Final Data Report – Submitted by the Social Science Research Center at Old Dominion University to

The Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance (HRCyber)

July, 2017

Introduction

The Social Science Research Center (SSRC) at Old Dominion University collaborated with the Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance (HRCyber) to provide data collection and evaluation support to the project. The SSRC conducted focus groups with business and education representatives and used that feedback to develop surveys for businesses and educational partners to assess the workforce needs of cybersecurity companies in Hampton Roads. Finally, the SSRC met with small groups of the educational partners to discuss the placement rate of cyber students into the workforce and other related issues. The information from those data collection efforts are presented in this final report.

Focus Groups

Focus groups were conducted with interested individuals who were attending the Virginia Beach Cyber Convention and Expo on October 6th, 2016 and the Cyber Threat Conference held at Thomas Nelson Community College on October 7th, 2016. Approximately 15-20 people attended each session. Focus group participants represented a variety of perspectives including local government, smaller and larger cyber companies, college students, the shipyard, Department of Defense, and higher education. The basic summaries for each question asked can be found in the Appendix. Below is a general summary of the more substantive questions.

Recruitment Efforts

Participants were asked how their company typically recruits cybersecurity professionals. The responses seemed to favor direct interpersonal contact with potential candidates or through personal networks. Common responses included: recruiters, college fairs, internship programs, veteran sources such as transition assistance program (TAP) classes for the military, direct referrals, and networking within personal networks. Other “traditional” methods such as job boards or classified postings were deemed by some as not very helpful.

Priority Skills/Knowledge Areas

Participants were asked to identify their top three priority skills/knowledge areas when hiring and/or training cybersecurity employees. The answers were varied and included the more technical skills necessary for positions in the cyber field such as prior programming experience, experience with vulnerability assessment, risk management, network detection and analysis, and penetration testing. However, other more basic skills were also mentioned including the need for lifelong learners who are passionate about cybersecurity, technical/proposal writing skills, soft skills/communication skills and customer service skills, and a general knowledge of how IT relates to business goals/strategies. These responses indicate the diverse nature of the skills and knowledge that businesses are seeking in their cyber employees.

Difficulty in Finding Qualified Applicants

Focus group participants were asked how difficult it was to find applicants with the skills and knowledge that they mentioned previously. The general consensus was that it is difficult for a variety of reasons. Some of the non-DOD participants shared that conventional recruitment methods do not always work and they have to rely on personal networks to hire. Others reported seeing "paper tigers" – these are applicants who appear to have the necessary qualifications/certifications but they cannot actually perform the specific job tasks and requirements.

Participants from local municipalities reported not being able to compete with salaries offered by private firms or DOD. This results in local governments becoming a training ground with high turnover. Those from DOD reported needing people with security clearances. The "perfect candidates" would have a 4-year degree, but also the hands-on skills, the certifications and the clearances. Finally, many participants agreed that many applicants with the necessary technical/cyber skills do not have good communication skills.

Educational Programs and Preparing the Cyber Workforce

Participants were asked how well the local educational programs were meeting their needs for a prepared cyber workforce. They were also encouraged to share what else they would like local educational institutions to know about their workforce needs. The need for training in specific areas included:

- Risk management
- Vulnerabilities in programming
- Penetration testing
- Certifications
- Understanding the software development cycle

Participants also shared the need for different mixture of skills or knowledge. Applicants are needed who can do more than one thing – particularly for employers that cannot pay for large IT departments or for specialists in every area. Many are looking for "geeks" or hackers but not necessarily needing those who are formally educated. Some participants pointed out that there are courses for which no one at the college/university is qualified to teach. Another mention was that coders need to also understand hardware.

For DOD, their needs are driven by the requirements in the contracts and so it would be helpful it educational partners were familiar with some of those general requirements. Other basic or soft skills were mentioned including: being able to facilitate communication between the board, IT department and programmers and how to work as a team.

Other specific recommendations for educational programs included: starting training/introducing skills at the public school level to get students interested early,

hosting/organizing hacking conferences or hack-a-thons, giving credit for internships, putting cyber into the general IT curriculum, including security in all CS programs. Finally, some participants mentioned the importance of the NIST framework and student access to security clearances.

Business and Educational Partner Web Surveys

The feedback from the focus groups was used to inform questions and response options for web-based surveys of business representatives and educational partners. The information from the surveys will help develop educational pathways from the public schools through community colleges, four-year institutions and continual professional development that will provide a capable and fully trained cybersecurity workforce for Hampton Roads. The survey was disseminated to over 200 business contacts asking about the cybersecurity workforce and their recruitment and hiring needs. Businesses were also encouraged to share the survey link with other business contacts who rely on the cybersecurity workforce. The educational survey was sent to 35 educational contacts in Hampton Roads.

Business Survey Summary

Email invitations to complete a survey of cyber workforce hiring needs were sent to business contacts in November, 2016. By February 20, 2017 a total of 34 business representatives completed the survey. The Appendix includes tables and charts for the survey results. This section will summarize some of the survey highlights.

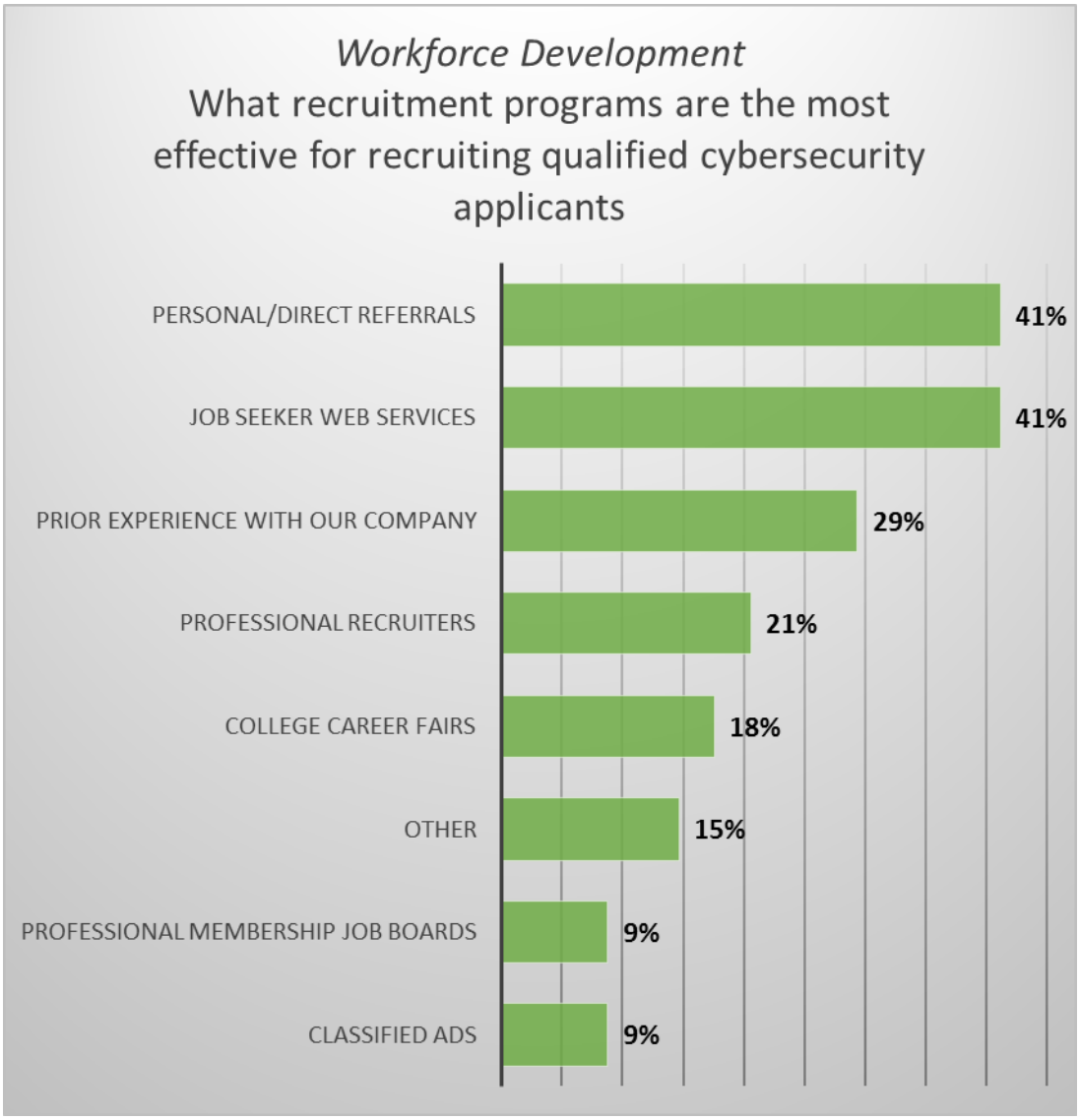
The respondents to the business survey represented private/for-profit companies (64.7%), federal, state, and municipal government (26.5%), and not-for-profit organizations (8.8%). The business respondents came from various industries including cybersecurity, education, insurance and local government. Respondents held primary positions such as cybersecurity manager/administrator (23.5%), CEO/CFO (11.8%) and IT manager/administrator (8.8%).

