

SUMMARY OF ITEM FOR ACTION
INFORMATION OR DISCUSSION

TOPIC: USM Cyber Programs Workforce Development Case Study

COMMITTEE: Economic Development and Technology Commercialization

DATE OF COMMITTEE MEETING: Thursday January 25, 2018

SUMMARY: The Business Higher Ed Forum (BHEF), a national organization representing the talent needs of business and industry, will present the preliminary findings of their Cybersecurity and STEM program case study that was conducted on behalf of the University System of Maryland. Addressing the growing demand for cybersecurity talent is a priority of USM and its institutions. BHEF's case study profiles system-wide efforts, as well as the approaches adopted by four campuses: The University of Maryland, College Park; the University of Maryland, Baltimore County; the University of Maryland University College; and Bowie State University to develop and attract a larger and more diverse array of students into this growing field. The study also focused on best practices around the country in addressing the talent demand, to include workplace-based learning, technical certification and internship programming.

ALTERNATIVE(S): This item is for information purposes.

FISCAL IMPACT: There is no fiscal impact

CHANCELLOR'S RECOMMENDATION: n/a

COMMITTEE RECOMMENDATION:

DATE:

BOARD ACTION:

DATE:

SUBMITTED BY: Tom Sadowski (410) 576-5742



University System of Maryland Case Study

*Board of Regents Committee on Economic
Development and Technology Commercialization*

January 25, 2018

Creating Solutions. Inspiring Action.®

About the Business-Higher Education Forum

The Business-Higher Education Forum (BHEF) is a membership organization of CEOs, college and university presidents, and other leaders who collaborate and form strategic partnerships to develop a highly skilled future workforce.

BHEF Value

BHEF members work together to:

- Produce a diverse, highly skilled talent pool to meet regional workforce demands;
- Create pathways to increase access to education;
- Improve alignment between education and the workforce.

BHEF members gain value from:

- Opportunities to form purposeful peer relationships between business and education counterparts;
- Access to BHEF's expertise and regional work;
- Insights on engaging diverse communities, best practices for collaboration, and case studies.

