PROGRAM OF STUDY

Cyber Security Technology AS Degree Program

CYBER SECURITY TECHNOLOGY Associate of Science degree is designed for students pursuing professional employment in information security for business. This degree program provides students with skills to enter the job market as information assurance technicians, information security analysts, network security professionals and cyber security technicians. Designed for both full-time and part-time students, this program is appropriate to both those currently employed and those seeking to enter the field. This degree program is also transferable to California State University at San Bernardino.

Courses required for the Associate degree major at Cerro Coso Community College may not be the same as those required for the corresponding major at a four-year school. Consult a counselor and visit www.assist.org to identify the courses needed for the major at your transfer school and to develop a plan that will best meet your goals.

You must complete a minimum of 60 units, including the courses listed in the major and general education requirements, with an overall GPA of 2.0 or better, and a grade of "A," "B," "C," or "P" in all courses for the major. A minimum of 12 units must be completed at Cerro Coso Community College.

Your transfer institution may require some of the major courses to be taken for a grade. Please consult a counselor and www.assist.org to determine any limitations on Pass/No pass grading in major preparation courses.

This program prepares students for careers in Information Security

Cyber Security Technician Information Technology Security Professional Information Assurance Technician Information Assurance Manager Security Analyst

Courses Note:
Some courses within the major may have a required prerequisite. If you feel you have equivalent knowledge and skills to those included in the prerequisite course through professional experience, licensure or certification, you have the opportunity to submit a Prerequisite Challenge to be reviewed by the faculty chair. For the Prerequisite Challenge to be considered, you must submit documentation/verification to substantiate the basis for the challenge. Please consult a counselor for more information regarding Prerequisite Challenge.

CSCI C101	Introduction to Computer Information Systems	3
CSCI C142	Information & Communication Technology Essentials	4
CSCI C143	Computer Network Fundamentals	3
CSCI C146	Introduction to Information Systems Security	3
CSCI C251	Introduction to Programming Concepts and Methodologies	3
CSCI C190	Introduction to Cybersecurity: Ethical Hacking	3
CSCI C193	System and Network Administration	3
CSCI C195	Introduction to Systems Analysis and Design	3
MATH C121	Elementary Probability and Statistics	4
	or	
MATH C121H	Elementary Probability and Statistics - Honors	5
	or	
MATH C130	Finite Mathematics	4
	or	
MATH C131	Basic Functions and Calculus for Business	4

Total: 29 - 30

Complete one of the following general education patterns:
OPTION A: Cerro Coso General Education Requirements: AA/AS degree
OPTION B: CSU General Education Breadth
OPTION C: IGETC - Intersegmental General Education Transfer Curriculum

Units

Total: 30 - 31

Total Units **60**

Program Learning Outcomes

1 . Configure, install, diagnose, and support hardware and software issues.
Assessment: This will be assessed by projects and scored with rubrics in course CSCI C142.

2 . Utilize identifying tools and methodologies that hackers use to break into a network computer and defend a computer and local area network against a variety of different types of security attacks using a number of hands-on techniques.
Assessment: This will be assessed by projects and scored with rubrics in course CSCI C146 and CSCI C190.

3 . Design, analyze, and support computer networks.
Assessment: This will be assessed by projects and scored with rubrics in course CSCI C143.

4 . Apply problem-solving, programming, and application development including the ability to design, test, debug, and implement complex computer programs.
Assessment: This will be assessed by projects and scored with rubrics in in course CSCI C251.

5 . Operate servers, storage, and virtualization including implementing and evaluating network security solutions.
Assessment: This will be assessed by projects and scored with rubrics in course CSCI C146 and CSCI C193.

6 . Read and interpret technical information, as well as communicate with and write clearly for wide ranges of audiences.
Assessment: This will be assessed by a project scored and with a rubric in course CSCI C101 and CSCI C195.

Program Matrix

Courses	**Program Learning Outcomes**					
	A	**B**	**C**	**D**	**E**	**F**
CSCI C101	X			X	X	X
CSCI C142	X				X	X
CSCI C143	X		X		X	X
CSCI C146	X	X	X		X	X
CSCI C190	X	X			X	X
CSCI C193	X		X		X	X
CSCI C195	X		X		X	X
CSCI C251				X		X
MATH C121				X		
MATH C121H				X		
MATH C130				X		
MATH C131				X		

Planning Summary

Program Cover

Recommended T.O.P. Code	0708.10
Units for Degree Major or Area of Emphasis	29
Total Units for Degree	60
Required Units-Certificate	29

Projected Annual Completers	50-100
Projected Net Annual Labor Demand (CTE)	150
Estimated FTE Faculty Workload	1
Number of New Faculty Positions	0
Est. Cost, New Equipment	50,000
Cost of New/Remodeled Facility	25,000
Est. Cost, Library Acquisitions	5,000
When will this program undergo review as part of college's Program Evaluation Plan?	70 = Fall 2019

Need

Enrollment and Completer Projections

The Cyber Security program is a new program that will fill a target need for industry. Employers have indicated a need for 100 employees in this area. In order to full this need, we will need to scale our program offerings to meet this need. We project enrollment in the program to be 150-200 in the four beginning courses. Students will choose between the Computer Information Systems and Cyber Security program following completion of the four core classes. Completer projections are 50-100 per year by 2018. For those students interested in transfer, the new model cyber security curriculum provides students with a pathway to California State University at San Bernardino in the Information Systems and Technology Bachelor of Science program. All of the courses offered in the CIS degree are accepted for transfer within the UC and CSU systems (source: assist.org) as well as other universities throughout the US.

Place of Program in Curriculum/Similar Programs

These courses also serve the Computer Information Systems Associate's certificate and degree.

'Similar Programs at other colleges in service area

There are no other colleges in our service area and the program does not represent unnecessary duplication. The program does not represent unnecessary duplication of training programs and other regional colleges offering a similar program are too far away to impact employer’s needs in our service area.

Labor Market Information & Analysis (CTE only)

The Cyber Security program has documented labor market demand for the degree and certificate. In the Cerro Coso service area there are many known jobs that are not documented because employer’s corporate offices are out of state. For example, positions appropriate for CIS grads such as those required by aerospace contractors, the Naval Air Warfare Center at China Lake, and even our own Cerro Coso Community College classified IT staff are not captured in this reporting system because the corporate offices are located outside our service area. Employers in the Indian Wells Valley have attended the Advisory Committee meetings over the past several years and have actively engaged in the discussions and development of the new certificate(s) and degree both for Computer Information Systems and Cyber Security Technology. While the numbers of job opportunities are reflective in the environmental scans attached, two local employers are not captured (Jacobs Technology and the Naval Air Warfare Center at China Lake). These two specific employers have come to the college in the past few months presenting their local hiring requirements. Each employer is estimating a minimum of 40-50 students needed for their organization. Internships and apprenticeship programs have recently been developed to provide a pipeline for employees. Environmental scan reports from EMSI, Burning Class and the Community College Review all project huge need that is only expected to expand. The Cyber Security job postings have grown 91% from 2010-2014 as compared to other IT postings (28%). The duration of the postings in cyber security is 47 days versus 36 days for all other IT jobs. Salaries for Cyber Security are $6,459 higher than all other IT postings (Cyber Security $83,934 versus IT $77,475). Additionally, California ranks first in the nation for the job postings (Burning Glass) and the percentage of growth from 2010-2014 was 75%. There were 28,744 job postings in California from 2010-14.

Employer Survey (CTE only)

Specific CSCI courses have been developed and delivered to meet the short-term and long-term needs of local employers. The CIS Advisory Committee formed a subcommittee for Cyber Security to review the national Homeland Security and National Security Administration. Additionally, the development team of the program includes top experts from NAWC and AltaOne. The department is responsive to requests for specific training programs and attempts to develop appropriate coursework as needed, dependent on staffing and budgetary constraints.

Explanation of Employer Relationship (CTE Only)

The Computer Information Systems/Information Technology/Cyber Security Advisory Committee continues to be the pivotal point in program development. The CIS Advisory Committee formed a subcommittee for Cyber Security to review the national Homeland Security and National Security Administration. Additionally, the development team of the program includes top experts from Naval Air Warfare Center at China Lake and AltaOne Federal Credit Union. The program was reviewed and approved by the subcommittee of experts.

List of Members and Advisory Committee (CTE Only)

Melissa Oliverez, Continental Labor; Johnson Daniel, Coso/Teragen contrastIT; Mary Lorber, Engility; Sean Callihan, Jacobs Engineering; Tom Della Santina, Jacobs Engineering; Vaughn Corbridge, HTii; Eileen Shibley, Monarch; Uwe Schmiedel, Monarch Edward Balcer, NAWC Keith Bennett, NAWC Heather Kenny, NAWC Tony Vitale, NAWC Margaret Porter, NAVAIR; Autumn Piotrowski, NAVAIR; Mark Henderson, NAVAIR Weapons Division; Linda Homer, NAVAIR Weapons Division; Angel Zammarron, NAVAIR Weapons Division John Paul, New Directions Technology, Inc; Kishor Joshi, Pertexa; Scott Lougheed, Saalex Paul McKenzie, Saalex

Recommendations of Advisory Commitee (CTE Only)

The Advisory Committee endorsed and recommended the Cyber Security Technician Certificate of Achievement and the Cyber Security Technology A.S.

Adequate Resources

Library and/or Learning Resources Plan

The Library and LRC are used to support the current program. The library is used to support research for the courses in the program. Five of the Cyber Security program is shared with the CIS courses, so there are adequate resources available. The additional three courses for the program may require additional books and materials for the program. The department faculty regularly works with the librarian to acquire books and materials for the area and programs. Additionally, several courses in the department are directly supported with Library research instructions tailored to the course by the library staff.

Facilities and Equipment Plan

Most on-site CIS courses at the IWV campus are taught in the Learning Resource Center. There are two computer lab classrooms. One classroom is equipped with 30 student stations and the third is equipped with 29 student stations. All rooms have an instructor station, an overhead projector, and whiteboards. Although iTV rooms are available to allow multiple campuses to participate in a single course, the rooms are not equipped with computer stations, limiting their usefulness for CSCI courses that require hands-on access to technology to achieve the student learning objectives. Increasingly, other disciplines (English, math, engineering, science) are requesting to use the computer classrooms for their own courses. It is expected that as the college continues to develop technical, engineering, and science programs, and as the use of computer technology is infused across the curriculum, the demand for these rooms will increase and additional facilities will be required. The classroom computers are rotated based on a set replacement schedule developed by the Technology Resource Team and implemented by the IT staff. Specialized software is installed upon request if supplied by the department. Because of the quickly changing nature of the computer industry, faculty, classroom, and lab computers should be kept current and replaced on a regular cycle as determined by the campus Technology Resource Team. Current hardware and software are necessary to be able to train students to be competitive in the workplace and for transfer to other programs. Classrooms must have computers, speakers, a projector, and the ability to play CDs and DVDs. Headsets are also needed.

Financial Support Plan

The college has used VTEA funds to further develop the CIS program in the past. In the 2016-17 academic year, a new Cyber Security Technology Plan (TOPS 708.10) will be developed and funds will be requested. If it determined that the college needs to be a Cisco certified partner, there will be space required, equipment required and an ongoing equipment cost that could be funded through federal grants for Cybersecurity.

Faculty Qualifications and Availability

Adjunct faculty with specialization in cyber security and information technology are available to fill the need initially for the program for the higher-level classes. Depending on the scaling of this program, there may be a need to hire a full time faculty member to shepherd the program. Entry level and mid-level course are currently staffed with current department staffing includes five full-time faculty split between several disciplines (BSAD, BSOT, CSCI, and DMA) and a large number of part-time faculty. Four full time faculty are assigned to the Indian Wells Valley (IWV) campus and the other is assigned to the Bishop and Mammoth campuses, leaving Kern River Valley and South Kern without full time faculty representation and support. There is a desire to build up programs in all college areas, but the ability to do so is limited by the availability of full time staffing in some areas

Compliance

Based on model curriculum (if applicable)	N/A
Licensing or Accreditation Standards	N/A
Student Selection and Fees	N/A

Conditions of Enrollment

burningglass
CAREERS IN FOCUS

March 2014

Job Market Intelligence:
Report on the Growth of Cybersecurity Jobs

Market Overview: Cybersecurity Jobs

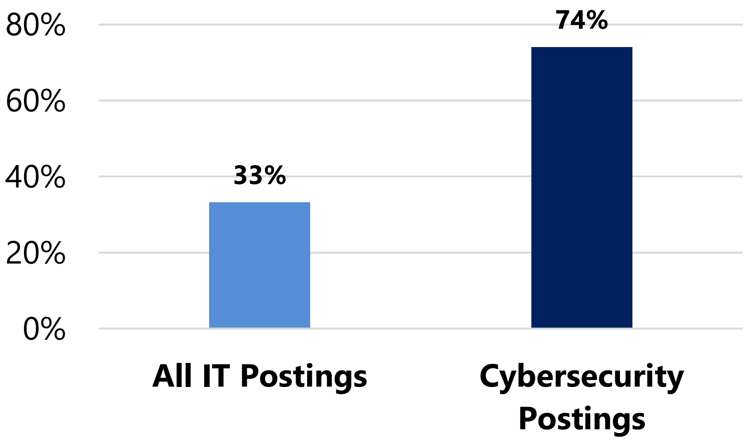
The Market for Cybersecurity Jobs Is Large and Growing

- In 2013, there were 209,749 postings for cybersecurity-related jobs nationally. **Cybersecurity jobs account for nearly 10% of all IT jobs.**
- Cybersecurity postings have **grown 74%** from 2007-2013. This growth rate is over 2x faster than all IT jobs.

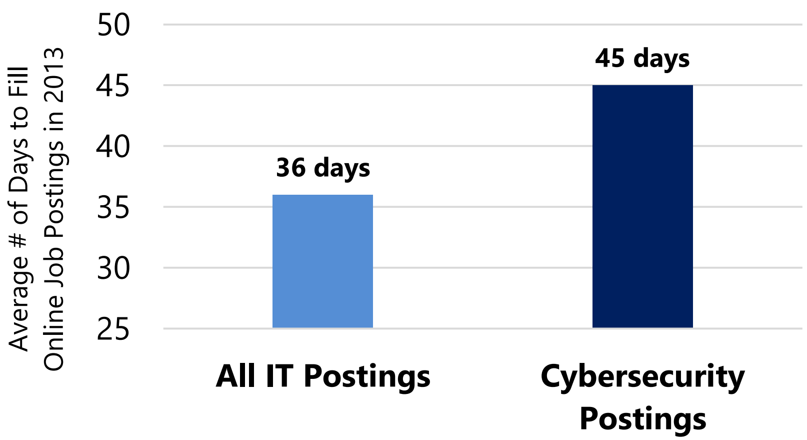
Demand for Cybersecurity Talent Is Outstripping Supply

- Cybersecurity job postings took **24% longer to fill than all IT job postings and 36% longer than all job postings.**
- The demand for cybersecurity talent appears to be outstripping supply. In the US, employers posted 50,000 jobs requesting CISSP, recruiting from a pool of only 60,000 CISSP holders.

Growth in Job Postings (2007-2013)



Posting Duration (2013)

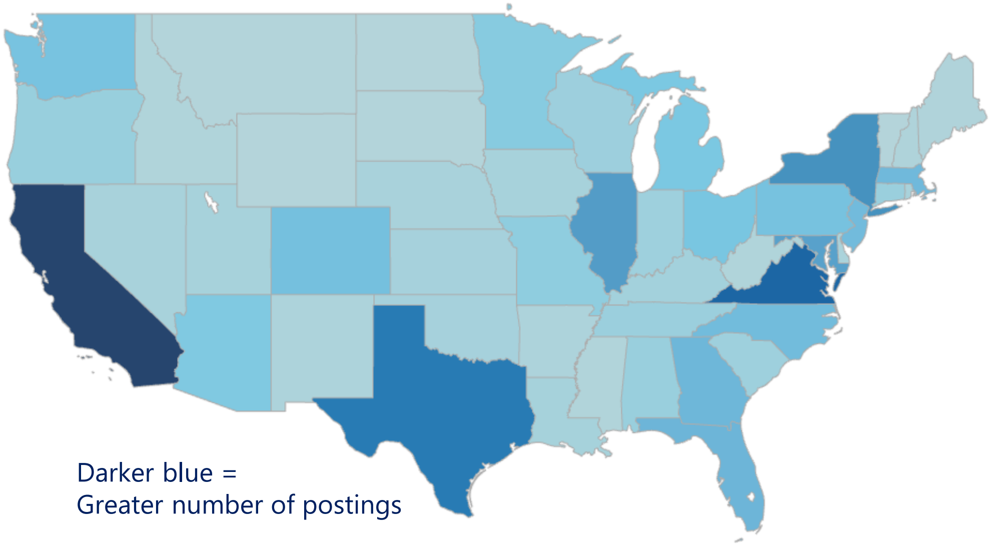


Cybersecurity Job Postings by State

Top States by Total Postings*

	State	Total Postings	Postings/ 10,000 Residents	% Growth (2007-2013)
1	California	27,084	7.1	64%
2	Virginia	20,507	25.1	53%
3	Texas	16,376	6.3	97%
4	New York	12,405	6.3	59%
5	Illinois	11,136	8.6	116%
6	Maryland	10,627	18.1	94%
7	Florida	7,923	4.1	46%
8	Georgia	7,539	7.6	214%
9	Massachusetts	7,107	10.7	76%
10	New Jersey	6,814	7.7	12%
11	North Carolina	6,676	6.8	129%
12	Colorado	6,039	11.6	158%
13	Pennsylvania	5,630	4.4	22%
14	Washington	5,444	7.9	76%
15	Ohio	5,086	4.4	34%

Cybersecurity Job Postings in 2013 By State



Darker blue =
Greater number of postings

*See Appendix 1 for state-level data tables on total postings and postings growth.

Cybersecurity Job Postings by City

Top Cities by Total Postings

	City (MSA)	Total Postings	% Growth (2007-2013)
1	Washington D.C.	23,457	35%
2	New York	15,632	38%
3	San Francisco/ San Jose	12,697	67%
4	Chicago	9,723	115%
5	Dallas	7,669	110%
6	Los Angeles	7,123	38%
7	Boston	6,336	87%
8	Atlanta	5,883	204%
9	Baltimore	4,514	116%
10	Seattle	4,470	63%

Top Cities by Growth

	City (MSA)	Total Postings	% Growth (2007-2013)
1	Atlanta	5,883	204%
2	Denver	3,482	200%
3	Austin	1,979	172%
4	Charlotte	2,410	127%
5	Portland (OR)	1,981	119%
6	Baltimore	4,514	116%
7	Chicago	9,723	115%
8	Phoenix	2,885	114%
9	San Diego	3,665	112%
10	Dallas	7,669	110%

*Top cities by growth were calculated by taking the top 25 cities by total postings, and ranking them by growth in job postigs

Cybersecurity: Demand by Industry Sector

- Professional Services, Manufacturing, and Finance are the leading industries for cybersecurity professionals.
- The share of cybersecurity jobs coming from the Manufacturing & Defense, Public Administration, and Retail Trade industries is increasing over time compared to other industries.

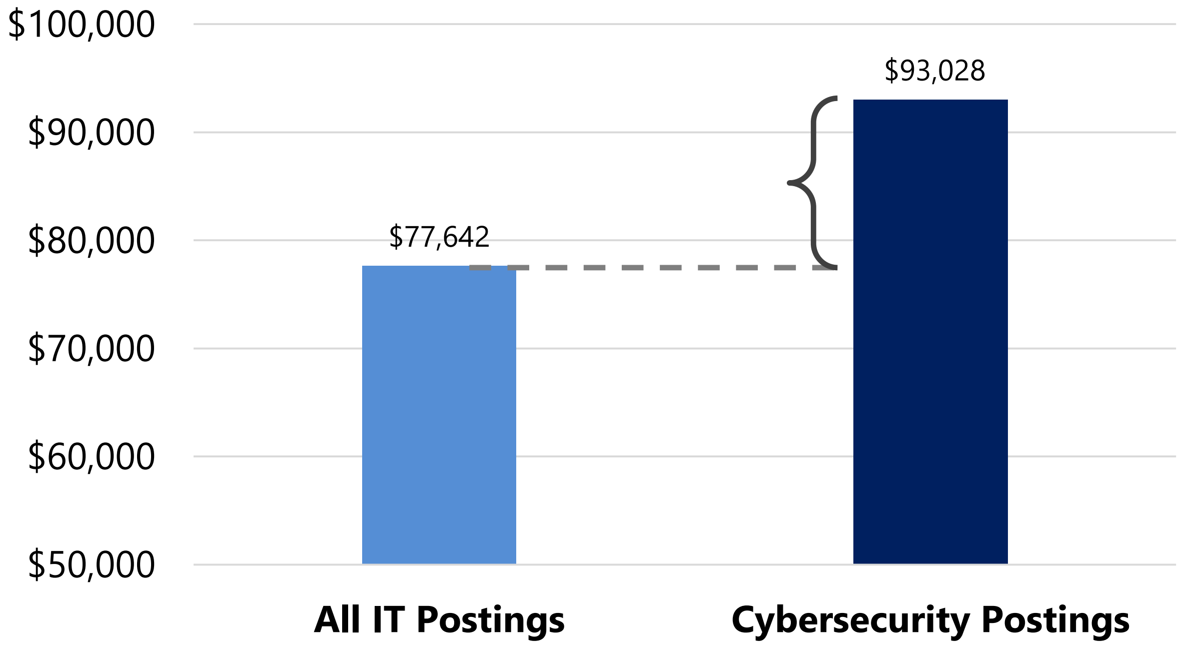
Industry Sector	% of Cybersecurity Postings	Number of Cybersecurity Postings (2013)	2010-2013 Postings Growth
Professional Services	38%	80,446	29%
Manufacturing & Defense*	14%	28,331	16%
Finance and Insurance	12%	24,145	89%
Information	8%	15,820	36%
Health Care	6%	12,257	73%
Public Administration	5%	11,204	N/A**
Retail Trade	5%	10,203	94%
Other	13%	27,384	N/A**

*Manufacturing Sector includes services divisions of a number of defense contractors (e.g. Raytheon) and computer manufacturers (e.g. Hewlett Packard).
** Industry growth rates are suppressed for the Public Administration and Other industry sectors because a significant portion of labor market demand in these industries exists offline.

Cybersecurity Jobs Offer Increased Salaries

Cybersecurity Jobs Pay a Premium

On average, cybersecurity salaries offer a premium of over $15,000 over the salaries for IT jobs overall.



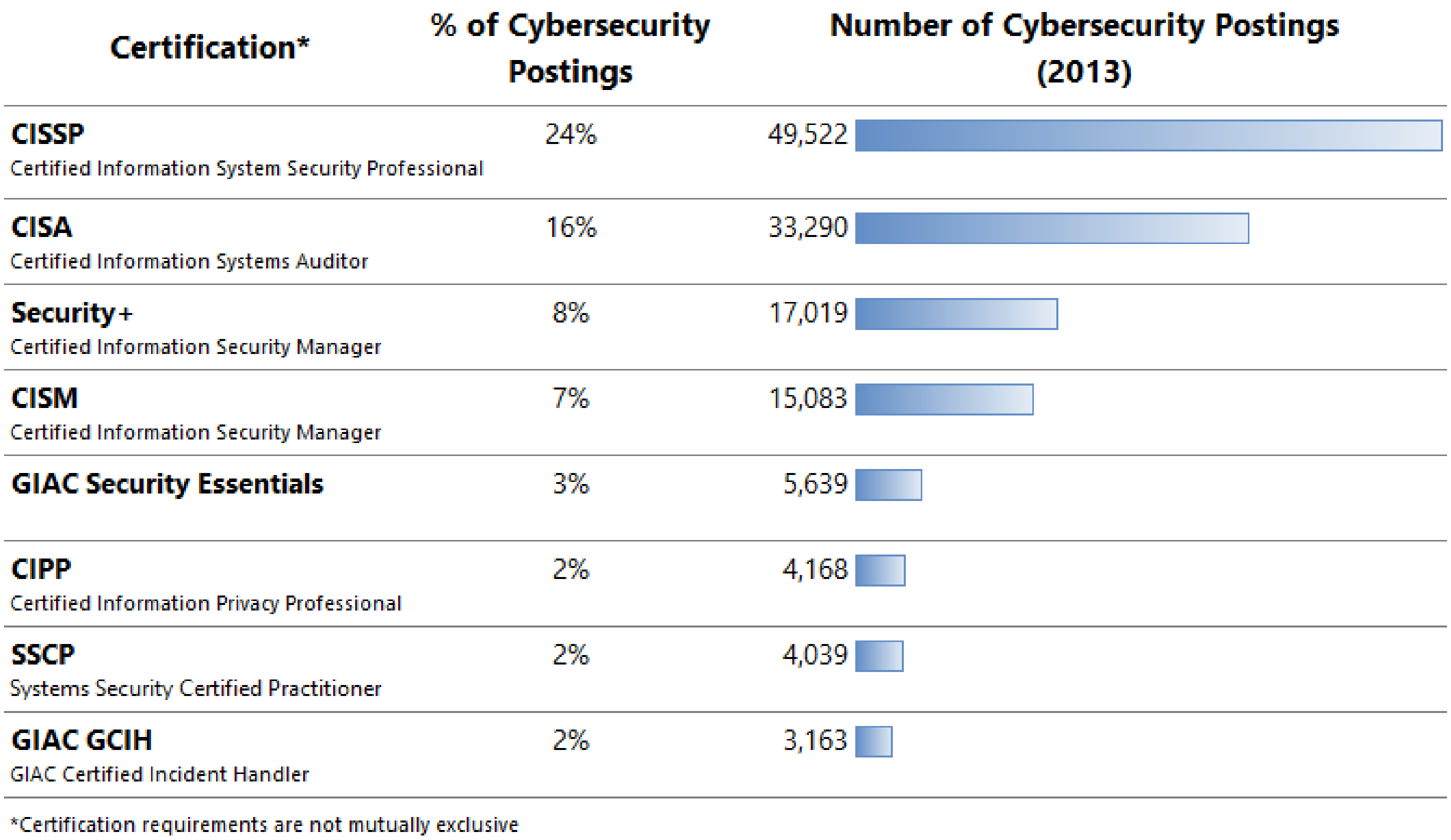
Cybersecurity: Demand by Role

Title	% of Cybersecurity Postings	Number of Cybersecurity Postings (2013)
Engineer (e.g. Security Engineer, Information Assurance Engineer)	28%	40,898
Manager/Administrator (e.g. Data Security Administrator, Information Security Manager)	19%	28,310
Analyst (e.g. IT Security Analyst, Cyber Intelligence Analyst)	18%	26,219
Specialist/Technician (e.g. IT Security Specialist, Infosec Technician)	9%	13,154
Auditor (e.g. IT Auditor, IT Sarbanes-Oxley Auditor)	5%	7,307
Architect (e.g. Security and Privacy Architect, Network Security Architect)	5%	6,670
Consultant (e.g. Network Security Consultant, Infrastructure Security Consultant)	4%	6,121

Demand for Certifications

Certification requirements are more common in cybersecurity roles than in IT generally.

- 51% of all cybersecurity positions request at least one of the certifications listed below.
- 14% of all IT positions request a certification of any kind.



Certification*	% of Cybersecurity Postings	Number of Cybersecurity Postings (2013)
CISSP Certified Information System Security Professional	24%	49,522
CISA Certified Information Systems Auditor	16%	33,290
Security+ Certified Information Security Manager	8%	17,019
CISM Certified Information Security Manager	7%	15,083
GIAC Security Essentials	3%	5,639
CIPP Certified Information Privacy Professional	2%	4,168
SSCP Systems Security Certified Practitioner	2%	4,039
GIAC GCIH GIAC Certified Incident Handler	2%	3,163

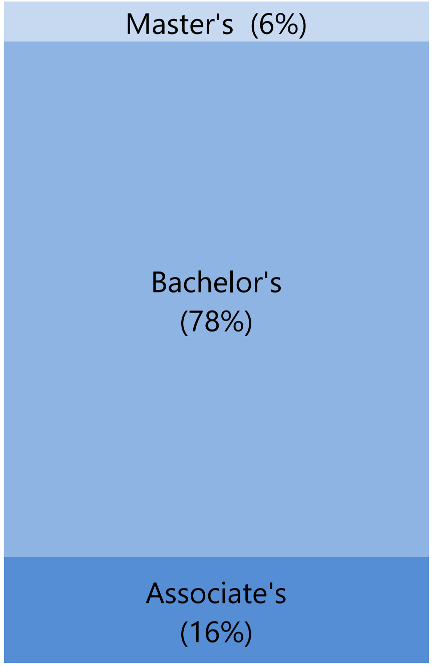
*Certification requirements are not mutually exclusive

Education and Experience Requirements

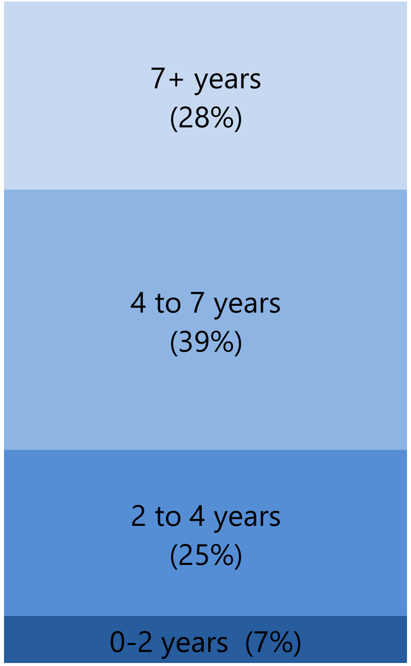
Cybersecurity Jobs Require Significant Education and Experience

- 84% of cybersecurity postings specify at least a Bachelor’s.
- 2/3 of cybersecurity postings require at least 4 years of experience.