Type of Agency	Percentage
Private/For-profit	64.7%
Federal/state/municipal government	26.5%
Not-for-profit	8.8%

Industry Category	Percentage
Other	26.5%
Cybersecurity (Hardware/Software/Services)	17.6%
Local Government	8.8%
Government Contractor	8.8%
Department of Defense	8.8%
Education	8.8%
Insurance	5.9%
Information Technology	5.9%
Healthcare	2.9%
Finance/Banking	2.9%
Consulting	2.9%

Primary Position/Title in Company/Organization	Percentage
Other*	52.9%
Cybersecurity Manager/Administrator	23.5%
CEO/CFO	11.8%
IT Manager/Administrator	8.8%
Human Resources/HR Manager	2.9%

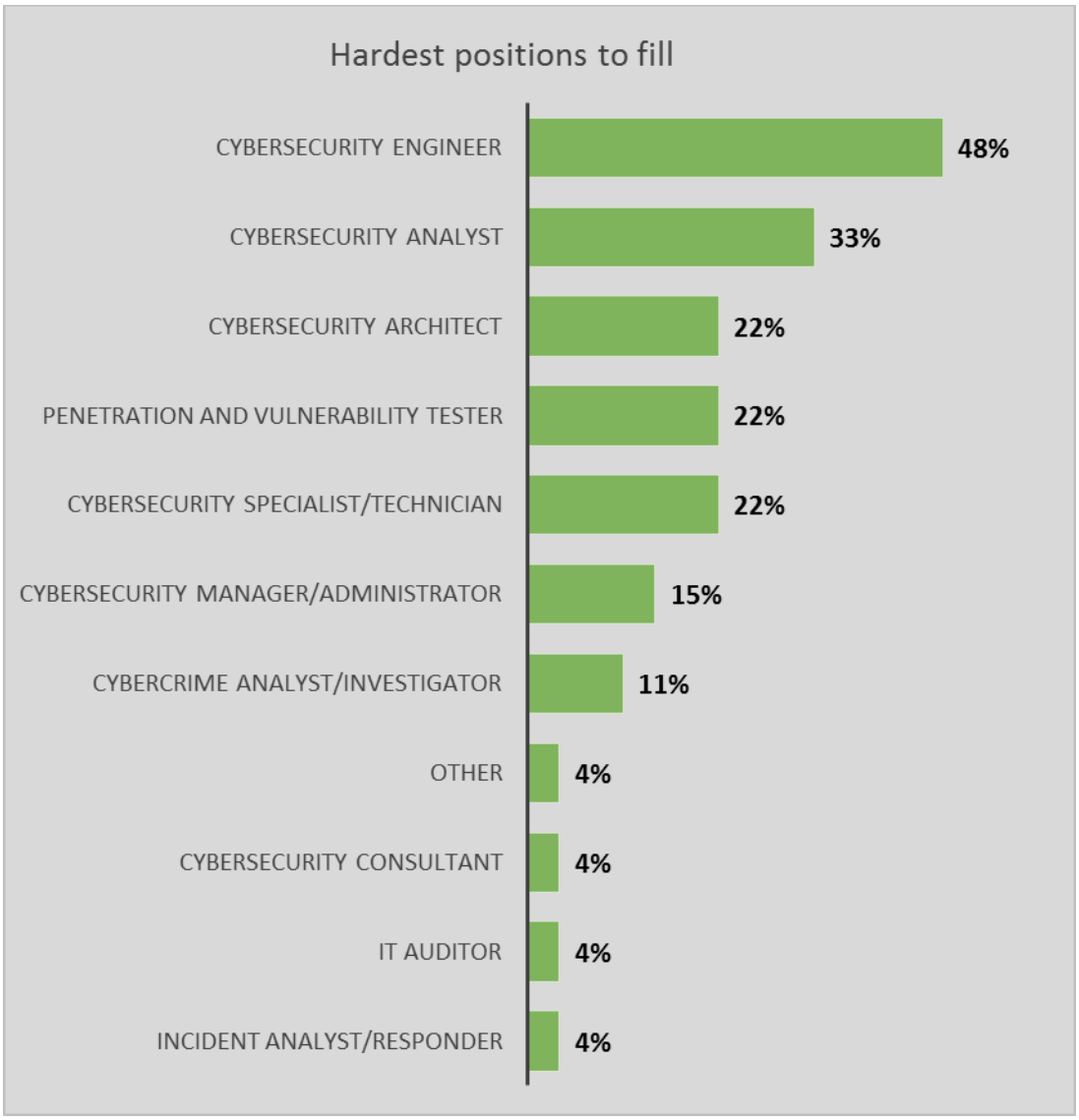
Regarding recruitment methods, the survey results support what was found in the focus groups. Personal/direct referrals are among the most effective as reported by 41% of business representatives while more traditional methods such as classified ads were not a top effective method.



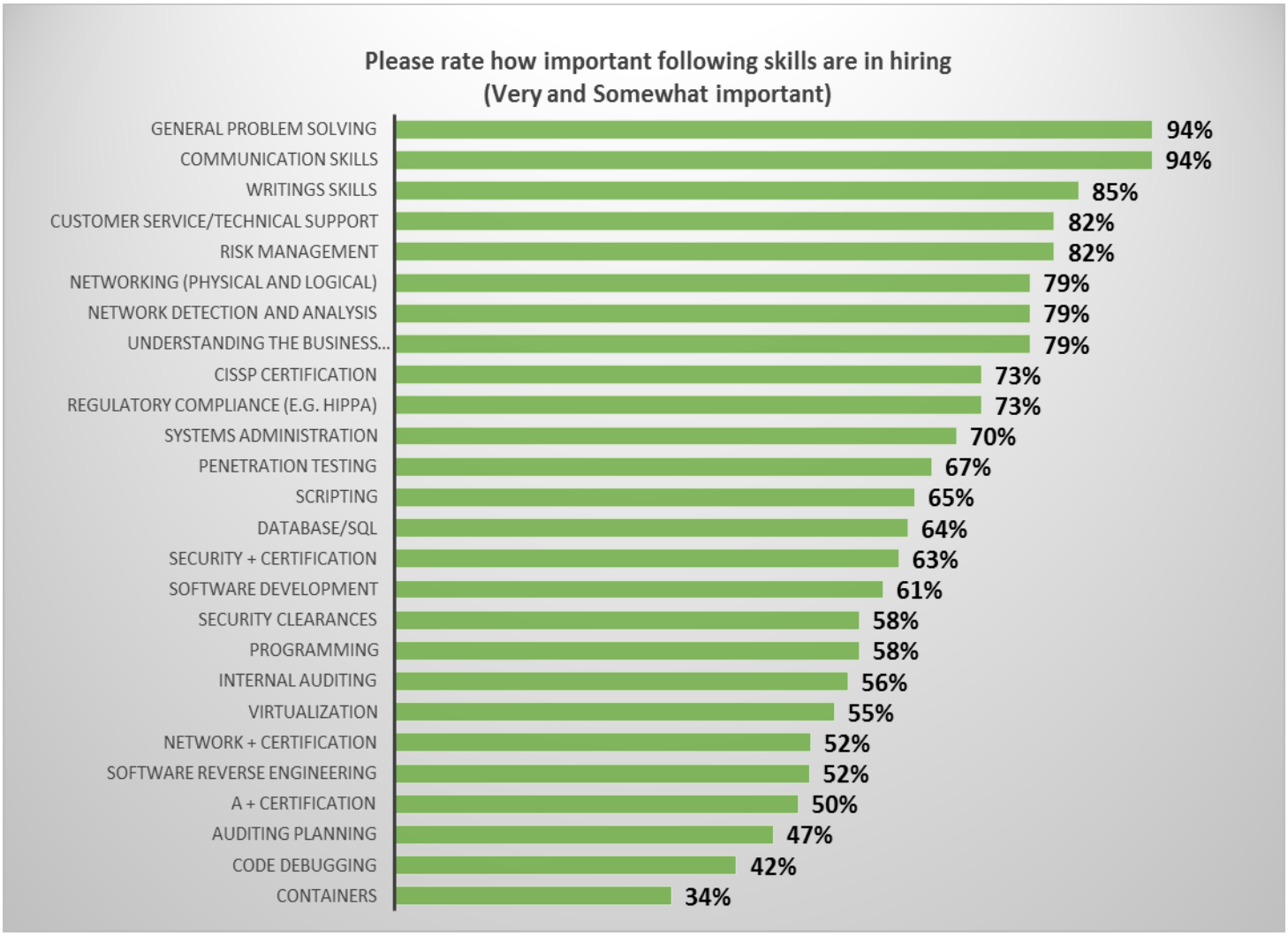
The 34 business representatives shared information on the number of current vacancies in their company for specific positions. Below are the total number of current vacancies reported for each position type. Cybersecurity analysts, engineers and consultants seem to be the most commonly reported vacancies for the responding businesses.