**Builds Action-Oriented
Relationships**



**Strengthens Members' Workforce
Initiatives**

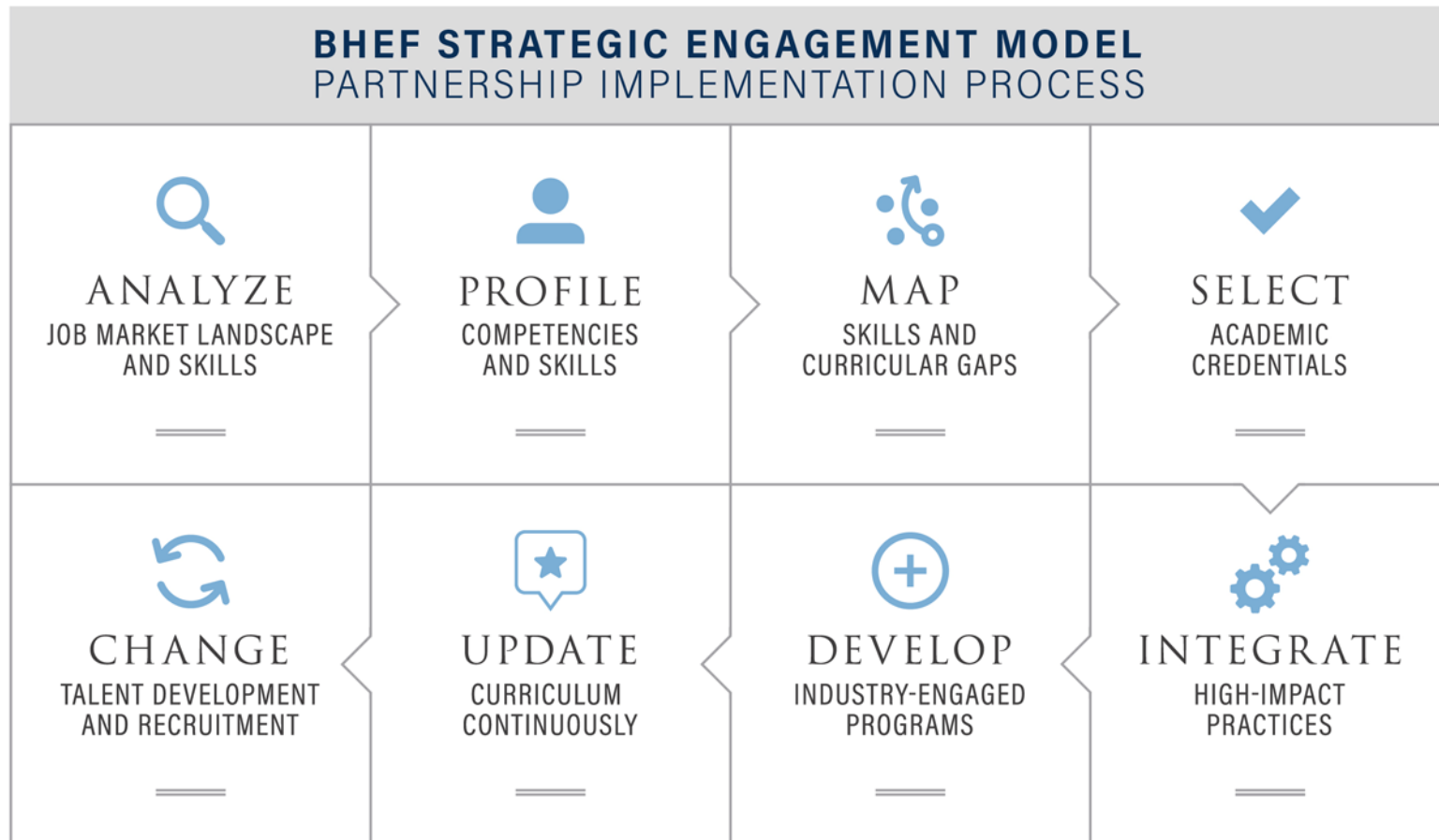


**Helps Practitioners Navigate
Emerging Trends and Challenges**

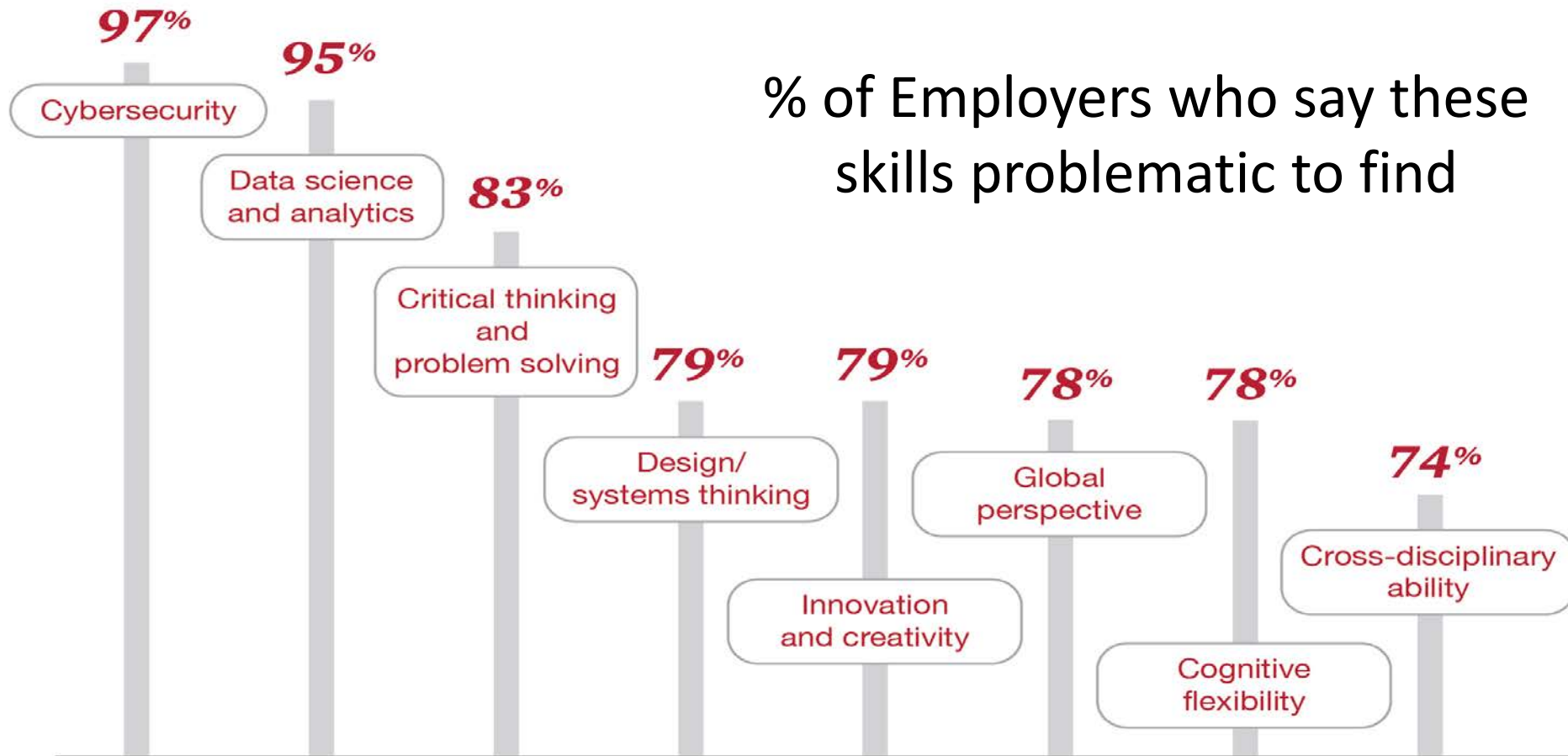


Strategic Partnership Implementation Process

BHEF partners with academic and business members and utilizes a rigorous methodology to assess workforce needs, identify curricular gaps, and co-design programs and courses to create and deepen existing partnerships.



Hardest to Hire Skills



Source: Business Roundtable (2017).