Minimum Education Level



Minimum Experience



Methodology

All jobs data in this report are drawn from Burning Glass's database of online job postings, which includes nearly 100M worldwide postings collected since 2007. Each day, Burning Glass visits over 32,000 online jobs sites to collect postings. Using advanced text analytics, over 70 data fields are extracted from each posting including job title, occupation, employer, industry, required skills and credentials and salary. Postings are then deduplicated and placed in a database for further analysis.

This report classifies cybersecurity jobs as those which have a cybersecurity-related title, require a cybersecurity certification or request cybersecurity specific skills. Cybersecurity related titles used to define the roles analyzed in this report include "network security", "information security", "information assurance", and "penetration tester". Cybersecurity skills include information assurance, cryptography, computer forensics, malware analysis, 800-53, and ArcSight. The cybersecurity related certifications are listed on Slide 7.

The data in this report use a broader definition of cybersecurity roles than Burning Glass's 2012 report examining the same topic. That report looked only at those roles with cybersecurity specific titles, whereas, this update includes jobs with cybersecurity titles, certifications or skills.

About Burning Glass

Burning Glass's tools and data are playing a growing role in informing the global conversation on education and the workforce by providing researchers, policy makers, educators, and employers with detailed real-time awareness into skill gaps and labor market demand. Burning Glass's job seeker applications power several government workforce systems and have been shown to have substantive impact on reemployment outcomes and on labor market literacy.

With headquarters in Boston's historic Faneuil Hall, Burning Glass is proud to serve a client base that spans six continents, including education institutions, government workforce agencies, academic research centers, global recruitment and staffing agencies, major employers, and leading job boards.

For More Information

Dan Restuccia
Director of Applied Research
t +1 (617) 227-4800
drestuccia@burning-glass.com
www.burning-glass.com

Appendix 1: Top Cities Ranked By Total Postings

	City (MSA)	Total Postings	% Growth (2007-2013)
1	Washington, D.C.	23,457	35%
2	New York	15,632	38%
3	San Francisco/San Jose	12,697	67%
4	Chicago	9,723	115%
5	Dallas	7,669	110%
6	Los Angeles	7,123	38%
7	Boston	6,336	87%
8	Atlanta	5,883	204%
9	Baltimore	4,514	116%
10	Seattle	4,470	63%
11	Philadelphia	4,032	-4%
12	San Diego	3,665	112%
13	Houston	3,648	67%

	City (MSA)	Total Postings	% Growth (2007-2013)
14	Denver	3,482	200%
15	Detroit	3,093	84%
16	Minneapolis	2,929	42%
17	Phoenix	2,885	114%
18	St. Louis	2,506	82%
19	Miami	2,496	29%
20	Charlotte	2,410	127%
21	Virginia Beach	2,335	74%
22	Portland (OR)	1,981	119%
23	Austin	1,979	172%
24	Tampa	1,932	58%
25	San Antonio	1,841	68%

Appendix 2: State-Level Data

	State	Total Postings	Postings/ 10,000 Residents
1	California	27,084	7.1
2	Virginia	20,507	25.1
3	Texas	16,376	6.3
4	New York	12,405	6.3
5	Illinois	11,136	8.6
6	Maryland	10,627	18.1
7	Florida	7,923	4.1
8	Georgia	7,539	7.6
9	Massachusetts	7,107	10.7
10	New Jersey	6,814	7.7
11	North Carolina	6,676	6.8
12	Colorado	6,039	11.6
13	Pennsylvania	5,630	4.4
14	Washington	5,444	7.9
15	Ohio	5,086	4.4
16	Michigan	4,691	4.7
17	Arizona	4,252	6.5
18	Minnesota	3,718	6.9
19	Missouri	3,079	5.1
20	Oregon	2,349	6.0
21	Alabama	2,266	4.7
22	Connecticut	2,234	6.2
23	Tennessee	2,134	3.3
24	Wisconsin	1,991	3.5
25	Indiana	1,916	2.9
26	South Carolina	1,846	3.9
27	Kentucky	1,451	3.3
28	Kansas	1,261	4.4
29	Oklahoma	1,253	3.3
30	Louisiana	1,229	2.7
31	Utah	1,202	4.2
32	Iowa	1,182	3.8
33	Hawaii	1,177	8.5
34	Nevada	1,103	4.0
35	Rhode Island	1,053	10.0
36	Nebraska	1,008	5.4
37	Delaware	836	9.1
38	New Mexico	703	3.4
39	Arkansas	679	2.3
40	New Hampshire	532	4.0
41	Maine	489	3.7
42	West Virginia	475	2.6
43	Idaho	434	2.7
44	Alaska	402	5.5
45	Mississippi	399	1.3
46	South Dakota	234	2.8
47	Montana	199	2.0
48	North Dakota	186	2.7
49	Vermont	141	2.3
50	Wyoming	109	1.9

Computer Information Systems Advisory Committee Meeting
Minutes
November 19, 2015

Members Present:

Name	Title	Company
Gerald Baker	NAWC, JT3 Department Manager	NAWC
Megan Callahan	Student	Cerro Coso Community College
Sean Callahan	IT Director	Jacobs
Mark Henderson	R&D Material Branch Head	NAWCWD
Linda Homer	Computer Scientist	NAVAIR
Valerie Karnes	Professor, CIS	Cerro Coso Community College
Amy Kennedy	Counseling Department	Cerro Coso Community College
Scott Lougheed	Program Manager	Saalex
Ashlin Mattos	Job Development Specialist	Cerro Coso Community College
Paul McKenzie	IA, System Administrator	Saalex
Karen O'Connor	Professor, BOT/Department Faculty Chair	Cerro Coso Community College
Melissa Olivarez	Operations Coordinator	Continental Labor
John Paul	Director	NDTI
Uwe Schmiedel	Director of Engineering	Monarch
Kara Tolbert	Continuing Education Manger	Cerro Coso Community College
Angel Zamarron	Pathways Program Coordinator	NAWC

Introductions

Valerie Karnes called the meeting to order and the members present introduced themselves, who they worked for and their role in the organization. Several members were absent due to travel and/or work schedules. Minutes will be sent out following the meeting.

A certificate of Appreciation was awarded to Sean Callahan of Jacobs who has served faithfully on the committee and has been instrumental in getting the first internship program started. He is moving to another job in January and will be a missed member of the Advisory Committee.

Minutes of the November 2015 meeting were reviewed and approved with no changes.

Committee Purpose and Overview

The purpose of the committee purpose and overview were reviewed. Employer advise and guidance to our programs is a critical component to the success of our programs.

Computer Information Systems/Business Information Worker Programs

The new Computer Information Systems program revised form the last meeting a year ago was reviewed and the committee was notified that the program work has been done and gone through the local college process and will be presented to the Kern Community College District Board of Directors in December. From there, it will go to the California Community College Chancellor's Office for state approval. We hope that March or April will approve the program in order to promote the program prior to registration for the summer and fall terms.

Karen O'Connor presented the new statewide program for Business Information Worker (BIW) and shared the components of our current Office Technology program.

The group discussed the value of hand-on training in the CIS program and/or a fully online program would be adequate. For the NAWC IT Apprenticeship program, Angel expressed the online program fits the needs of their workers, as they are required to work full time during the day. John Paul stated that the online flexibility was good for their workforce. After lengthy discussion, there was consensus in the value of hands-on experiences for the workforce and the hybrid model of having theory taught online with several required weekend (Flex Friday/Saturday) on campus would fit the needs of the employers and employees. Further discussion and needs for the volume of employees that would be needed in this area in the future suggests that one online section and perhaps on hybrid section would be needed to fill the online community and the IWV employers. Valerie will talk to administration about the possibility of running one hybrid section of CSCI C142, CSCI C143 and CSCI C146 in the course of a year to test the success of that model. The employers indicated that they would have the following needs for students in this pathway per year (Jacobs 30-40 employees per year, NAWC Apprenticeship Program 40-50 per year, Saalex 15 in the next six months with a 15% replacement rate each year, Continental Labor 6-10 per year and Monarch 1 per year). Other employers had to leave the meeting early or were not able to attend due to other commitments. Valerie will email and request their needs for annual employees. With over 100 potential placements per year, the college needs to expand the offerings to meet the employment needs in the Indian Wells Valley. From conversations at the meeting, this need is expected to increase each year. Employers are scrambling to hire in this area and sometimes end up hiring each other's employees to meet the needs. This is not a preferred method and they would like to have a pool to select future employees.

Karen O'Connor outlined the needs of college as far as any expansion to the course offerings and explained that if we offer the program on the campus, we need to know that there are sufficient students that would enroll. She asked about the best way for us to get the information to the employers and they indicated an email blast would be best.

Employers were asked if they would support the weekend labs and contribute to scenarios to prepare students to enter the job market. They would support and assist in the labs. The new Computer Information Systems Student Club will be meeting tomorrow to form and the labs could provide our current students with these experiences until a hybrid class could be offered. This will require a space at the college and equipment for both the student club and the future of an expanded program. Sean Callahan will send a configuration of what is needed to set up a network for these types of experiences.

Internships/Apprenticeship Programs

Sean Callahan outlines for the group the intermittent student employment program that he has championed at Jacobs. This employment program interviews top students in the CSCI C101 class that are on track to major in CIS and provides intermittent training and employment during the student college experience. During the time that they are not in class, they would go through a training program at Jacobs in Information Assurance, apply for a security clearance and be mentored for six months. As they complete their Security Plus class and certification, the students would be eligible for full time hire depending upon their performance as an intern.

Angel outlined the new NAWC Information Technology Apprenticeship program where students would work full time and take up to six units to continue their education. As the program is still in development, some of the details are yet to be worked out.

Other employers may be interested in developing similar internship/apprenticeship program and will work with Valerie and Ashlin.

Customized Training

Kara Tolbert outlined the customized training and reviewed with the committee the options that are available to them including non-credit professional development training, ETP funding and options for training. Kara offered to meet with them to outline the specific options for their organization. One offering that was discussed was the IT boot camps (A+, Net+ and Security+). The need for the PearsonVue training Center is also an important component that is needed by the base and the employers. Cerro Coso Community College lost its proctor due to an employee sudden death.

Industry needs - Cyber Security Certificate/Degree

The final discussion was about the new Cyber Security courses that are now being offered through C-ID at the college and the question about if the college needs a higher-level program than the Information Technology Plus certificate and Computer Information Systems degree. Do we need both programs?

The group reviewed the components and agreed that Cerro Coso Community College needs to develop not only a certificate, but a new Cyber Security Associate of Science degree and keep the Computer

Information Systems degree program as well. The programs would have the same first 4 classes (CSCI C101, 142, 143 and 146), but then would spin off into different directions.

The Computer Information Systems degree would serve the needs of computer operators, computer repair, computer networking and entry level to information assurance. It is important to keep this program, as it would fit the needs for IT professionals with a need for some security. There are also needs of Cyber Security that need a some IT content.

The Cyber Security program would serve the higher-level functions including cyber hacking, information security, computer forensics, and network defense. The Cyber Security program would meet the needs of their incumbent workforce for continual education. Employers stated that if a student completes a degree, they will be promoted and have an increase in salary. In the CIS and Cyber Security fields, continual education is crucial and employment is expected to continue to grow and expand. Paul will send Valerie the latest information on what would be required for the higher level program components and she will research the classes that will need to be developed and present it to the administration at the college. There will also be a need for dedicated classroom and additional faculty with expertise in these areas.

The meeting was adjourned at 1:10 pm.

Computer Information Systems Advisory Committee Meeting
Minutes
November 20, 2014

Members Present:

Name	Title	Company
Chris Harper	IT Infrastructure Manager	AltaOne
Tim Dawson	CEO	Approach Robotics
Kara Tolbert	Continuing Education Manger	Cerro Coso Community College
Valerie Karnes	Professor, CIS	Cerro Coso Community College
Frank Timpone	Professor, Business	Cerro Coso Community College
Karen O'Connor	Professor, BOT/Department Faculty Chair	Cerro Coso Community College
Lori Acton	Council Member	City of Ridgecrest
Melissa Olivarez	Operations Coordinator	Continental Labor
Daniel Johnson	Network & Controls Supervisor	Coso Operating Company
Sean Callahn	IT Director	Jacobs
Rich Christensen	Recruiter	Jacobs
Eileen Shibley	CEO	Monarch
Margaret Porter	Information Specialist	NAVAIR
Scott Fairfield	IT Specialist	NAVAIR
Linda Homer	Computer Scientist	NAVAIR
Kishor Joshi	Manager	Pertexa
Katherine Hu	Sr. Chemist/Environmental Lab Director	Searles Valley Mineral

The meeting was called to order by Valerie Karnes and the members present introduced themselves, who they worked for and their role in the organization. Several members were absent due to travel and/or work schedules. Minutes will be sent out following the meeting.

Minutes of the April 2014 meeting were reviewed and approved.

The committee purpose agenda was reviewed and employers raised the topic of internships/work experience and job shadowing as a need for most of the organizations. Discussion regarding our work experience courses, potential barriers to student completion and issues with security clearances for those working for the base. Advantages and benefits for students and employers in offering internships and work experience were also discussed. Students would benefit from real world experiences, which would enhance their education that could be noted on a resume. In addition, internships/work experiences could result in aiding in completion and job placement. Several attendees noted that they had internships while in school and that they not only enhanced their educational background, but also resulted in placements.

As Cerro Coso Community College work experience courses are not currently being offered, at this point there is no avenue for credit to be offered to students. A suggestion of offering a Work Experience certificate (new certificate) was brought forward as this would not change the current programs at the college, but will offer students a supplemental certificate that would be valued by employers. Valerie will check with the Counseling department and the CTE Dean to inquire about bringing these courses back and in the form of a certificate.

The Committee moved next to the Computer Information Systems program certificates that were brought forward for review.

The Data Analyst Certificate (12 units) certificate proposed the following courses below:

- ✓ BSAD 220 Principles of Project Management (3 units)
- ✓ BSAD 220 Problem Solving, Decision Making, and Computer Applications in Business (3 units)
- ✓ CSCI 251 Introduction to Visual Basic Programming (3 units)
- ✓ CSCI 270 Introduction to Database Design and Management (3 units)

The purpose of this certificate is to prepare students for positions in data collection, processing, and analysis and to provide a foundation for future training in big data analysis. The certificate would be offered online and includes four courses and could be completed in one year. The committee reviewed the certificate and approved it. The only suggestion was to have a SQL course. They indicated that there is a need and they would hire these students. One person from China Lake said that it would fit in the Configuration Management/ Data Management group at the base. They said they need an understanding of SQL but not Microsoft specific. They also said that the SQL could be in another course. Valerie will check with Matt Hightower about the content of CSCI C270 (Introduction to Database Design and Management) and inquire if SQL is included in the topics and assignments in this course.

The Information Technology Certificate (13 units) was reviewed next as a basic Information Technology certificate that would serve organizations hiring for various positions as noted in the purpose below. The courses identified for this certificate are:

- ✓ CSCI C101: Introduction to Computer Information Systems (3 units)
- ✓ CSCI C140/141 A+ Essentials (4 units)
- ✓ CSCI C143: Network + and Fundamentals of Networking (3 units)
- ✓ CSCI C146: Security + Fundamentals (3 units)

The purpose of this certificate is to prepare students for entry-level positions in computer repair, networking, cyber security and general information systems jobs. The certificate would be offered online and includes four courses (13 units) and can be completed in one year. The committee endorsed this certificate and said they would hire students with this type of certificate. It was noted that it would be good for students retraining with a desire to go into another field (IT). This proposed certificate would fit the need for students entering the Information Assurance positions (cyber security), basic help desk, entry-level network positions and general computer technicians. NAVAIR requires Security + certification prior to hiring, so this certificate fits their needs. Coso Operating company is currently hiring and A+ is a requirement and the addition of Security + would be a good thing to have for incoming employees. Sean Callahan (Jacobs) said the certificate is "perfect' for what they need at Jacobs.

Discussion regarding the value of hands-on laboratories was discussed and the committee expressed that additional hands-on laboratories would be valuable to the students and the employers. It was suggested that we have students note the hands-on laboratories in their resumes so employers would know that they did labs physically and not virtually. We discussed the optional tutoring sessions that had been proposed through the Annual Unit Plan process as well as the updating of curriculum that Valerie Karnes, Matt Hightower and Chris Harper will be doing in the spring term. They were fully supportive of this as an option.

After the review of the certificate, the committee reviewed the CIS Model Curriculum and the committee supported the degree pathway as well. Questions arose about the need for an Operating Systems certification. Currently NAVAIR uses SkillPort/SkillSoft which is self paced program for incoming employees. They didn't feel that we needed to add this to either the certificate or the degree program.

The Certification Testing Center at the college was brought up as a service for employers. They stated that this was a crucial service to the employers, students and community. They stated that the college needs to advertise this center more broadly so that potential candidates locally would know that they are able to take their exams on Friday at the college. Perhaps some advertising would be helpful.

Throughout the conversations regarding the CIS certificates and programs, employers noted that the ability of students to be computer literate and have MS Office experience was a basic skill that is required for any employment. Karen shared the Business Office Technology teaches these components and employers stated that the skills are an important basic skill that will lead to employment. Without these basic computer skills and MS Office knowledge, students would not be employable.

The question of CEU requirements for employees to keep their certifications current was raised. There is a need for those holding certifications to take 17 CEU a year (50 units over a three year program). Kara Tolbert from the Office of Continuing Education at the college brought up that the college could offer supplemental not for credit training to meet the needs of employers. She also talked about meeting the needs for customized training. Jacobs Technology and others will meet with Kara separately to discuss specific needs of the employers. Kara also talked about rolling out seminars and other types of trainings to industry in the valley. There was a lot of interest in these types of professional services to the valley. Many of the employers were not aware that the college had this type of service and/or ability to provide customized education not for credit. Advertisement of these services and offering to the community needs to be expanded.

Karen O'Connor provided an update about the Computer Science AS-T and the challenge with the additional three units that caused the program to be rejected by the state. Employers asked if we can have multiple classes with various units or if there was another "creative" method we can use. Karen stated that we are working with the Science and Math departments to come up with a solution. She inquired about the need for this computer science transfer program and the employers unanimously supported the need for this program in our valley to support the mission of the Naval Air Warfare Center at China Lake, local contractors, new companies bringing up manufacturing and high technological businesses in Ridgecrest. Other businesses in the valley will also need those with computer science skill levels as technology continues to increase. Employers will be submitting letters of support for the continuation of the pursuit of an AS-T in Computer Science so the college can provide evidence to the State of California of the need for this transfer program and their support.

Other needs employers presented included the need for students competent in manufacturing processes including fiberglass, cybernetics, AutoCad, ProEngineering and SolidWorks software packages. Additional needs include students having a combination of computer skills and medical background (Medical Terminology and Physiology) , Chemistry background for laboratory positions at Searles Valley Minerals. Linux (Red Hat Enterprise edition) operating system is an emerging need that needs to be incorporated into our classes in CIS.

The next meeting date will be either in late spring or in the fall depending on the needs of industry and the progression of the new curriculum in the spring term.

ACTION ITEMS

- ✓ Valerie Karnes will check with the Counseling department and the CTE Dean to inquire about bringing Work Experiences courses back and explore the possibility of creating an additional certificate that would provide value to the students and employers. It would not impact current programs.
- ✓ Valerie Karnes will check with Matt Hightower about the content of CSCI C270 (Introduction to Database Design and Management) and inquire if SQL is included in the topics and assignments in this course.
- ✓ Valerie Karnes will complete the Advisory Minutes and send out on Monday, November 24, 2014 for review.
- ✓ Kara Tolbert will meet with Sean Callahan to follow up on the CEU needs for Jacobs's employees.

- ✓ Kara Tolbert will contact other employers about their needs for continuing education and community services for employers
- ✓ Employers will send letters of support for the Associate of Science degree for Transfer (AS-T) in Computer Science to Valerie Karnes and Karen O’Connor.

STATE OF CALIFORNIA

CALIFORNIA COMMUNITY COLLEGES
CHANCELLOR'S OFFICE
1102 Q street
Sacramento, Ca 95811-6549
(916) 445-8752
http://www.cccco.edu

07/30/2016

Admin, CERRO COSO
College CIO
CERRO COSO

Dear Colleague:

In compliance with California Education Code section 70901 and California Code of Regulations, Title 5, Subchapter 2. Approval by the Chancellor, the California Community Colleges Chancellor’s Office Academic Affairs Division has reviewed and approved the following instructional program:

CURRICULUM INVENTORY RECORD
College: 522
Credit Status: Credit
Program Title: Cyber Security Technology
Program Award: A.S. Degree
Program Control Number: 35195
TOP Code: 070810
Program Goal(s): Career Technical Education (CTE)

For a program to be recognized by the U.S. Department of Education, the Accrediting Commission for Community and Junior Colleges/Western Association of Schools and Colleges (ACCJC/WASC) must approve the program as a substantive change. Once a program is approved by the California Community Colleges Chancellor’s Office (CCCCO), colleges must follow the steps outlined in the ACCJC Manual (www.accjc.org). Please note: colleges are not eligible to collect state apportionment or federal support for granting this award without first receiving approval from the Chancellor’s Office and the ACCJC.

For questions regarding this review please submit your written inquiry to curriculum@cccco.edu.

Sincerely,

Academic Affairs Division
California Community Colleges Chancellor's Office

C·O·E CENTERS OF EXCELLENCE

Inform Connect Advance

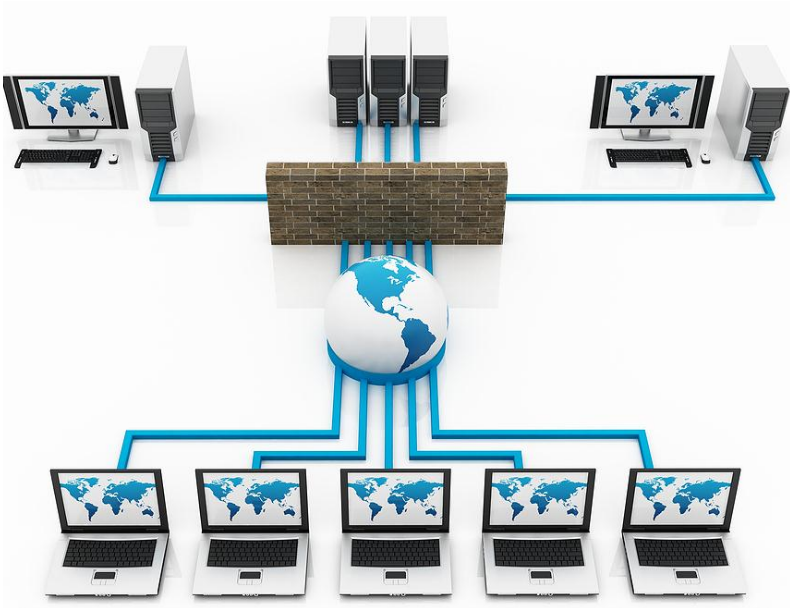
ENVIRONMENTAL SCAN

CYBERSECURITY

Los Angeles and Orange Counties

JUNE 2012

ENVIRONMENTAL SCAN



CENTER OF EXCELLENCE

Los Angeles and
Orange Counties

Audrey Reille, Director
Mt. San Antonio College
1100 N. Grand Avenue,
Walnut, CA 91789
909-274-6106
areille@mtsac.edu

www.coeccc.net

An Initiative of ECONOMIC & WORKFORCE DEVELOPMENT through the CALIFORNIA COMMUNITY COLLEGES

C·O·E CENTERS OF EXCELLENCE

Inform Connect Advance

Mission: The Centers of Excellence, in partnership with business and industry, deliver regional workforce research customized for community college decision making and resource development.

Vision: We aspire to be the premier source of regional economic and workforce information and insight for community colleges.

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

Contents

"There are only about 1,000 security specialists in the United States who have the specialized skills to operate effectively in cyberspace; however, the United States needs about 10,000 to 30,000 such individuals."

— Center for Strategic and International Studies, 2011[1]

Executive Summary

Cybersecurity is crucial not only to the economy but also to homeland security; therefore, training a qualified workforce to enter this field is a top priority for the United States. According to the Center for Strategic and International Studies, "There are only about 1,000 security specialists in the United States who have the specialized skills to operate effectively in cyberspace; however, the United States needs about 10,000 to 30,000 such individuals." [2]

To understand the regional workforce development needs for cybersecurity, the COE conducted secondary research, analyzed skill requirements from dozens of online job postings, and conducted a survey of 100 companies employing cybersecurity professionals. Respondents to the survey reported difficulty hiring Systems Analysts (87%), Security Support Specialists (86%), Programmers (86%), Computer Specialists (84%), Software Engineers (82%), Computer and Information Systems Managers (79%), Database Administrators (77%), Network and Computer Systems Administrators (76%) and Network Systems and Data Communications Analysts (72%).

In 2011, there were 163,607 jobs in Los Angeles and Orange Counties in the computer and information technology sector. Employment forecasts predict a 7% growth, adding 12,241 new jobs by 2016. Considering turnover rates and projected retirements, the number of job openings could be as high as 26,495 in the five-year period. Individuals working in computer and information technology jobs need to be knowledgeable about cybersecurity to perform their jobs, and thousands should become cybersecurity experts to meet the demand from employers.

This report presents data on the labor market (i.e., employment, job growth, wages), industry trends, employment requirements (skills, experience and education), existing community college programs, and recommendations to meet employers' needs. Colleges are encouraged to:

1. Consider adding courses in cybersecurity to their computer science programs.
2. Create new Certificates or Degrees in Cybersecurity.
3. Make sure that their programs and curriculum include the skills listed for cybersecurity occupations in this report (see appendix C for details).
4. Include representation from cybersecurity employers on advisory committees to be aware of new trends keep programs up to date.
5. Contact CyberWatch West[3], a valuable resource for curriculum development, partnership with businesses and services to students.
6. Coordinate with other colleges in the region to avoid duplication of efforts and possible competition.
7. Organize internships and opportunities for their students to gain hands-on experience.

[1] Center for a New American Security. "America's Cyber Future: Security and Prosperity in the Information Age, Volume I." June, 2011.

[2] Ibid.

[3] CyberWatch West: http://cyberwatchwest.org/

Introduction

The California Community Colleges System has charged the Centers of Excellence (COE), part of the Economic & Workforce Development (EWD) Network, to identify industries and occupations with unmet employee development needs and introduce partnering potential for colleges. The focus of this report is to examine the workforce development needs of cybersecurity occupations.

Accompanying the advances in modern computer technology there is a need for information, program, and network protection. It is the responsibility of cybersecurity professionals to protect such networks and electronic information systems from unauthorized access to sensitive information. Employee responsibilities are vast and may include functions such as: protecting computer and online-based systems as well as designing new systems, software, and processes that will be impervious, or at least resistant, to cyber attacks. Given this broad skill-set, the workforce expands well beyond the firms providing security-related goods and services (e.g. McAfee or Norton). In fact, every business storing and managing data via computer technology has a need for network and data security.

While computer technology offers many modern conveniences – such as mass data storage, online banking and bill paying, and digital collaboration, to name a few – it simultaneously creates a new world of virtual threats. Such threats range from viruses and worms, which can cause damage to personal computers, to identity and credit theft. In 2010 IBM found 8,000 new web vulnerabilities and attacks to online information, representing a 27% increase from the previous year.[4] It is the responsibility of cybersecurity professionals to protect the end user from such threats and to ensure that sensitive information remains private.

However, as illustrated in the leading quote of this report, there is a shortage of qualified cybersecurity professionals in the United States. In May 2011 Dice, North America's leading career website for technology and engineering professionals, reported that California has the largest shortage of qualified technology related talent, including cybersecurity, as there are nearly three jobs open to every computer science graduate. Further, Dice named Los Angeles as one of the most impacted areas.[5]

The purpose of this report is to determine the workforce development needs related to cybersecurity in Los Angeles and Orange Counties. Specifically, the Center of Excellence studied these occupations to determine: (a) job growth; (b) the most important skills, and educational and experience requirements to gain employment in the field; and (c) recommendations for the community colleges to strengthen cybersecurity curriculum.

To determine skill sets needed to work in cybersecurity, the COE conducted an in depth analysis of 44 job postings, consequentially compiling a list of 15 critical skills. In addition, 100 employers participated in an industry survey to determine the importance of each of the 15 skills for prospective job candidates, firm-level job growth, educational and experience requirements for new hires, and recommendations for the community colleges.

Industry Overview

Cybersecurity extends far beyond its roots in information technology. In fact, it can be found in nearly every industry that utilizes computer technology to store and manage information. The workforce is composed of various occupations that protect networks and electronic information systems from unauthorized access to sensitive information. As such cybersecurity spans both the private and public sectors.

[4] Takanhashi, Dean. "IBM Says it Sees 13 Billion Cybersecurity Alerts Every Day." March 31, 2011.

[5] Dice. "America's Tech Talent Crunch." May 1, 2011.

Cybersecurity in the Private Sector

In the private sector, cybersecurity is necessary in both business and our personal lives. In addition to being a key element of computing companies such as Intel and Google it is essential to most large industries such as health care, banking, and credit. The health care industry, for example, needs data security to protect patients' medical records. Banking requires rigorous online security to protect customer funds. And the credit industry requires elaborate security networks to ensure individuals' personal identity and information, amongst other things. In addition, any business storing company information via cyberspace requires intense security to ensure that valuable information is kept confidential.

