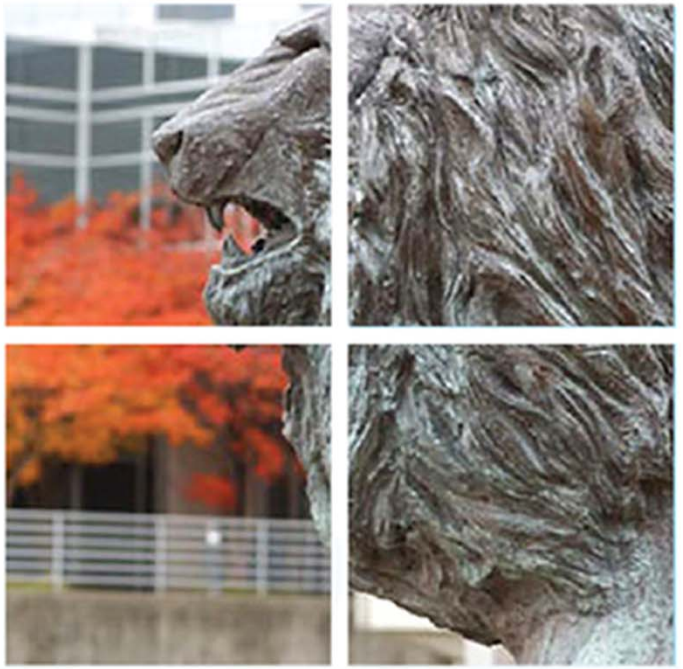
OLD DOMINION
UNIVERSITY
IDEA FUSION



Academic-Industry Collaboration for Workforce Development

Academic Initiatives

- Center for Cyber Security Education and Research
- Interdisciplinary Cybersecurity Majors
  - Cybersecurity
  - Cybercrime
  - Cyber operations
  - Enterprise cybersecurity
- Cybersecurity Learning Community
- Cybersecurity Living Learning Community
- NSA Funding for Risk Management Course
- Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance

Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance

HRCyber Project Status Update

Goal 1: Coordinate educational pathways between public high schools, community colleges, and four year institutions

Associated Activities with Goal 1	Status
Conduct monthly steering committee meetings	
Develop at least two articulation agreements (TCC-ODU agreement completed Dec 2016) (TNCC-ODU agreement completed April 2017)	
Identify curricula revisions (1st meeting held April 7, 2017)	
Create virtual lab	
Review and/or revise articulation agreements	

Goal 2: Gather information from the regional workforce about the knowledge units taught in cybersecurity programs and revise those curricula where needed.

Associated Activities with Goal 2	Status
Conduct two focus groups with employers to determine their views on cybersecurity (Completed October 2016)	
Complete cybersecurity workforce survey	
Conduct DACUM workshop and chart (Completed February 2017)	
Assess curricula revisions	
Complete cybersecurity educational survey	

HRCyber Project Status Update

Goal 3: Coordinate academic programming between educational institutions and workforce.

Associated Activities with Goal 3	Status
Conduct Cybersecurity Counselor Workshop (completed Feb 23, 2017)	
Create HRCyber homepage (Completed October 2016)	
Train faculty on Virtual Lab (ODU trained TNCC faculty on virtual lab)	
Train college counselors/academic on cybersecurity programs	

Goal 4: Strengthen the cybersecurity capabilities of the regional workforce.

Associated Activities with Goal 4	Status
Develop and produce at least four cybersecurity career awareness videos	
Conduct Cybersecurity Saturday Series for high school students and parents (March 2017)	
Host a cybersecurity workforce development summit in fall 2017	
Develop marketing material (HRCyber Brochure completed April 2017)	
Participate in regional cybersecurity summits and conferences	
Attend NICE Conferences (2016/2017) (Attended 2016 NICE Conference)	
Provide Virginia Beach High School Interns to regional cybersecurity employers	
Provide internships and apprenticeships to regional cybersecurity employers	

Summary of Employer Surveys

- Most positions are consultants, cybercrime analysts, and cybersecurity specialists.
- Most vacancies for cybersecurity analysts, consultants, incident analysts, engineers, and architects.
- Positions hardest to fill were cybersecurity engineers and analysts.
- Communication skills, general problem solving skills, risk management skills, and writing skills most often ranked as very important.
- Skills hardest to find were communication skills, general problem solving, CISSP certification, and penetration testing, but there was not much variation.

