

LESSONS LEARNED AND BEST PRACTICES

HAMPTON ROADS EDUCATIONAL,
WORKFORCE AND ECONOMIC
DEVELOPMENT ALLIANCE (HRCYBER)



“BRIDGING THE CYBERSECURITY TALENT GAP IN HAMPTON ROADS”

ABSTRACT

This report identifies lessons learned during the 18-month grant provided by NICE that established the Hampton Roads Education, Workforce and Economic Development Alliance.

Prepared by: John P. Costanzo | May 2018

Contents

Executive Summary..... 2

Project Background 4

Project Mission and Objective 4

Project goals and related activities..... 5

Lessons Learned: HRCyber Goals and Activities..... 7

 Goal 1: Coordinate educational pathways among public high schools, community colleges, and four year institutions. 7

 Goal 2: Gather information from the regional workforce about the knowledge and skills needed in cybersecurity programs and revise curricula as needed. 10

 Goal 3: Coordinate academic programming among educational institutions and workforce. 13

 Goal 4: Strengthen the cybersecurity capabilities of the regional workforce..... 14

Other Highlights and Accomplishments: 18

 Additional grant and funding opportunities. 18

 New Academic Programs..... 19

 Other Cybersecurity initiatives/Achievements in the region. 20

Executive Summary

This report provides insights into the lessons learned from the 18-month Department of Commerce, National Institute of Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE), Regional Alliances and Multi-stakeholder partnerships (RAMPS) funded project that established the Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber) which ran from October 2016 to April 2018.

HRCyber is a partnership of educational institutions, government agencies, non-profit organizations, and private employers focused on developing educational pathways from high school through community college to four year institutions and continued professional development providing a capable and fully trained cybersecurity workforce for the region. This is achieved by aligning regional educational and skills development offerings to the workforce practices and activities of business and non-profit organizations within the Hampton Roads region with the specific goal of supporting local economic development and job growth via establishment of a multi-stakeholder alliance. This is accomplished by addressing the workforce needs of cybersecurity employers and by increasing the pipeline of students pursuing cybersecurity careers from high schools, community colleges and universities.

HRCyber has four goals each with several associated activities. The four goals are: 1) Coordinate educational pathways among public high schools, community colleges, and four year institutions. 2) Gather information from the regional workforce about the knowledge and skills needed in cybersecurity programs. 3) Coordinate academic programing among educational institutions and workforce. 4) Strengthen the cybersecurity capabilities of the regional workforce.

Key lessons learned.

- 1) HRCyber's monthly meetings provided a means for a diverse group of stakeholders focused on developing the cybersecurity workforce to network, share best practices and create business connections.
- 2) The creation of articulation agreements between Old Dominion University and three community colleges (Tidewater, Thomas Nelson, and Northern Virginia) which articulated the community college Associate in Applied Science Information Systems Technology degree to a Bachelor of Science Interdisciplinary Studies – Cybersecurity degree will save transfer students 50 credit hours, 1.5 years of study, and over \$16,000 in tuition. These articulation agreements are a model other four year institutions can use to articulate their cybersecurity degrees.

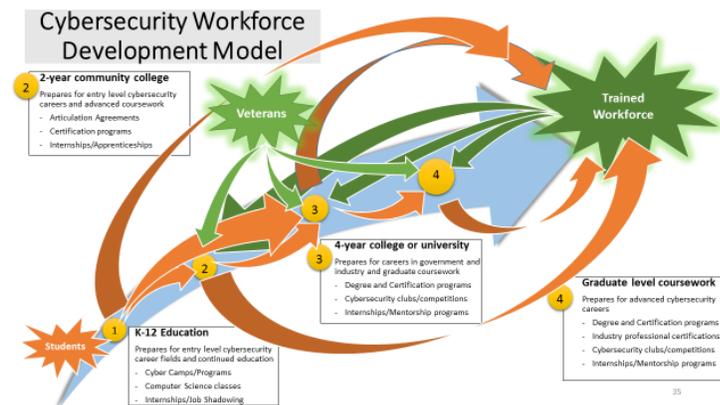
- 3) A regional survey of cybersecurity related businesses and educational institutions was conducted to evaluate the cybersecurity workforce needs. This survey provided a baseline that was used to revise curricula, determine the need for new academic programs, and develop new internship programs and opportunities. A key finding was the need for new employees to be well-trained in a variety of skills – both technical and non-technical. These non-technical skills include problem solving, written and communications skills, and customer service skills.
- 4) Partnering with the Virginia Space Grant Consortium proved to be invaluable to achieving many of the activities associated with this project. They produced five cybersecurity workforce videos, hosted a Cybersecurity Counselor Workshop for K-12 schools, hosted and completed a Developing a Curriculum (DACUM) workshop that evaluated the skills and duties associated with a Cybersecurity Analyst, hosted two Cyber Saturday events for high school students and their parents, and the managed the cybersecurity internship program.
- 5) The cybersecurity internship programs at both the high school and college level provided students with much needed work related experience in this career field. The City of Virginia Beach City Public Schools', Advanced Technology Center managed the high school program and they placed 20 students with several local cybersecurity businesses. This was one of the most successful activities conducted as part of this project. The college cybersecurity internship program, managed by the Virginia Space Grant Consortium, placed twenty six interns with cybersecurity companies. One of the most successful internship opportunities was with Sentara Healthcare who brought on eight interns. Both the high school and college cybersecurity internships will be continued under the GO Virginia funded project that continues much of the work started with this NIST funded project.
- 6) HRCyber hosted a Cybersecurity Workforce Summit as its culminating event. This summit showcased many of HRCyber's accomplishments. A series of panel discussions were held focusing on educational pathways, internships and apprenticeships, industry and educational cybersecurity survey results, Virginia Space Grant Consortium activities, and cybersecurity workforce and economic develop. Over 100 people, representing a diverse group, attended this event.
- 7) As a result of the positive impact HRCyber had across the region, over \$3.2 million dollars in additional grant funds were awarded to Old Dominion University. This includes Old Dominion University's Virginia Modeling and Simulation Center being awarded a \$1.2 million dollar grant from the Commonwealth of Virginia Go Virginia Initiative. This grant established the HRCyber Co-Lab which will continue many of the activities started under the NIST grant and expand into other growing fields like autonomous unmanned vehicles and big data.