The number of cyber attacks in the U.S. has grown tremendously over the past few years and can absorb an extensive amount of organizational resources. A study of 45 U.S. businesses, by the Ponemon Institute, discovered an alarming 50 successful cyber attacks per week. This averages out to one successful attack to each business every week. Further it was concluded that these attacks — ranging from theft of employee, credit, customer, and competitive business information — were estimated to cost a median-based average of $3.8 million yearly.[6] A recent press release from the U.S. Office of Homeland Security made claim that over $1 trillion of intellectual property has been stolen from U.S. businesses.[7]

Since information is the keystone of many modern organizations, it can be very costly if lost, leaked out, or stolen – even if by a single employee. A report by Google estimated that the average employee laptop contains $525,000 worth of sensitive information.[8] Therefore, to ensure the highest quality of information security, cybersecurity professionals are not only required to focus on the business at large, but also on determining the information access needs to each individual employee.

Further, cybersecurity is equally important at the personal level as it is to business. As individuals have the modern conveniences of online banking, bill paying, and social networking (to name a few), these capabilities create vulnerabilities to personal information. In 2010, the U.S. Department of Justice published a report claiming that 11.7 million persons, representing 5% of all North Americans above the age of 16, had experienced some form of identity theft within a two-year period.

These breaches of personal identity varied from breaking into personal credit cards and existing bank accounts to the theft of personal information (e.g. social security numbers).

Most common amongst the listed crimes was the unauthorized usages of personal credit cards, which impacted 6.2 million people over the same two-year period.[9] Given these outrageous statistics, it is critical that cybersecurity professionals are trained to develop networks, systems, and software that are impenetrable to such attacks.

Cybersecurity in the Public Sector

The full spectrum of cyber threats, however, runs all the way to the highest level of national security. According to President Barack Obama, in the 21st century, not only is North America's economic prosperity dependent on cybersecurity but it "is also a matter of public safety and national security."[10]

[6] Ponemon Institute. "First Annual Cost of Cyber Crime: Bench Mark Study of U.S. Companies." July 2010.

[7] Phillips, Leslie. "Senate Democrats Introduce Bipartisan Legislation Calling for New Safeguards for National Security, American Economy Against Cyber Attack." January 26, 2011.

[8] Google. "Off-Network Workers – the Weakest Link to Corporate Web Security," 2008.

[9] Langton, Lynn & Planty, Michael. "Victim of Identity Theft, 2008." U.S. Dept. of Justice, Bureau of Justice Statistics, December 2010

[10] Obama, President Barack. "Remarks By The President On Securing Our Nation's Cyber Infrastructure." May 29, 2009.

President Obama continued his remarks by asserting that we are dependent on computer networks to deliver our oil, gas, power and water – all of public interest.[11] Since these plants are controlled by online systems they are vulnerable to cyber threats and must be protected.[12]

On the other hand, cyber threats at the National level may take the shape of breaches to government systems, interferences with communications, and loss of classified military information, to name a few. According to a recent study published by the Center of New American Security, government networks experience 1.8 million cyber attacks each month. These attacks, varying in sophistication, target Congress and other federal agencies.[13] Further, U.S. intelligence officials predict that the next significant terrorist attack against the country will be a cyber attack aimed at damaging financial and government systems.[14]

Given the high level of concern with cybersecurity at the National level, multiple initiatives and bills have been passed to increase the security of North America's digital infrastructure. For example, on January 26, 2011 the Senate Committee on Homeland Security and Governmental Affairs introduced a bipartisan bill to put a stop to cyber crime aimed at harming our technology infrastructures.

"The legislation calls for urgent action to safeguard critical infrastructure, including the electric grid, military assets, the financial sector, and telecommunications networks. It urges incentive for the private sector to assess the risk of cyber terrorism and take action to prevent it and promote investments in the American IT sector, which will create high-paying jobs. The bill also seeks to improve the capability of the U.S. government to assess cyber risks, and to prevent, detect and respond to attacks. It calls for safeguards to protect consumers by preventing identity theft and guarding against abuses of personal information, and seeks to promote cooperation between nations in responding to cyber threats.[15]

Employer Survey

Cybersecurity professionals work across all industries. The Center of Excellence conducted an online employer survey to collect more information on businesses that employ cybersecurity professionals, industries, firm size, occupations, skills, job requirements and trends. One hundred businesses in Los Angeles and Orange counties responded to the survey. They indicated the industries to which they belong. Eleven percent (11%) of the firms surveyed was in the field of education. Another 11% were in health care and social services. Following these industries, 9% of the firms were in professional and technical services, 8% were in computer hardware or software, and 7% were in financial services.

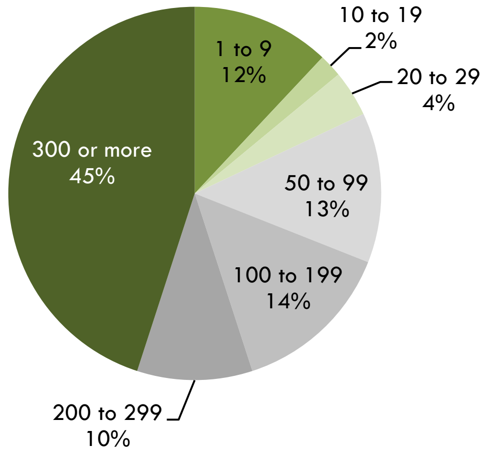
Exhibit 1: Percentage of cybersecurity firms connected to specific industries

Industries represented in the Employer Survey			
Education	11%	Engineering	6%
Health care/Social services	11%	Entertainment	6%
Professional and technical services	9%	Wholesale distribution and services	6%
Computer hardware or software	8%	Government	4%
Financial services	7%	Telecommunications	3%
Manufacturing	7%	Other[16]	22%

[11] Obama, President Barack. "Remarks By The President On Securing Our Nation's Cyber Infrastructure." May 29, 2009.
[12] Bliss, Jeff. "U.S. Nuclear Plants Vulnerable to Cyber Attacks, Analysts Say," November 17, 2010.
[13] Center for a New American Security. "America's Cyber Future: Security and Prosperity in the Information Age, Volume I." June, 2011.
[14] Serrano, Richard A. "U.S. Intelligence Officials Concerned About Cyber Attacks," February 11, 2011.
[15] Senate Committee on Homeland Security and Governmental Affairs. "Senate Democrats Introduce Bipartisan Legislation Calling for New Safeguards for National Security, American Economy Against Cyber Attack." January, 26, 2011.
[16] Industries reported as other: retail, insurance, professional services (business), real estate, travel and transportation, utilities, advertising, broadcast cable/television/radio/media, construction, legal, and non-profit.

The majority of firms (69%) that participated in this survey are large firms employing over 100 individuals; 13% are medium sized firms employing between 50 and 99 individuals; and 18% are small firms employing 49 individuals or fewer. Exhibit 2 illustrates firm size of our sample.

Exhibit 2: Sample Firm Size



Cybersecurity Trends

As computer technology becomes increasingly complex, so do its vulnerabilities. Due to their rapid emergence and adoption, mobile devices and mobility, social media, and cloud computing,[17] present some of the greatest challenges to the current cybersecurity workforce.

Mobile Devices and Mobility

Mobile devices have revolutionized personal communication and business alike. From a handheld device, individuals can access sensitive personal information including financial information and health records. Likewise, employees no longer need to be in their place of work to access sensitive company data. This vast access to private information creates several security concerns including the use of unsecured networks, personal negligence, and data leaks due to lost or stolen devices. Because of these threats a recent survey of 10,431 industry professionals commissioned by the (ISC)^2 – a global leader in educating and certifying information security professionals – has concluded that mobile devices could be the single most dangerous threat to organizations in the proximal future.[18]

Social Media

The overwhelming popularity of social networking sites makes them and their users a prime target for cyber crime. The vulnerabilities of these sites are based in part on the large amounts of personal information posted on them by their users. As the sites' owners encourage development of third party applications to monetize their infrastructure, the vulnerabilities grow.[19] However, the largest threat produced by these sites emerges as businesses link up to them for various networking actives. For example, Salesforce, a company that aids customers to effectively use cloud computing, is linked to Facebook and Google. Further, IBM has partnered with LinkedIn, a professional social networking site, and Salesforce. This linking creates a shared vulnerability for each of these enterprises as the breaching of one system could potentially give grant access to them all.[20]

[17] Frost & Sullivan. "The 2011 (ISC)^2 Global Information Security Workforce Study." March 31, 2011.
[18] Frost & Sullivan. "The 2011 (ISC)^2 Global Information Security Workforce Study." March 31, 2011.
[19] Barrett, Larry. " Systantec's 'Unlucky 13' Security Trends for 2010." November 20, 2009.
[20] Adhikari, Richard. "Online Trust: A Thing of the Past?" January 28, 2009.

Cloud Computing

Cloud computing is the practice of housing information, applications, and systems on a distant server rather than on an organization's server or individual's computer. It offers one of the most secure and cost effective ways of storing data and providing access to shared organizational resources and information.[21] However, this mode of computing also produces numerous security concerns that the current workforce is not adequately prepared to meet. In a survey conducted on behalf of the (ISC)^2, 74% of industry professionals reported the need for further training and skill development to be able to address the security challenges of cloud computing.[22]

Most Common Security Threats

Though current trends in technology – such as mobile devices and mobility, social media, and cloud computing – greatly impact the nature of cybersecurity, the workforce must also be equipped to handle the most common forms of cyber threats. Recently Norton has listed the top 11 most commonly occurring security threats. Below is a list of the top three. For a complete listing, see appendix B.[23]

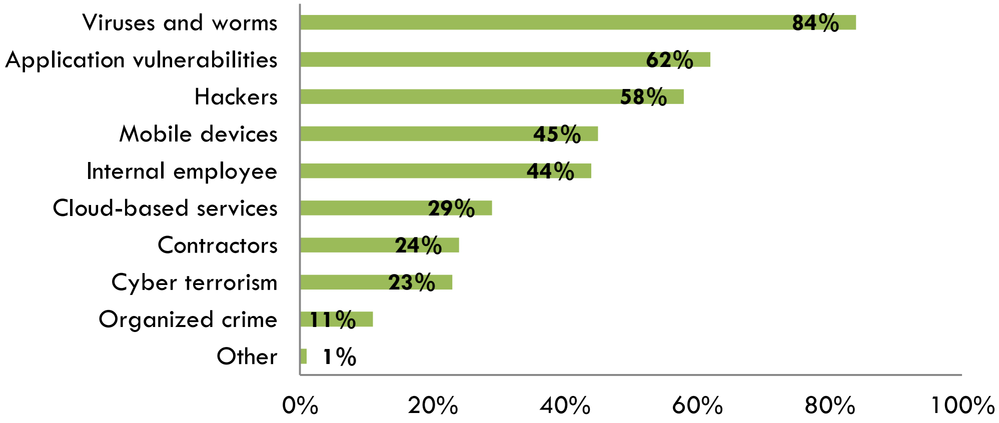
Viruses. A virus is a program that can replicate itself and infect a single device or network of computers without the user's permission or knowledge. The danger level and prevalence of viruses are extremely high, and can cause an entire network to crash, resulting in a massive loss of valuable information.

SPAM, SPIM, and SPIT are all forms of junk mail: SPAM via email, SPIM via instant messenger, and SPIT via internet technology. Though their danger level is generally low, they are extremely prevalent and can grant access to sensitive information if opened by the receiver.

Spoofing, phishing, and **pharming** are all forms of a program, web page, or individual falsification. Spoofing occurs when a person or program is being impersonated; phishing is the replication of a legitimate webpage; and pharming redirects online traffic to a counterfeit website. The danger level of these forms of falsification is high with an extremely high prevalence, and they can grant access to sensitive information if the user is not careful.

The COE survey also asked 100 employers to identify the most prevalent cybersecurity threats to their organizations.[24] The top threats include: viruses and worms (84%); application vulnerabilities (62%); hackers (58%); mobile devices (45%); and internal employees (44%).

Exhibit 3: Most Prevalent Cyber Threats to Employers



[21] Google. "Off-Network Workers – the Weakest Link to Corporate Web Security." 2008.

[22] Frost & Sullivan. "The 2011 (ISC)2 Global Information Security Workforce Study." March 31, 2011.

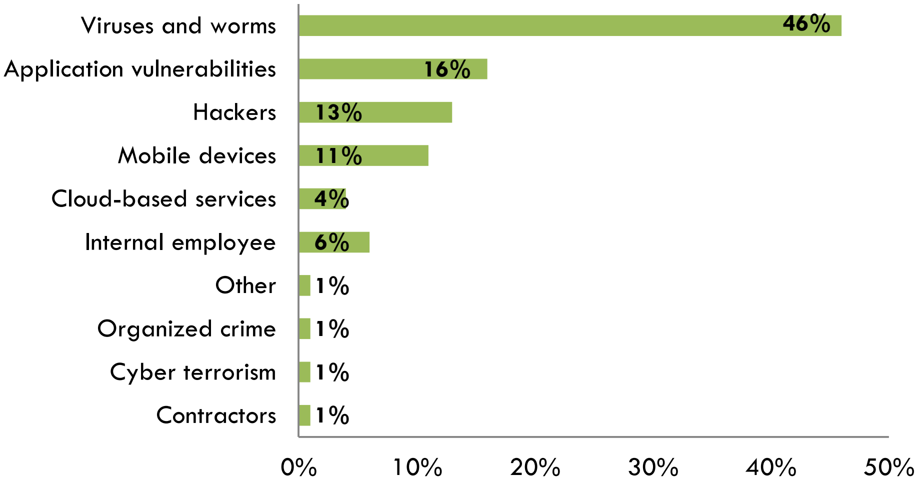
[23] Norton. Available at: http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx

[24] *Note*: Employers were allowed to give multiple responses regarding the most prevalent cyber threats to their organization.

Employers were also asked which threats posed the single greatest risk to their firm's security.

- Nearly half (46%) of employers claimed viruses and worms pose the greatest threat to their firm.
- 16% claimed that application vulnerabilities pose the greatest threat to their firm.
- 13% claimed that hacker pose the greatest threat to their firm.
- 11% claimed that mobile devices pose the greatest threat to their firm.

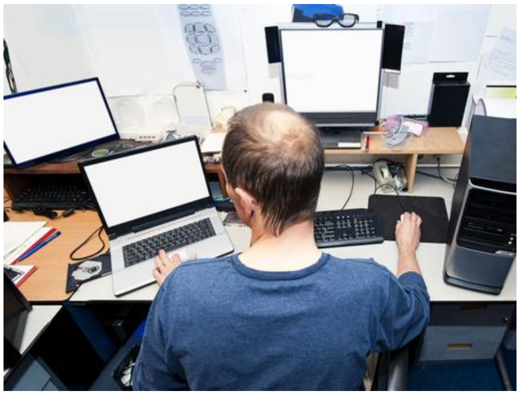
Exhibit 4: Greatest Cyber Threat to Employers



Occupational Overview

Cybersecurity professionals do not have specific occupational titles but are included in the broader Information Technology (IT) occupational titles listed below:

- Computer and information systems managers
- Computer programmer
- Computer software engineers, applications
- Computer software engineers, systems software
- Computer support specialists
- Computer system analysts
- Database administrators
- Network and computer systems administrators
- Network systems and data communications analysts
- Computer specialists, all other



Occupational Growth and Wages

Job forecasts predict a 7% growth rate in the next five years for IT professions in Los Angeles and Orange Counties — translating to 12, 241 new jobs. Adding turnover and retirements to job growth, the number of job openings is expected to reach 26,495 between 2011 and 2016. The data suggests the strongest growth, in number of new jobs, for computer software engineers and network system and data communication analysts. The occupation of computer programmer is the only one expected to decline slightly, by 1%. Exhibit 5 details the regional growth rate of each of the selected 10 occupations and their respective average hourly wages.

Exhibit 5: Projected Growth, Job Openings and Wages

Occupation	2011 Jobs	2016 Jobs	% Growth	New Jobs	Job Openings*	2011 Median Hourly Wage
Computer And Information Systems Managers	15,247	16,063	5%	816	2,054	$55.50
Computer Programmers	14,049	13,927	(1%)	(122)	1,340	$33.14
Computer Software Engineers, Applications	21,461	24,057	12%	2,596	3,498	$41.10
Computer Software Engineers, Systems Software	21,880	24,217	11%	2,337	3,256	$44.77
Computer Support Specialists	22,796	23,762	4%	966	4,122	$22.50
Computer Systems Analysts	21,145	22,517	6%	1,372	3,651	$33.90
Database Administrators	5,221	5,598	7%	377	812	$38.18
Network And Computer Systems Administrators	12,912	13,983	8%	1,071	2,148	$33.27
Network Systems And Data Communications Analysts	18,361	20,615	12%	2,254	3,904	$28.04
Computer Specialists, All Other	10,535	11,109	5%	574	1,709	$34.09
Total	**163,607**	**175,848**	**7%**	**12,241**	**26,495**	**$36.10**

Source: Economic Modeling Specialists, Inc. (EMSI); *Job Openings refers to new jobs (growth) plus replacements.

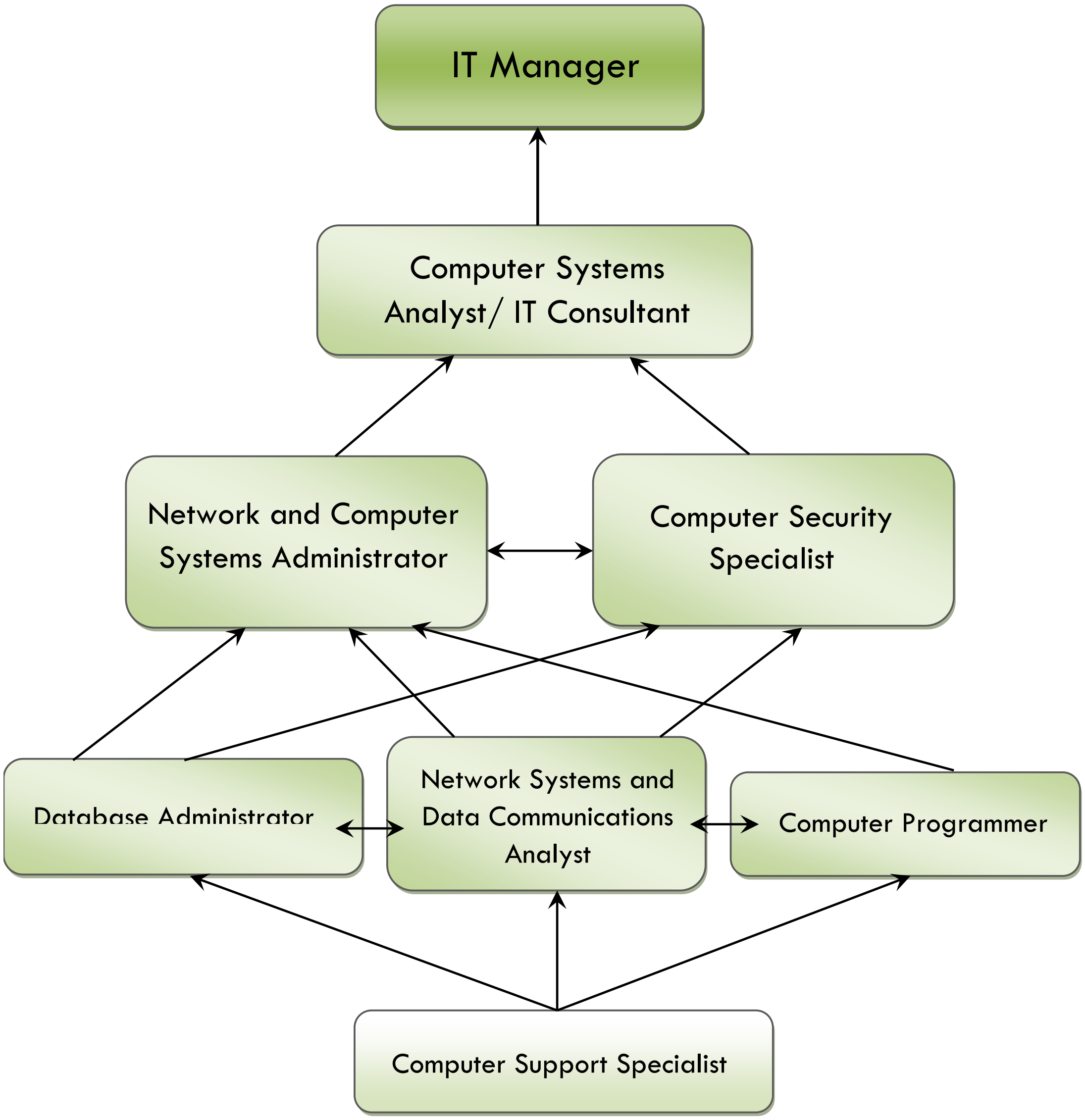
Job growth for these occupations is being driven by three important factors:[25]

- The complexity of devices, systems, networks, applications, and users drives security concerns and the need to protect information and data. This is highlighted above in discussing a few modern trends that impact security needs.
- Security is becoming operationalized. As a part of this movement, both government and business are moving towards proactive, as opposed to reactive security.
- Government compliance requires due diligence and a longer-term strategy: Government regulations are forcing organizations to evaluate and modify their business processes and operations with security in mind.

These trends and challenges present an excellent opportunity for training at the Community Colleges as individuals seek to complete their first post-secondary degree or certificate, upgrade skills, seek professional development, or simply continue in lifelong learning. Median hourly wages for these professionals range from $22.50 for entry level jobs such as Computer Support Specialists, to $55.50 for Computer and Information Systems Managers. Cybersecurity jobs offer high wages and an appealing career ladder.

[25] Godbe Research. Computer and Information Security Labor Market Study, June 2006.

Cybersecurity Career Ladder

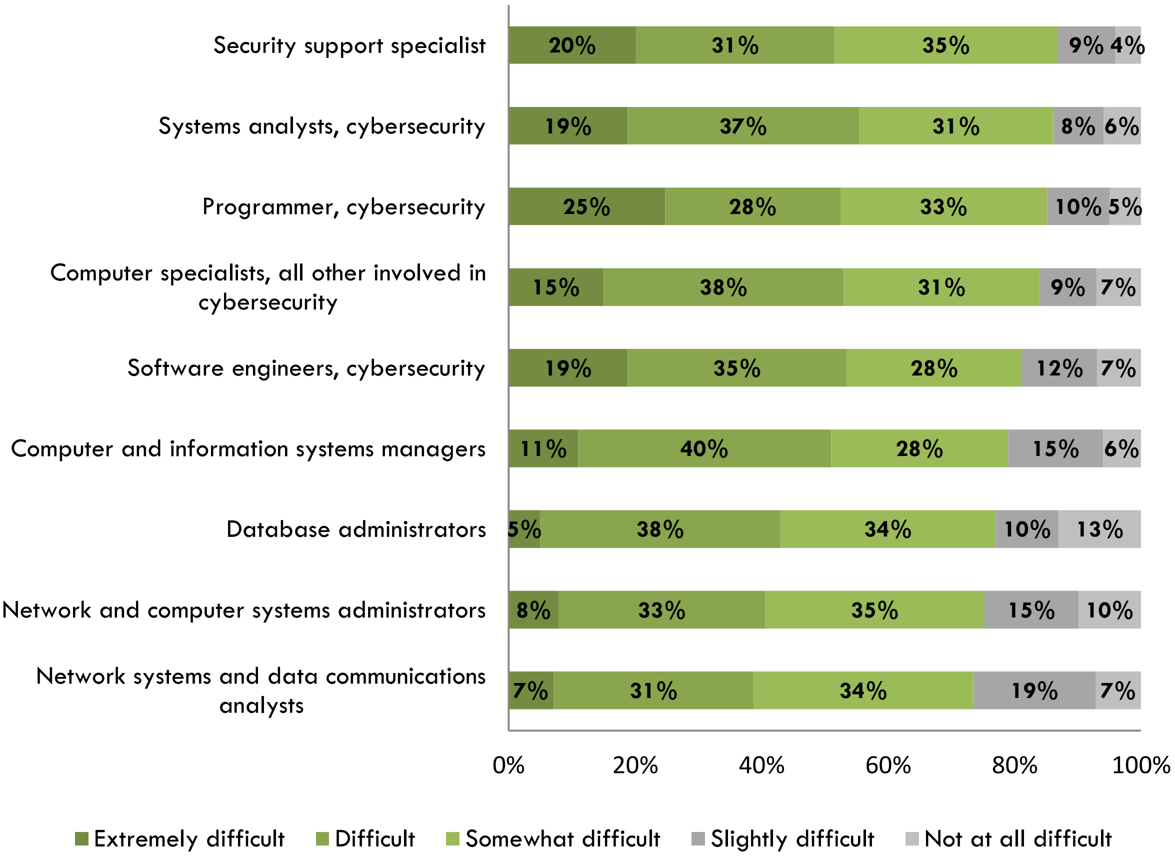

IT Manager
Computer Systems Analyst/ IT Consultant
Network and Computer Systems Administrator
Computer Security Specialist
Database Administrator
Network Systems and Data Communications Analyst
Computer Programmer
Computer Support Specialist

Source: careeronestop.org, www.careeronestop.org/competencymodel/careerpathway/ReviewCareerPathways/IT_CPW.pdf

Employer Needs and Challenges

The majority of employers surveyed in Los Angeles and Orange Counties indicated that they experience at least some degree of difficulty hiring qualified applicants in all of the cybersecurity occupations. Exhibit 6 illustrates these hiring challenges.

Exhibit 6: Difficulty in Hiring for Cybersecurity Occupations



Note that the previous section on labor market information had 10 occupations. For the purpose of the survey, we grouped two similar occupations together (Computer Software Engineers, Applications, and Computer Software Engineers, Software) to make it easier for employers to respond.

Skill Requirements

To understand the primary skill sets needed to perform each of the selected jobs, the COE conducted an in depth analysis of 44 job postings throughout Los Angeles and Orange Counties. A list of the top 15 skills needed to work each occupation was created.

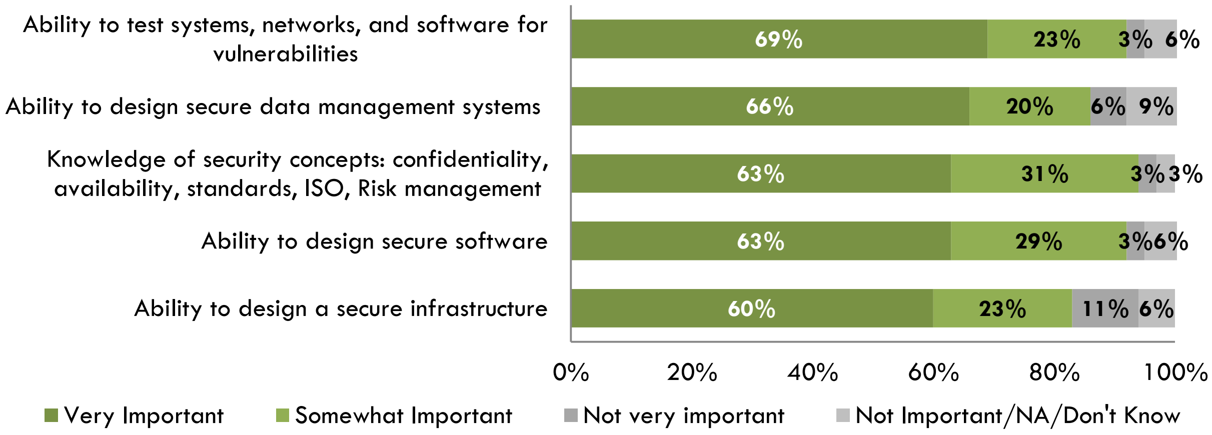
Following the compilation of the skills list, 100 regional employers were asked to validate the importance of each skill needed for a potential job candidate. Following are the top five skills for each occupation and their respective importance for prospective job candidates. For a complete list of the 15 skills identified and their importance see Appendix C.

Cybersecurity programmers

Cybersecurity programmers write programs, work to update, repair, and modify existing programs. Employers reported that:

- The most valued skill for cybersecurity programmer is the ability to test systems, network, and software for vulnerabilities (69% very important).
- Additional very important skills are the ability to: design secure data management systems (66%); design secure software (63%) and infrastructure (63%); and knowledge of security concepts (63%).

Exhibit 7: Cybersecurity Programmers (N=35)

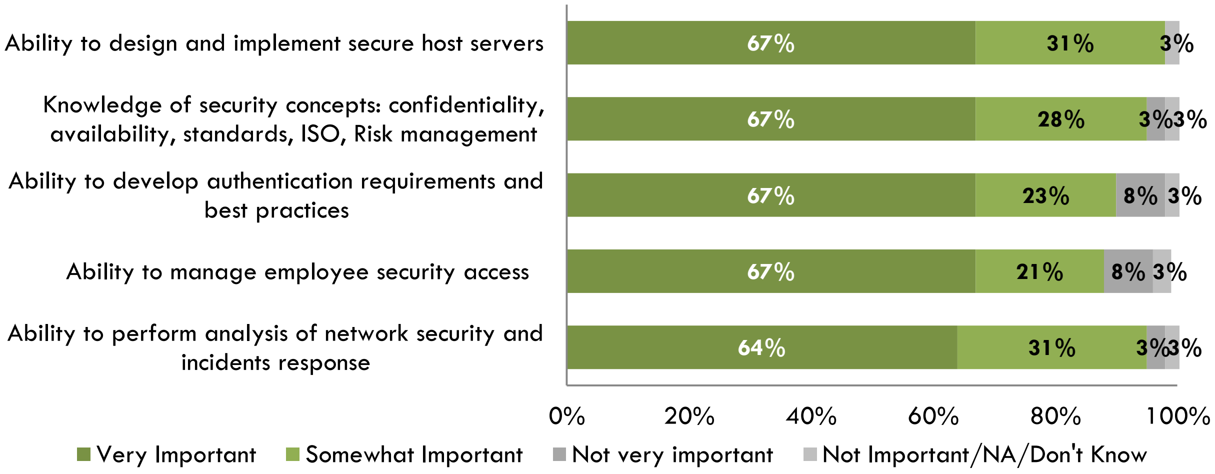


Cybersecurity software engineers

Cybersecurity software engineers develop, enhance, and maintain security software sold to customers and business partners.