Summary of Employer Surveys

- Just 14.7% were very familiar with cybersecurity education programs
- All employers viewed co-ops and apprenticeships as at least somewhat effective and most viewed internships as at least somewhat effective.
- Regarding the NIST framework, were rarely rated as excellent and most negatively rated on resilience and restoration.
- Also rated low on managing risk and responding.
- Areas where new hires needed more preparation included problem solving, risk management, incident detection/response and protecting from threats, overseeing and governing cybersecurity work, and business fundamentals (but not a lot of variation).
- Doing better preparing in areas of teamwork and technology
- Received more comments about needing CISSP cert and penetration testing.

DACUM Themes

- Assessing Risk
- Protecting Information Assets
- Detecting cybersecurity events
- Reacting to cybersecurity events
- Restoring secure environment
- Increasing security awareness
- Maintaining professional knowledge

Communication skills --- quotes

- *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*

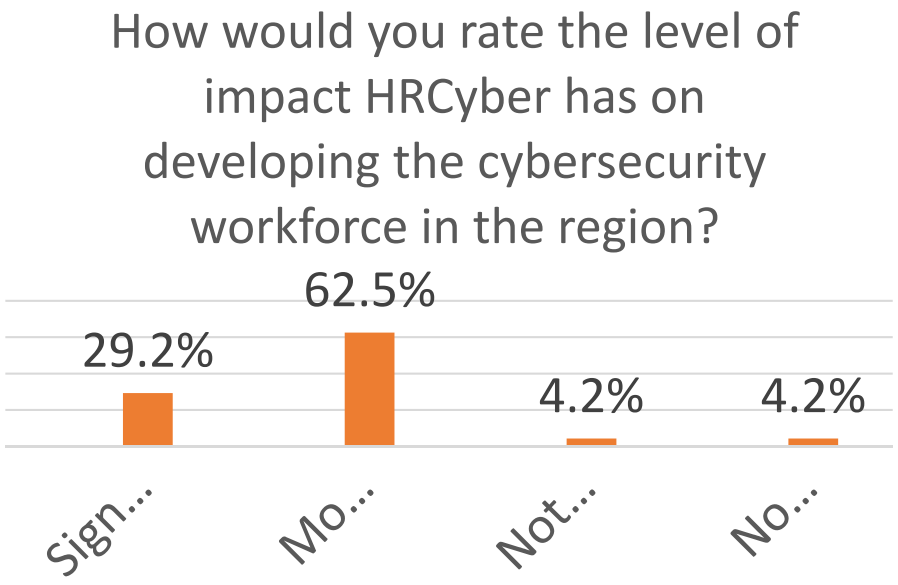
Gaps -- quotes

- Creative thinking skills are lacking
- But the hands-on labs are not sufficient, like attack and defense.
- Problem solving…adaptive
- Business courses
- Hands-on/experiences

---- *Duties* ----	*Tasks*										
A Assess Cyber Risks	A.01 Identify info system assets	A.02 Identify security vulnerabilities	A.03 Identify attack vectors	A.04 Quantify business value of assets	A.05 Brief stakeholders *	A.06 Review policies and procedures	A.07 Test response processes	A.08 Create virtual test environments			
B Protect Information Assets	B.01 Create protection plan	B.02 Create contingency plan	B.03 Create disaster recovery plan	B.04 Provision user accounts	B.05 Implement access controls (i.e. black lists, white lists, geofence)	B.06 Install network devices (i.e. IDS, IPS, firewall, web filter)	B.07 Configure network devices (i.e. IDS, IPS, firewall, web filter)	B.08 Install host-based security systems (i.e. antivirs, malware, sensors)	B.09 Configure host-based security systems (i.e. anti-virus, malware, sensors)	B.10 Create investigative and configuration scripts	B.11 Ensure data encryption (i.e. data at rest, data in transit removeable media)
	B.12 Ensure physical security controls	B.13 Ensure environmental controls	B.14 Recommend security requirements	B.15 Manage wireless access points	B.16 Create network diagrams	B.17 Maintain network diagrams	B.18 Create penetration test plans	B.19 Request ASI	B.20 Backup critical data	B.21 Manage network device life-cycles	B.22
C Detect Cybersecurity Events	C.01 Monitor network devices	C.02 Analyze output of network devices	C.03 Analyze threat feeds	C.04 Monitor wireless access points	C.05 Review network diagrams	C.06 Set audit flags	C.07 Analyze external data (i.e. darknet, passive DNS, BGP)	C.08 Document historical findings	C.09 Maintain historical Packet Capture (PCAP)	C.10 Analyze audit logs	C.11 Analyze vulnerability scans
	C.12 Hunt potential threats in network traffic	C.13 Conduct organizational penetration tests	C.14 Generate penetration test documentation	C.15 Challenge personnel need-to-know/authori-zations							
D React to Cybersecurity Events	D.01 Initiate response procudures	D.02 Assess security event	D.03 Report event to supervisor *	D.04 Determine escalation	D.05 Communicate with stakeholders *	D.06 Maintain stakeholder call list	D.07 Contain security incident	D.08 Trace source of threat	D.09 Preserve evidence of event	D.10 Document steps taken	D.11 Estimate damage of security incident
	D.12 Sever network activity	D.13 Report estimated time of restoration	D.14 Document evidentiary process								
E Restore Secure Environment	E.01 Determine scope of restoration	E.02 Create restoration plan	E.03 Coordinate restoration efforts	E.04 Rebuild info system	E.05 Reimage information system	E.06 Restore critical data	E.07 Test restored environment	E.08 Validate restored environment	E.09 Document lessons learned	E.10 Document recovery processes	
F Increase Security Awareness	F.01 Create security awareness materials	F.02 Create acceptable use policies	F.03 Participate in security exercises	F.04 Distribute security info to users	F.05 Conduct cybersecurity training	F.06 Conduct phishing campaign	F.07 Reverse engineer malware	F.08 Conduct security awareness assessment	F.09 Report assessment results	F.10 Recommend procedures to correct security issues	
G Maintain Professional Knowledge	G.01 Complete cybersecurity training	G.02 Maintain industry certifications	G.03 Read technical literature (i.e. books, blogs, articles, etc.)	G.04 Attend professional confer-ences	G.05 Maintain operating environment qualifications	G.06 Practice through trial and error	G.07 Maintain professional memberships				