Position	Total Current Vacancies
Cybersecurity Analyst	**27**
Cybersecurity Engineer	**22**
Cybersecurity Consultant	**21**
Cybersecurity Specialist/Technician	**16**
Cybersecurity Architect	**15**
Incident Analyst/Responder	**15**
Cybersecurity Manager/Administrator	**12**
Penetration and Vulnerability Tester	**11**
Cybercrime Analyst/Investigator	**6**
IT Auditor	**5**

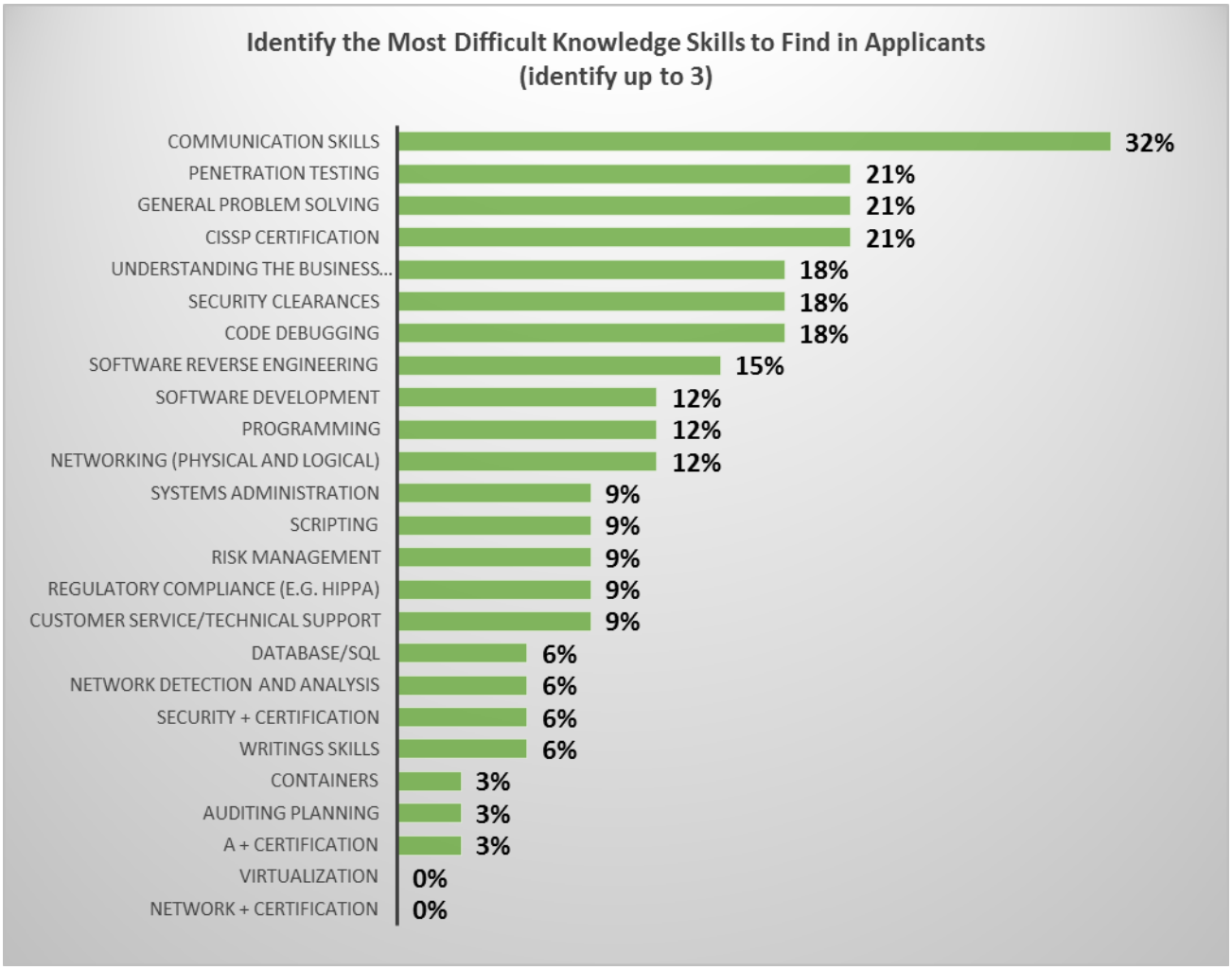
The information on vacancies is generally consistent with the feedback from business representatives about the hardest positions to fill. Cybersecurity analyst (33%) and engineer (48%) ranked among the most commonly mentioned as hard to fill. More than one in five business respondents (22%) also mentioned cybersecurity architect, penetration and vulnerability tester and cybersecurity specialist and technician as among the hard to fill positions. IT auditor (4%) and incident analyst/responder (4%) were selected by a lower percentage of businesses as hard to fill. Cybersecurity consultant was also not frequently selected as difficult to fill yet it was third-highest in terms of number of current vacancies.



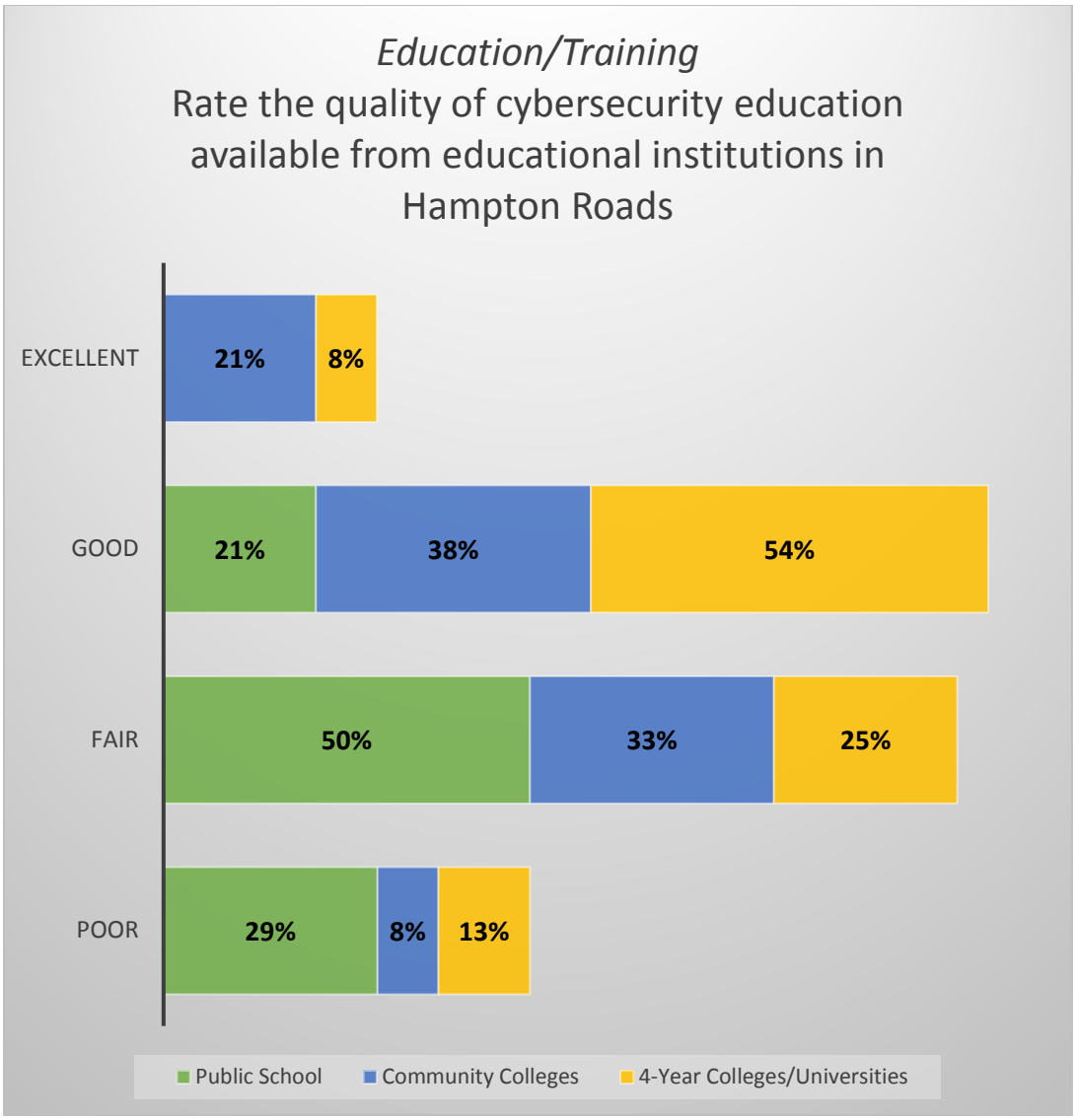
Business representatives were asked to rate the importance of certain skills and knowledge. The survey results were fairly consistent with the focus groups results in the variety of skills and their importance ratings. Risk management (82%), networking (79%) and network detection and analysis (79%) were among the technical skills most often selected as at least somewhat important. However, general problem solving (94%), communication skills (94%), and writing skills (85%) were among the more basic skills that were rated as important – in higher percentage than the more technical skills.