- Employers reported that the most valued skills for cybersecurity software engineers is the ability to: design and implement secure host servers; develop authentication requirements and best practices; manage employee security access; and knowledge of security concepts (all 67% very important).
- Employers indicated that an additional very important skill is the ability to perform analysis of network security and incidents response (64%).

Exhibit 8: Cybersecurity Software Engineers (N=39)

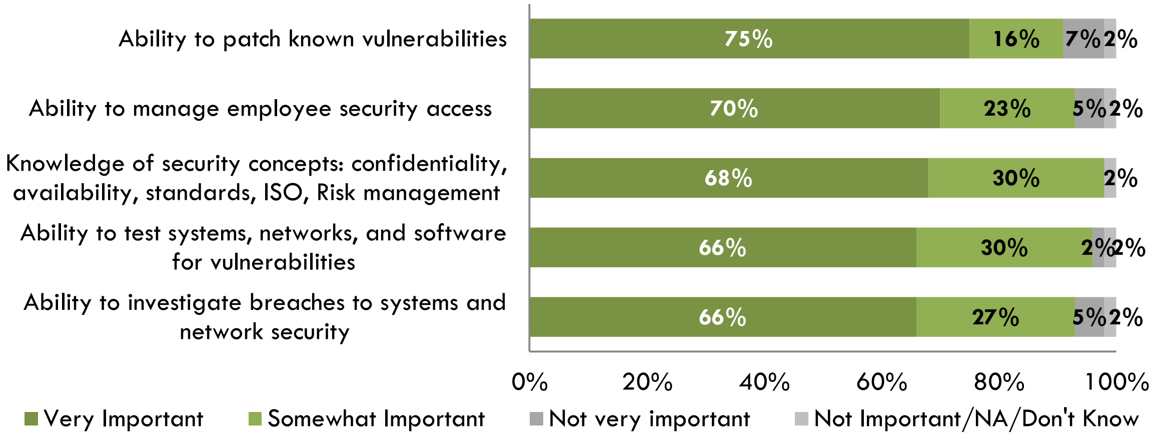


Security support specialists

Security support specialists help customers, business partners, and those within their organizations to safely utilize their computer equipment.

- Employers reported that the most valued skill for security support specialists is the ability to patch known vulnerabilities (75% very important)
- Employers indicated that additional very important skills are: the ability to manage employee security access (70%); knowledge of security concepts (68%); the ability to test systems, network, and software for vulnerabilities (66%); and the ability to investigate breaches to system and network security.

Exhibit 9: Security Support Specialist (N=44)

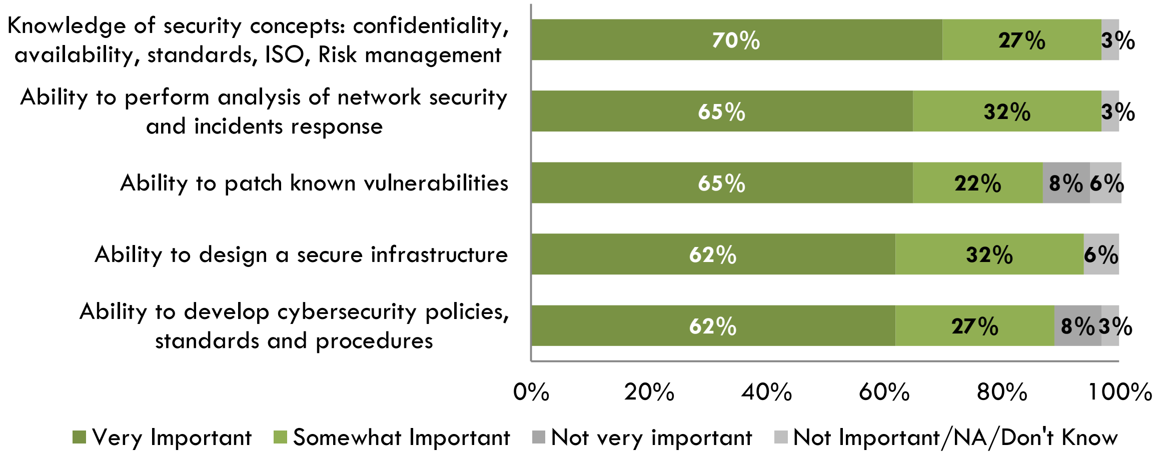


Systems Analysts, Cybersecurity

Security systems analysts investigate security problems and help the user to find solutions. Analysts may perform these tasks for individuals or for the business a whole.

- Employers reported that the most valued skill for cybersecurity systems analysts is knowledge of security concepts (70% very important).
- Employers indicated that additional very important skills are the ability to: perform analysis of network security and incidents response (65%); patch known vulnerabilities (65%); design a secure infrastructure (62%); and develop cybersecurity policies, standards, and procedures (62%).

Exhibit 10: Systems Analysts, Cybersecurity (N=37)

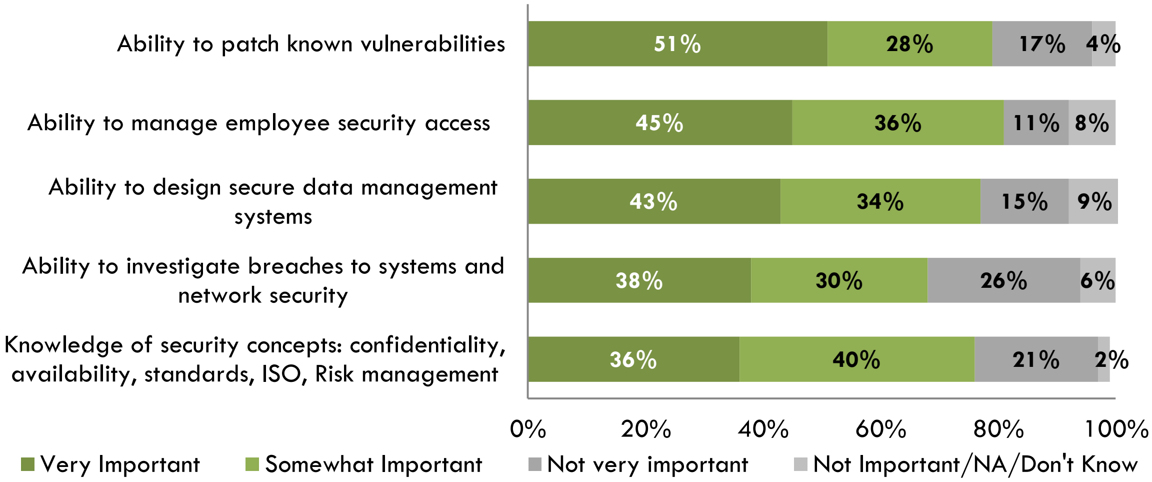


Cybersecurity database administrators

Database administrators of cybersecurity develop ways to store data both safely and effectively. They identify user needs, develop databases, and perform system tests.

- Employers reported that the most valued skill for cybersecurity database administrators is the ability to patch known vulnerabilities (51% very important).
- Employers indicated that additional very important skills are the ability to: manage employee security access (45%); design secure data management systems (43%); investigate breaches to systems and network security (38%); and knowledge of security concepts (36%).

Exhibit 11: Cybersecurity Database Administrators (N=47)

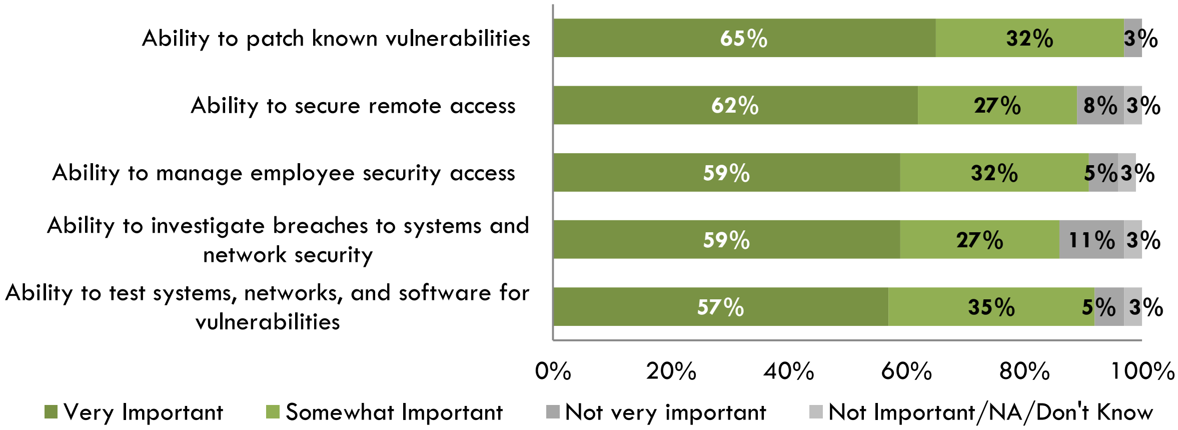


Network and computer systems administrators

Network and computer systems administrators work with businesses to design, install, and support the computer system for the organization.

- Employers reported that the most valued skill for network and computer systems administrators is the ability to patch known vulnerabilities (65%).
- Employers indicated that additional very important skills is the ability to: secure remote access (62%); manage employee security access (59%); investigate breaches to systems and network security (59%); and test systems, network, and software for vulnerabilities (57%).

Exhibit 12: Network and Computer Systems Administrators (N=37)

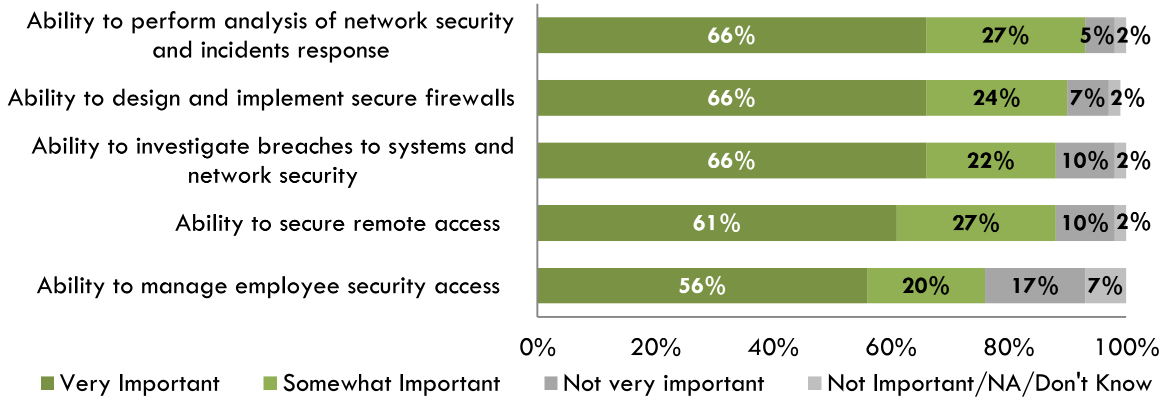


Network systems and data communications analysts

Network systems and data communications analysts work with data communications systems such as local area networks (LAN), wide area networks (WAN), company intranets, internet, etc. They perform tests and recommend improvement to these communications systems.

- Employers reported that the most valued skill for network systems and data communications analysts is the ability to perform analysis of network security and incidents response (66% very important).
- Employers indicated that additional very important skills are the ability to: design and implement secure firewall (66%); investigate breaches in systems and network security (66%); secure remote access (61%); and manage employee security access (56%).

Exhibit 13: Network Systems and Data Communications Analysts (N=41)

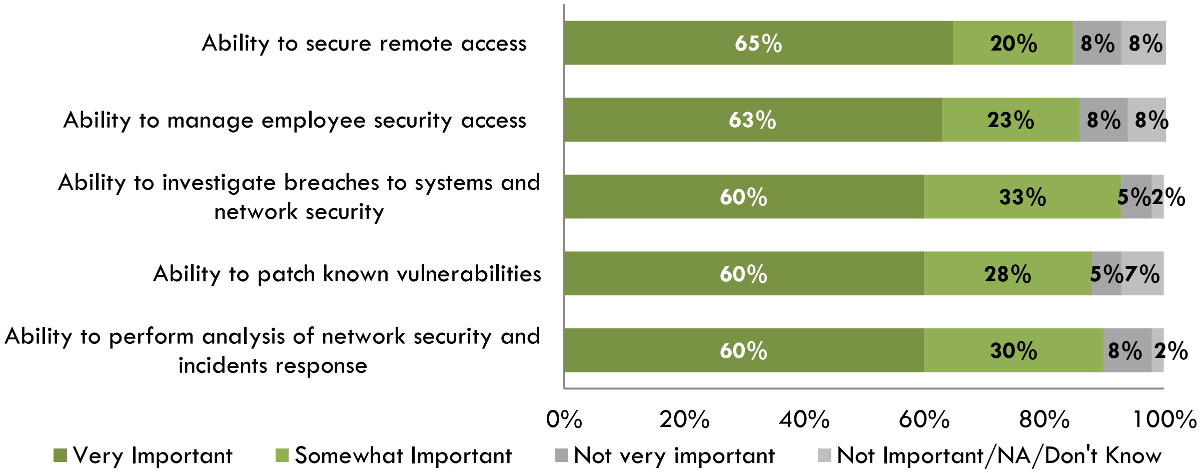


Computer specialists involved in cybersecurity, all other

This term includes all cybersecurity workers not already included in the previous categories.

- Employers reported that the most valued skill for these professional is the ability to secure remote access (65% very important).
- Employers indicated that additional very important skills are the ability to: manage employee security access (63%); investigate breaches to systems and network security (60%); patch known vulnerabilities (60%); and perform analysis of network security and incidents response (60%).

Exhibit 14: Computer Specialists involved in Cybersecurity, All Other (N=40)

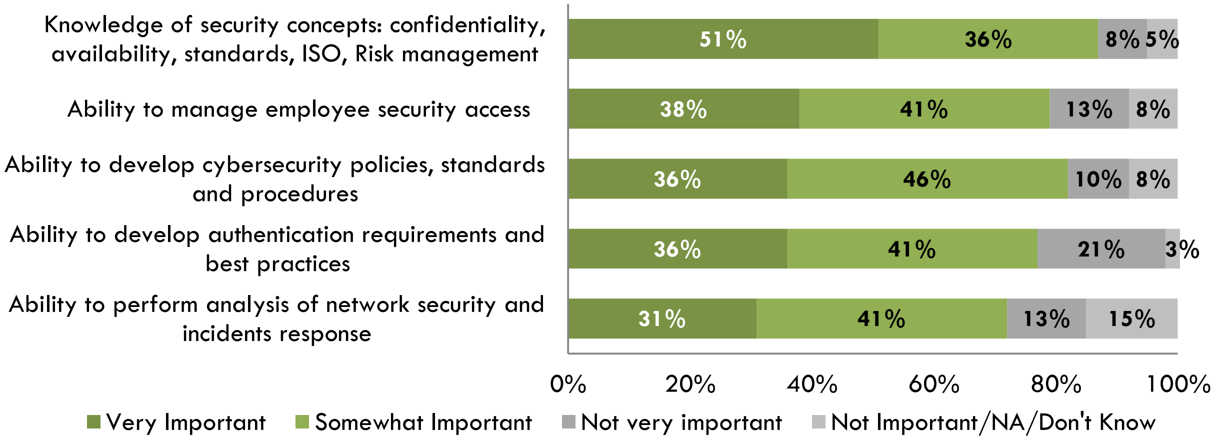


Computer and Information Systems Managers

Computer information systems managers are responsible for researching computer-related use in their organizations. They also oversee use the use and implementation of technology and technical solutions in their organizations.

- Employers reported that the most valued skill for computer information systems managers is the knowledge of security concepts: confidentiality, availability, standards, ISO, risk management (51% very important).
- Employers indicated that additional very important skills are the ability to: manage employee security access (38%); develop cybersecurity policies, standard, and procedures (36%); develop authentication requirement and best practices (36%); and perform analysis of network security and incidents response (31%).

Exhibit 15: Computer and Information Systems Managers (N=39)

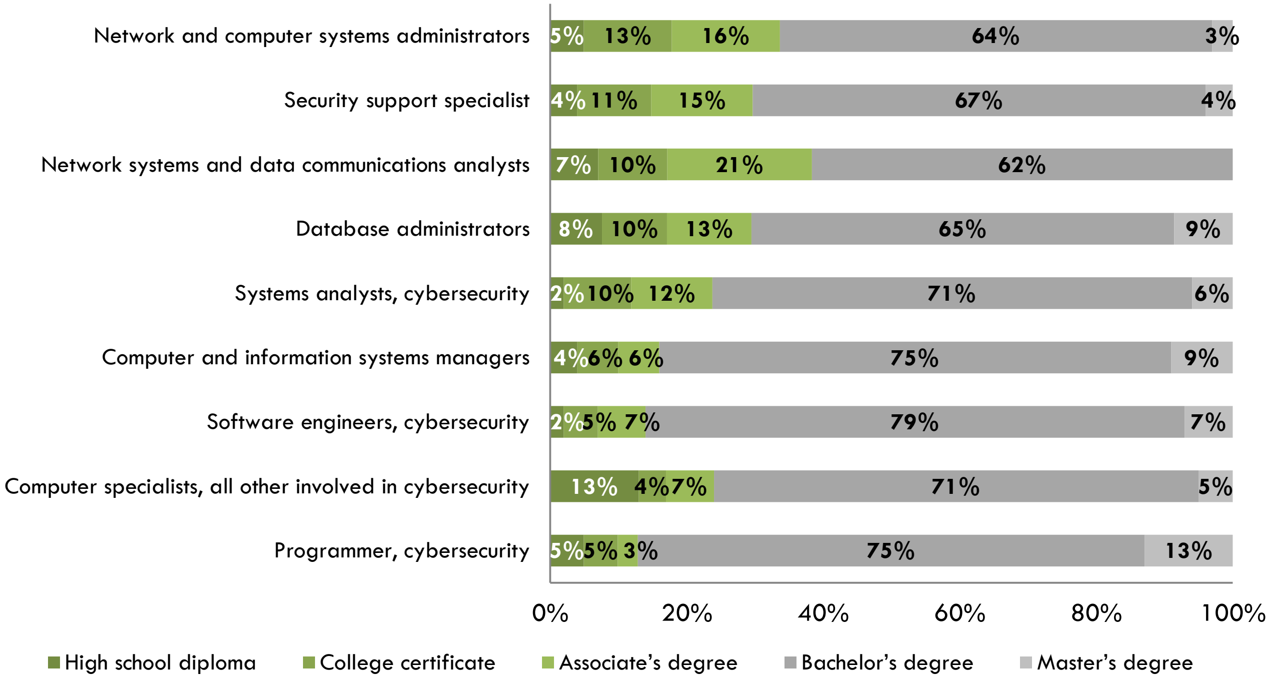


Educational Requirements

Employers surveyed were asked what their educational requirements for cybersecurity job candidates were. Exhibit 16 illustrates the preferred level of education for each occupation.

- For most occupations, employers prefer a Bachelor's degree.
- However, employers do indicate that there are entry level positions available for individuals with a Certificate or Associate degree:
    - 31% of employers claim to prefer hiring network systems and data communications analysts with an Associate's degree or Certificate.
    - 29% of employers claim to prefer hiring network systems and computer systems administrators with an Associate's degree or Certificate.
    - 26% of employers claim to prefer hiring security support specialists with an Associate's degree or Certificate.
- These results suggest that the Community College can play a critical role in preparing students to:
    - Begin a career in cybersecurity, and/or
    - Transfer into a Bachelor's degree program.

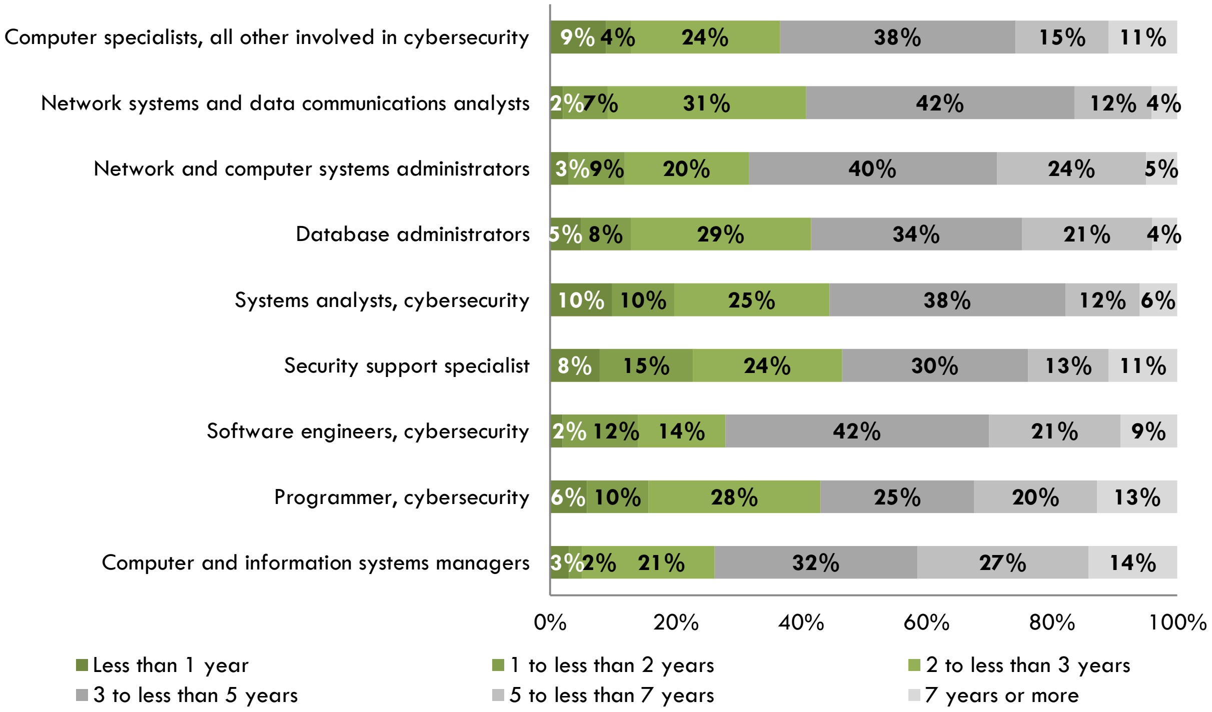
Exhibit 16: Preferred Level of Education for Cybersecurity New Hires



Work Experience Requirement

Employers were also asked their requirements for work experience when hiring for cybersecurity jobs. The majority of employers require at least two years of experience to gain employment. Thus community colleges should strive to build internships opportunities into cybersecurity programs to give students an opportunity to prove themselves and perhaps get hired in an entry-level position, to obtain practical skills and build experience.

Exhibit 17: Preferred Level of Experience When Hiring



Community Support and Resources

Regional colleges that want to address the training needs of cybersecurity professionals have access to the following resources:

Exhibit 18: Cybersecurity Resources

Organization	Services Provided
Center for Security Systems and Information Assurance www.cssia.org	"Advances Cyber Security education programs at the secondary and post-secondary levels by providing innovative teaching and learning opportunities through skills based student competitions and faculty professional development."
CyberWest Watch cyberwatchwest.org	"Cyberwatch West offers the most current information in Cybersecurity in the form of educational partnerships, business industry partnerships, professional, and student development programs and events."
DHS Cyber Security R&D Center www.cyber.st.dhs.gov	Partners with public and private sectors to increase valid cybersecurity research.
National Security Agency, Information Assurance www.nsa.gov/ia/ia_at_nsa	Offers training and security awareness support, as well as assessment and solutions for information security.
The Center for a New American Security www.cnas.org	"Develops strong, pragmatic and principled national security and defense policies."
Cyber Security Forum Initiative www.csfi.us	"Provides Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the US Government, US Military, Commercial Interests, and International Partners."
International Information Systems Security Certification Consortium, (ISC²) www.isc2.org	A world leader for certifying cybersecurity professionals.
Building a Cybersecurity Pipeline: Call to Serve www.ourpublicservice.org/OPS/programs/calltoserve/schools	A joint effort of the Partnership for Public Service and the Office of Personnel Management dedicated to partnering with college campuses to educate students about careers in the federal government.[26]

[26] Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, and TechAmerica. "Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper." March, 8, 2011.

College Response

Community Colleges in Los Angeles and Orange Counties

Training and education from the community colleges in Los Angeles and Orange Counties range from individual courses to certificate and Associate degree programs. Exhibit 19 presents a summary of community college offerings. For a detailed list of programs and courses see Appendix D.

Exhibit 19: Regional Security Programs, Certificates, and Courses

College	Degree Program	Certificate or Award	Number of Cybersecurity Courses
Cerritos College		Cyber Security Certification	5 Courses
Citrus College			1 Course
Coastline Community College		Computer Networking Certificate: Concentration in Security	11 Courses
		Network Security Specialist Certificate	17 Courses
Cypress College		Computer Forensics Certificate	6 Courses
El Camino College			1 Course
Fullerton College			2 Courses
Glendale Community College			1 Course
Irvine Valley College			2 Courses
Long Beach Community College		Information Security Certificate	5 Courses
LA City College			1 Course
LA Southwest College			1 Course
LA Trade Tech College			2 Courses
Mt. San Antonio College	A.S. in Computer and Network Security		7 Courses
		CIS Professional Certificate in Network Security	3 Courses
		Information and Operating Systems Security Certificate	3 Courses
Orange Coast College			2 Courses
Pasadena City College			4 Courses
Rio Hondo College			3 Courses
Saddleback College		Information Security: Security Occupational Skills Award	8 Courses
Santa Ana College			1 Course
Santa Monica College			4 Courses
West Los Angeles College	A.S. or A.A. - Computer Network and Security Management		15 Courses
		Certificate of Achievement- Computer Network & Security Management	14 Courses
		Low-Unit Certificate of Achievement in Computer Network & Information System Security	11 Courses

Other Training Providers

Many private training and education providers such as DeVry University, ITT Technical Institute, Westwood College, the United Education Institute, Versitas, or Hands On Technology Transfer, Inc., offer courses in computer technology. However, the cost of attending any of these providers' courses is much higher than community colleges' cost. In addition, it is preferable for students to take courses which can be transferred to four-year universities. Obtaining a more advanced degree will expand students' career opportunities in cybersecurity.

Gap Analysis

In spite of the high number of educational institutions that prepare students for information technology careers, the number of completions remains lower than the number of job openings for every program in the region. Exhibit 20 presents the number of job openings (new jobs and replacement jobs), the number of completion the same year (2010) and the gap, meaning the difference between open positions and students completing corresponding programs. These figures were provided by EMSI, based on completion data reported by educational institutions to IPEDS. Data includes all education institutions (i.e., community colleges, universities, proprietary schools etc.).

Exhibit 20: Gap Analysis per Program in LA/OC

CIP Code	Program Name	Number of Job Openings	Number of Completions	Gap
11.0103	Information Technology	2,155	543	1,612
11.0201	Computer Programming/Programmer, General	260	93	167
11.0501	Computer Systems Analysis/Analyst	1,689	59	1,630
11.0701	Computer Science	1,386	1,159	227
11.0802	Data Modeling/Warehousing and Database Administration	105	10	95
11.0901	Computer Systems Networking and Telecommunications	1,039	503	536
11.1001	System Administration/Administrator	479	32	447
10.1006	Computer Support Specialist	643	9	634
11.9999	Computer and Information Sciences and Support Services, Other	542	47	495

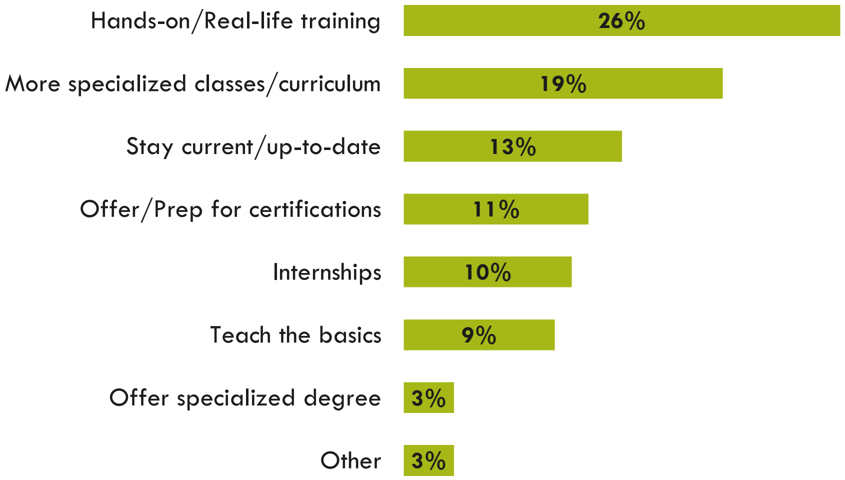
Source: EMSI

Implications and Recommendations for Community Colleges

Employer Suggestions

Respondents to the COE survey were asked to offer recommendations for Community Colleges regarding training the future cybersecurity workforce. Their responses were as follows:

Exhibit 21: Employer Recommendations



Employers emphasized the importance of applying skills directly in the classroom, working on real-life cybersecurity cases, and organizing internships for the students to gain experience. They also recommended adding more classes specific to cybersecurity to information technology programs. They highlighted the importance of staying current in a field that changes extremely rapidly.

