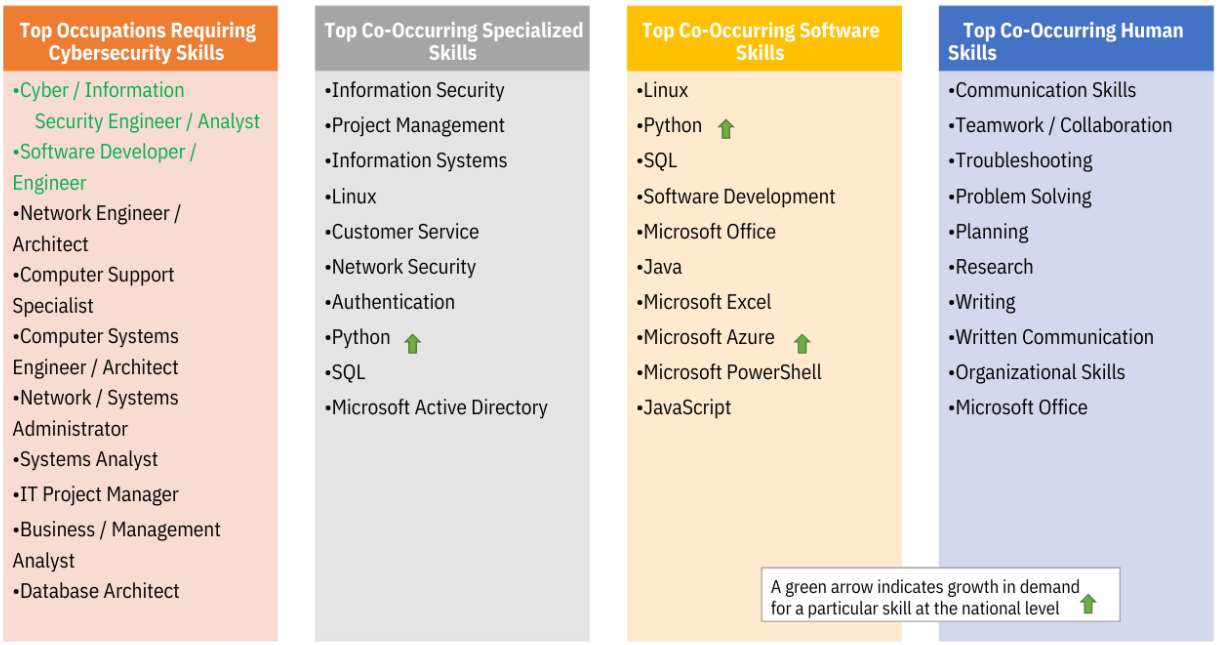

Figure 2 details a summary of top occupations requiring a cybersecurity skill set and the top 10 co-occurring specialized skill sets, including software skills and human skills detailed within the graphic. The skills with upward green arrows show increased demand at the national level. Benzing's job posting analysis identified the top ranking Specialized and Software skills as Information Security, Project Management, Information Systems, Linux, Python and SQL. The top ranking Human/Soft skills are Communication, Teamwork/Collaboration Troubleshooting and Problem Solving.

The region has a broad spectrum of training providers including community college, public four-year colleges and universities, private colleges and other postsecondary options producing an average of 1,097 certificates or credentials annually. The following Figure 3 provides a list of programs with five-year completion data (from 2016 to 2020) within our regional educational system.

Figure 3: Cybersecurity Educational Program Data

Educational Program Data

Program	Completions (2016)	Completions (2017)	Completions (2018)	Completions (2019)	Completions (2020)	Five-Year Average
Computer Science	367	572	546	614	656	551
Computer Support Specialist	132	157	97	88	64	108
Computer Systems Networking and Telecommunications	101	92	109	113	76	98
Computer and Information Systems Security/Auditing/Information Assurance	79	74	107	80	154	99
Computer Programming/Programmer, General	76	92	112	134	94	102
Network and System Administration/Administrator	53	57	90	99	23	64
Data Modeling/Warehousing and Database Administration	34	32	36	30	15	29
Information Technology	23	33	35	33	26	30
System, Networking, and LAN/WAN Management/Manager	7	5	4	5	6	5
Computer Graphics	2	1	1	2	3	2
Computer and Information Sciences and Support Services, Other	1	4	2	2	3	2
Computer and Information Sciences, General	0	0	3	8	14	5
Telecommunications Technology/Technician	0	0	0	0	6	1
North (Greater Sacramento) Totals	**875**	**1,119**	**1,142**	**1,208**	**1,140**	**1,097**

Note: Completions count the number of awards issued in the academic year ending in (XXXX). These counts include certificates,associate degrees, and bachelor degrees only.