Project Background

In October 2016, Old Dominion University was awarded a grant by the U.S. Department of Commerce as one of five regional alliances and multi-stakeholder partnerships (RAMPS) to stimulate cybersecurity education and workforce development under the National Initiative for Cybersecurity Education (NICE) objectives. This grant established the Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber). This grant ran from October 2016 to April 2018.

HRCyber provided an opportunity to bring together community and private organizations focused on expanding the cybersecurity ecosystem in the Hampton Roads region. Crossing multiple boundaries and priorities, HRCyber coordinated efforts from a host of partners to address this key economic development issue. These organizations included the region’s community colleges, three large public school districts, universities, several cybersecurity related businesses, non-profit organizations, and the advocacy and support of local government economic development offices. By bringing together this diverse group, HRCyber fostered mutually beneficial relationships and expanded existing relationships. To illustrate the amount of interest generated by this project, the number of partners grew from 16 to over 40 in less than six months; showing the region’s desire to expand the cybersecurity workforce and economic opportunities.

Project Mission and Objective



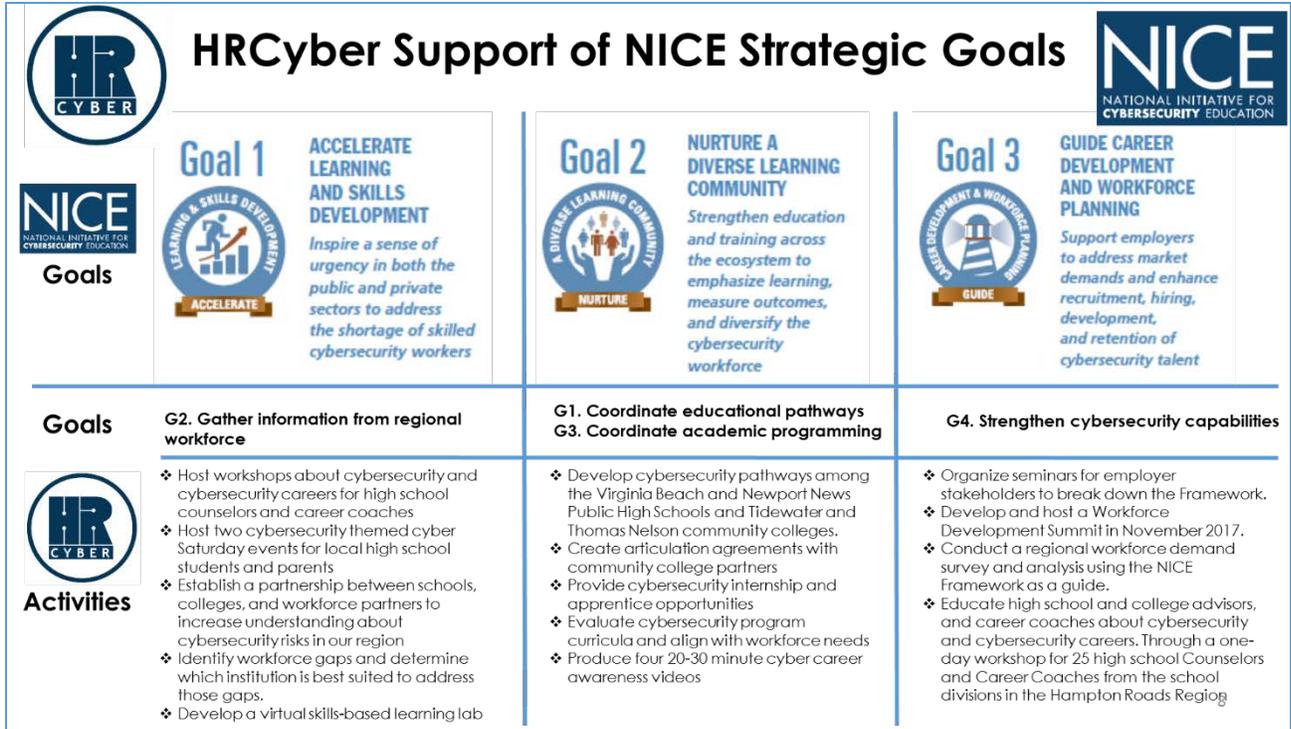
Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber) is a partnership among educational institutions, government agencies, non-profit organizations, and private employers focused on developing educational pathways from high school through community

college to four year institutions and continued professional development providing a capable and fully trained cybersecurity workforce for the region.