Conclusion

Cybersecurity is important not only for business' success, but also for homeland security, and to protect individuals' privacy rights and safety. Firms must be prepared to face new threats that can arise each day, and need the expertise of cybersecurity professionals. There is a shortage of qualified cybersecurity experts in the country, and colleges have to play a key role in preparing a pipeline. Employment projections predict the creation of 12,241 new jobs between 2011 and 2016 (a 7% growth in 5 years). Adding replacement jobs (due to retirement and turnover), the number of job openings may be as high as 26,495 in Los Angeles and Orange Counties.

Cybersecurity jobs are in high demand, continue to grow, and offer high wages as well as career ladders. The number of students completing programs in computer and information science continues to be lower than the number of job openings. The gap is even more problematic for cybersecurity jobs. Employers who responded to our survey reported difficulty for all of the occupations studied. The highest level of difficulty (extreme difficulty) was reported for hiring Programmers, Security Support Specialists and Systems Analysts. Although not the majority, some employers require less than two years of work experience and an Associate degree or certificate, making community college students good candidates for these job opportunities.

Recommendations

Only two community colleges in the Los Angeles-Orange region offer an Associate Degree in Cybersecurity (Mt. San Antonio College and West Los Angeles College). Seven colleges offer Certificates in cybersecurity (see appendix D for details), and twenty have related courses. Given the high demand for cybersecurity professionals, there is an opportunity for more colleges to develop Certificates and Degree Programs in cybersecurity. It is recommended that colleges:

1. Consider adding courses in cybersecurity to their computer and information technology programs.
2. Create new Certificates or Degrees in Cybersecurity.
3. Make sure that their programs and curriculum include the skills listed for cybersecurity occupations in this report (see appendix C for details).
4. Include representation from cybersecurity employers on advisory committees to be aware of new trends keep programs up to date.
5. Contact CyberWatch West,[27] a valuable resource for curriculum development, partnership with businesses and services to students.
6. Coordinate with other colleges in the region to avoid duplication of efforts and possible competition.
7. Organize internships and opportunities for their students to gain hands-on experience.

[27] CyberWatch West: http://cyberwatchwest.org/

References and Resources

Adhikari, Richard. “Online Trust: A Thing of the Past?” January 28, 2009. (http://www.internetnews.com/security/article.php/3799141/Online+Trust+A+Thing+of+the+ast.htm)

Barrett, Larry. “ Systantec’s ‘Unlucky 13’ Security Trends for 2010.” November 20, 2009. (http://www.internetnews.com/security/print.php/3849371)

Bliss, Jeff. “U.S. Nuclear Plants Vulnerable to Cyber Attacks, Analysts Say,” November 17, 2010. (http://www.businessweek.com/news/2010-11-17/u-s-nuclear-plants-vulnerable-to-cyber-attacks-analysts-say.html)

Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, and TechAmerica. “Improving our Nation’s Cybersecurity through the Public-Private Partnership: A White Paper.” March, 8, 2011. (http://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf)

Center for a New American Security. “America’s Cyber Future: Security and Prosperity in the Information Age, Volume I.” June, 2011. (http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20I_0.pdf)

Dice. “America’s Tech Talent Crunch.” May 1, 2011. (http://marketing.dice.com/pdf/Dice_TechTalentCrunch.pdf)

Edmunds Community College Digital Forensics and Information Security. (http://infosec.edcc.edu/)

Evans, Karen and Reeder, Franklin. “A Human Capital Crisis in Cybersecurity: Technical Proficiency

Matters,” Center for Strategic and International Studies, November, 2010.(http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf)

Frost & Sullivan. “The 2011 (ISC)^2 Global Information Security Workforce Study.” March 31, 2011.(https://www.isc2.org/uploadedFiles/Landing_Pages/NO_form/2011GISWS.pdf)

Google. “Off-Network Workers – the Weakest Link to Corporate Web Security,” 2008(http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/a/help/intl/en/security/pdf/off_network_workers.pdf)

Godbe Research. Computer and Information Security Labor Market Study, June 2006.

Langton, Lynn & Planty, Michael. “Victim of Identity Theft, 2008.” U.S. Department of Justice: *Bureau of Justice Statistics*, December, 2010 (http://bjs.ojp.usdoj.gov/content/pub/pdf/vit08.pdf).

Mt. San Antonio Community College Regional Information Systems Security Center. (http://rissc.mtsac.edu/RISSC_NEW/default.asp)

Norton. (http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx).

Obama, President Barack. “Remarks by the President on securing our Nation’s cyber infrastructure.” May 29, 2009. (http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure).

Phillips, Leslie. “Senate Democrats Introduce Bipartisan Legislation Calling For New Safeguards For National Security, American Economy Against Cyber Attack.” January 26, 2011.(http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_i=e7362a98-5056-8059-7668-42e3de5aa933) ($1 trillion in intellectual property stolen)

Ponemon Institute. “First Annual Cost of Cyber Crime: Bench Mark Study of U.S. Companies.” July 2010. (http://www.riskandinsurancechalkboard.com/uploads/file/Ponemon%20Study%281%29.pdf).

Senate Committee on Homeland Security and Governmental Affairs. “Senate Democrats Introduce Bipartisan Legislation Calling for New Safeguards for National Security, American Economy Against Cyber Attack.” January, 26, 2011. (http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20I_0.pdf).

Serrano, Richard A. “U.S. Intelligence Officials Concerned About Cyber Attacks,” February 11, 2011.(http://www.latimes.com/news/nationworld/nation/la-na-intel-hearing-20110211,0,2209934.story)

Takanhashi, Dean. “IBM Says it Sees 13 Billion Cybersecurity Alerts Every Day.” March 31, 2011. (http://venturebeat.com/2011/03/31/ibm-says-it-sees-13-billion-cybersecurity-alerts-every-day/)

Appendix A: How to Utilize this Report

This report is designed to provide current industry data to:

- Define potential strategic opportunities relative to an industry's emerging trends and workforce needs;
- Influence and inform local college program planning and resource development;
- Promote a future-oriented and market responsive way of thinking among stakeholders; and,
- Assist faculty, Economic Development and CTE administrators, and Community and Contract Education programs in connecting with industry partners.

The information in this report has been validated by employers and also includes a listing of what programs are already being offered by colleges to address those workforce needs. In some instances, the labor market information and industry validation will suggest that colleges might not want to begin or add programs, thereby avoiding needless replication and low enrollments.

About the Centers of Excellence

The Centers of Excellence (COE), in partnership with business and industry, deliver regional workforce research customized for community college decision making and resource development. This information has proven valuable to colleges in beginning, revising, or updating economic development and Career Technical Education (CTE) 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 total grant amount (grant number 10-305-024 for $205,000) represents funding for multiple projects and written reports through the Center of Excellence. The Centers aspire to be the premier source of regional economic and workforce information and insight for California's community colleges.

More information about the Centers of Excellence is available at **www.coeccc.net**.

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.

Appendix B: Complete List of Most Common Security Threats

Below is a complete list of Norton's top 11 most commonly occurring security threats:[28]

Viruses. A virus is a program that can replicate itself and infect a single device or network of computers without the user's permission or knowledge. The danger level and prevalence of viruses are extremely high, and can cause an entire network to crash, resulting in a massive loss of valuable information.

SPAM, SPIM, and SPIT are all forms of junk mail: SPAM via email, SPIM via instant messenger, and SPIT via internet technology. Though their danger level is generally low, they are extremely prevalent and can grant access to sensitive information if opened by the receiver.

Spoofing, phishing, and pharming are all forms of a program, web page, or individual falsification. Spoofing occurs when a person or program is being impersonated; phishing is the replication of a legitimate webpage; and pharming redirects online traffic to a counterfeit website. The danger level of these forms of falsification is high with an extremely high prevalence and they can grant access to sensitive information if the user is not careful.

Spyware refers to software that is installed on a computer without user consent. The danger level and prevalence of spyware is high and can result in the loss of sensitive information, even the changing of computer setting which can lead to system slowing.

Keystroke logging (keylogging) is a software program designed to capture keystrokes (e.g. user input, such as passwords and credit card account information). They are often installed by a Trojan horse or virus. Because they capture sensitive user information their danger level and prevalence are high.

Adware is a form of software that is used to automatically direct a user to an advertisement. Though highly prevalent, it is relatively harmless unless being used as spyware.

Botnets are automated software agents that can create interaction with communities of users in a manner that is personalized to each individual. Because botnets typical run programs such as worms, Trojan horses, and backdoors they are considered to be highly dangerous. They are also highly prevalent.

Worm. Like a virus, a worm is a program that can replicate itself and infect a single device or network of computers without the user's permission or knowledge. Unlike a virus, a worm does not need to attach itself to a program, thus it is extremely dangerous. Worms are highly prevalent.

Trojan horse. A Trojan horse is a piece of software that poses as another piece of software or an application. At first it may function properly, but quickly begins to steal sensitive information and cause system malfunction. Trojans are extremely dangerous, but only moderately prevalent.

Blended threats employ a combination of attacks (e.g. worms, Trojan horses, and viruses sent together) to breach the security of a computer system. They are extremely dangerous, but only moderately prevalent.

Denial-of-service attack (DoS attack). A DoS is an attempt to make resources unavailable to its end user. Because these attacks are often launched through a network of systems they are especially dangerous to large businesses and government, and can be highly dangerous. However, they are not very prevalent.

[28] Norton. Found at: http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx

Appendix C: Complete List of Occupational Skills

Exhibit 21: Computer and Information Systems Managers (N=39)

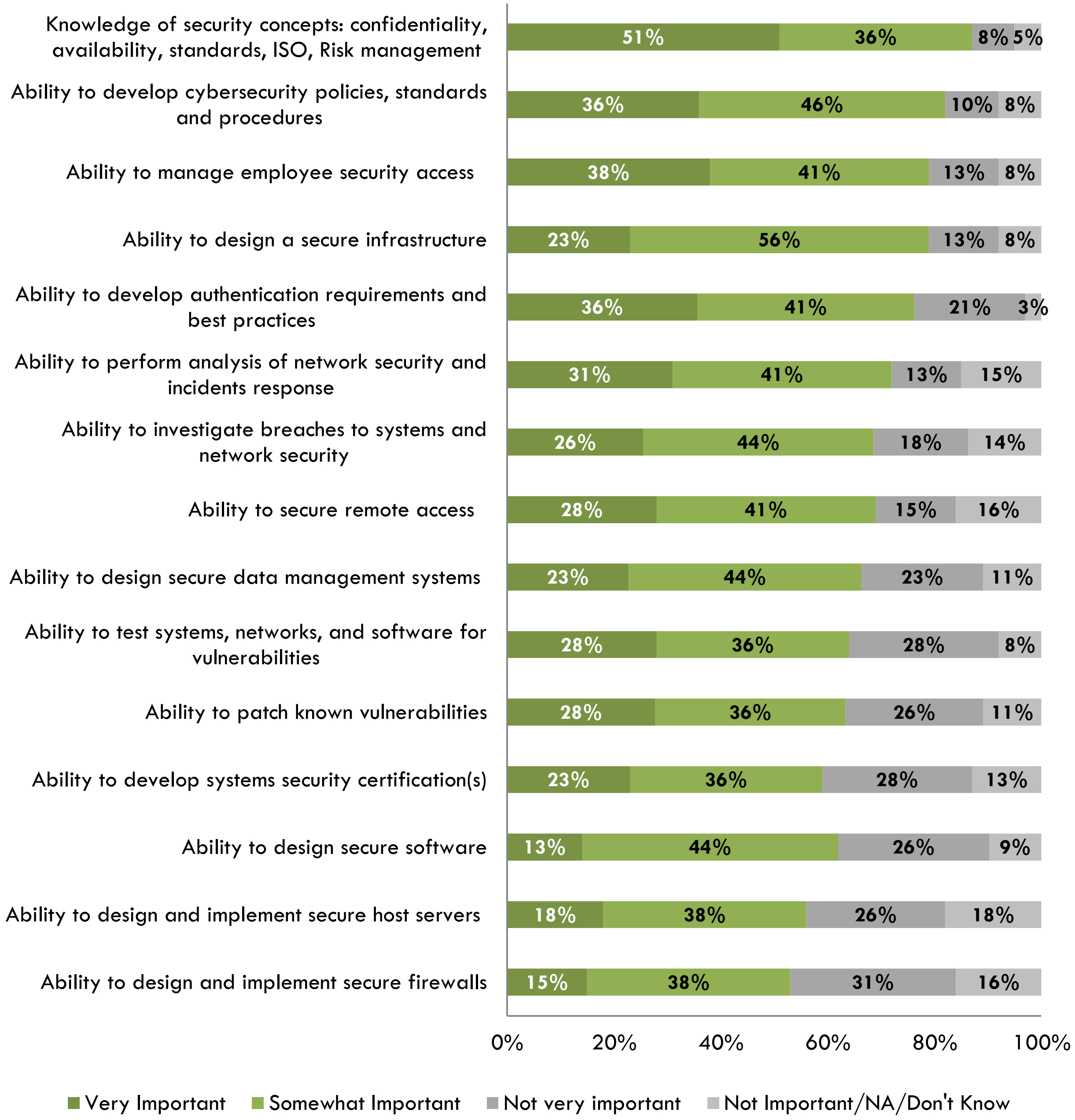


Exhibit 22: Programmer, Cybersecurity (N=35)

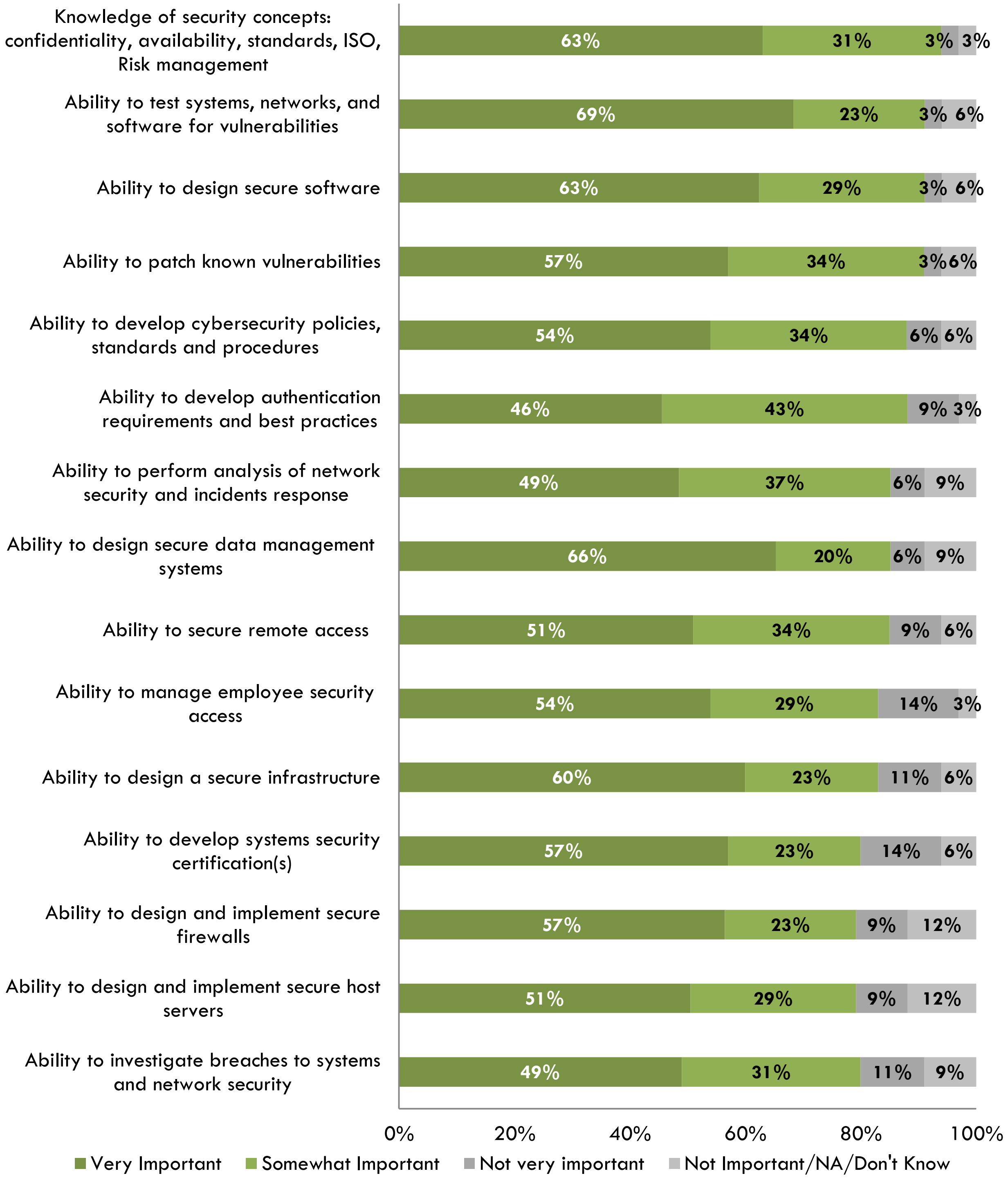


Exhibit 23: Software Engineers, Cybersecurity (N=39)

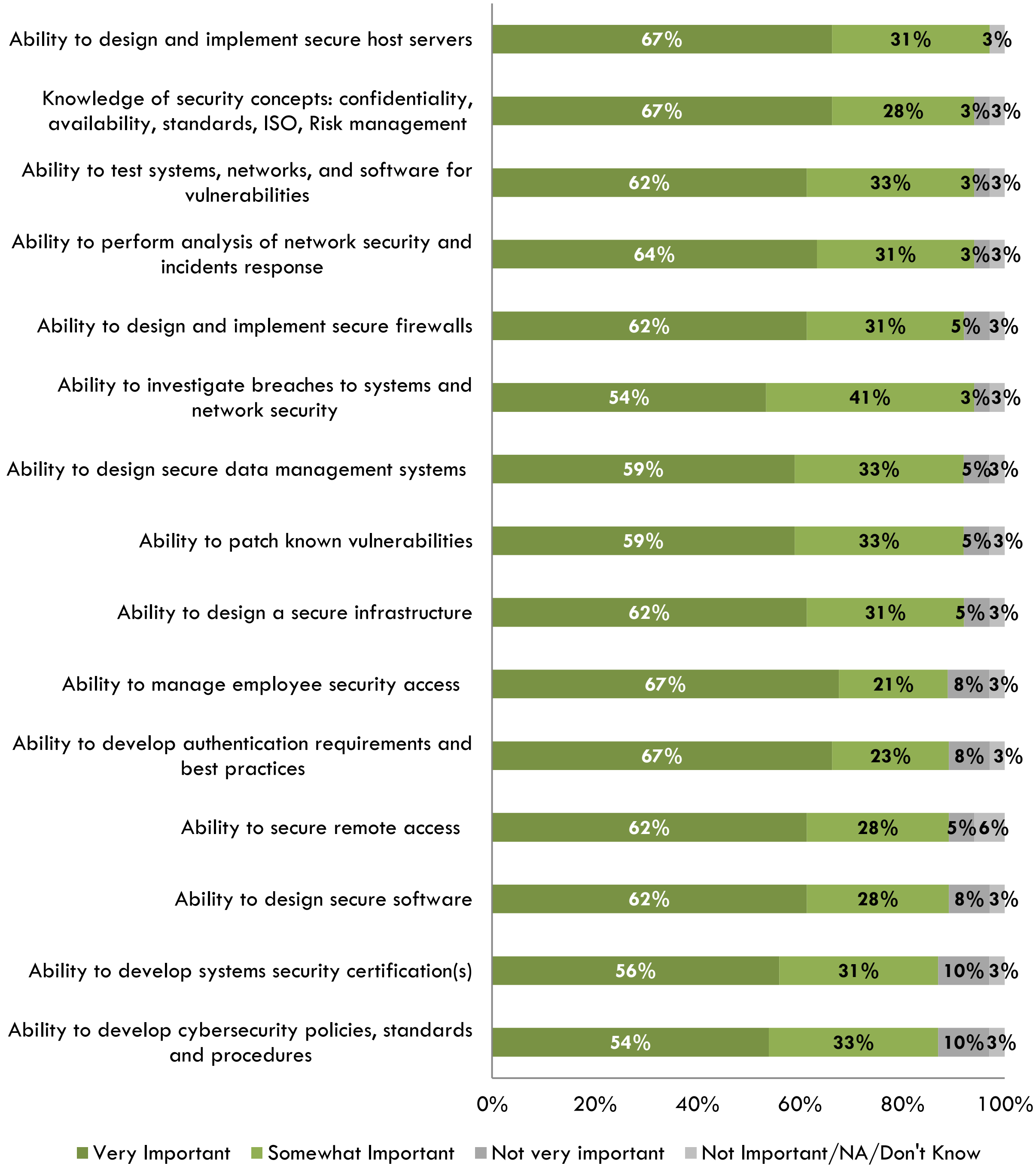


Exhibit 24: Security Support Specialist (N=44)

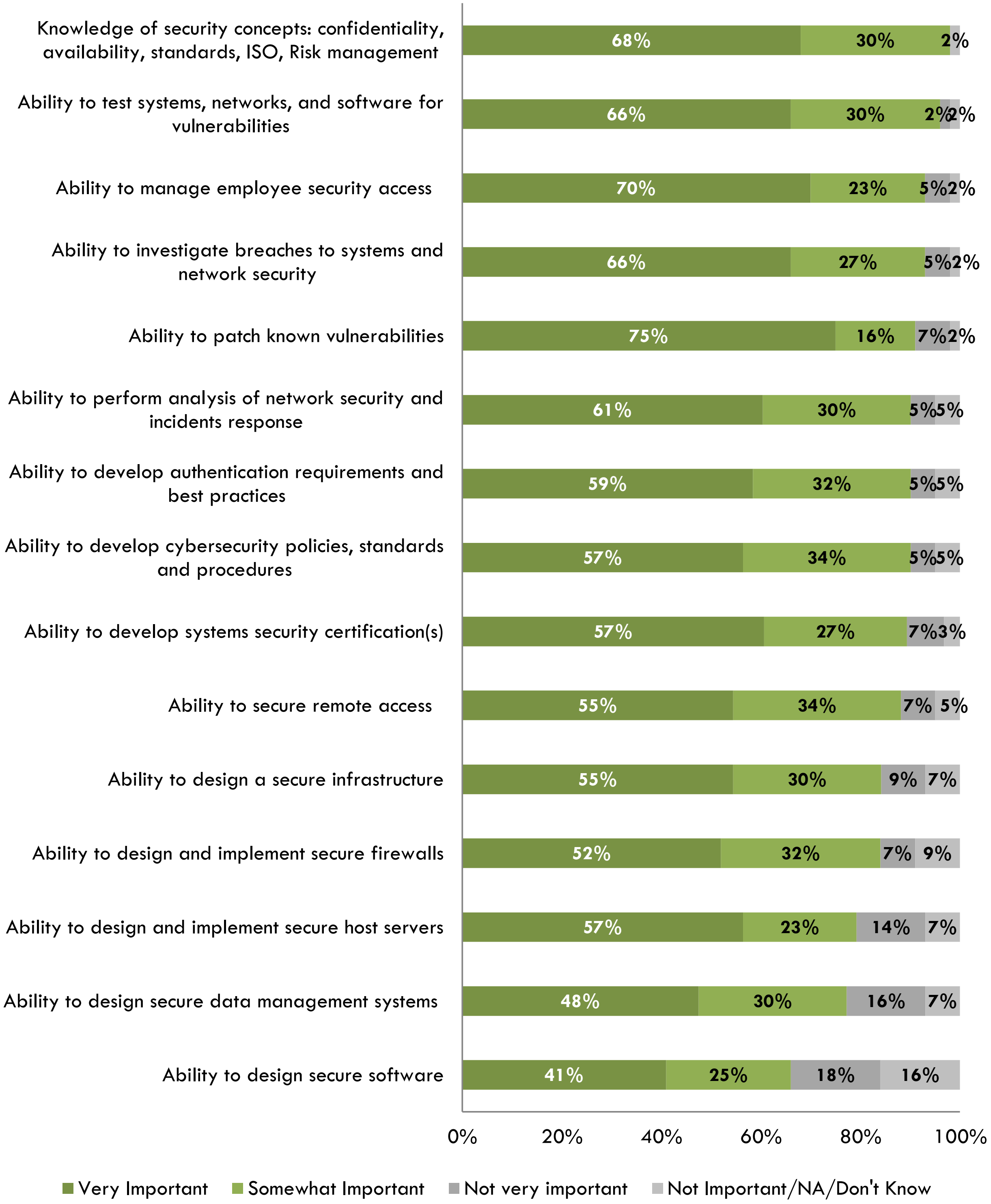


Exhibit 25: Systems Analysts, Cybersecurity (N=37)

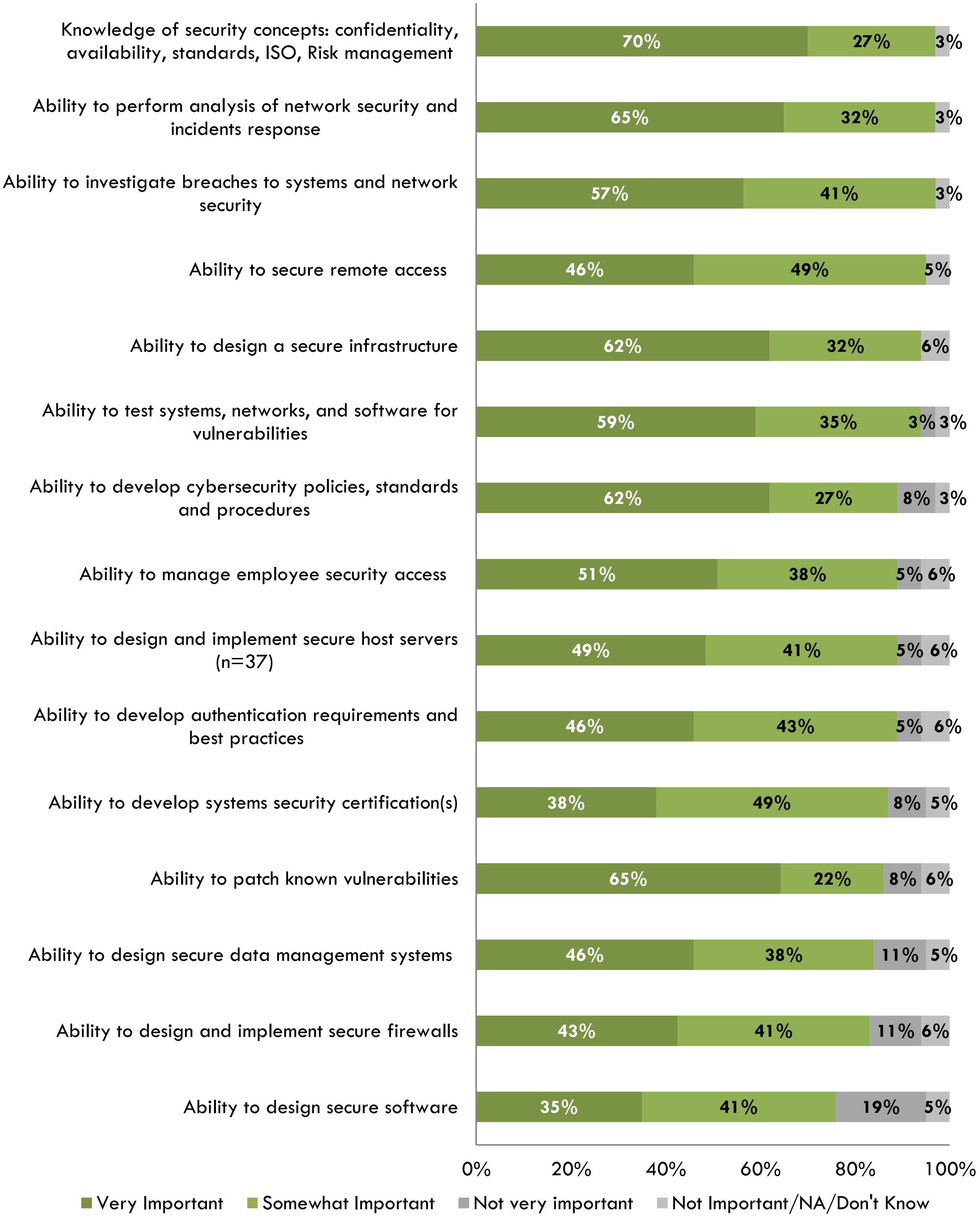


Exhibit 26: Database Administrators (N=47)