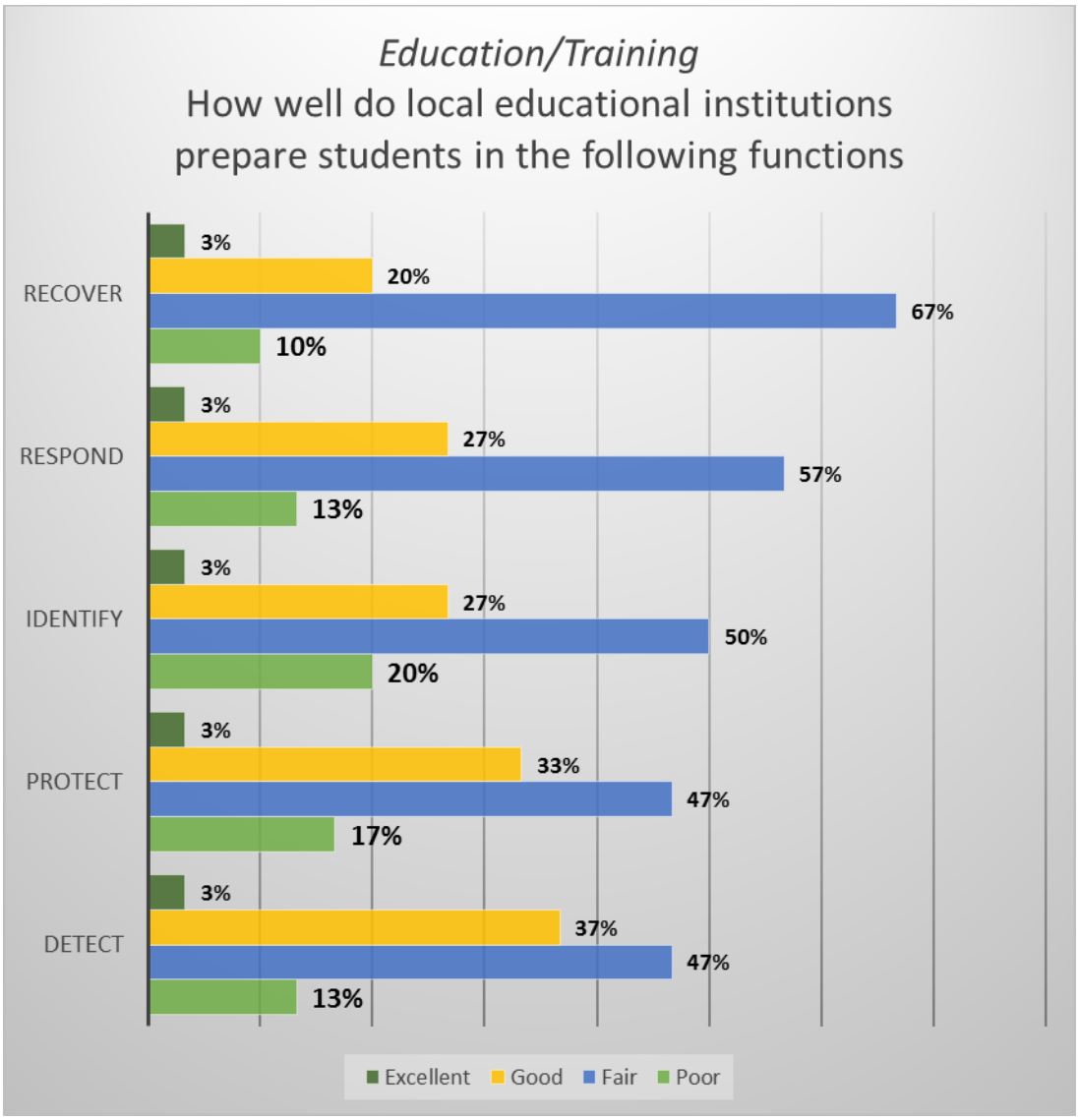
Businesses were also asked to identify the most difficult knowledge skills to find in applicants. Once again, some of the more basic skills were mentioned as often (if not more) than the technical skills including communication skills (32%), general problem solving (21%), and understanding the business environment (18%). Penetration testing (21%), CISSP certification (21%), and security clearances were selected among the most difficult skills to find – which is consistent with the focus group results.



Businesses were asked to rate the quality of cybersecurity education available from the educational institutions in Hampton Roads. Public schools received no “excellent” ratings while 21% of businesses described the education from community colleges as excellent. Only 8% describing local four-year colleges and universities as excellent. More than half of business representatives (54%) described the quality of education from colleges/universities as good, compared to 38% rating community colleges and 21% rating local public schools as good. Public schools received the highest percentage of businesses rating them as “poor” at 29% compared to 8% for community colleges and 13% of four-year colleges/universities.



Business representatives were asked how well local educational institutions prepared students in various categories based on the NIST framework. The majority of businesses responded "fair" to most categories with two-thirds (67%) responding fair to the recovery category (maintaining plans for resilience and restoring capabilities/services that were impaired due to a cybersecurity event). More than half (57%) responded fair to the respond category (developing/implementing the appropriate activities to take action for a detected cybersecurity event). The largest percentage of "poor" ratings were for identify (20%) (developing organization understanding to manage cybersecurity risk to systems, assets, data, and capabilities) and protect (17%) (develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services). Only 3% of businesses rated educational institutions as excellent in any of the NIST categories.



Business representatives were also asked to rate how prepared new hires are in a series of workplace competencies. The table below shows the bottom 5 areas and the top 5 areas. Over half of businesses (53%) indicated that new hires are not well prepared in overseeing and governing cybersecurity work or in business fundamentals. More than 40% indicated that new hires are not well prepared in problem solving and decision making, risk management and investigating threats. These areas were among those mentioned as most important and/or as difficult to find in new applicants earlier in the survey.

Those areas that were more likely to be rated as somewhat or very prepared included: working with tools and technology, teamwork, planning and organizing, security provision system and cybersecurity technology. This includes some of the non-technical skills that have previously been identified as important.

Competency Area	% Not Well or Not at All Prepared
Oversee and Govern Cybersecurity Work	**53%**
Business Fundamentals	**53%**
Problem Solving and Decision Making	**44%**
Risk Management	**44%**
Investigating Threats	**43%**
Competency Area	**% Somewhat or Very Prepared**
Working with Tools and Technology	**82%**
Teamwork	**79%**
Planning and Organizing	**76%**
Security Provision System	**73%**
Cybersecurity Technology	**71%**

Business representatives were asked to identify gaps in the educational preparation of the cyber workforce as well as provide comments on the specific actions that local educational institutions can take to better prepare the cyber workforce. Below are some examples of some of the comments. These examples reflect trends in the survey data in terms of the needed skills and the need for skills beyond the technical skills as well as the work being done by the HRCyber workgroup (e.g., developing the DACUM to inform the pathways for cyber education).

- Creative thinking skills are lacking. We can teach technology...we can't teach deductive reasoning.
- Cybersecurity is a very hands-on industry in addition to theory and concepts. Many education programs have good curriculum for teaching students theories and concepts like cryptography, network security, CIA concepts, etc. But the hands-on labs are not sufficient, like attack and defense. However, in real world operations, those hands-on experience is profoundly important.
- Students are not taught how things work and how to problem solve today. They are generally rushed through a very basic curriculum.
- It is not a continuum. We need to start at K-12 and go from there. We must drive interest, not just expertise.

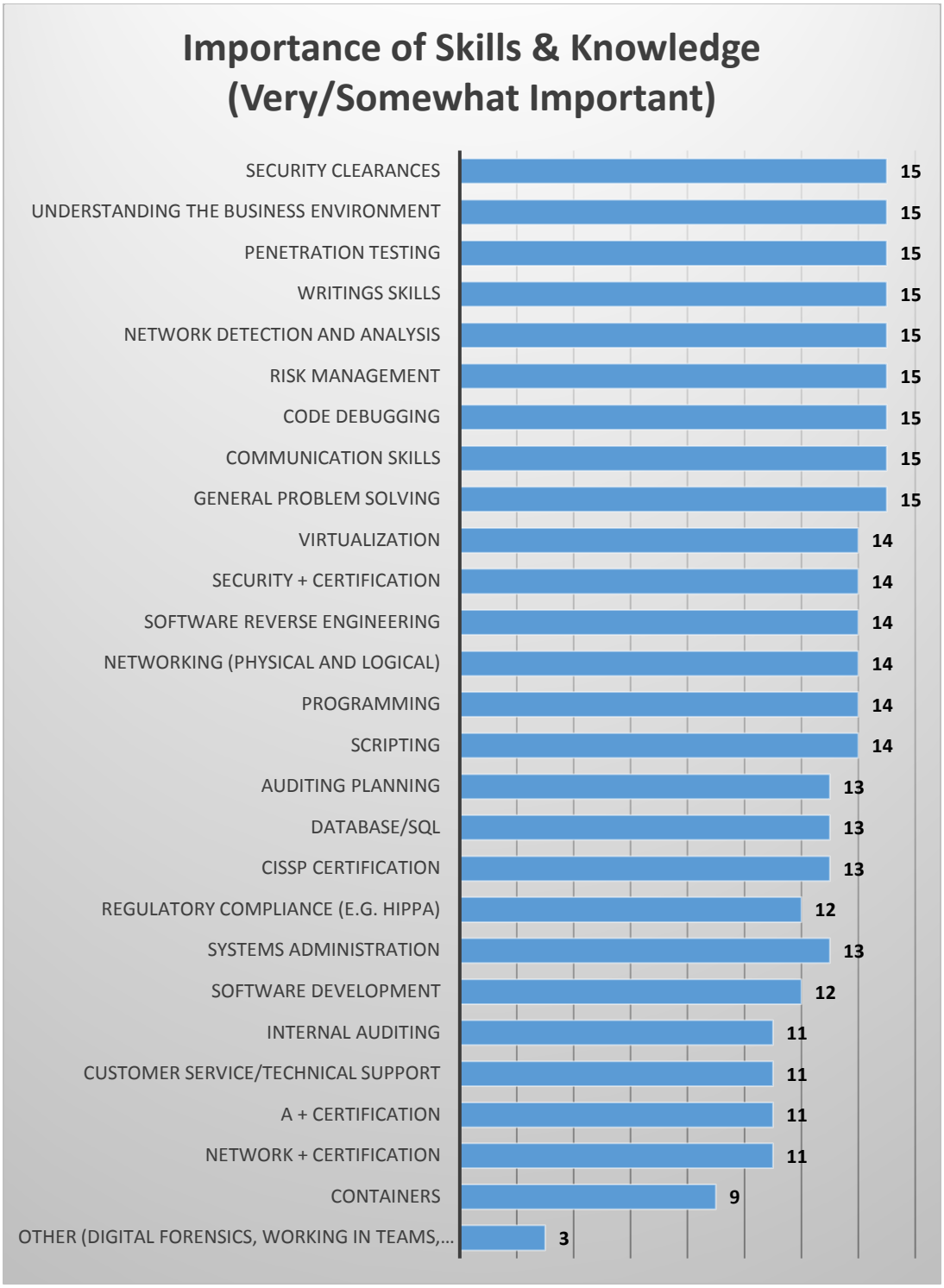
- The workforce is getting trained on what we know and the battlefield is evolving so fast that by the time they get here the skills have changed. Must be adaptive.
- Combine the humanities with technological curricula.
- Educational institutions can work together to create an educational process or path that will work towards developing a cybersecurity professional from entry level to senior manager/leader.
- We need to create large scale platform and large number of practical hands-on labs to strengthen the knowledge of students obtained from lectures.
- Work needs to be done to promote critical thinking and problem solving skills.