HRCyber Partner Azimuth Check Survey Results

- The majority of partners feel that HRCyber has had at least a moderate impact on the regional cybersecurity workforce:



Suggestions for improving impact on cybersecurity workforce in the region:

- Continue the current efforts/work - (6)
- More marketing/"get the word out" – (5)
- Engage with others (workforce, educational partners, employers) – (4)
- Curricular suggestions – (2)
- Seek more funding – (1)
- Other (3)

HRCyber Partner Azimuth Check Survey Results

- 89% of partners believe that HRCyber is an initiative that should be continued past the initial 18 month grant ending in Dec. 2017 (the other 11% didn't respond to the question item)
- Most significant benefit HRCyber has provided to partners (selected comments):
  - "Access to trained workforce"
  - "Articulation/transfer between TCC and ODU"
  - "Awareness and connectivity with HRCyber community leaders"
  - "Clear and consistent collaboration with a variety of cyber industry representatives in the region"
  - "Educational transfer pathways"
  - "Provided a view into what academia is trying to coordinate in the region"
  - "Shared knowledge and resources"
  - "Visibility into the state of CS educational and workforce development capability/offerings across our region"

Cybersecurity Workforce and Educational Data Collection

Recruitment:

- Recruiters, college fairs, internship programs, veteran sources (TAP), 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 Skill/Knowledge Areas:

- Technical skills necessary such as prior programming experience, vulnerability assessment, risk management, network detection and analysis, and penetration testing.
- 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.