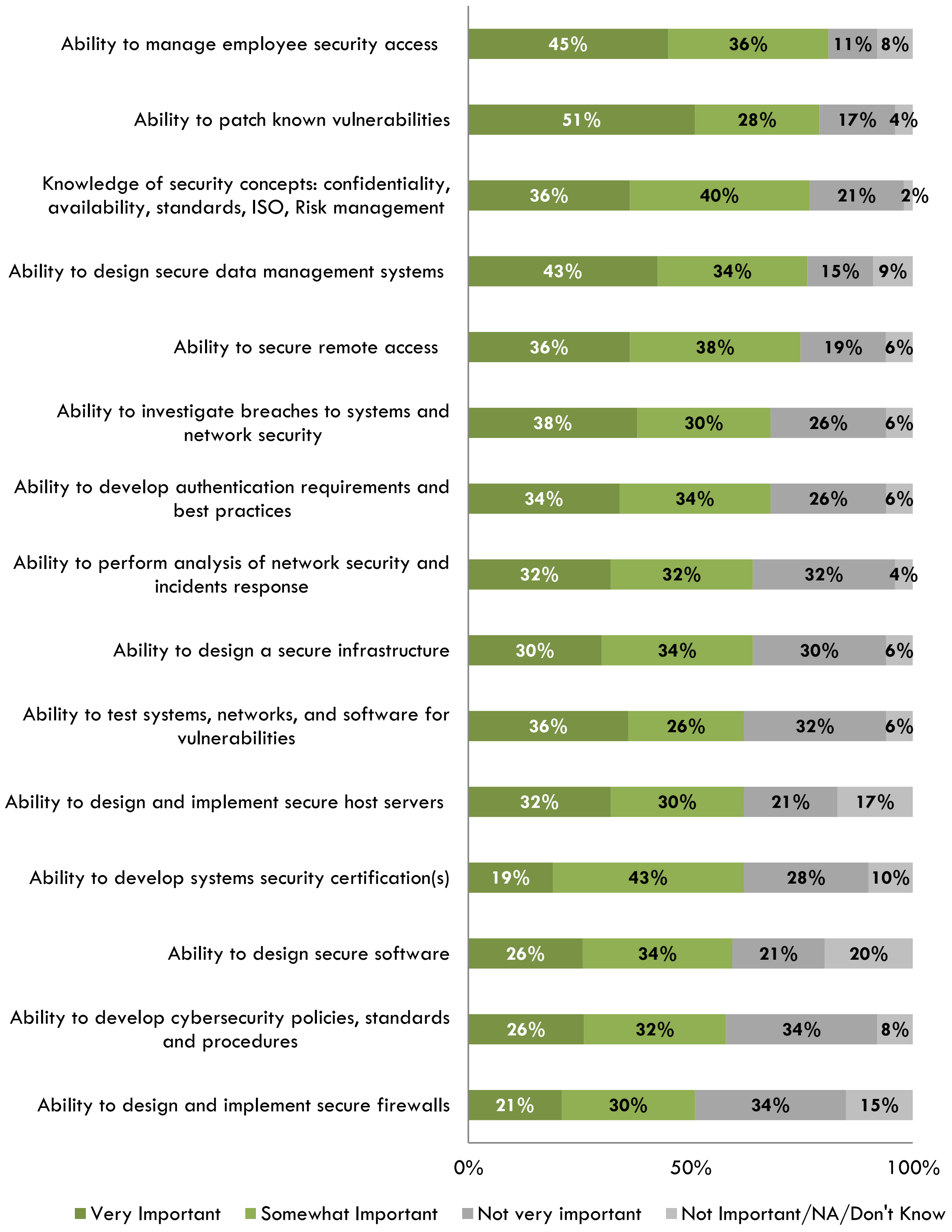


Exhibit 27: Network and Computer Systems Administrators (N=37)

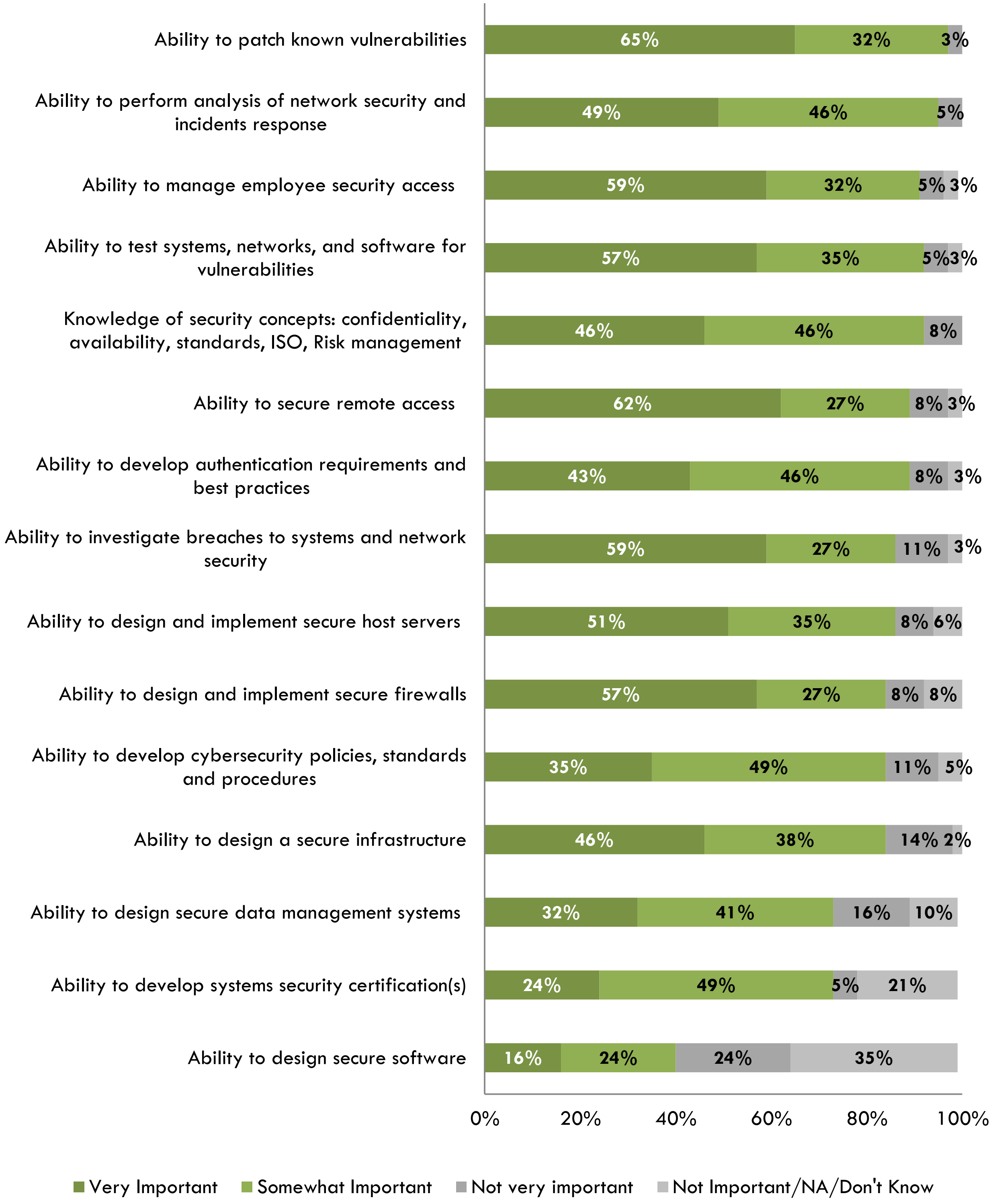


Exhibit 28: Network Systems and Data Communications Analysts (N=41)

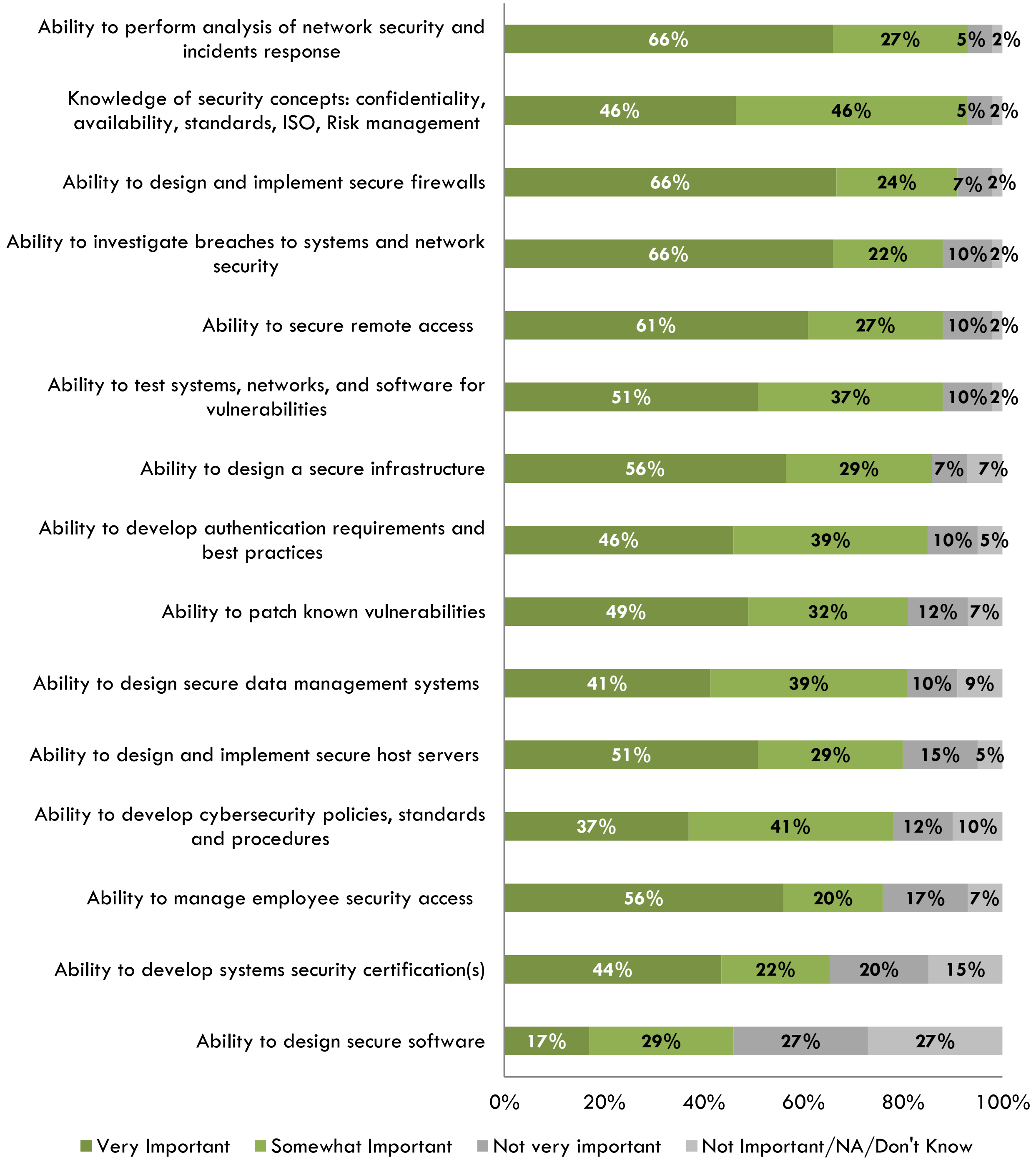
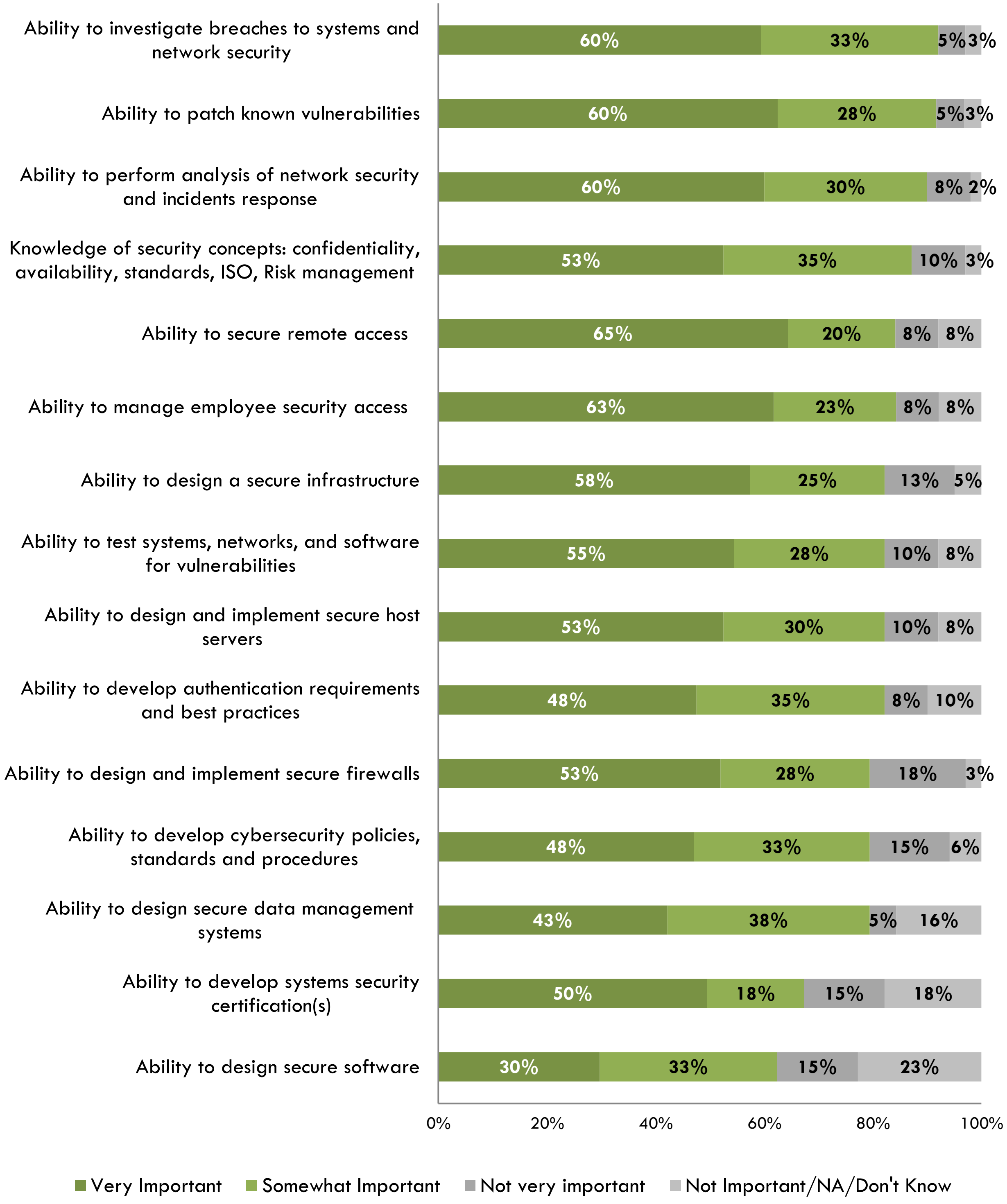


Exhibit 29: Computer Specialists, All Others, involved in Cybersecurity (N=40)



Appendix D: Complete List of Regional Programs and Courses

Cerritos College
Cyber Security Certification, 17 units, 5 classes:

- Network Fundamentals (required)
- Introduction to Wireless Networking (required)
- Network Security Fundamentals (required)
- Special Topics in Security (required)
- Microsoft Windows Security (required)

Citrus College
4 units, 1 class:

- Network and Computer Security

Coastline Community College
Computer Networking Certificate: Concentration in Security, 27 units, 11 classes:

- Security Essentials (required)
- Ethical Hacking (required)
- A + Essentials Hardware (required)
- Network +/Introduction to Networking (required)
- Configuring MS Windows 7 (required)
- CompTIA Linux (required)
- Cisco Fundamentals/CCNA 1 (required)
- Introduction to Geographic Information Systems (elective)
- Certified Wireless Network Administrator (elective)
- Cisco ASA, PIX, and Network Security (elective)
- Linux Networking and Security (elective)

Network Security Certificate, 39 units, 17 classes:

- Security Essentials (required)
- Ethical Hacking (required)
- MS Server 2008: Network Infrastructure (elective)
- Cisco ASA and Network Security (elective)
- Intrusion Detection Systems (elective)
- Firewall and Access Control Lists (elective)
- Computer Forensics (elective)
- Exploring Computer Forensics (elective)
- Certified Wireless Network Administrator (elective)
- Cisco Security Virtual Private Networks (VPNs) (elective)
- Cisco ASA, PIX, and Network Security (elective)
- Cisco IPS/CCSP (elective)
- Linux Networking and Security (elective)
- Advanced Linux Security (elective)
- Certified Information Systems (elective)
- Security Professional (CISSP) (elective)
- Become a Security Consultant (elective)

Cypress College
Computer Forensics Certificate, 18 units, 6 classes:

- Computer Forensics I (required)
- Computer Forensics II (required)
- Cyber Crime (required)
- Comp Forensics Legal Aspects (required)
- Analysis of Digital Media (required)
- Computer Forensics Capstone (required)

15 units, 5 classes:

- Internet Security (ISA) Server
- Network Security
- Anti-Hacking Network Security
- CCNA Security

El Camino College
4 units, 1 class:

- CompTIA Security+ Certification Preparation for Computer Hardware Systems

Fullerton College
5 units, 2 classes:

- Personal Computer Security
- Network Security Fundamentals

Glendale Community College
3 units, 1 class:

- Advanced Networking: Security

Irvine Valley College
5.5 units, 2 classes:

- Fundamentals of Computer Security for Home Users
- Fundamentals of Network Security

Long Beach Community College
Information Security Certificate, 13.5 units, 5 classes:

- Networking Fundamentals (required)
- i-Net+Internet Technologies (required)
- Introduction to Information Security (required)
- Network Security Fundamentals (required)
- LINUX Networking and Security (recommended)

Los Angeles City College
3 units, 1 class:

- UNIX System Security

Los Angeles Southwest College
3 units, 1 class:

- Computer Forensics I

Los Angeles Trade Tech College
6 units, 2 classes:

- Network Security Fundamentals
- Web Security

Mt. San Antonio College
A.S. Degree in Computer and Network Security, 28 units, 7 classes:

- Telecommunication Networking (required)
- Windows Server Network & Security Administration (required)
- Cisco CCNA Networking Fundamentals and Routing (required)
- Network Vulnerabilities and Countermeasures (required)
- Network Analysis and Intrusion Detection Systems (required)
- Network Security and Firewalls (required)
- Linux Networking and Security (required)

CIS Professional Certificate in Network Security, 12 units, 3 courses:

- Network Vulnerabilities and Countermeasures (required)
- Network Analysis and Intrusion Detection Systems (required)
- Network Security and Firewalls (required)

Information and Operating Systems Security Certificate, 10 units, 3 courses

- Practical Computer Security (required)
- Principles of Information Systems Security (required)
- Operating Systems Security (required)

Orange Coast College
7 units, 2 classes:

- Network Security Design
- Ethical Hacking and Network Defense

Pasadena City College
12 units, 4 classes:

- Fundamentals of Network Security
- CCNA Security
- Network Security 1
- Network Security 2

Rio Hondo College
9 units, 3 classes:

- Introduction to Information Security
- Network Security I
- Network Security II

Saddleback College
Information Security: Security Occupational Skills Award, 24 units, 8 classes:

- Information Security Fundamentals (required)
- Network Defense and Countermeasures (required)
- Information Security Management (required)
- Security + (required)

- Cyberlaw (required)
- Network and Security Administration Using UNIX/LINUX
- Advanced Network and Security Administration Using UNIX/LINUX
- Introductory Computer Forensics

Santa Ana College
3 units, 1 class:

- Internet Security

Santa Monica College
12 units, 4 classes:

- Computer Security Concepts
- Secure Server Installation and Administration
- Security in VB.NET Applications
- Security in J2EE Applications

West Los Angeles College
Associate of Arts or Science Degree- Computer Network and Security Management Option,
45 units, 15 classes:

- Operating Systems (required)
- Introduction to Linux+ (required)
- Introduction to Computer Networks (required)
- Introduction to Cisco Network Fundamentals (required)
- Introduction to Cisco Routers (required)
- Introduction to Computer and Information Security I (required)
- Introduction to Microsoft Server Operating System (required)
- Network and Information System Security (required)
- Linux.Apache.MySQL.Virtual and Cloud Computing (elective)
- Administering Computer Networks and Security (elective)
- Microsoft Networking Infrastructure Administration (elective)
- Introduction to Windows Active Directory Services (elective)
- Information Storage Management/Virtual Server (elective)
- Microsoft SQL Server (elective)
- Microsoft Exchange Server (elective)

Certificate Of Achievement - Computer Network & Security Management, 30 units, 14 classes:

- Operating Systems (required)
- Introduction to Linux+ (required)
- Introduction to Computer Networks (required)
- Introduction to Cisco Network Fundamentals (required)
- Introduction to Cisco Routers (required)
- Introduction to Computer and Information Security I (required)
- Introduction to Microsoft Server Operating System (required)
- Network and Information System Security II (required)
- Linux.Apache.MySQL.Virtual and Cloud Computing (elective)
- Microsoft Networking Infrastructure Administration (elective)
- Introduction to Windows Active Directory Services (elective)
- Information Storage Management/Virtual Server (elective)

- Microsoft Exchange Server (elective)
- Microsoft Exchange Server (elective)

Low-Unit Certificate of Achievement in Computer Network & Information System Security, 16 units, 11 classes:

- Introduction to Computer Networks (required)
- Introduction to Computer and Information Security I (required)
- Network and Information System Security II (required)
- Linux.Apache.MySQL.Virtual and Cloud Computing (elective)
- Administering Computer Networks and Security (elective)
- Microsoft Networking Infrastructure Administration (elective)
- Introduction to Windows Active Directory Services (elective)
- Information Storage Management/Virtual Server (elective)
- Microsoft Exchange Server (elective)
- Installing, Configuring, Administering Microsoft SQL (elective)
- A+ & Network+ Hardware Lab (elective)

Cyber Security Advisory Sub-Committee Meeting

Agenda

February 4, 2016

Attendees

Present:

Edward	Balcer	NAWC
Keith	Bennett	NAWC
Christopher	Harper	AltaOne
Uwe	Schmiedel	Monarch

Absent:

Heather	Kenny	NAWC
Tony	Vitale	NAWC
Autumn	Piotrowski	NAVAIR

Introductions

Introductions were done by each attendee.

Minutes of previous meeting

No minutes were reviewed, but Valerie reviewed the meeting outcomes from November 2016 that prompted the development of the Cyber Security program.

Committee Purpose/Overview

Valerie reviewed the purpose of the meeting. The purpose was to review the Cyber Security degree and certificate components that are approved by Homeland Security and NSA to make sure that it aligns with the needs of local employers.

Discussions

The proposed National Security Administration/Homeland Security curriculum was reviewed and the group thought the certificate and degree were a good baseline of skills for entering cyber security and information assurance. Future development of higher-level certificate was reviewed as well and discussion of the CISSP as a component was determined to be a good goal. It is understood that the CISSP has a requirement for personnel to work in the discipline for three to five years. Valerie said a higher level certificate will probably be several years away.

Edward Balcer reported that NAWC is having problems getting qualified personnel hired fast enough. They need Security Analyst and Information Assurance personnel. Valerie shared the new internship program with Jacobs Technology and the NAWC Apprenticeship program.

Additionally NAWC China Lake has a need to educated/train existing engineers and computer scientist in cyber security. Another requirement brought up is that the base analysts for weapons products will need to be trained in cyber security. There is an expectation that there will be a new strategic initiative

Discussions (Continued)

that all program development and operations personnel will need to be trained in cyber awareness. There was an estimated 1100 personnel in Edwards group and only three personnel are trained. While there is no mandate right now, it is expected that it will become required. There are 800 scientists and engineers in Test and Evaluation and 30-50 will need to be trained in the next five years.

Monarch being a small business is interested in graduates that have experience with Linux and the Internet of Things (IoT). They agreed that the certificate/degree is a good baseline.

AltaOne has needs for IT staff. Chris Harper is involved in the development of this program as an adjunct and has previously stated that they have a difficult time finding qualified candidates for the bank.

Edward (NAWC) shared that they also look for the aptitude in candidates.

Next meeting date

Valerie will send out the minutes to the meeting for review and editing. The group will meet with the Computer Information Systems Advisory Committee at the fall meeting.

CTE Program Narrative

NAME OF COLLEGE: Cerro Coso Community College

CONTACT: Dr. Corey Marvin

PHONE NUMBER: 760-375-6201

EMAIL ADDRESS: cmarvin@cerrocoso.edu

DATE: April 27, 2016

DIVISION: CTE

FACULTY: Valerie Karnes

PROGRAM NAME: Cyber Security Technology

REASON FOR APPROVAL REQUEST (Check One):

- □ [✓ New Program Proposal]
- □ Program Revision Proposal (Substantial or TOP Code Changes)
- □ Locally Approved

TYPE OF DEGREE:

- □ Certificate of Achievement
- □ Associate of Arts
- □ [✓ Associate of Science]
- □ Associate of Arts for Transfer
- □ Associate of Science for Transfer
- □ Other

TRANSFER APPLICABILITY: [✓ Yes] □ No □

ATTACHMENTS/INFORMATION REQUIRED:

Labor/Job Market Data and Analysis
Advisory Committee Meeting Minutes
List of Advisory Committee Members
Employer Survey, if applicable

1. Statement of Program Goals and Objectives

Identify the goals and objectives of the program. For CTE programs, the statement must include the main competencies students will have achieved that are required for a specific occupation. The statement must, at a minimum, clearly indicate the specific occupations or fields the program will prepare students to enter and the basic occupational competencies students will acquire.

If the program is selective, describe relevant entry criteria and the selection process for admission to the program. Specify all mandatory fees that students will incur for the program aside from the ordinary course enrollment fee.

Statement of Program Goals and Objectives

The goals of this new degree are to fill a documented need in the area of cyber security, information security and information assurance of our service area employers. The degree is designed for students pursuing professional employment in information security for business. This degree program provides students with skills to enter the job market as information security specialists, information security technicians, information assurance technicians, networking security technicians, and cyber security technicians. Designed for both full and part-time students, this program is appropriate to both those currently employed and those seeking to enter this field. The courses are aligned with industry degree and students are prepared to take the A+ exam, Net+ exam, Security+ and Server+ exam.

Program Learning Outcomes:

1. Configure, install, diagnose, and support hardware and software issues.
2. Utilize identifying tools and methodologies that hackers use to break into a network computer and defend a computer and local area network against a variety of different types of security attacks using a number of hands-on techniques.
3. Design, analyze, and support computer networks.
4. Apply problem-solving, programming, and application development including the ability to design, test, debug, and implement complex computer programs.
5. Operate servers, storage, and virtualization including implementing and evaluating network security solutions.
6. Read and interpret technical information, as well as communicate with and write clearly for wide ranges of audiences.

2. Catalog Description

Enter exactly as it will appear in the catalog, including program outcomes. The description must also

- *Convey the certificate's goals(s) and objectives*
- *Provide an overview of the knowledge and skills that students who complete the requirements must demonstrate (student learning outcomes)*
- *List all prerequisite skills or enrollment limitations*
- *Mention any risks, such as occupations that are inherently competitive or low-salaried and/or occupational areas where inexperienced graduates are not generally hired.*
- *For CTE programs, the description must list the potential careers students may enter upon completion.*

- *Convey what the student may expect as an outcome*

If applicable, reference accrediting and/or licensing standards. If there is a widely recognized certification provided by a professional association, specify whether the program will fully prepare completers for the recognized professional certification.

The goals of this new degree are to fill a documented need in the area of cyber security, information security and information assurance of our service area employers. The degree is designed for students pursuing professional employment in information security for business. This degree program provides students with skills to enter the job market as information security specialists, information security technicians, information assurance technicians, networking security technicians, and cyber security technicians. Designed for both full and part-time students, this program is appropriate to both those currently employed and those seeking to enter this field. The courses are aligned with industry degree and students are prepared to take the A+ exam, Net+ exam, Security+ and Server+ exam.

Cyber Security Technician Associate of Science degree is designed for students pursuing professional employment in information security for business. This degree program provides students with skills to enter the job market as information assurance technicians, information security analysts, network security professionals and cyber security technicians. Designed for both full-time and part-time students, this program is appropriate to both those currently employed and those seeking to enter the field. This degree program is also transferable to California State University at San Bernardino.

Students exiting this program are prepared to enter the fields of information security, network security, information assurance or cyber security. Students can demonstrate the following student learning outcomes.

1 . Configure, install, diagnose, and support hardware and software issues.
2 . Utilize identifying tools and methodologies that hackers use to break into a network computer and defend a computer and local area network against a variety of different types of security attacks using a number of hands-on techniques.
3 . Design, analyze, and support computer networks.
4 . Apply problem-solving, programming, and application development including the ability to design, test, debug, and implement complex computer programs.
5 . Operate servers, storage, and virtualization including implementing and evaluating network security solutions.
6 . Read and interpret technical information, as well as communicate with and write clearly for wide ranges of audiences.

Students entering this program develop all the skills necessary to be successful are taught in the first course in the career pathway (CSCI C101). Jobs in information security and cyber security are in high demand and pay from $86,000 (per Labor Market data attached).

3. Program Requirements

- ✓ *The program requirements must be consistent with the catalog description. The number of units, specific course requirements and the sequence of the courses must be coherent, complete and appropriate. Display the program requirements in a table format that includes all courses required for completion of the program (core requirements and required or restricted electives), subtotal of core units, and total program units. For each course, indicate the course department number, course title, and unit value.*

Display of Program Requirements

Core Courses	**Title**	**Units**
CSCI C101	Introduction to Computer Information Systems	3
CSCI C142	Information & Communication Technology Essentials	4
CSCI C143	Computer Network Fundamentals	3
CSCI C146	Security+ Fundamentals of Networks	3
CSCI C251	Introduction to Programming Concepts and Methodologies	3
CSCI C190	Introduction to Cyber Security: Ethical Hacking	3
CSCI C193	System and Network Administration	3
CSCI C195	Introduction to Systems Analysis and Design	3
MATH C121	Elementary Probability and Statistics Or MATH C121H Elementary Probability and Statistics – Honors Or	4-5
MATH C130	Finite Mathematics Or	4
MATH C131	Basic Functions and Calculus for Business	4
	Total Core Courses	**29-30**

Program (PR) Requirements Summary Table:

Major Total:	29-30 Units
College GE Requirements	21 Units
Electives	9 Units
Total Units	60 Units

Completion of CSU-GE Breadth or IGETC pattern 30 units
TOTAL UNITS 60 units

Proposed A.S. Sequence:
Year 1, Fall = 15 units
Year 1, Spring = 15 units
Year 2, Fall = 15 units
Year 2, Spring = 15 units

TOTAL UNITS: 60 units

Display of Proposed Sequence

First Semester	**Units**
CSCI C101	3
CSCI C142	4
General Education	5
Total	**15**

Second Semester	**Units**
CSCI C143	3
CSCI C146	3
General Education	9
Total	15

Third Semester	**Units**
CSCI C190	3
CSCI C193	3
MATH C121/130/131	4-5
General Education	4-5
Total	**15**

Fourth Semester	**Units**
CSCI C195	3
CSCI C251	3
General Education	9
Total	**15**

7. **Master Planning** (Background and Rationale)

Given the stated goals and objectives, address the role the proposed program will fulfill in the college's mission and curriculum offerings. This discussion may include some history of the program proposal origins, a description of the program purpose, and/or the program's relevancy for the region and college.