Educational Partners Survey Summary

Email invitations to complete a survey about cyber education and the cyber workforce in Hampton Roads were sent to 35 educational contacts in February, 2017. A total of (15) partners completed the survey. Given the sample size, the results below are provided using the number of respondents versus percentages. The respondents represented four year colleges and universities (n=7), community colleges (n=4) and public schools (n=2).

Type of Agency	n
Four year college or university	7
Community College	4
Public school (K-12)	2
Other	2

Educational partners were asked to rate the importance of various skills and knowledge areas for students entering the cybersecurity workforce. Security clearances, understanding the business environment, penetration testing, writing skills, network detection and analysis, risk management, code debugging, communication skills, and problem solving were rated as either somewhat or very important by all responding educational partners (n=15). General problem solving, scripting, communication skills and physical/logical networking were rated as very important by two-thirds or more of the responding educational partners (10 or more). General problem solving, communication skills plus risk management and writing skills were among the areas that were also most highly rated by the business representatives. The educational partners did not rate customer service/technical support as important as the business representatives (only 3 rated it as very important). Both the business representatives and the educational partners ranked auditing and planning and containers as less important than most of the other skills.

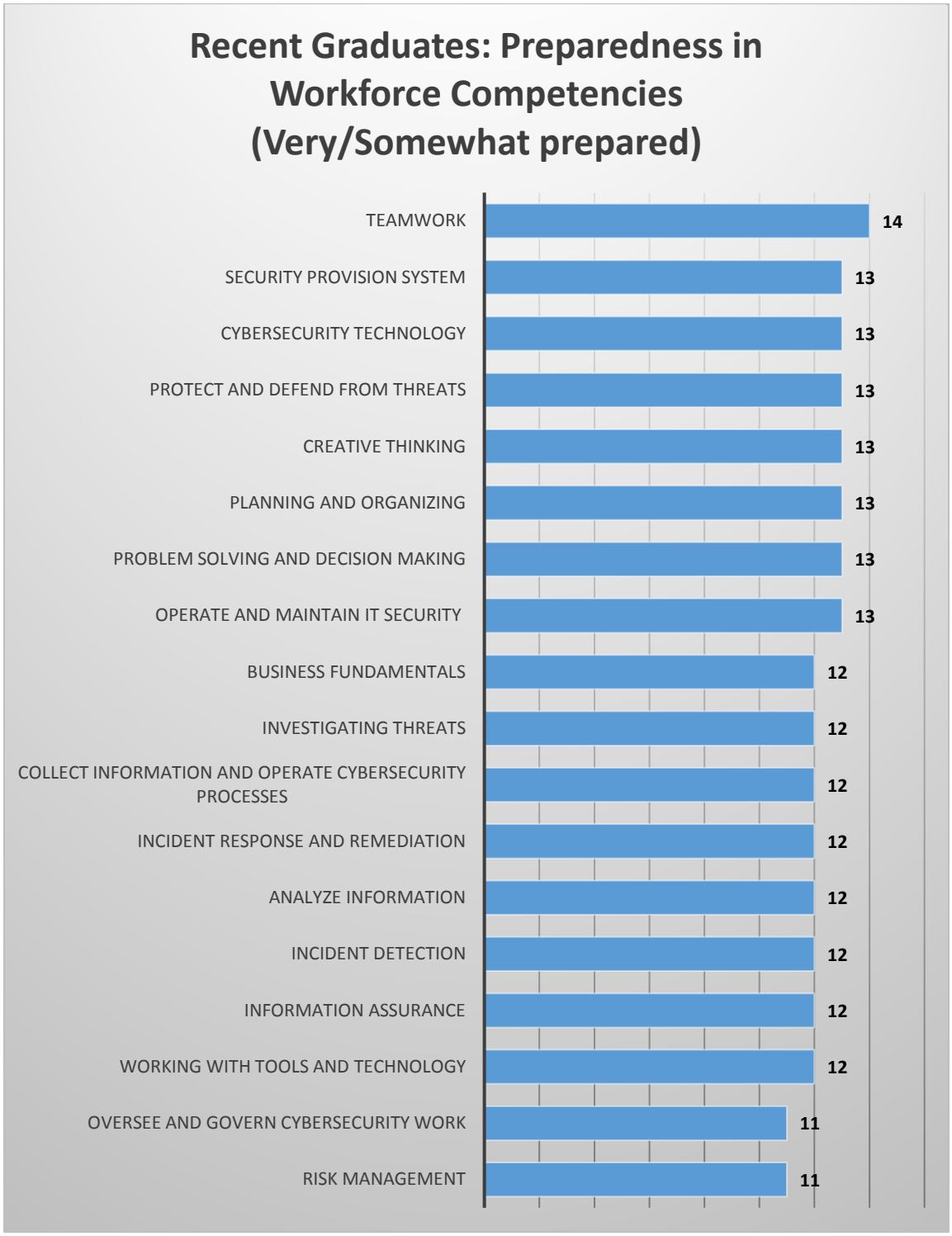


The educational partners were also asked about the most difficult skills to find qualified instructors to teach. They rated software reverse engineering, security clearances, penetration testing and Security + certification as the most difficult. This is somewhat encouraging as there is not a lot of overlap between these difficult skills to find in

instructors and the skills that employers have the most difficulty finding in applicants (communication skills, penetration testing, general problem solving, and CISSP certification). This suggests that the educational partners should be well-equipped to teach the skills that employers have difficulty finding in applicants (with perhaps the exception of penetration testing).

The educational partners were also asked to indicate how well prepared recent cybersecurity graduates are in a variety of workplace competencies. The majority of educational partners indicated that recent graduates were at least somewhat prepared in all of the workplace competencies. Teamwork (n=14) was rated most highly in terms of preparedness followed by security provision system, cybersecurity technology, protecting and defending from threats and creative thinking (n=13). Teamwork (79%) and creative thinking (68%) were also rated highly by employers. However, while 73% (11 out of 15) educational partners rated recent graduates as at least somewhat

prepared in all of the workplace competencies), the percentage of business representative ranking as at least somewhat prepared was lower for many of the competencies (e.g., 47% for business fundamentals, 59% for incident response and remediation, 57% for investigating threats).



When asked about the quality of cybersecurity education that is available from the local educational institutions, the educational partners rated the quality of education higher than did the business representatives. The largest discrepancy in quality ratings was for community colleges where 80% (n=12) of educational partners rated the quality as excellent or good compared to 58% of business representatives. Only 63% of business representatives rated the quality of education from four-year colleges/universities as excellent or good compared to 73% of educational partners. Only 40% of educational partners and 21% of businesses rated the local public schools as good or excellent.

Quality Rating of Cybersecurity Education that is available from…	Excellent/Good Educational Partners (n/%)	Excellent/Good Businesses (%)
Public schools	**6/40%**	**21%**
Community Colleges	**12/80%**	**58%**
4-Year Colleges/Universities	**11/73%**	**63%**

Educational partners were asked to identify gaps in the educational preparation in the current cybersecurity workforce. Below is a summary of some of the comments. Some of the comments reflect the need for certain skills as identified by businesses and educational partners. Other comments reflected the need or lack of qualified instructors while others focused on specific educational/curricular needs or focus areas.

- Ongoing training in technology and communication skills needed
- Tough to grow programs without qualified educators
- More time spent working with cybersecurity tools hands-on versus memorizing
- Most education programs focus on STEM aspects and less attention given to multidisciplinary factors such as cyber laws, criminal justice, ethics, etc.
- Computational thinking – thinking as computers and hackers
- DOE is creating courses for different clusters instead of creating courses as a system and this is problematic
- Forward thinking to plan a doctoral program for the future

The educational partners were also asked what local educational institutions can do to better prepare the cybersecurity workforce. Many of the recommendations reflect the activities of the HRCyber workgroup including coming together to determine courses from public school to college, establishing a virtual lab, and strengthening partnerships with industry and government to offer internship opportunities. Below is a summary of some of the comments:

- Ensure students who want positions supporting the Federal government or DOD have the necessary certifications

- Integrate more multidisciplinary factors into cybersecurity programs
- Provide interdisciplinary courses
- Establish and deepen relationships with local industry partners and ask for input when developing programs
- Start early in K-12 to teach programmatic logic and thinking. Identify those with aptitude and/or passion
- Come together as a group and outline courses from K1 through college
- Hands-on virtual labs
- Strengthen partnerships with local business, industry, military and government to offer internship opportunities to cybersecurity students.

Placement Rate and Time to Place for Cyber Students

The SSRC met with small groups of educational representatives to discuss the placement rate of students into the workforce and related issues. Representatives from ODU, the community college system, a for-profit institution, and a local public school division participated. The questions focused on the experiences of students after they graduate (e.g., if they continue their education or enter the job market as well as the challenges they face).

The general consensus among the participants is that the various educational institutions need to develop better systems and methods for tracking students post-graduation. Feedback from the participating public school, which conducts a survey one year after graduation, indicates that nearly all cyber students go on to either a two-year or four-year institution and many are working part-time as well. Any other information is often collected anecdotally from teachers who have kept in contact with individual students after graduation. There were other examples of a few students being hired right out of high school for some cybersecurity jobs or taking advantage of the dual enrollment programs to go right into a two-year or four-year cyber program.

The community college system is just starting to implement a tracking system that will track a student's progress from the admissions process through graduation and even post-graduation. Assigning the various specializations, like cyber, a specific program code will allow them to track the progress of students through the degree program. Word has also spread about the recent articulation agreement between ODU and Tidewater Community College and so students are coming in with intentions of going into cybersecurity. The articulation agreement "has been paramount" to the interest in cyber.