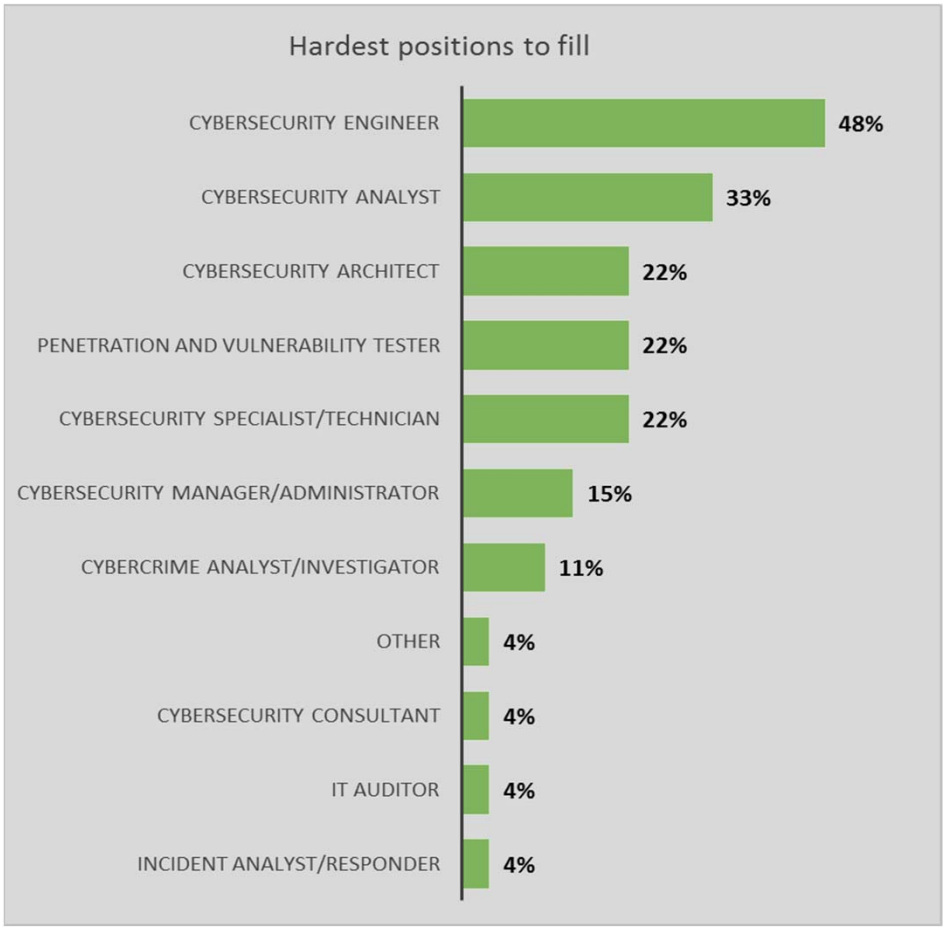
Focus group – highlighted results, cont.:

- Difficulty Finding Qualified Applicants:
  - The general consensus was that it is difficult for a variety of reasons.
    - Conventional recruitment methods do not always work = rely on personal networks to hire.
    - Others reported seeing "paper tigers".
    - Smaller orgs/municipal orgs reported not being able to compete with salaries offered by private firms or DOD.
    - DOD needs people with security clearances.
    - Many applicants with the necessary technical/cyber skills do not have good communication skills.

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 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 Representative Web Survey Results



Business Representative Web Survey Results

Top rated skills when hiring (very/somewhat important):

- General problem solving (94%)
- Communication skills (94%)
- Writing (85%)
- Customer service/Technical Support (82%)
- Risk Management (82%)
- Networking (79%)
- Network detection and analysis (79%)

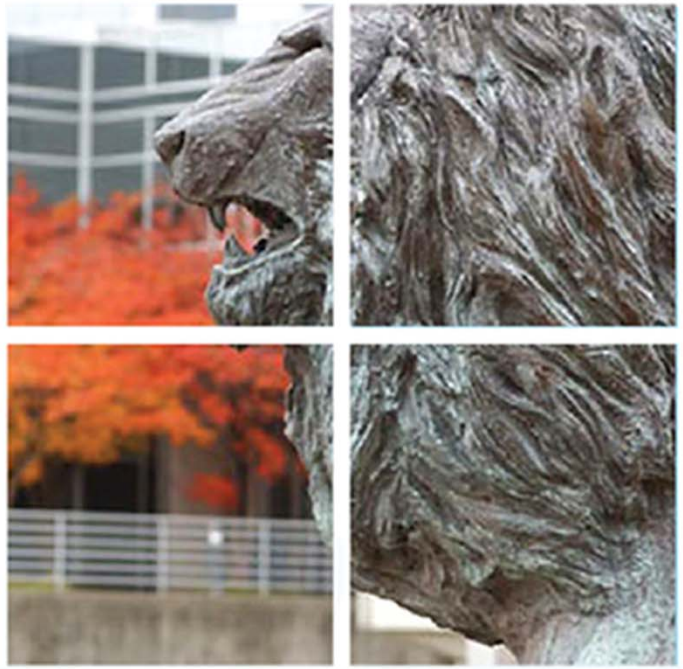
Business Representative Web Survey Results