The proposal must demonstrate a need for the program that meets the stated goals and objectives in the region the college proposes to serve with the certificate. A proposed new certificate must not cause undue competition with an existing program at another college.

If any expenditures for facilities, equipment or library and learning resources are planned, please explain the specific needs in this section.

If the program is to be offered in close cooperation with one or more specific employers, a discussion of the relationship must be provided.

There has been an increasing need in our service area, state and across the country for qualified entry-level personnel to enter the Cyber Security, Information Technology Security, Network Security, and Information Assurance. This need continues to expand as the networks and hackers and hostile groups infiltrate systems in major organizations. The Cyber Security Associate Degree of Science will provide students with a baseline of courses to be immediately employed in Cyber Security, Information Assurance, and Information Security. The employer community within our service area supports the need for this degree. The employer community within our service area supports the need for this degree and has requested over one hundred graduates per year. Program development has been driven by the employers in our service area and the national need for technicians in this field.

Most on-site courses at the IWV campus are taught in the Learning Resource Center. There are two computer lab classrooms. One classroom is equipped with 30 student stations and the third is equipped with 29 student stations. All rooms have an instructor station, an overhead projector, and whiteboards. Although iTV rooms are available to allow multiple campuses to participate in a single course, the rooms are not equipped with computer stations, limiting their usefulness for CSCI courses that require hands-on access to technology to achieve the student learning objectives. Increasingly, other disciplines (English, math, engineering, science) are requesting to use the computer classrooms for their own courses. It is expected as the college continues to develop science, technology, engineering, and as the use of computer technology is infused across the curriculum, the demand for these rooms will increase and additional facilities will be required. In addition, if the college pursues a partnership with Cisco to further develop an Information Technology/Cyber Security/Information Assurance program, it will be required to have a dedicated laboratory to be designated as a Cisco certified college.

The college has used VTEA funds to further develop the Computer Information Systems program in the past and it is expected that the new Cyber Security program will also be supported by VTEA funds. A VTEA program plan has already been developed and submitted for funding to fund the needs of an emerging program for 2016-2017. If it determined that the college needs to be a Cisco certified partner for higher level certificate or degree, there will be space required, equipment required and an ongoing equipment cost that could be funded through federal grants for Cyber Security.

The Library and Learning Resource Center are used to support the current program. The library is used to support research for the courses in the program. Five of the Cyber Security program is shared with the Computer Information Systems courses, so there are adequate resources available. The additional three courses for the program may require additional books and materials for the program. The department faculty regularly works with the librarian to acquire books and materials for the area and programs. There have been recent additions to the electronic library resources that will support both the Computer Information Systems and Cyber Security Program. Additionally, several courses in the department are directly supported with Library research instructions tailored to the course by the library staff.

The program was developed and is supported by the Computer Information Systems Advisory Committee and the Cyber Security Sub-committee. An internship program with Jacobs Technology and the Naval Air Warfare Center at China Lake demonstrates the strong commitment of industry to this program. Employers are interviewing and hiring student interns that have completed the first course in the sequence (CSCI C101) with the expectation that the students will complete the Cyber Security Certificate of Achievement and the Cyber Security degree program within three years. This is a direct result of a close relationship with employer needs. The five employers on the Advisory Committee are also considering adopting the Jacobs model of internships.

7. Need for Program

a. Enrollment and Completer Projections

Address and justify the number of projected students or "annual completers" to be awarded the certificate each year after the program is fully established.

The Cyber Security program is a new program that will fill a target need for industry. Employers have indicated a need for 100 employees in this area. In order to full this need, we will need to scale our program offerings to meet this need. We project enrollment in the program to be 150-200 in the four beginning courses. Students will choose between the Computer Information Systems and Cyber Security program following completion of the four core classes. Completer projections are 50-100 per year by 2018.

For those students interested in transfer, the new model cyber security curriculum provides students with a pathway to California State University at San Bernardino in the Information Systems and Technology Bachelor of Science program. All of the courses offered in the CIS degree are accepted for transfer within the UC and CSU systems (source: assist.org) as well as other universities throughout the US.

b. Labor Market Information (LMI)

Summarize the Labor Market Information (LMI) and employment outlook (Including citation for the source of the data) for students exiting the program.

Enter table or chart as a separate attachment.

The attached Labor Market report for Information Security/Cyber Security/Information Assurance shows a regional need for 164 jobs with the 2020 projections to be 200 jobs. This represents a 22% increase in jobs. While this shows demonstrated need, in the Cerro Coso service area there are many known jobs that are not documented because employer's corporate offices are out of state. For example, positions appropriate for IT/CIS/Cyber Security graduates such as those required by aerospace contractors, the Naval Air Warfare Center at China Lake, and even our own Cerro Coso Community College classified IT staff are not captured in this reporting system because the corporate offices are located outside our service area.

The Cyber Security program has documented labor market demand for the degree and certificate. In the Cerro Coso service area there are many known jobs that are not documented because employer's corporate offices are out of state. For example, positions appropriate for Cyber Security graduates such as those required by aerospace contractors, the Naval Air Warfare Center at China Lake, and even our own Cerro Coso Community College classified IT staff are not captured in this reporting system because the corporate offices are located outside our service area.

Employers in the Indian Wells Valley have attended the Advisory Committee meetings over the past several years and have actively engaged in the discussions and development of the new certificate(s) and degree for Computer Information Systems and Cyber Security Technology. At first, we believed that the Information Technology Plus certificate would fill the entire need. Following the CIS Advisory Committee Meeting in November 2015, the employers indicated that they needed a more specific cyber security program (COA and AS) as well as the CIS program. Faculty attended the Information and Communication Technology state conference in January 2016, which outlined the needs and forecast for Cyber Security programs. Additionally, there was an announcement that there was a model program that was fully transferrable to CSU San Bernardino. This new program will share the IT Plus certificate and then students will be able to select the IT pathway or the Cyber pathway.

While the numbers of job opportunities are reflective in the environmental scans attached, two local employers are not captured (Jacobs Technology and the Naval Air Warfare Center at China Lake). These two specific employers have come to the college in the past few months presenting their local hiring requirements. Each employer is estimating a minimum of 40-50 students needed for their organization. Internships and apprenticeship programs have recently been developed to provide a pipeline for employees. Employers are hiring directly out of our first level class with the understanding that students will take the remaining courses to earn their certificate and then their degrees. In December, they hired three students for the internship program and anticipate hiring the fourth in March/April. We are preparing students now to interview in mid to late April. Jacobs plans to hire three to four students per quarter for the internship program.

Environmental scan reports from EMSI, Burning Class and the Community College Review all project huge need that is only expected to expand. The Cyber Security job postings have grown 91% from 2010-2014 as compared to other IT postings (28%). The duration of the postings in cyber security is 47 days versus 36 days for all other IT jobs. Salaries for Cyber Security are $6,459 higher than all other IT postings (Cyber Security $83,934 versus IT $77,475). Additionally, California ranks first in the nation for the job postings (Burning Glass) and the percentage of growth from 2010-2014 was 75%. There were 28,744 job postings in California from 2010-14.

c. Employer Survey (if applicable)

When strong LMI data is not available, an employer survey may be submitted. Provide a copy of the survey, including the number of those surveyed, number of responses, and a summary of the results. The survey must address the extent to which the proposed degree or certificate will be valued by employers.

Specific CSCI courses have been developed and delivered to meet the short-term and long-term needs of local employers. The CIS Advisory Committee formed a subcommittee for Cyber Security to review the national Homeland Security and National Security Administration. Additionally, the development team of the program includes top experts from NAWC at China Lake, Monarch and AltaOne. The department is responsive to requests for specific training programs and attempts to develop appropriate coursework, as needed, dependent on staffing and budgetary constraints. Informal surveys have been done at the CIS and Cyber Security Advisory Committees and this program is being driven by local, state and national needs.

7. Place of Program in Curriculum/Similar Programs

Review the college's existing program inventory, then address the following questions:

- *Do any active inventory records need to be made inactive or changed in connection with the approval or the proposed program? If yes, please specify.*
- *Does the program replace any existing program(s) on the college's inventory? Provide relevant details if this program is related to the termination or scaling down of another program(s).*
- *What related programs are offered by the college?*

These courses also serve the Computer Information Systems Associate's degree. The Information Technology Plus certificate is the first level of the Computer Information Systems pathway and provides students a first step into the industry. The second level certificate (Cyber Security certificate) has several additional courses that result in another certificate and finally adding General Educational requirements; students will earn an Associate Degree of Science..

There are no other colleges in our service area and the program does not represent unnecessary duplication. The program does not represent unnecessary duplication of training programs and other regional colleges offering a similar program are too far away to impact employer's needs in our service area.

7. Similar Programs at Other Colleges in Service Area

List similar programs offered at other colleges within the Central/Mother Lode Region that may be adversely impacted. Enter 'none' if there are no similar programs.

College	Program
None	

Supporting documentation required

Labor Market Information

In a separate attachment, provide current Labor Market Information showing that jobs are available for program completers within the local service area. Statewide or national LMI may be included as supplementary support but evidence of need in the specific college service area or region is also necessary.

List of Members of Advisory Committee

This list must include advisory committee member names, job titles, and affiliations.

Name	Title	Affiliation
Melissa Oliverez	Manager	Continental Labor
Johnson Daniel	Network Administrator	Coso/Teragen contrastIT
Mary Lorber	Software Architect/Program Mgr	Engility
Sean Callihan	STARS IT/IA Director	Jacobs Engineering
Tom Della Santina	STARS IT/IA/Business Director	Jacobs Engineering
Rich Christenson	Recruiter	Jacobs Engineering
Vaughn Corbridge	VX-9 TIMS PM/Analyst	HTii
Eileen Shibley	CEO	Monarch
Uwe Schmiedel	IT Director	Monarch
Edward Balcer	Head, Weapons & Energetics Technology Assurance Branch	NAVAIR Weapons Division

Keith Bennett	Information Assurance	NAWC China Lake
Tony Vitale	Information Assurance	NAWC China Lake
Margaret Porter	Information Assurance	NAWC China Lake
Autumn Piotrowski	Information Assurance	NAWC China Lake
Mark Henderson	Directed Energy Manager	NAWC China Lake
Linda Homer	Software Programmer	NAWC China Lake
John Paul	Program Manager	New Directions Technology, Inc
Kishor Joshi	CEO	Pertexa
Scott Lougheed	Director	Saalex
Paul McKenzie	Director	Saalex

Recommendation of Advisory Committee (Meeting Minutes)

In a separate attachment, provide minutes of the advisory committee meetings at which the program was discussed and approved, with relevant areas highlighted, as well as a summary of the advisory committee recommendations.

Occupation Overview

EMSI Q3 2015 Data Set

February 2016

3000 College of Heights Blvd
Ridgecrest, California 93555
760.384.6258

Parameters

Occupations

Code	Description
15-1122	Information Security Analysts

Regions

Code	Description
6027	Inyo County, CA
6029	Kern County, CA
6051	Mono County, CA
6071	San Bernardino County, CA
6107	Tulare County, CA

Timeframe

2015 - 2020

Datarun

2015.3 – QCEW Employees

Information Security Analysts in 5 Counties

Information Security Analysts (SOC 15-1122):

Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses. Excludes “Computer Network Architects” (15-1143).

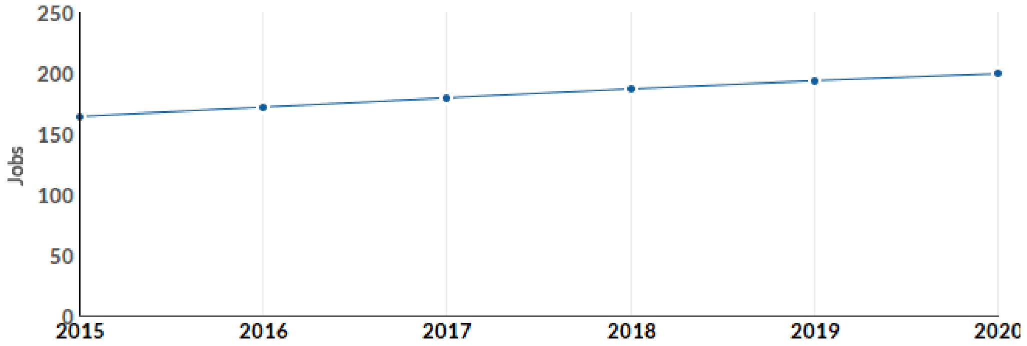
Sample of Reported Job Titles:
Computer Security Specialist
Information Systems Security Officer
Security Analyst
Information Security Manager
Systems Analyst
Systems Administrator
Security Specialist
Security Director
Programmer Analyst
PC Analyst (Personal Computer Analyst)
Related O*NET Occupation:
Information Security Analysts (15-1122.00)

Occupation Summary for Information Security Analysts

164 Jobs (2015) 77% below National average	+22.0% % Change (2015-2020) Nation: +16.4%	$44.48/hr Median Hourly Earnings Nation: $42.74/hr

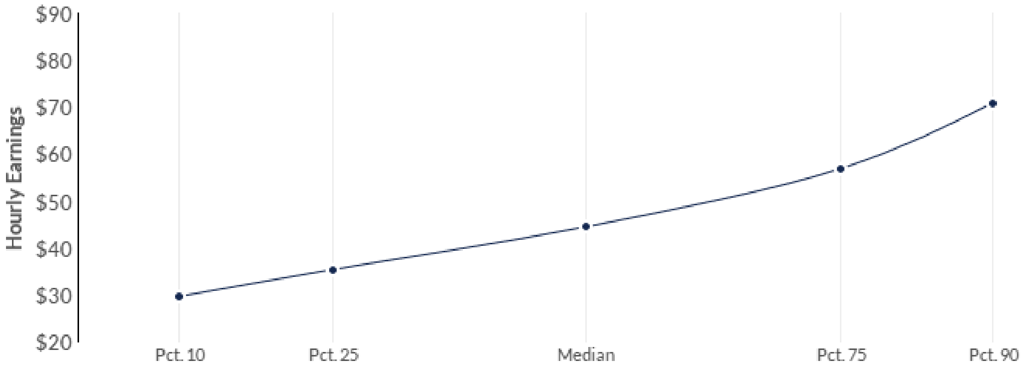
Growth for Information Security Analysts (15-1122)

164	200	36	22.0%
2015 Jobs	2020 Jobs	Change (2015-2020)	% Change (2015-2020)

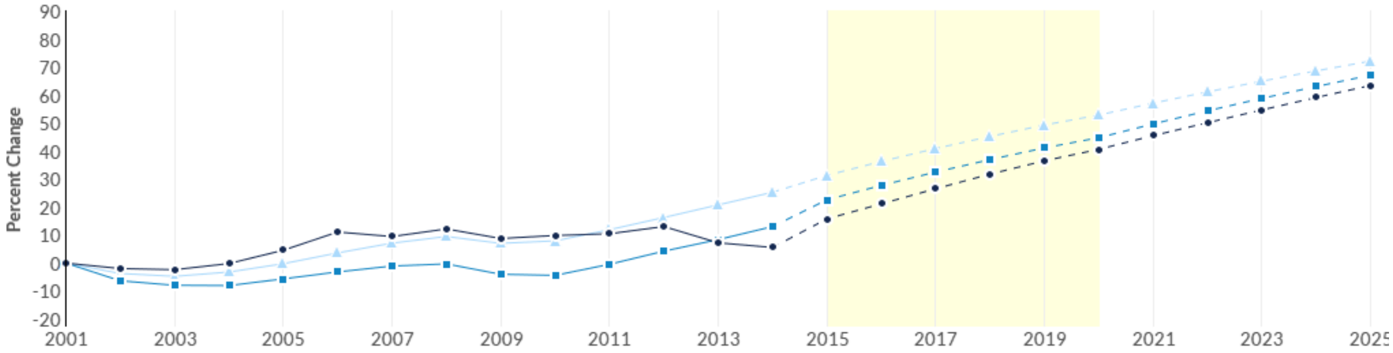


Percentile Earnings for Information Security Analysts (15-1122)

$35.34/hr	$44.48/hr	$56.82/hr
25th Percentile Earnings	Median Earnings	75th Percentile Earnings

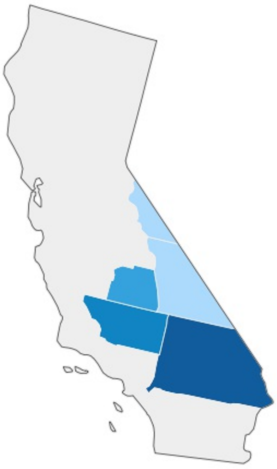


Regional Trends



	Region	2015 Jobs	2020 Jobs	Change	% Change
●	Region	164	200	36	22.0%
■	State	8,688	10,258	1,570	18.1%
▲	Nation	84,774	98,689	13,915	16.4%

Regional Breakdown



County	2020 Jobs
San Bernardino County, CA	110
Kern County, CA	67
Tulare County, CA	19
Inyo County, CA	<10
Mono County, CA	<10

Job Postings Summary

65

Unique Postings (Dec 2015)

262 Total Postings

4 : 1

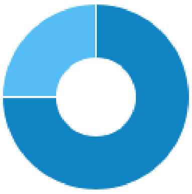
Posting Intensity (Dec 2015)

Regional Average: 4 : 1

There were 262 total job postings for *Information Security Analysts* in December 2015, of which 65 were unique. These numbers give us a Posting Intensity of 4-to-1, meaning that for every 4 postings there is 1 unique job posting.

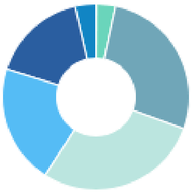
This is close to the Posting Intensity for all other occupations and companies in the region (4-to-1), indicating they are putting average effort toward hiring this position.

Occupation Gender Breakdown



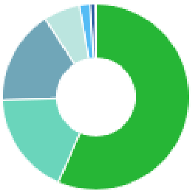
	Gender	2015 Jobs	2015 Percent
●	Males	123	75.0%
●	Females	41	25.0%

Occupation Age Breakdown



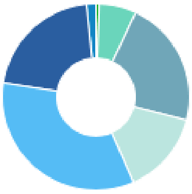
	Age	2015 Jobs	2015 Percent
●	14-18	0	0.1%
●	19-24	5	3.3%
●	25-34	45	27.2%
●	35-44	47	28.6%
●	45-54	34	20.7%
●	55-64	27	16.5%
●	65+	6	3.6%

Occupation Race/Ethnicity Breakdown



	Race/Ethnicity	2015 Jobs	2015 Percent
●	White	93	56.6%
●	Hispanic or Latino	29	17.9%
●	Asian	27	16.4%
●	Black or African American	10	6.3%
●	Two or More Races	3	1.9%
●	American Indian or Alaska Native	1	0.8%
●	Native Hawaiian or Other Pacific Islander	0	0.2%

National Educational Attainment



	Education Level	2015 Percent
●	Less than high school diploma	0.6%
●	High school diploma or equivalent	6.4%
●	Some college, no degree	22.0%
●	Associate's degree	14.4%
●	Bachelor's degree	34.0%
●	Master's degree	21.0%
●	Doctoral or professional degree	1.6%

Occupational Programs

11	503	17
Programs (2014)	Completions (2014)	Openings (2014)

CIP Code	Program	Completions (2014)
11.0901	Computer Systems Networking and Telecommunications	135
11.0103	Information Technology	127
11.0701	Computer Science	68
11.1002	System, Networking, and LAN/WAN Management/Manager	67
11.1003	Computer and Information Systems Security/Information Assurance	31

Industries Employing Information Security Analysts

Industry	Occupation Jobs in Industry (2015)	% of Occupation in Industry (2015)	% of Total Jobs in Industry (2015)
Other Computer Related Services	15	9.2%	0.6%
Corporate, Subsidiary, and Regional Managing Offices	13	7.9%	0.1%
Custom Computer Programming Services	<10	4.2%	0.6%
Local Government, Excluding Education and Hospitals	<10	4.0%	0.0%
Computer Systems Design Services	<10	3.9%	0.7%

Appendix A - Data Sources and Calculations

Location Quotient

Location quotient (LQ) is a way of quantifying how concentrated a particular industry, cluster, occupation, or demographic group is in a region as compared to the nation. It can reveal what makes a particular region unique in comparison to the national average.

Occupation Data

EMSI occupation employment data are based on final EMSI industry data and final EMSI staffing patterns. Wage estimates are based on Occupational Employment Statistics (QCEW and Non-QCEW Employees classes of worker) and the American Community Survey (Self-Employed and Extended Proprietors). Occupational wage estimates also affected by county-level EMSI earnings by industry.

Completers Data

The completers data in this report is taken directly from the national IPEDS database published by the U.S. Department of Education's National Center for Education Statistics.

Institution Data

The institution data in this report is taken directly from the national IPEDS database published by the U.S. Department of Education's National Center for Education Statistics.

Industry Data

EMSI industry data have various sources depending on the class of worker. (1) For QCEW Employees, EMSI primarily uses the QCEW (Quarterly Census of Employment and Wages), with supplemental estimates from County Business Patterns and Current Employment Statistics. (2) Non-QCEW employees data are based on a number of sources including QCEW, Current Employment Statistics, County Business Patterns, BEA State and Local Personal Income reports, the National Industry-Occupation Employment Matrix (NIOEM), the American Community Survey, and Railroad Retirement Board statistics. (3) Self-Employed and Extended Proprietor classes of worker data are primarily based on the American Community Survey, Nonemployer Statistics, and BEA State and Local Personal Income Reports. Projections for QCEW and Non-QCEW Employees are informed by NIOEM and long-term industry projections published by individual states.

Staffing Patterns Data

The staffing pattern data in this report are compiled from several sources using a specialized process. For QCEW and Non-QCEW Employees classes of worker, sources include Occupational Employment Statistics, the National Industry-Occupation Employment Matrix, and the American Community Survey. For the Self-Employed and Extended Proprietors classes of worker, the primary source is the American Community Survey, with a small amount of information from Occupational Employment Statistics.

State Data Sources

This report uses state data from the following agencies: California Labor Market Information Department

From: Allyson Adams [mailto:allyson.adams@scccd.edu]
Sent: Monday, May 16, 2016 8:24 AM
To: Corey Marvin <cmarvin@cerrocoso.edu>
Cc: Karri Hammerstrom <Karri.Hammerstrom@reedleycollege.edu>
Subject: Approval: Associate of Science Degree in Cyber Security Technology from Cerro Coso Community College

Approval: Associate of Science Degree in Cyber Security Technology from Cerro Coso Community College

Congratulations. Your request for approval of the Associate of Science Degree in Cyber Security Technology from Cerro Coso Community College has been **approved by the colleges in the Central/Mother Lode Region** with nine endorsement approval votes from Bakersfield College, Clovis Community College, Fresno City College, Cerro Coso Community College, West Hills College Coalinga, West Hills College Lemoore, College of the Sequoias, Columbia College, and Taft College.

Please include this email as evidence of regional approval. You have the original signature pages, so no need to re-submit these. Your new program will also be posted with approved programs on the Central/Mother Lode regional website.

Cerro Coso Community College Associate of Science Degree in Cyber Security Technology:

- **Request for Program Review Received:** 4/29/16
- **Forwarded to CRC Program Reviewers:** 4/29/16
- **CRC Program Reviewer Endorsement Approval**: 5/13/16 by nine votes (Bakersfield College, Clovis Com Community College, West Hills College Coalinga, West Hills College Lemoore, College of the Sequoias, C
- **College Notified of Program Approval:** 5/16/16

Please let me know if you have any questions. Thank you!

Karri Hammerstrom
Regional Chair of the Central/Mother Lode Regional Consortium
390 W. Fir Avenue, Building 'A', #204E, Clovis, CA 93611
Karri.hammerstrom@reedleycollege.edu
(559) 324-6444
www.crconsortium.com

Allyson Adams
Administrative Aide
Central / Mother Lode Regional Consortium
allyson.adams@scccd.edu
(559) 324-6444

Minutes
Central / Mother Lode Regional Consortium
Annual Planning Conference
June 6-8, 2016 Monterey, CA

Meeting Attendees:
Steering Committee: Salvador Vargas (San Joaquin Delta), Thad Russell (COS), Pedro Mendez (Modesto JC), Jim Andersen (Merced College), Jacob Jackson (Fresno City College), Klaus Tenbergen (Columbia), David Clark (Reedley College), Linda Thomas (Clovis Community College), Cindy Collier (Bakersfield College), Tony Cordova (Taft College), Sam Aunai (Porterville College), Robert Pimentel (West Hills College, Coalinga), Michael Kane (Cerro Coso), Dave Bolt (for James Preston, West Hills College, Lemoore), Karri Hammerstrom (Regional Chair (RC)/SCCCD)

DSNs/TAPs: Dennis Mohle (ICT/DM DSN), Lorinda Forrest (Small Business DSN), Shelley Attix (Retail, Hospitality, Tourism DSN), Gurminder Sangha (Advanced Manufacturing DSN), Jeanette Benson (Global Trade and Logistics DSN), Linda Zorn (SN, for Valerie Fisher – HWI DSN), Nancy Gutierrez (SN, for Lori Marchy - Ag, Water and Environ. Tech. DSN), David Teasdale (Prop 39 Project Director TAP), Nora Seronello (Centers of Excellence TAP), Bob Hawkes (K-14 Pathways Director)

Guests: See last page

Monday, June 6, 2016

1. Welcome, introductions and conference overview
2. Presentation on the evolution of CTE at CA Community Colleges - Walter Di Mantova
3. Presentation on the collaboration between Central Valley Higher Education Consortium (CVHEC) and Central Regional Consortium - Dr. Sandra Caldwell, Dr. Benjamin Duran, Karri Hammerstrom
4. Panel on Dean's Leadership Academy module - Jim Andersen, David Clark, Salvador Vargas
5. Discussion of CCCCO directives in relationship to $200M Guidance - Walter Di Mantova, Karri Hammerstrom

Tuesday, June 7, 2016

1. M/S/A April 19, 2016 Meeting Minutes
2. M/S/A Receive and File: Program Endorsement Approvals, FY 2015-16 (*4/16/16-6/3/16*):

Program name	College name	Approval Due Date
Police Science AS Degree	San Joaquin Delta College	5/9/2016
Automation Technician - Mechatronics COA	San Joaquin Delta College	5/10/2016
Automation Technology - Mechatronics AS Degree	San Joaquin Delta College	5/10/2016
Computer Network Security Technology AS Degree	San Joaquin Delta College	5/10/2016
Electrical Technology - General Electrician Trainee COA	San Joaquin Delta College	5/10/2016
Electrical Technology AS Degree	San Joaquin Delta College	5/10/2016
Machining Technology AS Degree	San Joaquin Delta College	5/10/2016

Solar Photovoltaic Installation Technician COA	San Joaquin Delta College	5/10/2016
Fire Fighter Academy I COA	Bakersfield College	5/12/2016
Executive Chief Fire Officer COA	Bakersfield College	5/12/2016
Cyber Security Technician COA	Cerro Coso	5/13/2016
Cyber Security Technology AS-T Degree	Cerro Coso	5/13/2016
Advanced Information Systems AS Degree	Porterville College	5/25/2016
Business Information Systems AS Degree	Porterville College	5/25/2016
Computer Information Systems AS Degree	Porterville College	5/25/2016
Public Safety AS Degree	Porterville College	5/25/2016

3. Regional Chair report highlights:
    a. Regional plan must be approved by January, 2017. A series of planning meetings will be held for all stakeholders; a pre-planning meeting targeted to CIOs held on July 27, 2016. More details will follow.
    b. Vice Chancellor Van Ton-Quinlivan will be hosting a briefing for the CRC regarding the $200M Strong Workforce Program:

        Conference Call Details: June 22, 2016; 10:00 am – 11:00 am
        Phone: 888-886-3951
        Passcode: 9849864

    c. A webinar on the new Dual Enrollment Toolkit will be taped and available for viewing. The toolkit can be found at http://www.careerladdersproject.org/ccccode/.
    d. A goal for next year would be to identify a program(s) to pre-approve curriculum for multiple colleges; LA/OC has a model to review.
    e. Linnie Bailey has been contracted to compile the narrative portion of CTE EF Final Reports. She will be contacting all CRC colleges in the near future. RC reminded all colleges that project reports can be submitted as soon as the project is completed.

4. CRC Strategic Planning (see attached slides)
   Eric Ryan reviewed the strategic planning process, asking steering committee members for feedback on what has worked or not worked during the last year. Highlights from strategic area champions included:
    a. Communication and Leadership
        i. The importance of getting the consortium's 'house' in order before involving other entities.
        ii. CRC marketing focus should first be colleges.
    b. Curriculum, Programs and Pathways
        i. Program approval process is working well. Items to consider: when does the area reach saturation with programs? Are programs portable, scalable?
        ii. It would be helpful to have a complete inventory of CTE programs in the CRC Region.
        iii. Example - Workplace Internship regional project has held two meetings discussing strategies and best practices.
        iv. How do community colleges become strong partners with K-12? Tulare/Kings Linked Learning is an excellent model.
        v. A comment was made to add 'tutoring' to this section of the strategic plan
    c. CTE Student Support Services

        i. Necessity of documenting what the region look like in terms of embedded CTE counselors.

    d. Research and Data

        i. Necessity of ongoing solicitation of reports concerning the region and notification when those reports are posted.

