BHEF BUSINESS-HIGHER EDUCATION FORUM

Case Study: University System of Maryland

Building a Diverse Cybersecurity Talent Ecosystem to Address National Security Needs

USM TEAMS WITH REGIONAL EMPLOYERS TO CREATE INNOVATIVE PATHWAYS TO JOBS

Cybersecurity Talent Challenges

The University System of Maryland (USM), a BHEF member, is surrounded by employers—businesses and government agencies—with an urgent demand for highly skilled cybersecurity professionals.

40,000 JOB OPENINGS FOR CYBERSECURITY POSITIONS IN THE WASHINGTON, D.C. METRO AREA IN 2017

While the demand for cybersecurity professionals has been high, the supply has been inadequate. In 2015, more than 200,000 cybersecurity positions in the U.S. went unfilled.

According to survey data, employers in the Washington, D.C. region consider it particularly difficult to find qualified candidates for cybersecurity jobs. The challenge is partly rooted in the level of education and experience cited as a minimum qualification.

84% OF CYBERSECURITY JOB POSTINGS IN THE WASHINGTON, D.C. AREA REQUIRE AT LEAST A BACHELOR'S DEGREE AND AT LEAST THREE YEARS OF RELEVANT WORK EXPERIENCE

However, when assessing the environment, USM found:

- Pathways into cybersecurity careers had not been clearly defined.
- The field is evolving rapidly, making it difficult for higher education to keep pace.
- The only way to meet this demand at scale is to collaborate with business and government to develop pathways and to attract more women and members of underrepresented groups.

USM's Solution

In 2012, BHEF was awarded a grant to work with USM and Northrop Grumman Corporation to develop undergraduate pathways in cybersecurity. A few years later, USM built on this work by collaborating with businesses and government agencies. The goal: develop cybersecurity pathways on multiple campuses to build a diverse regional cybersecurity talent ecosystem.

USM's efforts grew out of a series of planning activities, studies, and regional workforce assessments highlighting the need to sharply increase graduation rates in STEM fields, particularly among women and underrepresented minorities—and particularly in cybersecurity. This focus on STEM and cybersecurity led USM to pursue a coordinated system-level effort.

USM and MITRE

In 2014, USM partnered on a system-level basis with MITRE Corporation, which operates a federally funded R&D center dedicated to cybersecurity. Through this partnership, MITRE gained access to the cybersecurity expertise of USM's faculty and USM students gained access to cybersecurity internships at MITRE.

USM also recognized that to diversify the region's cybersecurity ecosystem, there were advantages in having institutions develop their own pathways, consistent with each institution's strengths.

USM now offers a variety of academic programs that prepare students for careers in cybersecurity. These programs include:

- Bachelor's degrees on residential campuses
- Online programs that serve working adults
- Competency-based certification programs

To ensure that USM graduates have the skills that employers need, these programs were all designed in partnership with companies and government agencies.

USM's strategic partnership with BHEF has strengthened the linkages between industry and higher education, driving innovative undergraduate programs to help meet critical workforce needs. . . . Together, USM and BHEF are helping position Maryland at the epicenter of cybersecurity.

Robert L. Caret, Chancellor, University System of Maryland (former)

University Efforts

Cybersecurity-focused efforts at institutions in the USM system are summarized below.

University of Maryland, College Park (UMD)

- USM's flagship research university.
- Partnered with Northrop Grumman to develop nation's first honors program in cybersecurity.
- Launched Advanced Cybersecurity Experience for Students (ACES) in 2012. ACES includes:
  - A living-learning program (2 years) for 75 new students per year.
  - A minor in cybersecurity (2 years) for 50 new students per year.
- Northrop Grumman has supported ACES through funding and curriculum design, and by having employees serve as adjunct faculty and mentors.
- UMD also launched the Maryland Global Initiative for Cybersecurity and is home to the Maryland Cybersecurity Center.

University of Maryland, Baltimore County (UMBC)

- In 2013, launched Cyber Scholars, a high-touch, resource-intensive program, initially supported by Northrop Grumman.
- Cyber Scholars includes Cyber Associates (full program participants) and Cyber Affiliates (participate as space allows).
- Cyber Scholars participate in internships, research, and a Cyber Practicum.
- 70% are women; 30% are underrepresented minorities.
- Home to a cyber incubator for cybersecurity startups.

University of Maryland University College (UMUC)

- Dedicated to serving adult learners, mainly through online programs.
- Designed cybersecurity curriculum with input from companies and government experts.
- Offers both bachelor's and master's degrees in cybersecurity.
- In its first year, 10,000 students enrolled in UMUC's cybersecurity programs.

Bowie State University

- A historically black college and university (HBCU) focused on science and technology.
- Participated in a grant to develop pathways to increase participation of underrepresented minorities in the cybersecurity workforce.
- Offers two bachelor's programs focused on cybersecurity.
- Has established experiential learning, with laboratories and internships.

Towson University

- Pioneered the first cybersecurity track in Maryland; one of the first in the US.
- Five cybersecurity programs at the undergraduate and graduate levels.
- Conducts leading-edge cyber research.

Community college partners have also been important. In just one year, more than 3,000 community college students transferred into UMUC's undergraduate cybersecurity programs.

Early Returns

USM has provided cybersecurity opportunities for full- and part-time students, veterans and active duty service members, women, and members of underrepresented groups.

In the first few years since making cybersecurity a priority, USM institutions awarded more than 10,000 bachelor's degrees in cybersecurity-related programs and many students have participated in internship and work-based learning experiences. Graduates are in demand for high-paying jobs, with the vast majority earning at least $70,000 in their first position.

Recommendations

In analyzing USM's experience working to build a diverse cybersecurity talent ecosystem and in speaking with multiple people throughout the USM system, as well as employers, BHEF developed the following recommendations for others seeking to build a talent ecosystem.

Primary Recommendation

Expand and improve student cyber work-based learning experiences so students can gain the experience that employers desire before entering the workforce.

Recommendations for Policymakers

- Continue to formally assess workforce needs at the state level in order to rapidly respond to new opportunities to create in-demand programs.
- Use convening power to set a workforce-development agenda in motion.
- Prioritize cybersecurity in state government.
- Fund public higher education to enable strategic workforce development.

Recommendations for Higher Education Leaders

- Accelerate program development by leveraging institutional strengths and existing partnerships.
- Create programs that reflect and reinforce the institution's niche.
- Ground program curricula in practitioner expertise.
- Promote meaningful engagement between students and business and government partners.
- Ensure partnerships are mutually beneficial.
- Invest in efforts to attract and retain students from underrepresented groups, especially women.
- Identify and remove barriers to collaboration.

Recommendations for Business Leaders

- Commit to deep engagement with academic partners.
- Be open to talent from nontraditional pathways.
- Engage all sectors in cyber workforce development.
- Cultivate and recruit a diverse workforce.

Additional Resources

See the full case study of USM's experience Building a Diverse Cybersecurity Talent Ecosystem. Also, see the BHEF website and BHEF's many publications.