Industry Panel Discussion

- **Tania Webb,** Managing Director, Deloitte
- **Benjamin Troglia,** Associate Director, Accenture
- **Andrew Maroun,** Director of Information Security, Golden 1 Credit Union
- **David Bitter,** Cybersecurity Manager, SMUD




Panel Overview

Deloitte is a global professional services firm that serves commercial and government clients. Having been with Deloitte for twenty five years, Tania Webb currently oversees government practice, with her current role leading Deloitte's Risk and Financial Advisory

team in California. Services offered include tax, audit, insurance, human capital/ human resources, broader technology, risk assessment, and financial advisory.

Accenture is a global consulting firm with nearly 700,000 employees throughout the world. Within Accenture's security focus, the company assists clients in preparing and responding to threats, prevention and response to cyber attacks, and transforming different enterprises with new security footprints and security services management. Accenture hires employees with all educational attainment levels, from high school diplomas and GEDs to applicants with Associate's Degrees, Bachelor's Degrees, and beyond. Benjamin Troglia is an Associate Director at Accenture with 14 years of experience in designing, building and operating security solutions for public service clients.

Golden 1 Credit Union is a not-for-profit, member-owned financial institution with over one million members/consumers that regularly invests in the community. Financial services provided include traditional retail banking, home lending, and indirect lending. With the increase in digital banking, Golden 1's fifteen person cybersecurity team works to prevent and respond to attacks and fraud with internal departments. The company uses recruiting organizations, networking, and internal promotions to fill positions as they come available. Andrew Maroun is the Director of Information Security and has been with the organization for four years.

SMUD is a community owned, not for profit electric utility serving the Greater Sacramento region's 1.5 million customers. The organization has approximately 2,200 employees and many contractors. David Bitter is a Cybersecurity Manager within SMUD's thirty position cybersecurity department including the following positions; cybersecurity engineering, integrated security operations, emergency operations incident management, identity and asset management, audit, assessment and monitoring management, asset security, host and network security, cybersecurity risk, compliance and privacy specialist, and others. The company currently has six open positions within the department and regularly hosts interns.

A Day in the Life

The employer panel communicated information on job components and daily tasks for cybersecurity occupations. The more entry level positions tasks include phishing reports, threat intelligence, system alerts, investigation of anomalies, threat hunting. Specialist occupations can include penetration testing, incident management, data privacy and protection, policy and compliance. Analysts may go through an entire life cycle of rolling out technology and implementing different modules within a company or organization's system. The panel discussed the need for both generalists who have broad knowledge and can move within teams,

and specialists who can be trained or hired to fill specific roles in compliance, policy and other specialty roles.

Essential Skills and Passionate Candidates

In addition to technical skills, the employer panel stated essential/human skills are also crucial. With many positions, written and verbal communication skills are important to be able to communicate to users and executive management in conversation and report writing. Tania Webb explained the necessity for cybersecurity applicants to understand the "why" (the reason and purpose) of security within organizations and companies. Panelists discussed looking for applicants' efforts to stay on top of the field outside of college classes due to the field and industry changing rapidly. This can include following trends within virtual cybersecurity communities on Twitter and/or Reddit or through online literature. All panelists emphasized seeking candidates who demonstrate passion about their work since a genuine interest is generally indicative of individual effort to stay on top of industry changes.

Credentials, Top Skills, and Certifications

Panelists agreed the majority of positions require a Bachelor's degree or years of experience equivalent while acknowledging entry points for individuals with an Associate's, certificate or high school diploma. Specific skills identified by the panel correlated to those identified by Benzing including Linux, Python and Network Security. Two certifications were identified to improve employability and/or promotion opportunities, CompTIA Security+ and SANS.

Hands On Experience Valued

The panel was unanimous that cybersecurity candidates need to have experience outside of the classroom. They indicated when reviewing resumes they look for participation in clubs, competitions, hack-a-thons, and other examples of applied skills. This correlates with job posting data highlighted by Benzing indicating the majority of cyber position postings requesting three to five years of experience.

Breaking into the Industry

In addition to affirming passion and aligned extracurricular activities, panelists stressed the importance of participating in internships to learn hands-on cybersecurity skills and knowledge. Panelists also recommended students pursue or have more opportunities to gain public speaking experience to build their communication skills. Networking was also emphasized as a way for students to build connections with employers to help them attain roles within their future cybersecurity careers. Employers recommended students connect with current professionals in the ICT industry to start conversations about mentoring, internship, and/or employment opportunities.

Conclusion

The ICT advisory concluded with thanking the guest speakers and panelists for sharing their time and expertise. Email contact information of the planning team members was shared and is listed below:

- Ebony J. Benzing, Research Manager, Center of Excellence - **ebony.benzing@losrios.edu**
- Renee John, Project Leader, Valley Vision - **renee.john@valleyvision.org**
- Caitlin Blockus, Project Manager, Valley Vision - **caitlin.blockus@valleyvision.org**
- Jared Amalong, Director of Computer Science & Digital Learning, Sacramento County Office of Education - **jamalong@scoe.net**
- Markus Geisler - Professor of Computer Information Science began the Information and Communication Technologies Advisory - **geisslm@crc.losrios.edu**