HRCyber aligns regional educational and skills development offerings to the workforce practices and activities of business and non-profit organizations within the Hampton Roads region with the specific goal of supporting local economic development and job growth via establishment of a multi-stakeholder alliance. This is accomplished by

addressing the workforce needs of cybersecurity employers and by increasing the pipeline of students pursuing cybersecurity careers from high schools, community colleges and universities.

Figure 1: HRCyber goals linkage to NICE strategic goals.



Project goals and related activities

HRCyber’s four goals are aligned with the NICE strategic goals of accelerate learning and skills development, nurture a diverse learning community, and guide career development and workforce planning. See Figure 1

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

A central goal of this project is to coordinate cybersecurity educational pathways among those educational institutions participating in HRCyber. The primary activities associated with this goal are:

- Conduct monthly steering committee meetings.
- Develop at least two articulation agreements between the community colleges and ODU and other partner institutions.
- Create a virtual lab.

- Identify curricula revisions.

Goal 2: Gather information from the regional workforce about the knowledge and skills needed in cybersecurity programs and revise curricula as needed.

The second goal of HRCyber is to generate an understanding about the types of knowledge cybersecurity professionals need in the Hampton Roads region across the board swath of cybersecurity careers. The primary activities associated with this goal are:

- Conduct focus groups with employers to determine their views on cybersecurity knowledge units and required skills.
- Survey regional employers to assess their cybersecurity workforce needs.
- Conduct Developing a Curriculum (DACUM) workshop and develop a DACUM chart to create workforce-driven curricula.
- Survey cybersecurity educational partners.
- Assess curricular revisions.

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

The third goal of HRCyber is to improve the coordination of academic programming between educational institutions and the regional workforce. This involves developing stronger ties between each educational institution and connecting these institutions with the workforce.

The primary activities associated with this goal are:

- Conduct a Cybersecurity Counselor Workshop.
- Create the HRCyber homepage and informational brochure.
- Training faculty on the virtual lab.
- Train college counselors and academic advisors on cybersecurity programs.

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

The fourth goal of HRCyber is to strengthen the cybersecurity capabilities of the regional workforce. The primary activities associated with this goal are:

- Develop and produce cybersecurity career awareness videos.
- Conduct Cyber Saturday series for high school students and parents.
- Host a cybersecurity workforce development summit in fall 2017.
- Provide Virginia Beach high school interns to regional cybersecurity employers.
- Provide internships and apprenticeships to regional cybersecurity employers.
- Participate in regional cybersecurity summits and conferences.

Lessons Learned: HRCyber Goals and Activities

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

A central goal of this project is to coordinate cybersecurity educational pathways among those educational institutions participating in HRCyber.

Activity 1. Conduct monthly meetings.

Monthly meetings kept the alliance partners informed about what was happening with the project and in the region regarding cybersecurity. During a mid-project survey, the alliance partners were asked if the quality of information provided during the meetings was of value. Over 47% rated the meetings as “excellent” and over 52% rated them as “good.” In addition, 85% of the survey respondents said they attended these meetings regularly. These two points indicate a high level of interest and involvement by the partners by their willingness to devote time in participating in these meetings.

These meetings also provided an opportunity for the partners to network and develop new connections. This is illustrated with the establishment of the first cyber apprenticeship in the country between Peregrine Technical Solutions and Tidewater Community College. In addition, Peregrine is also working with Thomas Nelson Community College to create a second cyber apprenticeship. The monthly meetings allowed Peregrine to make the connection with these community colleges resulting in the apprenticeship programs. Through this work, additional companies are looking to develop their own apprenticeships in cybersecurity. This would not be happening without the networking opportunities provided by HRCyber.

Activity 2. Develop articulation agreements between the community colleges and ODU and other partner institutions.

As a result of this project, Old Dominion University developed articulation agreements with three Virginia Community Colleges – Tidewater Community College, Thomas Nelson Community College, and Northern Virginia Community College. The agreements articulated the community college Associate of Applied Science Information Systems Technology degree to the Bachelor of Science Interdisciplinary



Studies – Cybersecurity degree at Old Dominion University. The first agreement completed between Old Dominion and Tidewater became the model for the other two agreements and can be used by other 4-year universities to develop their own articulation agreements. These agreements allow transfer students to complete both their associate and bachelor degree with 121-124 credit hours, saving them 50 credit hours, 1.5 years of time, and \$16,750 in tuition. It is estimated that the first students to transfer under these agreements will be in fall 2018. The political value these agreements have is also measured by the fact that the governor of Virginia, Secretary of Technology, Secretary of Education and two state delegates participated in the first signing ceremony at the state capital.