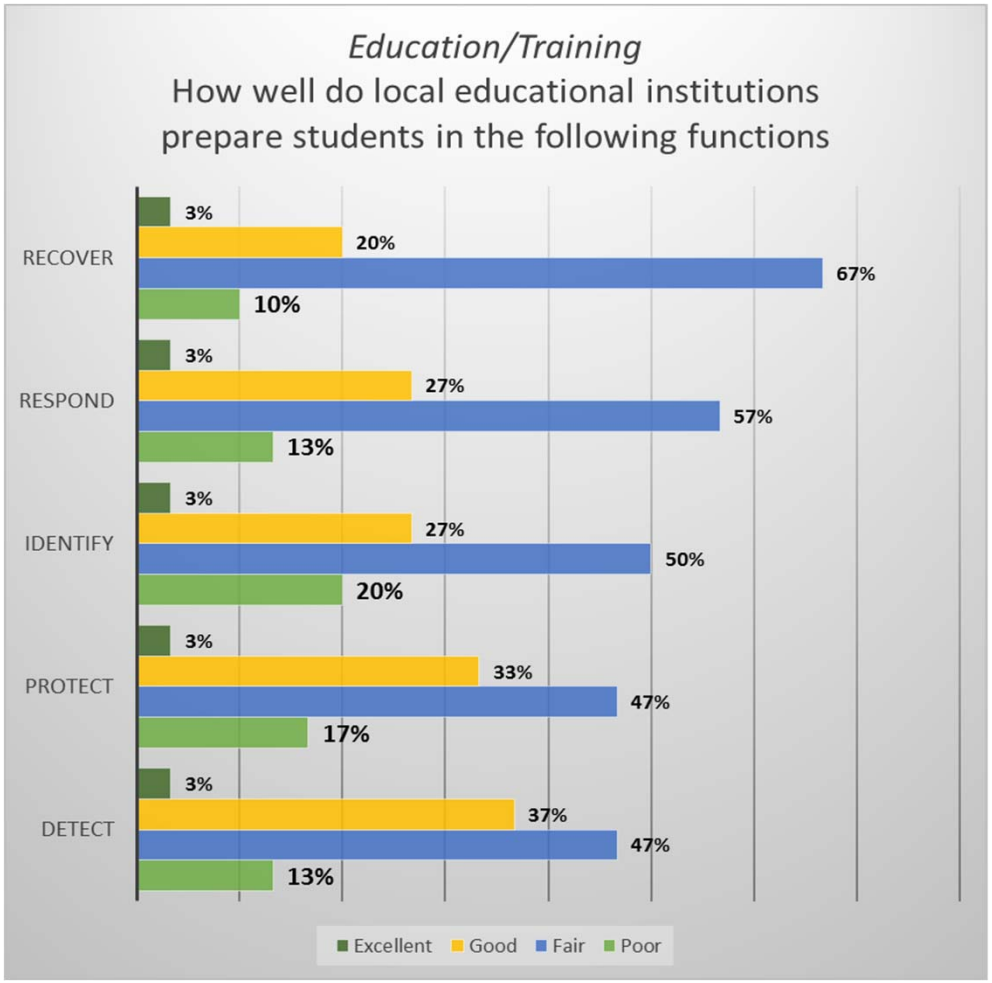
Most difficult knowledge skills to find in applicants:

- Communication skills (32%)
- General problem solving (21%),
- Penetration testing (21%),
- CISSP certification (21%),
- Understanding the business environment (18%)
- Security clearances (18%)
- Code debugging (18%)

OLD DOMINION
UNIVERSITY

IDEA FUSION





Not many excellent ratings – most were in the "fair" category

Protecting and detecting had highest % of "good" ratings

Identifying had the highest % of "poor" ratings.

Business Representative Web Survey Results

Gaps in the educational preparation of the cyber workforce and specific actions that local educational institutions can take to better prepare the cyber workforce:

Creative thinking skills are lacking. We can teach technology...we can't teach deductive reasoning.
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.

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.

Good news – HRCyber is working on all of these….

Educational Partner Web Survey Results

Importance of skills/knowledge areas for students entering the workforce(very/somewhat important):

- Security clearances (15)
- Understanding the business environment (15)
- Penetration testing (15)
- Writing skills (15)
- Code debugging (15)
- General problem solving skills (15)

Educational Partner Web Survey Results

Most difficult knowledge/skills areas to find qualified professors/instructors to teach:

- Software reverse engineering (8)
- Security clearances (5)
- Penetration (5)
- Security + Certification (3)

Educational Partner Web Survey Results

- How well prepared recent cybersecurity graduates are in workplace competencies (very/somewhat prepared):
  - Teamwork (14).....compared to 79% business
  - Security provision system (13).... compared to 73% business
  - Creative thinking (13)....compared to 68% business
  - Problem solving and decision making (13)...compared to 44% businesses – not well/not at all prepared
  - Operate and maintain IT security (13)....compared to 70% business

Educational Partner Web Survey Results

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%

The educational partners rated the quality of education higher than did the business representatives

Educational Partner Web Survey Results

- 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

- 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.

Changes we made...

- Required internship
- Revised lab to include communications focus
- Two new majors
- Course re-design