The for-profit institution indicated that 84% of Associate of Science and 86% of Bachelor of Science are placed in the field within six months. Many of their students (60%) are former military so their prior experience and security clearance makes them attractive to employers. Additionally, 70% of the associate students want to go on to a bachelor's program.

Old Dominion University's cyber degree programs are relatively new and have yet to produce graduates. The programs should produce their first graduates in the 2017-2018 academic year. Initial reports indicate that ODU students are finding placements for internships within the industry and that internships are now a required part of the cyber curriculum. Ideas for an exit survey for graduating students were discussed to try and track what students are doing after graduation and what companies are hiring them or if they are going on to graduate degrees.

Since the cyber degrees at ODU are concentrations within the interdisciplinary studies (IDS) program, official statistics such as those kept by SCHEV will not track for cyber, but instead for IDS. Further, there is the issue of students from related areas (e.g., Computer Sciences) getting jobs in cybersecurity but they may be missed because their degree is not directly cybersecurity. A suggestion was made to partner with the academic departments to try and track students since many will keep in contact with professors. One participant shared that institutions across the nation are struggling with trying to keep in contact and track students post-graduation but those who have been more successful have partnered with the individual departments.

Other barriers discussed by the educational partners included issues with employers wanting cyber employees to have or be eligible for security clearances. This creates problems for ODU's international students who are foreign nationals who are not able to get clearance. This prohibits those students from getting government cybersecurity jobs. Additionally, students' social media presence can discourage potential employers from hiring them if the content of their social media is questionable. Faculty and staff try to communicate with students about the importance of their social media presence in the future when looking for employment.

The community college system has encountered issues with Human Resource practices that can be overly restrictive for qualified applicants to find jobs. While the business community talks about needing critical thinkers, there are humanities students that have those skills and could be retrained, but from a Human Resources perspective, they would not be eligible given some of the other criteria in the job announcements. For example, the shipyards have issues with their hiring practices and have many IT jobs that are unfilled. While apprenticeships have been suggested as way to help fill some positions, the funding is not there to support such a program – at least at one local shipyard.

Summary

The data collected from business representatives and educational partners regarding the cybersecurity workforce in Hampton Roads revealed the need for applicants who are well-trained in a variety of skills – both technical and non-technical. The feedback from the focus groups and surveys showed the diverse nature of the skills and knowledge that businesses are seeking in their cyber employees. While prior programming experience, experience with vulnerability assessment, risk management, network detection and analysis, and penetration testing are important, so too are skills that allow employees to problem solve as well as write and communicate effectively with customers and other non-technical staff.

Perhaps reflecting the varied nature of desired skills, business representatives reported that personal and direct contact with applicants were among the most effective recruitment methods. These methods allow businesses to more closely ascertain the overall skill set of applicants. Many businesses indicated that new hires are not well prepared in overseeing and governing cybersecurity work, business fundamentals, problem solving/decision making, risk management, and investigating threats. These areas were among those mentioned as most important and/or as difficult to find in new applicants.

The educational partners provided feedback that was consistent with some of the business data, however, there were also some discrepancies in the perceived importance of certain skills as well as how prepared new applicants are for the workforce. Network detection and analysis, general problem solving, communication skills plus risk management and writing skills were among the areas that were rated as important by both the business representatives and the educational partners. However, the educational partners did not rate customer service/technical support as important as the business representatives (only 3 rated it as very important). Educational partners were also more likely to rate the quality of cybersecurity education that is available in Hampton Roads as excellent or good compared to the business representatives.

Recent graduates/applicants were rated as generally prepared in terms of teamwork and creative thinking. However, while the majority of educational partners rated recent graduates as at least somewhat prepared in all of the workplace competencies, the percentage of business representative ranking applicants as at least somewhat prepared was lower for many of the competencies (e.g., 47% for business fundamentals, 59% for incident response and remediation, 57% for investigating threats).

Both the educational partners and the business representatives shared comments that reflect the need for a better-prepared workforce in a variety of skill areas as well as the need for collaboration between education, business, the military, and other industries to identify the best pathway for future cyber workers. The educational partners agree that

better systems or processes for tracking students post-graduation are necessary to assess the flow of students into cybersecurity careers as well as college programs. Recommendations for internships, virtual labs, and collaborative curriculum development are all activities that have been undertaken by the HRCyber workgroup. Continued collaboration amongst the various educational representatives as well as the business community is encouraged to ensure that the educational offerings remain relevant for the changing demands within cybersecurity.

Focus groups summary

Focus groups were conducted with interested individuals who were attending the Virginia Beach Cyber Convention and Expo on October 6th, 2016 and the Cyber Threat Conference held at Thomas Nelson Community College on October 7th, 2016. Approximately 15-20 people attended each session. Focus group participants represented a variety of perspectives including local government, smaller and larger cyber companies, college students, the shipyard, Department of Defense, and higher education.

What types of cybersecurity positions does your company employ?

Network engineers

Software engineers

Hardware engineers

System engineers

Security engineers

Intrusion and forensic departments

Where does your company typically recruit cybersecurity professionals?

Recruiters

Professors recruiting in classrooms would help

College fairs

Intern programs

Veteran sources – TAP classes

Direct referrals

Networking/personal networks

Job boards were deemed by some not to helpful

If you had to choose the top three priority skills/knowledge areas when hiring and/or training cybersecurity employees, what would they be?

Prior programming

Engineering background

Security +

Lifelong learners – need to be passionate about cybersecurity

Vulnerability assessment

Risk management

Network detection & analysis

Industrial control networks

Accounting/technical finance skills

Technical/proposal writing skills

Soft skills/communication skills/customer service skills

Compliance

Deep packet inspection

Critical factors of cybersecurity

Security clearances

Security for the operational person

How IT relates to business goals/strategies – what is the impact on business?

Penetration testers/penetration testing

Systems architecture

Legacy + cutting edge knowledge

Certifications + classroom knowledge

Foreign nationals/foreign language skills – for work in foreign countries to build trust

How easy/difficult is it to find qualified applicants with these skills?

General consensus is that it is hard – conventional recruitment methods don't necessarily work and rely on personal networks to hire (at least for non-DOD businesses)

See "paper tigers" – appear to have the necessary qualifications/certifications but they can't "sit down and do the thing" that needs to be done – perhaps need proficiency testing

Municipalities cannot afford to pay salaries that DOD can – become a training ground and this results in higher/quicker turnover

Need people with security clearances – DOD/contractors

Perfect candidates would have the 4-year degree, but also the hands-on skills, the certifications and the clearances

Cyber penetration is easy to talk about but hard to do

Many do not have good communication skills

Applicants want to be in a competitive environment so need to move away from acting like "old fogies" – (e.g., don't block Facebook at the office)

Do you have current or regularly vacant positions that are hard to fill? If so, what are those positions?

Want people to advance through the company rather than changing companies

Municipalities – training ground issues b/c of lower salaries – e.g., web developers

Service desk personnel

Healthcare/health and human services see some turnover

How well are local educational program meeting your needs for a prepared workforce? What else would you like local educational institutions to know about your workforce needs?

For DOD, needs driven by the requirements in the contracts

Want cyber-hunters

Need to teach risk management

Need to be able to facilitate communication between the board, IT department and programmers

Coders need to also understand hardware

Need to understand the software development cycle

How to work as a team

Looking for geeks/hackers – not necessarily formally educated. Some courses there is no one at college/university who is qualified to teach needed courses

Hacking conferences/Hack-a-thons could be beneficial

Need to start training/introducing skills at the public school level – the kids are interested

Certifications are needed and will put students ahead b/c they are required

Give students credit for internships – internships should be a big part of the NIST curriculum

NIST foundation is important/RMF

Need to put cyber into the general IT curriculum – security needs to be in all CS programs

Students need access to education and security clearances

Applicants that can do more than one thing – particularly for employers that can't pay for large IT departments or for specialists in every area

Top ten vulnerabilities in programming – not teaching security for the operational person

Penetration testing

Do you see the start of emerging training needs you think your employees may need over the next 1-2 years and the longer term?

OSCP certifications

Routers and routing

Databases and how data is transferred through the web; Containers – larger companies starting to us them

RMF/the gov't mandating security from the beginning

Need to understand audit logs

Students should be required to do internships

Software defined networks/soft switches

VLANS

Hardware platforms to combat attacks

Security and networks and are merging and so are the jobs – same person doing the same job

Homeland security issues with IOT and sensor technology – Smart cars/Smart cities

Need to engage younger populations – forums like the conference are good for keeping people informed

Some discussion that the very technical people do not have the best communication/writing skills – some disagreement whether employers should just accept that or not

Employer/Business Survey Results

Email invitations to complete a survey of cyber workforce hiring needs were sent to over 200 business, educational partners and other contacts in November, 2016. Those initial contacts were also asked to forward the survey link to others who might have cyber hiring needs. By February 20, a total of 34 business representatives completed the survey.

Profile of Respondents:

Type of Agency	Percentage
Private/For-profit	64.7%
Federal/state/municipal government	26.5%
Not-for-profit	8.8%

Industry Category	Percentage
Cybersecurity (Hardware/Software/Services)	17.6%
Local Government	8.8%
Government Contractor	8.8%
Department of Defense	8.8%
Education	8.8%
Insurance	5.9%
Information Technology	5.9%
Finance/Banking	2.9%
Consulting	2.9%
Healthcare	2.9%
Other	26.5%

Primary Position/Title in Company/Organization	Percentage
Cybersecurity Manager/Administrator	23.5%
CEO/CFO	11.8%
IT Manager/Administrator	8.8%
Human Resources/HR Manager	2.9%
Other*	52.9%

* Included information/security officer, vice president, and other types of management and administrator positions.