For additional information on the articulation agreements please see the following links:

- [TCC and ODU articulation agreement.](#)
- [TNCC and ODU Articulation agreement.](#)
- [NOVA and ODU articulation agreement.](#)

Another benefit created through the work started with these articulation agreements is a strengthening of the strategic partnership between these community colleges and the 4-year universities. In particular, Old Dominion University partnered with both TCC and TNCC, and other 4-year universities, on additional grant opportunities including a \$1.2 million grant provided by GO Virginia to continue the work started with HRCyber and the NIST/NICE RAMPS funding.

Activity 3. Create a virtual lab.

This grant allowed Old Dominion University to expand its cybersecurity virtual laboratory and opened it up to educational institutions outside of the university network. The lab provides a secure and user-friendly environment for students to remotely engage in hands-on labs, which are a critical component of many cybersecurity courses. The enterprise Cisco routers, switches, and security appliances in the laboratory provide comprehensive protection for the laboratory as well as shield the campus network from accidental cyber-attacks. The high-end workstations, together with the Cisco networking gears, enables students to create not only virtual networks, but also real world network environments connected by physical routers and switches. Such processes emulate highly realistic cyber-attacks and defenses.



Various hands-on laboratories have been developed and deployed in the virtual laboratory, supporting the cybersecurity courses currently offered by ODU. To provide seamless access to the ODU virtual lab for HRCyber Alliance partners, the ODU Information Technology Services upgraded the equipment in the lab. ODU guest accounts were

created for a list of faculty at TNCC and TCC. The partners are able to utilize web browsers to log in their ODU guest accounts, and seamlessly access the virtual lab from their guest accounts. A demonstration session was conducted in May 2017 for the faculty of TNCC. Feedback from lab participants will be sought in order to expand the virtual lab and develop additional hands-on labs. Over 150 K-12 students used the lab as part of a series of cybersecurity summer camps and it was used by 100 ODU cybersecurity students to work on projects and other course work.

Activity 4. Identify curricula revisions.

Curricula revision is a continuous process. In April 2017, a workshop was conducted with the project's educational partners to discuss the various tools available for reviewing their cybersecurity curricula in order to meet the workforce needs. Some of the tools provided included the results of the cybersecurity workforce and educational surveys conducted as part of this project, as well as the Developing the Curriculum (DACUM) chart that was generated from the DACUM workshop. One direct result from the curricula workshop was that Old Dominion changed the internship requirement for its cybersecurity students from optional to required. This change was made because the HRCyber industry partners said there was a need for students and entry-level employees to have relevant work experience in cybersecurity and information technology.

As a result of the initiative to continually offer courses and programs that meet the current and future workforce needs, several new cybersecurity and cybersecurity related programs were created.

- Old Dominion created three new cybersecurity bachelor degrees: Bachelor of Science Interdisciplinary Studies in Cybercrime, Bachelor of Science Interdisciplinary Studies in Cyber Operations, and Bachelor of Science in Business Administration in Information Technology with a focus on enterprise cybersecurity. All three programs will be offered starting in fall 2018.

- Old Dominion received a NSA Cybersecurity Core Curricula Development Grant to create a course in cybersecurity risk management.
- Old Dominion is waiting for approval of a Master of Science Cybersecurity.
- Norfolk State is pursuing the development of a Master of Science in Cyberpsychology.

Goal 2: Gather information from the regional workforce about the knowledge and skills needed in cybersecurity programs and revise curricula as needed.

The second goal of HRCyber is to generate an understanding about the types of knowledge cybersecurity professionals need in the Hampton Roads region across the board swath of cybersecurity careers.

Activity 1. Survey regional employers and educational partners to assess cybersecurity workforce needs.

A key element of determining the cybersecurity workforce needs of the region was to conduct a survey of cybersecurity employers. This survey focused on assessing the skills and knowledge of new hires, their desired skills and knowledge, identification of difficulty in finding candidates that meet their needs, and an evaluation of the local education programs that prepare future cybersecurity employees. This workforce survey was developed with feedback provided during three focus groups. A second survey was conducted on the educational partners, K-12, community college, and 4-year universities to provide a comparison of what the employers said was needed/wanted to what was being taught. Overall these surveys provided a baseline that was used to revise curricula, determine the need for new academic programs, and develop new internship programs.

Summary of Survey Findings. The complete results of both surveys can be found on the HRCyber Website – <http://securitybehavior.com/hrcyber/>.

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’ feedback 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 representatives 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, and 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.

Activity 2. Conduct Developing a Curriculum (DACUM) workshop and develop a DACUM chart to create workforce-driven curricula.