5. Presentation on Labor Market Information
   Nora Seronello discussed Demand and Supply Data Tools from the COE. These excel tables are an excellent source for regional LMI, and are updated twice a year. The tables can be accessed at http://coeccc.net/supply-demand/.

6. Presentation on the State of Perkins in CRC Region - JeanClaude Mbomeda
7. Presentation on Managing Perkins Funds - Robin Harrington

Wednesday, June 8, 2016

1. Presentation of Regional Updates by DSNs and TAPs
2. Additional Reports and Announcements
    a. Discussion of SW Contract Education Task Force - David Teasdale
    b. Discussion of Counselor Conference, September 9, 2016 – Lorinda Forrest
3. Breakout Sessions
    a. Track A: Deep Dive-Informal Roundtable Discussion on $200M Regional Planning
    b. Track B: Lean Canvas Model
4. Presentation on LaunchBoard 2.0 – Renah Wolzinger
5. Conference Adjournment

Standing Steering Committee Conference Calls

2nd Monday of the Month, 9:30am, as needed

- June 13
- July 11
- August 8
- September 12
- October 10
- November 14
- December 12
- January 9
- February 13
- March 13
- April 10
- May 8

CALIFORNIA COMMUNITY COLLEGES
Doing What MATTERS™
FOR JOBS AND ECONOMY

www.doingwhatmatters.cccco.edu

Upcoming CRC 2016-2017 Meetings

August 3, 2016; 9:00am-2:00pm
Clovis Community College, Herndon Campus

September 26, 2016; 4:00pm-8:00pm
Omni Ranch Las Palmas Hotel, Rancho Mirage
(Pre-CCCAOE)

November 17, 2016, 9:00am-2:00pm
Modesto Junior College

February 9, 2017, 9:00am-2:00pm
Columbia College, Sonora

Date TBD, 4:00pm-8:00pm
Pre-Spring CCCAOE

June 12-14, 2017
CRC Annual Planning Conference, Monterey

Additional Meetings

Date TBD
CVHEC Fall Board Meeting
CVHEC Spring Board Meeting

Pre-Regional Plan Meeting – CIO focus
SAVE THE DATE – JULY ~~26 &~~ 27, 2016
Clovis Community College, Herndon Campus

Central / Mother Lode Regional Consortium Planning Conference

Monterey, CA
June 6-8, 2016

CALIFORNIA COMMUNITY COLLEGES
Doing What MATTERS™
FOR JOBS AND THE ECONOMY

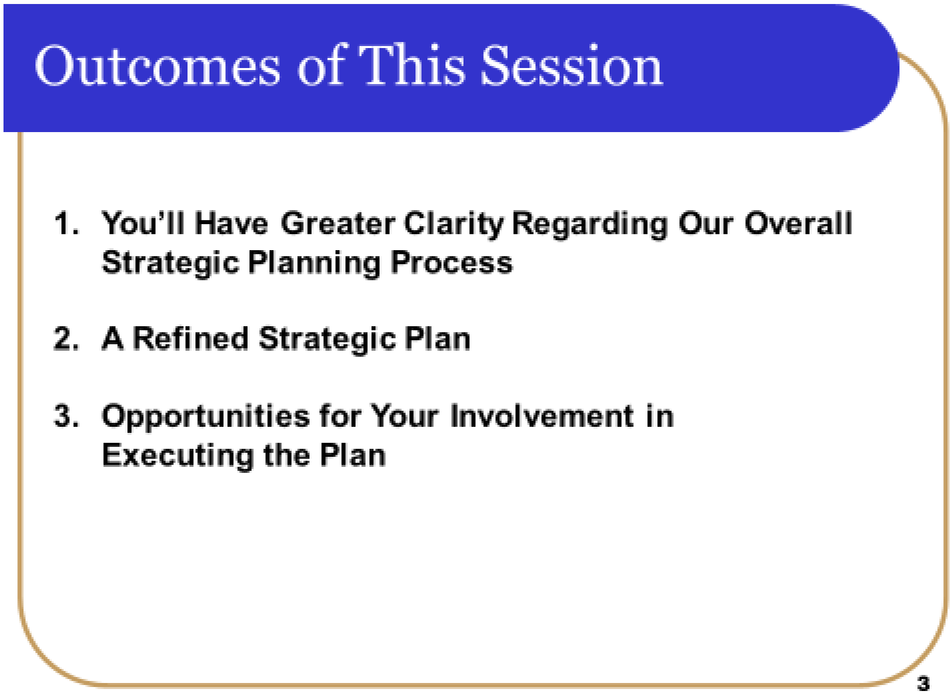
Getting Started

- Introductions
- 9:00- 12:00; Break at 10:15-10:30ish
- Agenda

  -- Debrief of What Has and Hasn't Been Working

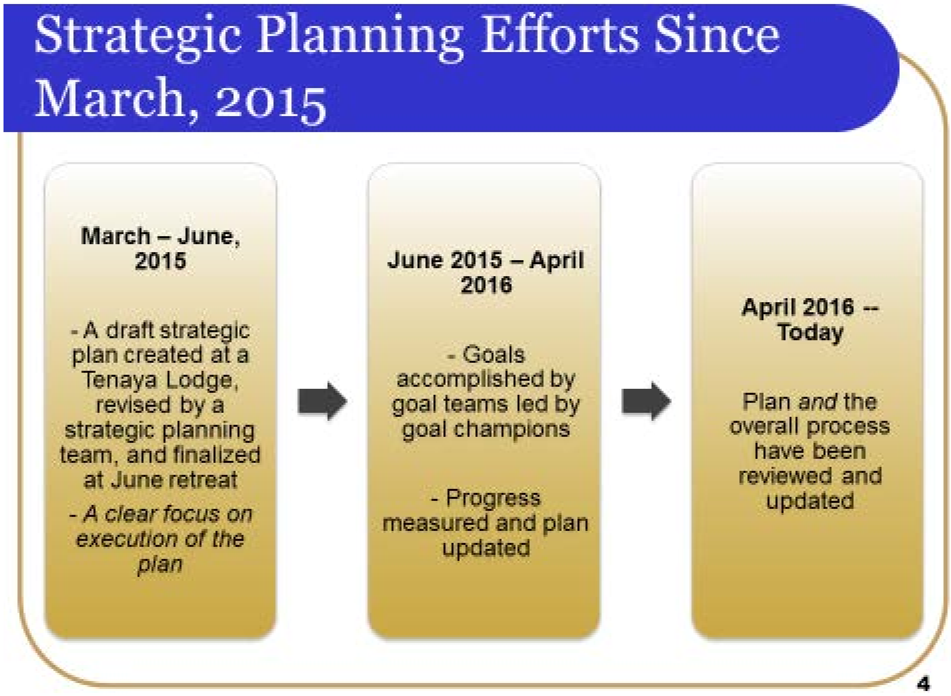
  -- Reporting Out of Progress from Last Year

  -- Review of Draft of Revised Plan
- Outcomes



Outcomes of This Session

1. **You'll Have Greater Clarity Regarding Our Overall Strategic Planning Process**
2. **A Refined Strategic Plan**
3. **Opportunities for Your Involvement in Executing the Plan**



Strategic Planning Efforts Since March, 2015

March – June, 2015

- A draft strategic plan created at a Tenaya Lodge, revised by a strategic planning team, and finalized at June retreat

- A clear focus on execution of the plan

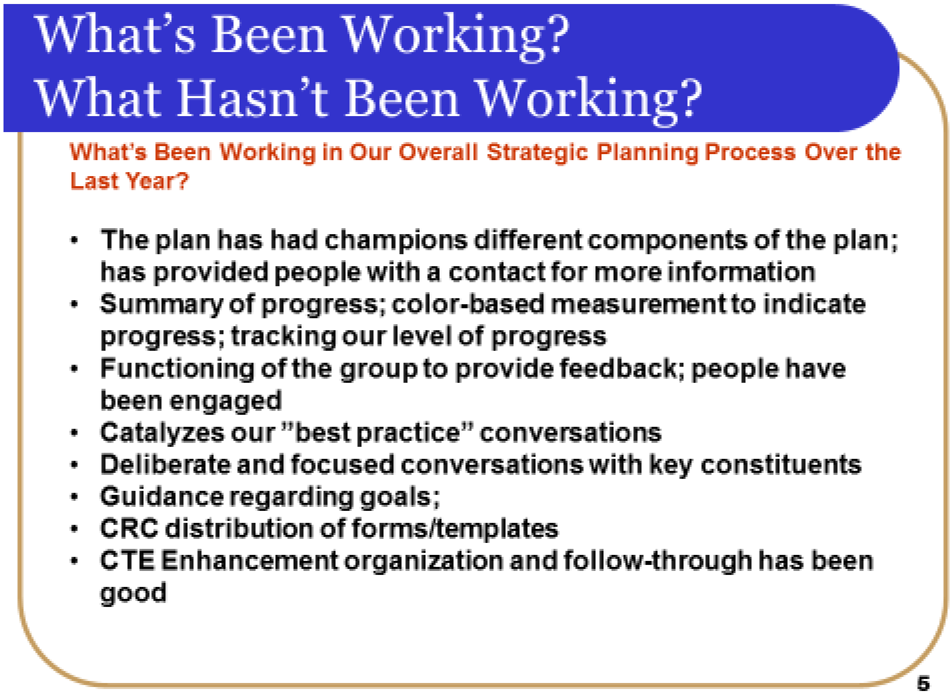
June 2015 – April 2016

- Goals accomplished by goal teams led by goal champions

- Progress measured and plan updated

April 2016 -- Today

Plan *and* the overall process have been reviewed and updated

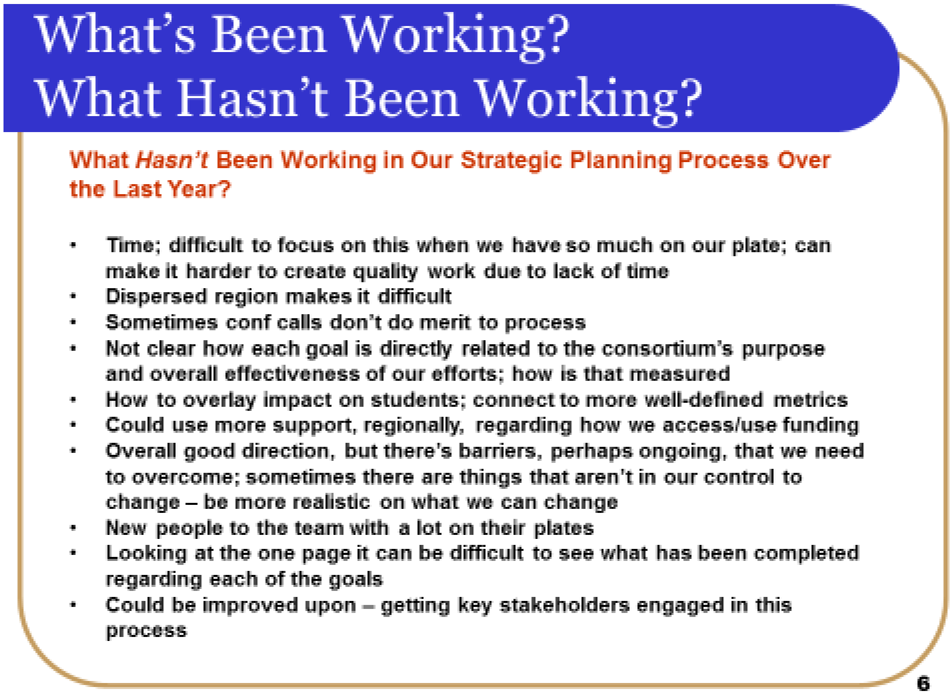


What's Been Working? What Hasn't Been Working?

What's Been Working in Our Overall Strategic Planning Process Over the Last Year?

- The plan has had champions different components of the plan; has provided people with a contact for more information
- Summary of progress; color-based measurement to indicate progress; tracking our level of progress
- Functioning of the group to provide feedback; people have been engaged
- Catalyzes our "best practice" conversations
- Deliberate and focused conversations with key constituents
- Guidance regarding goals;
- CRC distribution of forms/templates
- CTE Enhancement organization and follow-through has been good

5

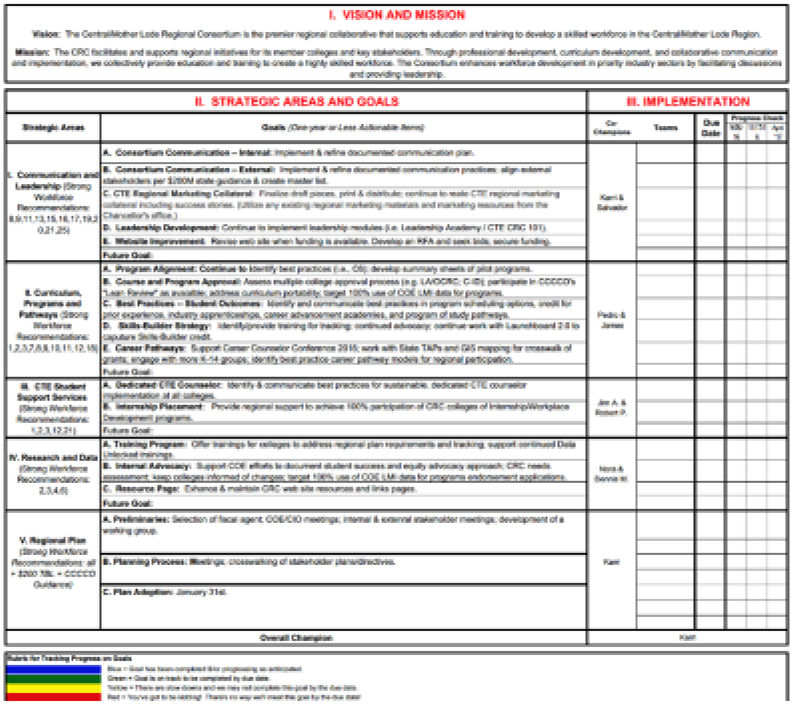


What's Been Working? What Hasn't Been Working?

What *Hasn't* Been Working in Our Strategic Planning Process Over the Last Year?

- Time; difficult to focus on this when we have so much on our plate; can make it harder to create quality work due to lack of time
- Dispersed region makes it difficult
- Sometimes conf calls don't do merit to process
- Not clear how each goal is directly related to the consortium's purpose and overall effectiveness of our efforts; how is that measured
- How to overlay impact on students; connect to more well-defined metrics
- Could use more support, regionally, regarding how we access/use funding
- Overall good direction, but there's barriers, perhaps ongoing, that we need to overcome; sometimes there are things that aren't in our control to change – be more realistic on what we can change
- New people to the team with a lot on their plates
- Looking at the one page it can be difficult to see what has been completed regarding each of the goals
- Could be improved upon – getting key stakeholders engaged in this process

6



I. VISION AND MISSION

Vision: The Central/Mother Lode Regional Consortium is the premier regional collaborative that supports education and training to develop a skilled workforce in the Central/Mother Lode Region.

Mission: The CRC facilitates and supports regional initiatives for its member colleges and key stakeholders. Through professional development, curriculum development, and collaborative communication and implementation, we collectively provide education and training to create a highly skilled workforce. The Consortium enhances workforce development in priority industry sectors by facilitating discussions and providing leadership.

II. STRATEGIC AREAS AND GOALS		III. IMPLEMENTATION					
					Progress Check		
Strategic Areas	**Goals** *(One year or Less Actionable Items)*	Co-Champions	Teams	Due Date	10/15	1/16	4/16
I. Communication and Leadership (Strong Workforce Recommendations: 8,9,11,13,15,16,17,19,20,21,25)	**A. Consortium Communication – Internal:** Implement & refine documented communication plan.	Karri & Salvador					
	B. Consortium Communication – External: Implement & refine documented communication practices; align external stakeholders per $200M state guidance & create master list.						
	C. CTE Regional Marketing Collateral: Finalize draft pieces, print & distribute; continue to scale CTE regional marketing collateral including success stories. (Utilize any existing regional marketing materials and marketing resources from the Chancellor's office.)						
	D. Leadership Development: Continue to implement leadership modules (i.e. Leadership Academy / CTE CRC 101).						
	E. Website Improvement: Revise web site when funding is available. Develop an RFA and seek bids; secure funding.						
	Future Goal:						
II. Curriculum, Programs and Pathways (Strong Workforce Recommendations: 1,2,3,7,8,9,10,11,12,18)	**A. Program Alignment:** Continue to identify best practices (i.e., C6); develop summary sheets of pilot programs.	Pedro & James					
	B. Course and Program Approval: Assess multiple college approval process (e.g. LA/OCRC; C-ID); participate in CCCCO's "Lean Review" as available; address curriculum portability; target 100% use of COE LMI data for programs.						
	C. Best Practices – Student Outcomes: Identify and communicate best practices in program scheduling options, credit for prior experience, industry apprenticeships, career advancement academies, and program of study pathways.						
	D. Skills-Builder Strategy: Identify/provide training for tracking; continued advocacy; continue work with LaunchBoard 2.0 to capture Skills-Builder credit.						
	E. Career Pathways: Support Career Counselor Conference 2016; work with State TAPs and GIS mapping for crosswalk of grants; engage with more K-14 groups; identify best practice career pathway models for regional participation.						
	Future Goal:						
III. CTE Student Support Services (Strong Workforce Recommendations: 1,2,3,12,21)	**A. Dedicated CTE Counselor:** Identify & communicate best practices for sustainable, dedicated CTE counselor implementation at all colleges.	Jim A. & Robert P.					
	B. Internship Placement: Provide regional support to achieve 100% participation of CRC colleges of Internship/Workplace Development programs.						
	Future Goal:						
IV. Research and Data (Strong Workforce Recommendations: 2,3,4,6)	**A. Training Program:** Offer trainings for colleges to address regional plan requirements and tracking; support continued Data Unlocked trainings.	Nora & Bonnie M.					
	B. Internal Advocacy: Support COE efforts to document student success and equity advocacy approach; CRC needs assessment; keep colleges informed of changes; target 100% use of COE LMI data for programs endorsement applications.						
	C. Resource Page: Enhance & maintain CRC web site resources and links pages.						
	Future Goal:						
V. Regional Plan (Strong Workforce Recommendations: all + $200 TBL + CCCCO Guidance)	**A. Preliminaries:** Selection of fiscal agent; COE/CIO meetings; internal & external stakeholder meetings; development of a working group.	Karri					
	B. Planning Process: Meetings; crosswalking of stakeholder plans/directives.						
	C. Plan Adoption: January 31st.						
Overall Champion		Karri					

Rubric for Tracking Progress on Goals

🟦	Blue = Goal has been completed &/or progressing as anticipated.
🟩	Green = Goal is on track to be completed by due date.
🟨	Yellow = There are slow downs and we may not complete this goal by the due date.
🟥	Red = You've got to be kidding! There's no way we'll meet this goal by the due date!

Vision and Mission

Vision: The Central/Mother Lode Regional Consortium is the premier regional collaborative that supports education and training to develop a skilled workforce in the Central/Mother Lode Region.

Mission: The CRC facilitates and supports regional initiatives for its member colleges and key stakeholders. Through professional development, curriculum development, and collaborative communication and implementation, we collectively provide education and training to create a highly skilled workforce. The Consortium enhances workforce development in priority industry sectors by facilitating discussions and providing leadership.

Five Strategic Areas

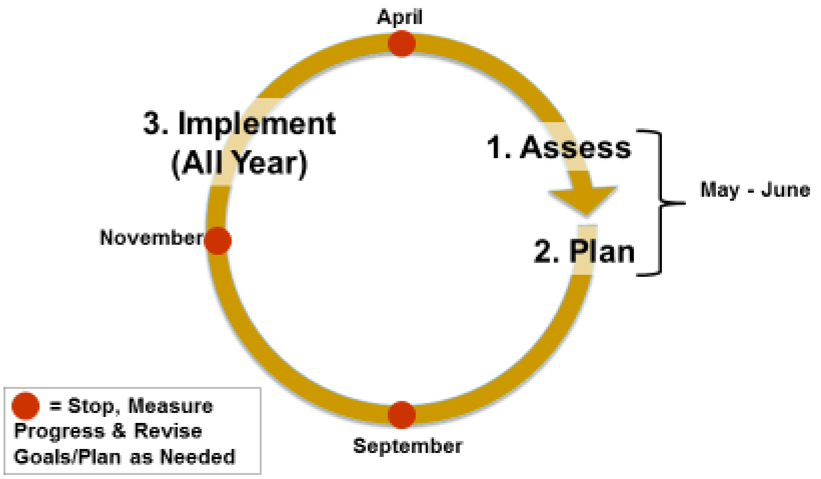
1. Communication and Leadership

2. Curriculum Program and Pathways
3. CTE Support Services
4. Research and Data

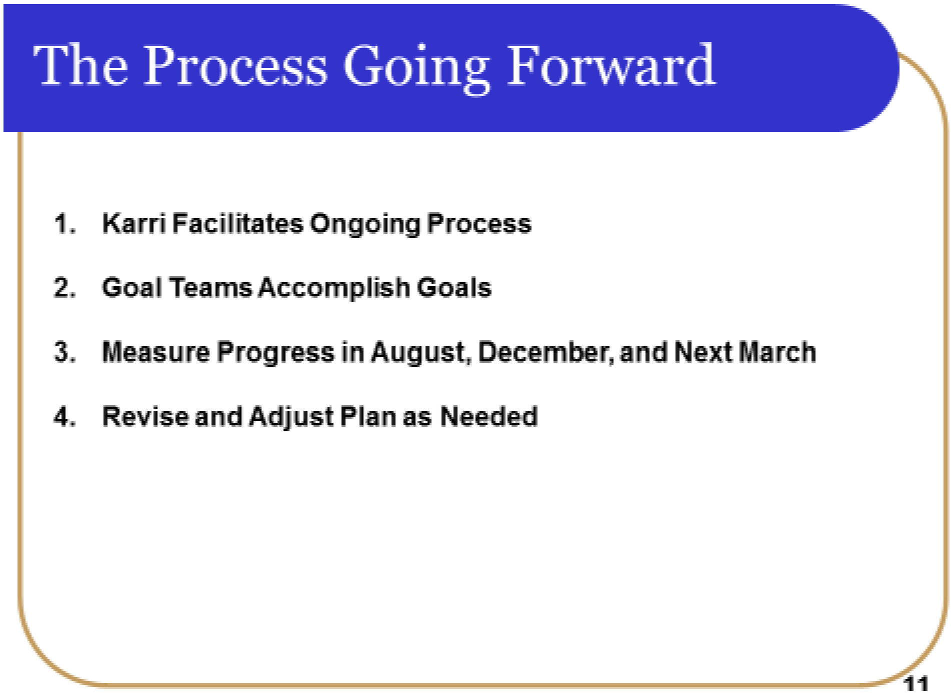
5. Regional Plan

9

The Consortium's Annual Three-phase Strategic Planning Cycle



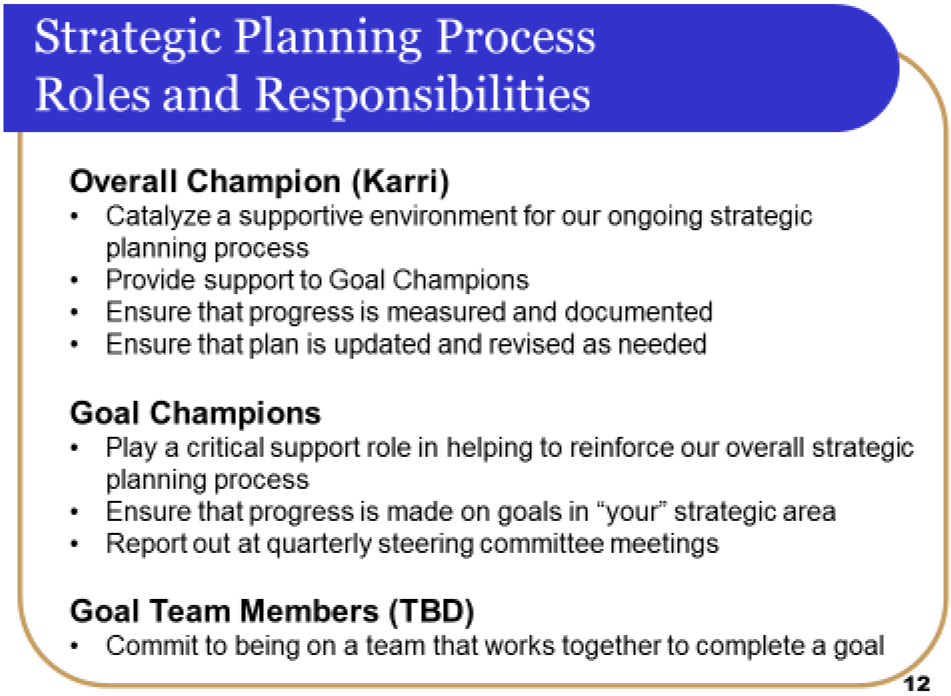
10



The Process Going Forward

1. **Karri Facilitates Ongoing Process**
2. **Goal Teams Accomplish Goals**
3. **Measure Progress in August, December, and Next March**
4. **Revise and Adjust Plan as Needed**

11



Strategic Planning Process Roles and Responsibilities

Overall Champion (Karri)

- Catalyze a supportive environment for our ongoing strategic planning process
- Provide support to Goal Champions
- Ensure that progress is measured and documented
- Ensure that plan is updated and revised as needed

Goal Champions

- Play a critical support role in helping to reinforce our overall strategic planning process
- Ensure that progress is made on goals in "your" strategic area
- Report out at quarterly steering committee meetings

Goal Team Members (TBD)

- Commit to being on a team that works together to complete a goal

12

Next Steps

1. **All:** If you haven't done so already, be sure to let Karri know if you have any input to the goals on the strategic plan.
2. **All:** If you haven't done so already, be sure to let one of the goal champions know if you'd like to engage in completing one of the goals on the strategic plan.
3. **Goal Champions, Eric, Karri:** ASAP, set up conference calls to review the goals within each respective strategic area.
4. **Karri (with input from others):** Clarify what key, practical projects can be a focus of the consortium this year, with the objective of sharing these throughout the network and deep into the colleges
5. **Karri:** Consider facilitating a more in-depth conversation with the regional steering committee (or a subset therein) regarding the overall strategic planning process, direction, strategies, etc.

13

Thank You!

CALIFORNIA COMMUNITY COLLEGES
Doing What MATTERS™
FOR JOBS AND THE ECONOMY

14

Annual Planning Conference Attendees				
1	Allyson	Adams	Admin. Aide	CRC
2	Jim	Andersen	Dean	MCCD
3	Bobby	Anderson	Dean	MCCD
4	Shelley	Attix	DSN	RHT
5	Sam	Aunai	Dean	Porterville
6	Diane	Baeza	Program Director	KCCD
7	Stephanie	Baltazar	Specialist	Bakersfield
8	Janet	Barbeiro	Assistant to VC	SCCCD
9	Colby	Barker	Adult Ed Coord.	CCOE
10	Jeanette	Benson	DSN	GTL
11	Patrick	Bettencourt	Dean	MJC
12	Dave	Bolt	VP	WHCCD
13	Sandra	Caldwell	President	Reedley
14	David	Clark	Dean	Reedley
15	Cindy	Collier	Dean	Bakersfield
16	Shelly	Conner	Dean	MCCD
17	Tony	Cordova	Director	Taft
18	Kris	Costa	Manager	TCOE
19	Clint	Cowden	Director	WHCCD
20	Walt	Di Mantova	Dean	CCCCO
21	Benjamin	Duran	Exec. Director	CVHEC
22	Lorinda	Forrest	DSN	Business
23	Autumn	Gardia	Director	MCCD
24	Leticia	Garza	Program Manager	KCCD
25	Sean	Glumace	TAP	
26	Araceli	Gonzalez	Counselor	MCCD
27	Jennifer	Hamilton	Dean	MJC
28	Karri	Hammerstrom	Regional Chair	CRC
29	Bob	Hawkes	TAP	K-14
30	Rozanne	Hernandez	Program Manager	Bakersfield
31	Barbara	Hioco	Vice Chancellor	SCCCD
32	Jacob	Jackson	Dean	FCC
33	Michael	Kane	Dean	Cerro Coso
34	Julie	Lynes	Counselor	FCC
35	JeanClaude	Mbomeda	CRC Grant Monitor	CCCCO
36	John	Means	Associate Chancellor	KCCD
37	Pedro	Mendez	Dean	MJC
38	Dennis	Mohle	DSN	ICT
39	Lori	Morton	Business Engagement	FCOE

40	Gillian	Murphy	Dean	SJDC
41	Audrey	Newsom		Workability
42	Robert	Pimentel	Dean	WHCCD
43	Martha	Robles	Dean	MJC
44	Thad	Russell	Dean	COS
45	Gurminder	Sangha	DSN	Adv. Manuf.
46	Nora	Seronello	TAP	Coe
47	Giselle	Simon	Pathway Director	WHCCD
48	Lorraine	Smith	Dean	FCC
49	David	Teasdale	TAP	Prop 39
50	Klaus	Tenbergen	Dean	Columbia
51	Brenda	Thames	VPI	MJC
52	Linda	Thomas	Dean	SCCCD
53	Garrett	Thomas	Program Manager	Porterville
54	James	Todd	VPSS	MJC
55	Kara	Tolbert	Manager	Cerro Coso
56	Salvador	Vargas	Dean	SJDC
57	Louann	Waldner	Provost	COS
58	Tim	Woods	Dean	FCC
59	Linda	Zorn	SN	