Information about Company Positions and Vacancies:

Positions Your Company Employs	Percentage
Cybersecurity Analyst	70.6%
Cybersecurity Specialist/Technician	67.6%
Cybersecurity Engineer	64.7%
Cybersecurity Manager/Administrator	61.8%
Cybersecurity Consultant	52.9%
Cybersecurity Architect	47.1%
Penetration and Vulnerability Tester	44.1%
Incident Analyst/Responder	38.2%
IT Auditor	26.5%
Cybercrime Analyst/Investigator	26.5%
Other	5.9%
None	14.7%

Number of Positions	Range	Median	Mean*
Cybersecurity Specialist/Technician	0-2,000	2.0	107
Cybercrime Analyst/Investigator	0-1,000	3.0	117
Incident Analyst/Responder	0-800	3.0	78
IT Auditor	1-500	2.0	66
Cybersecurity Analyst	0-1000	2.0	59
Cybersecurity Consultant	0-3,000	2.0	210
Penetration and Vulnerability Tester	0-600	1.0	56
Cybersecurity Manager/Administrator	0-300	1.0	19
Cybersecurity Engineer	0-1,000	1.5	57
Cybersecurity Architect	0-400	1.5	36
Other (Only 2 responses)	10-200	105	105

*rounded to the nearest whole number

Number of Vacancies	Range	Median	Mean
Cybersecurity Specialist/Technician	0-10	0.0	1.1
Cybercrime Analyst/Investigator	0-2	1.0	1.0
Incident Analyst/Responder	0-10	0.5	1.5
IT Auditor	0-2	0.0	0.7
Cybersecurity Analyst	0-10	1.0	1.6
Cybersecurity Consultant	0-10	1.0	1.6
Penetration and Vulnerability Tester	0-5	0.0	1.2
Cybersecurity Manager/Administrator	0-4	0.0	0.8
Cybersecurity Engineer	0-10	1.0	1.3
Cybersecurity Architect	0-10	0.0	1.3
Other	N/A	N/A	N/A

Information about Recruitment, Hiring and Qualifications of Cyber Employees:

Most Effective Recruitment Methods*	Percentage
Job Seeker Web Services	41.2%
Personal/direct referrals	41.2%
Prior experience with our company	29.4%
Professional recruiters	20.6%
College career fairs	17.6%
Classified Ads	8.8%
Professional Membership Job Boards	8.8%
Other	14.7%

*Respondents were asked to select the two (2) most effective methods.

*Hardest Position to Fill	Percentage
Cybersecurity Engineer	48.1%**
Cybersecurity Analyst	33.3%**
Penetration and Vulnerability Tester	22.2%
Cybersecurity Architect	22.2%
Cybersecurity Specialist/Technician	22.2%
Cybersecurity Manager/Administrator	14.8%
Cybercrime Analyst/Investigator	11.1%
Incident Analyst/Responder	3.7%
IT Auditor	3.7%
Cybersecurity Consultant	3.7%
Other	3.7%

*Respondents were asked to select the 2 most difficult.
**Two most difficult positions to fill.

Importance of Skills and Knowledge				
	Very Important	**Somewhat Important**	**Somewhat Unimportant**	**Not at all important**
Communication Skills	72.7%	21.2%	6.1%	0.0%
General Problem Solving	66.7%	27.3%	6.1%	0.0%
Risk Management	57.6%	24.2%	18.2%	0.0%
Writings Skills	51.5%	33.3%	15.2%	0.0%
Customer service/Technical support	48.5%	33.3%	15.2%	3.0%
Network Detection and Analysis	42.4%	36.4%	6.1%	15.2%
Networking (Physical and Logical)	42.4%	36.4%	6.1%	15.2%
CISSP Certification	39.4%	33.3%	9.1%	18.2%
Security clearances	39.4%	18.2%	15.2%	27.3%

Importance of Skills and Knowledge				
	Very Important	Somewhat Important	Somewhat Unimportant	Not at all important
Security + Certification	37.5%	25.0%	12.5%	25.0%
Understanding the business environment	36.4%	42.4%	18.2%	3.0%
Regulatory Compliance (e.g. HIPPA)	30.3%	42.4%	15.2%	12.1%
Scripting	29.0%	35.5%	25.8%	9.7%
Systems Administration	27.3%	42.4%	21.2%	9.1%
Programming	27.3%	30.3%	30.3%	12.1%
Software Development	27.3%	33.3%	21.2%	18.2%
Code Debugging	24.2%	18.2%	39.4%	18.2%
Software Reverse Engineering	24.2%	27.3%	24.2%	24.2%
Virtualization	21.2%	33.3%	27.3%	18.2%
A + Certification	15.6%	34.4%	28.1%	21.9%
Internal Auditing	15.6%	40.6%	25.0%	18.8%
Network + Certification	15.2%	36.4%	27.3%	21.2%
Database/SQL	15.2%	48.5%	21.2%	15.2%
Penetration Testing	12.1%	54.5%	18.2%	15.2%
Auditing Planning	9.4%	37.5%	31.3%	21.9%
Containers	9.4%	25.0%	43.8%	21.9%
Other	75.0%	0.0%	0.0%	25.0%

Three (3) Most Difficult Knowledge Skills to Find in Applicants	
	Percentage
Communication Skills	32.4%*
General Problem Solving	20.6%*
CISSP Certification	20.6%*
Penetration Testing	20.6%*
Code Debugging	17.6%
Understanding the business environment	17.6%
Security clearances	17.6%
Software Reverse Engineering	14.7%
Networking (Physical and Logical)	11.8%
Programming	11.8%
Software Development	11.8%
Scripting	8.8%
Systems Administration	8.8%
Regulatory Compliance (e.g. HIPPA)	8.8%
Customer service/Technical support	8.8%
Risk Management	8.8%
Writings Skills	5.9%

Three (3) Most Difficult Knowledge Skills to Find in Applicants	
	Percentage
Security + Certification	5.9%
Network Detection and Analysis	5.9%
Database/SQL	5.9%
Containers	2.9%
A + Certification	2.9%
Auditing Planning	2.9%
Internal Auditing	0.0%
Virtualization	0.0%
Network + Certification	0.0%
Other	8.8%

*3 Most Difficult Knowledge Skills to Find (3 tied w/ 20.6%)

Feedback on Education Institutions and Preparation of Students:

Familiarity with Cybersecurity Education Programs in Hampton Roads	Percentage
Very familiar	14.7%
Somewhat familiar	52.9%
Not very familiar	8.8%
Not at all familiar	23.5%

Quality Rating of Cybersecurity Education that is Available from …				
	Excellent	**Good**	**Fair**	**Poor**
Community Colleges	20.8%	37.5%	33.3%	8.3%
4-Year Colleges/Universities	8.3%	54.2%	25.0%	12.5%
Public School	0%	20.8%	50.0%	29.2%

Use of Educational Opportunities/Programs	Percentage
Co-ops	22.2%
Internships	92.6%
Apprenticeships	29.6%

Effectiveness of Programs in Preparing New Hires				
	Very effective	Somewhat effective	Somewhat ineffective	Very ineffective
Co-ops	50.0%	50.0%	0.0%	0.0%
Internships	32.0%	60.0%	8.0%	0.0%
Apprenticeships	50.0%	50.0%	0.0%	0.0%

How Well Local Educational Institutions Prepare Students in:				
(Categories based on the NIST Framework)	Excellent	Good	Fair	Poor
Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	3.3%	26.7%	50.0%	20.0%
Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.	3.3%	33.3%	46.7%	16.7%
Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	3.3%	36.7%	46.7%	13.3%
Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	3.3%	26.7%	56.7%	13.3%
Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	3.3%	20.0%	66.7%	10.0%

How Prepared New Hires are in the Following Workplace Competencies …				
	Very prepared	Somewhat prepared	Not well prepared	Not at all prepared
Working with Tools and Technology	23.5%	58.8%	17.6%	0.0%
Teamwork	20.6%	58.8%	20.6%	0.0%
Creative Thinking	20.6%	47.1%	29.4%	2.9%
Operate and Maintain IT Security	20.0%	50.0%	26.7%	3.3%
Protect and Defend from Threats	20.0%	40.0%	33.3%	6.7%
Cybersecurity Technology	19.4%	51.6%	25.8%	3.2%
Problem Solving and Decision Making	17.6%	38.2%	35.3%	8.8%
Collect Information and Operate Cybersecurity processes	16.7%	50.0%	26.7%	6.7%
Information Assurance	12.9%	48.4%	32.3%	6.5%
Oversee and Govern Cybersecurity Work	10.0%	36.7%	43.3%	10.0%
Risk Management	9.4%	46.9%	34.4%	9.4%
Planning and Organizing	8.8%	67.6%	20.6%	2.9%
Investigating Threats	6.7%	50.0%	33.3%	10.0%
Analyze Information	6.7%	60.0%	23.3%	10.0%
Security Provision System	6.7%	66.7%	20.0%	6.7%
Incident Detection	6.3%	53.1%	31.3%	9.4%
Incident Response and Remediation	3.1%	56.3%	31.3%	9.4%
Business Fundamentals	0.0%	47.1%	50.0%	2.9%

Business Survey Open-Ended Responses

Skill selected as one of the three most difficult to find in current Applicants and Explanation

Scripting:

- *Many can script but difficult to find those that do it well with experience*
- *This is a specialized skill that requires additional training*

Programming:

- *People just want apps and don't learn to code*

Software development:

- *Applicants in the area are not skilled in C/C++*
- *Diversity in languages is a must*

Code debugging:

- *Lack of experience*
- *Lack of programs in education*
- *School programs struggle to teach basic programming skills, debugging is glossed over at best but it is essential to good security*

Software reverse engineering:

- *Lack of programs in education*
- *Requires a broad range of programming/scripting experience in a variety of languages*
- *Schools struggle to provide basic programming skills, reversing out code is much more difficult and an advanced topic that is rarely covered.*

Risk management:

- *Few people have this skill*
- *Shortage in trained personnel*
- *Students don't have any experience*

Writing skills:

- *Considered a soft skill in the field*
- *Effective writing in a clear and concise way is a difficult find in today's market*

Security+ certification:

- *Experience with certification*
- *Students are unaware it's CRITICAL to have in our industry*

CISSP certification:

- *Experience with certification*
- *Government role requirements*
- *Not many available*
- *Shortage in qualified personnel*
- *Students are unaware it's CRITICAL to have in our industry*
- *This is a hard exam, yet the requirement is becoming more standard*

- *The is one of the more difficult certifications to pass*

Penetration testing:

- *Applicant pool not robust*
- *Few qualified candidates*
- *Lack of programs in education*
- *Most positions do not fund for putting people through clearance process and there is a scarcity of people with good penetration testing skills. Most are scanner operators.*
- *Requires extensive technical knowledge, years of experience, and demand is high*
- *The one that the enemy is changing the most rapidly. It's the most difficulty to stay up to date on.*
- *This is a specialized skills that requires additional training.*

Communication skills:

- *Applicants very technical*
- *Employees like to keep everything to themselves*
- *Few applicants have the ability to speak and communicate clearly*
- *If you can't communicate your skills effectively, you can't thrive in customer environments*
- *Interaction with customers is important. You have to be able to translate complex technical information into consumable business information*
- *Often people don't know how to speak or write properly. Their body language is often an issue whether it is gestures or appearances*
- *Overall, my hiring demographic is an hourly/minimum wage person who struggles in this area*
- *Writing and presenting*
- *You must be able to communicate on different levels when dealing in business. Not everyone in a business is technologically savvy*

Network detection and analysis:

- *Often find applicants can't deliver what is on resumes*
- *Requires extensive technical knowledge, years of experience, and demand is high*

Auditing planning:

- *Few qualified candidates*

Systems administration:

- *Across broad systems – Linux and windows*

Regulatory compliance (e.g., HIPPA):

- *Few qualified candidates*
- *Governance oriented*
- *Wide array compliance standards*

Networking (physical and logical):

- *Crucial foundation skill for cyber security, many younger applicants kips over this for other security certs*
- *Requires both broad and specific level of knowledge*
- *Understanding and engagement with network security*

Containers:

- *Too few understand why it is important*

Understanding the business environment:

- *Lack of experience*
- *Many not interested in the business aspect*
- *Most IT professionals fail to see how they fit in the bigger picture*
- *None really works in our industry in Info Sec. It is in its infancy here*

Customer service/technical support:

- *It is hard to find the right demeanor for certain positions where the candidate has a genuine and caring attitude*
- *Not enough people are great at this*
- *The demographic that I am hiring is youngers and struggles in this area, seems as though they are not taught the basics of good customer service*

Security clearances:

- *Clearance process takes much longer, limiting the candidate pool*
- *Government role requirements*
- *If you don't have the security clearance, it is hard to get one*
- *No prior government/military background*
- *Shortage in cleared personnel when combining need for qualification and knowledge*

General problem solving:

- *Most have book knowledge but no practical application*
- *Not enough people are great at this*
- *Seeing a problem is one thing, but finding the solution to fix it is not. Stop, step back, look at the situation from the outside. The solution is there. Sometimes it takes thinking outside of box*
- *Students are generally force-fed a curriculum and not taught how to solve problem and understand issues*
- *The demographic that I am hiring is typically younger and struggles in this area, seems as though they are not taught the basics of this in their life experiences*
- *The difference between education and wisdom. Problem solving sills are the accumulated wisdom and experience in doing actual cyber security work. A degree and cert are just evidence of education and commitment*

Other:

- *Applicants in the area are not trained in data visualization*
- *Too many people don't have a good sense of judgement and they just don't get why things happen*
- *Applicants in the area are not experienced in Full Stack (MEAN, ELK) design*

<u>Describe gaps in educational preparation that you see in the cybersecurity workforce:</u>

- A+ and Security + Certification - Need on job training and real-world experience.
- Computer Science is lacking the most. As a developer of tools to be used in Cyber Security, a software developer with a firm understanding of Computer Science fundamentals is critical. Defense programming and concepts and a firm understand of data structures are needed.

Students are completing a degree program without understanding socket communication, or the OSI model. Less emphasis is needed on programming as a trade-school, and more as a science. The trade-school approach teaches programming and not computer science, which leads to exploitable and vulnerable software, further enabling security threat actors.

- Creative thinking skills are lacking. We can teach technology...we can't teach deductive reasoning.
- Cybersecurity is a very hands-on industry in addition to theory and concepts. Many education programs have good curriculum for teaching students theories and concepts like cryptography, network security, CIA concepts, etc. But the hands-on labs are not sufficient, like attack and defense. However, in real world operations, those hands-on experience is profoundly important.
- Employees are too dependent on computer programs and can't always problem solve.
- I am not well enough informed in this area to answer this question
- I don't think educational institutions prepare students for the business aspects of cybersecurity such as business continuity over security risks.
- In the Hampton Roads area, the major gap exists between the run time and experience of certified, prior military candidates verses college graduates with no run time - academia must compensate with work coops, collateral training/certification.
- It is not a continuum. We need to start at K-12 and go from there. We must drive interest, not just expertise.
- Knowledge and partnerships w/ local governments to partner and provide knowledge for both parties.
- Many candidates have minimal higher education in cybersecurity or partial work toward an industry certification.
- More lab time with real world situations. Theory is great but the challenge must be to put that theory into practice with real world hands on experience, a simulation run in a computer lab would put them in a real world situation with results and consequences.
- My newer employees have gone into cyber for money and become less as they aren't prepared with technical skills on specific specialties.
- Not educating students enough and helping them be aware.
- Not enough direct application of education
- Students are not taught how things work and how to problem solve today. They are generally rushed through a very basic curriculum.
- The workforce is getting trained on what we know and the battlefield is evolving so fast that by the time they get here the skills have changed. Must be adaptive.
- There appears to be a gap in the area of NIST and other Cybersecurity frameworks. Additionally, gaps in the impact that human behavior has on cybersecurity. There is also a gap in the knowledge and use of available tools used detect, protect, prevent, and mitigate cyber threats.
- Use of national Risk Management Framework in accordance with NIST 800 series of documents for Information Assurance.
- While many students receive a broad education, because they only specialize in one section, it makes it harder when they come into the workforce and have to know a lot of moving parts; they end up applying for jobs that do not have the same path of what they learned in school.

What specific actions can local educational institutions do to better prepare the cybersecurity workforce:

- A+ and Security+ Certifications - More collective job fairs.
- Capture the flag and hacking competitions are good, but a different way would be to set up a computer lab, present real world problems, attacks, etc. and see how they respond, do they panic? Do they think outside the box and come up with a practical solution to overcome the situation. Example, set up a company, have two teams one monitors and protects the company, the their attacks. A computerized version of Risk, Chess etc. We do this in our company all the time to test vulnerabilities.
- Combine the humanities with technological curricula.
- Communicate across all of the tribes of interest in cyber security, cyber opportunity, and cyber education.
- Create partnerships with the DOD and graduate your students with a security clearance.
- Educational institutions can work together to create an educational process or path that will work towards developing a cybersecurity professional from entry level to senior manager/leader. For example, K-12 focus on cybersecurity awareness and save computing and intro/college prep for cyber disciplines. Junior college focus on cyber/computer related certifications in preparation to enter workforce with credentials. Also focus on business and cyber interrelationship. 4-year institutions focus on cyber/information technology management and how cyber/information technology support the business. Graduate level focus on how cyber/information technology along with security impacts an organization's strategic goals and objectives.
- I think that having cybersecurity business courses would be a good start. This would prepare them for the business challenges they will face with upper management and different lines of business.
- Make students more aware and provide opportunities
- More time behind keyboard, less time in traditional learning environments (reality vs theory)
- Partner with vendors like Symatec and McAff and intern with local cyber business.
- Provide specific instruction with regards to Risk Management Framework in accordance with NIST 800 series of documents.
- Raise the standards of the coursework. I often interview many students that have taken coursework and received grade 'A' for the course named for the topic in discussion. However, the students cannot answer basic elementary questions. Students with undergraduate degrees in Computer Science focused in C++ do not know "multiple inheritance", or how/why it is useful. A Freshman at Virginia Tech is better suited for a position over a program graduate from Old Dominion University.
- Recruit and train according to a systematic program, including communication, law, management, business principles.
- See what kind of jobs are out there and either prepare students for that; or help students find a more direct job for which they knew a lot about.
- Solicit co-ops and analysis with/from: 1. Sera-Brynn - cyber auditing, PCI compliance, Cyber Risk Assessment Address: 5806 Harbour View Blvd #204, Suffolk, VA 23435 Phone: (757) 243-1257 Hours: Open today · 8:30AM–4PM https://sera-brynn.com/ 2. Mitnik Security - global ghosting, penetration testing, incident response, forensics, exploit exchange, expert witness services, vulnerability testing, product claims testing https://www.mitnicksecurity.com/site/contact-mail
- Table-Top Exercises within a live environment government, public, or private sector.

- Understand that investing in on-going training is a critical success factor.
- We need to create large scale platform and large number of practical hands-on labs to strengthen the knowledge of students obtained from lectures.
- Work needs to be done to promote critical thinking and problem solving skills.