Another key activity, conducted to address the cybersecurity workforce needs was a two-day Developing a Curriculum (DACUM) workshop in December 2016. This workshop was hosted by the Virginia Space Grant Consortium, a key partner on this project. A total of 10 employers participated in the workshop. The workshop brought together representatives from multiple cybersecurity businesses in the region to evaluate the tasks and duties associated with a Cybersecurity Analyst. The result was a DACUM chart that outlines the tasks required to complete the duties of: assess cyber risks, protect information assets, detect cybersecurity events, react to cybersecurity events, restore secure environment, increase security awareness, and maintain professional knowledge. This chart was used to revise curricula and in gaining a better understanding of the skills required to be taught to be a cybersecurity professional. A side benefit of this workshop was it allowed for various companies to interface with other organizations that they might not otherwise work with. This allowed the continuation of networking opportunities. Many of the participants in the DACUM workshop, who also contributed to the Cyber Saturday events, were interviewed for the

Cyber Workforce Videos, and became key contributors to most of the other HRCyber events and activities.

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

The third goal of HRCyber is to improve the coordination of academic programming between educational institutions and the regional workforce. This involves developing stronger ties between each educational institution and connecting these institutions with the workforce.

Activity 1. Conduct a Cybersecurity Counselor Workshop for K-12 schools and train college/university counselors and advisors on cybersecurity programs

The Virginia Space Grant Consortium hosted a Cybersecurity Counselor Workshop in February 2017 for twenty-seven K-12 school counselors, career coaches, and career and technical education (CTE) teachers for multiple school districts. Information was provided on education pathways leading to a career in cybersecurity and two industry partners provided a snapshot of the state of the cybersecurity job market in the region. A panel discussion from local K-12 school districts was held outlining the various cybersecurity courses being offered across the region. This workshop allowed different school districts to learn about the educational pathways available to their students and it was an excellent networking opportunity. They were able to develop relationships and see how the other school districts were preparing students for a potential cybersecurity career.

HRCyber also provided information to college/university counselors and advisors about the various educational cybersecurity pathways available, focusing on the articulation agreements with the community colleges and new programs that are being set to start in fall 2018. This information was provided during the Old Dominion University Advising Network conference in September 2017 and at the HRCyber Cybersecurity Workforce Summit in October 2017.

Activity 2. Create the HRCyber homepage and informational brochure.

To provide easy access and generate awareness about HRCyber and the state of cybersecurity within the region, a website was created. This site is the primary means of archiving information related to this project. The address of the website is: <http://securitybehavior.com/hrcyber/>. Material on the website was updated on an as needed basis and it included current events, news stories, links to alliance partners, cybersecurity resources, a link to the HRCyber Workforce Needs Survey, and links to key partners. There were over 5,600 hits on this site since launching in December 2016.

Another tool that was developed to share information regarding educational cybersecurity programs offered across the region was an information brochure (<http://securitybehavior.com/hrcyber/doc/HRCyberPromobroFINAL.pdf>). An infographic highlighting the various achievements of HRCyber was also created (http://securitybehavior.com/hrcyber/images/hr_cyber_infograph.png). Both of these tools were used to provide stakeholders with information on HRCyber and to celebrate the successes of this project. They proved to be useful for our partners to share with their stakeholders when discussing the value that HRCyber brought to the region.

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

The fourth goal of HRCyber is to strengthen the cybersecurity capabilities of the regional workforce.

Activity 1. Develop and produce cybersecurity career awareness videos.



The Virginia Space Grant Consortium (VSGC) developed five videos related to various cybersecurity career fields and workforce development. These videos are posted at www.vsgc.odu.edu/cyber and are available to the public. These videos were developed over several months and after 19 interviews were conducted with

partners and key stakeholders. Partners interviewed for the video series included NIST, NASA Langley Research Center, Peregrine Technical Solutions, Packet Forensics, G2-Ops, AERMOR, Newport News Shipyard, Sentara Healthcare, and Langley Federal Credit Union. Each video is approximately 10 minutes in length. Topics include Cybersecurity – The Big Picture; Career Pathways; Accessing the Cybersecurity Job Field; The Cybersecurity of Things; and Protecting and Serving. Since this video series was launched, it received over 4,000 visits. This video series can be used to augment instruction on the cybersecurity workforce and highlight what cybersecurity professionals do on a daily basis. It has been used by high schools to entice students towards this career field.

Activity 2. Conduct Cyber Saturday series for high school students and parents.

The Virginia Space Grant Consortium held two Cyber Saturday events in March 2017. The first was hosted by Thomas Nelson Community College and was attended by 43 students and 22 parents. The second was hosted by Tidewater Community College and the Advanced Technology Center in Virginia Beach and had 49 students and 19 parents attend. Both events had two tracks – one for students engaging them in various

activities and one for parents with information sessions focused on career opportunities, cybersecurity programs, and ways to protect their family. Partners from the FBI, Sentara Healthcare, Newport News Shipyard, Sera Brynn, G2Ops, and Packet Forensics participated in both events. Some of the student activities included Wi-Fi Password Cracking, Capture the Flag, Foot Printing, Port Scanning, and Cyber Physical Systems (including drones). Both of these events provided an opportunity for both parents and high school students to be exposed to the value of cybersecurity and a benefits of a career in this field. It is expected that the Virginia Space Grant Consortium will continue these events as part of the normal high school programs.

Activity 3. Provide Virginia Beach high school interns to regional cybersecurity employers.



Advanced Technology Center, Virginia Beach, recognizes companies that hosted high school students in a 30-hour cybersecurity internship.

One of the most successful activities completed by HRCyber was the establishment of a high school cybersecurity internship program. This program was run by the City of Virginia Beach Public Schools, Technical and Career Education department. Students participating in this program were selected from several classes: Cybersecurity & Network Administration, CISCO Networking, Computer Systems Technology, and Software & Game Development. The internship program consisted of 30-hours of paid cybersecurity work with local cyber companies. HRCyber provided \$300 for each

student (\$10/hour). Twenty students were selected for this program. The students who participated were able to successfully complete all tasks assigned during their internships. Several were asked to remain on for additional time and one was offered a part-time position after completion of the internship. The Advanced Technology Center held an appreciation breakfast that highlighted the businesses and student interns.



G2OPS CEO, Tracy Gregorio, presents certifications of appreciation to two Virginia Beach high school students after completing their 30-hour cybersecurity internships.

All of the feedback from both the students and the businesses show that this program was very successful. G2OPS, one of our cybersecurity industry partners, said this about the work completed as part of the internship program:

“G2OPS hosted 3 interns in April 2017. These interns aided in the completion of numerous cybersecurity projects including validating baseline architectures and configurations, introducing Intrusion Protection capabilities within a Local Area Network, and providing assistance satisfying regulatory compliance requirements.” VP & Chief Security Strategist, G2OPS

The model created by Virginia Beach is now being used by several other K-12 districts in the region for the GO Virginia funded Virginia Cyber Alliance and they will start placing students during the 2018-2019 school year.

Activity 4. Provide internships and apprenticeships to regional cybersecurity employers.

Another big accomplishment was the establishment of cybersecurity internships for college students. Through the VSGC’s Commonwealth STEM Industry Internship program (CSIIP), HRCyber worked with local cybersecurity employers to identify internship opportunities and to place interns within their companies. Twenty-six interns were placed with various companies across the region, with eight students placed at Sentara Healthcare in a new internship partnership. These internships were very successful and provided the students with valuable experience in the cybersecurity workforce, something that employers specifically said they were looking for during our cybersecurity workforce survey. This initiative is being continued under the Go Virginia funded project (Virginia Cyber Alliance) with the goal of placing 20 interns per year.

“The internship has been a fantastic avenue of experience! I have learned so much in the six months I have been there and I have become very confident in the roles of a security analyst.”
ODU Intern with Sentara

Activity 5. Host a cybersecurity workforce development summit in fall 2017 and participate in regional cybersecurity summits and conferences.

One positive outcome of this project was the linking of multiple cybersecurity stakeholders within the region together at various meetings and events. Starting in November 2016, HRCyber participated in a series of round table discussions related to growing the cybersecurity workforce in the region. These discussions were hosted by the City of Virginia Beach Economic Development Office. As a result of these meetings several new employers became involved with HRCyber. In September 2017, HRCyber participated in a panel discussion entitled “Cyber Solutions to the Growing Threat,” that was also put together by the City of Virginia Beach for a delegation from the Danish Embassy. In addition to these, HRCyber co-sponsored the Thomas Nelson Community College 2017 Regional Cybersecurity Conference: Cybersecurity and the Internet of Everything.



HRCyber Cybersecurity Workforce Summit Educational Pathway panel discussion.

Finally, HRCyber hosted a Cybersecurity Workforce Summit in October 2017. This summit brought together over 100 participants representing public school districts, community colleges and universities, local, state and federal organizations, non-profits and cybersecurity businesses. The primary purpose of the summit was to highlight the achievements of HRCyber and to provide information to the public on cybersecurity educational programs and employment opportunities in the region. A series of panel discussions

were held focusing on educational pathways from high school through four-year universities, internships and apprenticeships, industry and educational cybersecurity surveys, activities conducted by the Virginia Space Grant Consortium, and finally a workforce and economic develop panel. State Senator Frank Wagner was the keynote speaker.

The end results of the various business round table meetings and conferences were: the expansion of the cybersecurity ecosystem within Hampton Roads by linking stakeholders together, providing various stakeholders with information on what HRCyber is doing to help fill the cybersecurity workforce gap, and showing businesses and educational institutions ways to partner on finding qualified candidates to fill the cybersecurity workforce needs within Hampton Roads.

Other Highlights and Accomplishments:

Additional grant and funding opportunities.

As result of the positive impact HRCyber Alliance had across the region, over \$3.2 million in additional grants funds were awarded to Old Dominion University and additional funding opportunities are being developed across all educational institutions.

In January 2018, Old Dominion University's Virginia Modeling and Simulation Center (VMASC) was awarded a major grant through the Commonwealth of Virginia Go Virginia Initiative. This grant was developed through cooperation with HRCyber and Old Dominion. The Go Virginia State Board approved this project along with four others during their December 12, 2017 meeting. The HRCyber Co-Lab project was approved for two years of funding totaling \$1,285,426 – \$642,713 per year. This funding will allow the work started under HRCyber to continue to develop and expand the cybersecurity ecosystem within Hampton Roads and other regions across Virginia and to formalize the organization. The project will focus on four pillars: 1) outreach through a Virginia Cyber Trail, which will allow collaboration between educators, researchers, employers across Virginia; 2) innovation through industry collaborations by connecting industry to academic and federal labs and technologies to accelerate innovation and technology; 3) creation of a Cyber Arena that will be a highly-advanced collaboration hub providing a virtual environment for stakeholders to test and analyze cybersecurity techniques and new technologies; and 4) jobs creation and workforce development through Digital Entrant programs that take current internships and apprenticeships and expand them to accelerate placement of transitioning military and graduates to open cybersecurity jobs. Please use this site to see the Go Virginia press release regarding this and the other approved projects – <http://govirginia.org/2017/12/go-virginia-board-approves-first-grants/>.

Old Dominion University faculty also submitted proposals and were awarded grants related to national cybersecurity initiatives, including the following:

- Engineering Management and Systems Engineering researchers were awarded \$115,000 through The National Security Agency Cybersecurity Core Curricula Development Grant to develop a course in cybersecurity risk management to support the President's Cybersecurity National Action Plan.
https://www.odu.edu/news/2017/6/nsa_grant#.WjKNh2eWypo
- The Department of Electrical and Computer Engineering was awarded a three-year \$360,000 NSF Research Experience for Undergraduates (NSF REU) program. This grant provides ten undergraduate students from across the country with research

opportunities in cybersecurity during the 10-week summer program.

https://www.odu.edu/news/2017/4/nsf_undergrad_research#.WjKM7GeWypo

- Old Dominion University was awarded a multi-year National Science Foundation grant of \$500,000 to address cybersecurity workforce shortages through increased educational and training opportunities. This grant will continue some of the work started with HRCyber's emphasis on developing articulation agreements and educational pathways to assist in filling the multitude of open cybersecurity positions within the region and state. <https://www.odu.edu/about/odu-publications/insideodu/2017/11/30/topstory2>
- Old Dominion University was awarded a five-year National Science Foundation grant of \$1,000,000 to provide 18 scholarships to low-income students in the cybersecurity program as part of the S-STEM Track program. http://www.odu.edu/news/2018/4/cybersecurity_grant?utm_source=homepage&utm_medium=interactive&utm_campaign=HP-Slider#.WstxEWeWypo

Old Dominion also has two NSF grants pending:

- The Scholarship for Future Workforce in Information Security, Analytics and Entrepreneurship, is a 5 year proposal totaling \$1,000,000. This project will create a scholarship fund for up to 60 students per year (\$10,000 each) pursuing Information Systems and Technology or Enterprise Cybersecurity degree programs.
- SaTC (Education): An interdisciplinary examination of cybersecurity pathways between regional higher education institutions, is a 2 year project totaling \$300,000. This project will study and evaluate the success of the NICE RAMPS grant (HRCyber) and further its efforts to strengthen the pathways established as part of the NICE RAMPS grant.

New Academic Programs.

Starting in fall 2017, Old Dominion University began offering two new Bachelor of Science Interdisciplinary Studies majors in cybersecurity – Cybercrime and Cyber Operations. In addition to these two new majors, ODU also started a Bachelor of Science in Business Administration–Information Technology, with a focus on enterprise cybersecurity. In fall 2018, ODU will offer a Master of Science Cybersecurity degree.

While not a new program, Old Dominion University's Interdisciplinary Bachelor of Science degree with a major in Cybersecurity has seen exponential growth since first being offered in fall 2015. It started with 11 majors that semester and it is estimated that it will have over 230 starting in fall 2018; in addition, the first 16 students graduated from this program in spring 2018. There was also growth in the cybersecurity minor during this same time: 10 students in fall 2015 to 90 in fall 2017. This continued growth shows the program's value in providing qualified employees to the cybersecurity workforce and it is expected that this growth will accelerate now that the articulation agreements in cybersecurity are active.

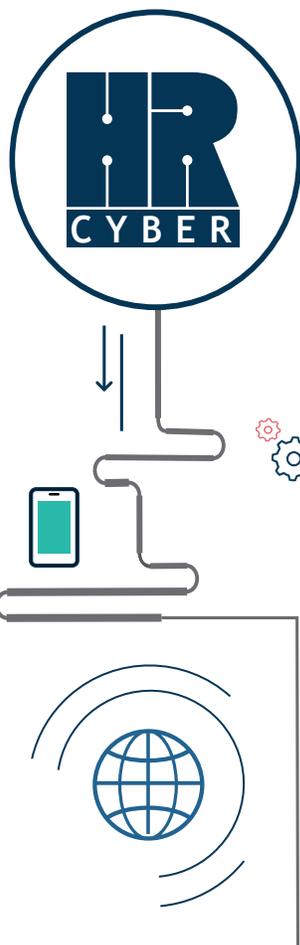
Other Cybersecurity initiatives/Achievements in the region.

Regent University opened a state-of-art cyber range training center in a partnership with Cyberbit Ltd., in October 2017. <https://www.regent.edu/news-events/regent-university-launches-state-art-cyber-range-training-center-cyberbit/>

Thomas Nelson Community Colleges received designation as a National Center of Excellence in Cyber Defense Education in August 2017. <http://tncc.edu/news/thomas-nelson-community-college-receives-designation-national-center-excellence-cyber-defense>

For additional information on HRCyber accomplishments please visit the HRCyber Alliance webpage at <http://securitybehavior.com/hrcyber/> or contact Dr. Brian Payne (bpayne@odu.edu) or John Costanzo (jcostanz@odu.edu).

Special thanks to NIST/NICE for funding this project and to all of HRCyber's partner organizations for your efforts in making this project a great success.



HAMPTON ROADS CYBERSECURITY EDUCATION, WORKFORCE AND ECONOMIC DEVELOPMENT ALLIANCE (HRCYBER)

Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber) is a partnership between educational institutions, government agencies, non-profit organizations, and private employers focused on developing educational pathways from high school through community college to four year institutions and continued professional development providing a capable and fully trained cybersecurity workforce for the region.

HRCyber aligns regional educational and skills development offerings to the workforce practices and activities of business and non-profit organizations within the Hampton Roads region with the specific goal of supporting local economic development and job growth via establishment of a multi-stakeholder Alliance. This is achieved by addressing cyber workforce needs and increasing the pipeline of students pursuing cybersecurity careers from high schools, community colleges, and universities.

The goals and activities of HRCyber parallel the NICE strategic plan and include:

- GOAL 1...> Coordinate educational pathways among public high schools, community colleges and four year universities
- GOAL 2...> Gather, organize and make available information from the regional workforce about the knowledge and skills needed in cybersecurity programs using the NICE-identified knowledge, skills, and abilities framework and revise curricula where needed
- GOAL 3...> Coordinate academic programming among educational institutions and workforce to ensure relevance and linkages to the NICE Framework
- GOAL 4...> Strengthen the cybersecurity capabilities of the regional workforce which includes a large complex of military bases, joint forces, federal facilities, and defense-related businesses, as well as healthcare companies

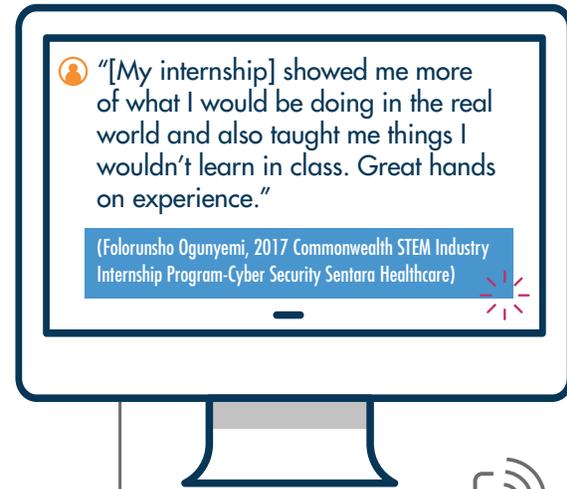


CURRENT OUTPUTS FROM HRCYBER'S EFFORTS INCLUDE THE FOLLOWING:

- Creation of a website that serves as a portal where regional stakeholders can learn more about cybersecurity in the region
- Creation of an infrastructure including multiple stakeholders from education, workforce development, industry, governmental agencies, and non-profits
- Completion of 3 Articulation agreements making it easier for students to move between higher education institutions in the region (TCC & ODU, TNCC & ODU, NOVA & ODU)
- Completion of 5 Career videos for individuals interested in learning more about cybersecurity
- Completion of a curriculum matrix from an occupational analysis of a cybersecurity analyst in the region
- Completion of a Cyber Counselor Workshop for high school career coaches and guidance counselors
- Completion of 2 Cyber Saturday Workshops for high school students and parents interested in learning more about cybersecurity education and career potential
- Expansion of the ODU cybersecurity virtual laboratory for training regional high school and college students
- Completion of the HRCyber Workforce and Economic Development Summit

of visits for the HRCyber website

▶ 5686 ◀



Partners	42 and growing
Interns	13 VA Beach high school students 26 college students
Credits saved by Articulation agreements	40+ credit hours 1.5 years of school
Tuition saved by Articulation agreements	\$15,000 in tuition \$1,500 in books
Individuals attending our summit	100
HRCyber partners supporting continuation	90% of partners
Students accessing virtual lab	200+
Counselors and advisors trained	55
High school students and parents participating in Cyber Saturday	100 students 50 parents

For more information visit: securitybehavior.com/hrcyber/

Funding for this project was provided by the Department of Commerce National Initiative for Cybersecurity Education (NICE), Regional Alliances and Multistakeholder Partnership to Stimulate (RAMPS) Cybersecurity Education and Workforce Development program.