Cybersecurity

BHEF has served as a leader in defining the cybersecurity talent landscape and working with members to launch new programs and partnerships to meet industry's changing demands.

- Conducted Burning Glass analysis for Massachusetts, NYC, DC, Maryland, and Virginia
- DC, Maryland, and Virginia
 - Lead partners include Virginia Governor's Office, NVTC, ONR, AIA, Sloan Foundation, USM, UVA, VT, and GWU
 - Future Cyber Leaders Program
 - Co-hosted Commonwealth Conference on Cyber and Education and Virginia Governor's Cyber Physical Systems Summit
 - Mini grants for new cyber pathways
- Facilitated new programs in cyber at Cal Poly; Illinois State; Miami Dade College; Northeastern; San Jose State; University of Maryland, College Park; University of Maryland, Baltimore County; and University of Massachusetts
- Partner with NSA, NIST, and NGA around national efforts

USM Responds to Maryland's Cybersecurity Workforce Demand

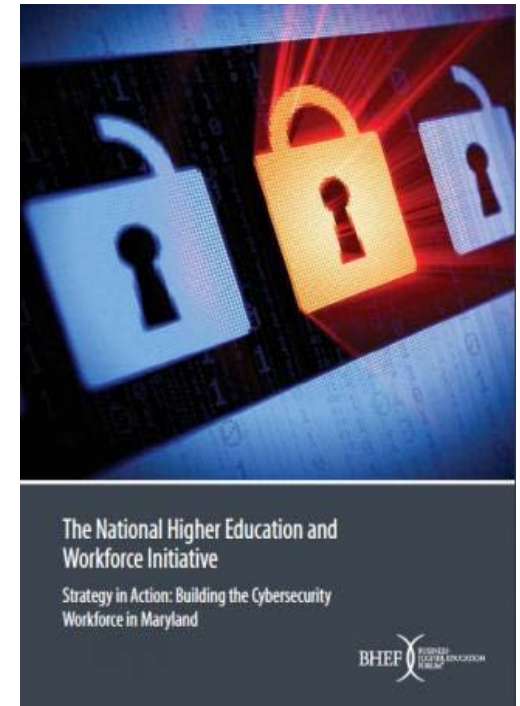
USM's involvement in cybersecurity was catalyzed through the Governor's STEM Task Force, which resulted in an August 2009 report entitled *Investing in STEM to Secure Maryland's Future*.

- Cyber was identified as an area of significant opportunity for the state
- Led to a USM self-study by the Maryland Cybersecurity Task Force of USM with two key recommendations from a 2011 report
 - Enhance and extend higher educational offerings related to cyber security and information assurance
 - Establish more partnerships among education and government and private industry and leverage the resources available
 - Also cited the various roles that institutions in the System were playing—or could play—in cyber
- Four campuses were designated as Centers of Academic Excellence or Research Excellence in Information Assurance by the NSA and the DHS
- With the support of a \$400,000 grant awarded to BHEF by the Alfred P. Sloan Foundation in 2012, USM and UMD worked with Northrop Grumman Corporation and BHEF to develop an initiative that brought together the Maryland Governor's office, state university system, business leaders, and other stakeholders to expand the regional cybersecurity workforce
- BHEF provided USM with a sub-award of \$135,000 for research and seed funding on multiple campuses

Facilitating the Development of New Programs

University of Maryland ACES Honors Program

Northrop Grumman-University of Maryland partnership created the nation's first cyber honors program, and the long-term partnership has grown the program to meet national security needs.



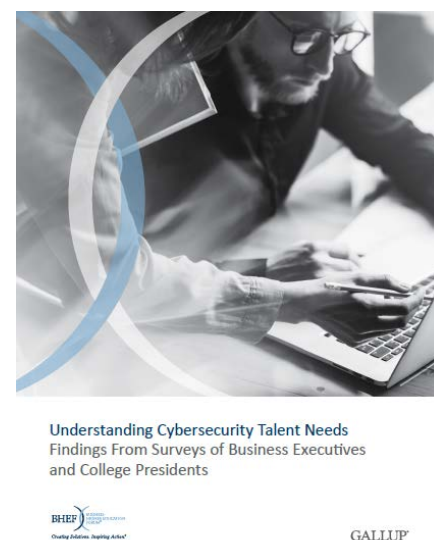
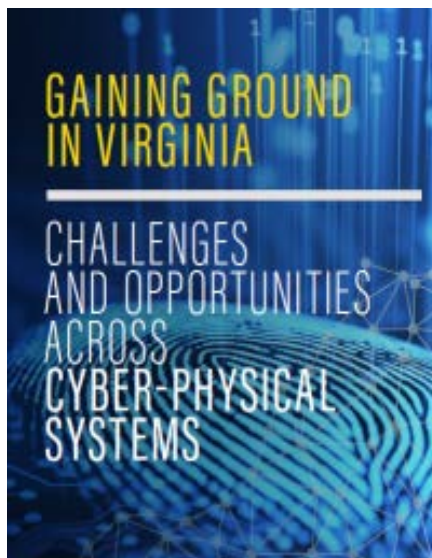
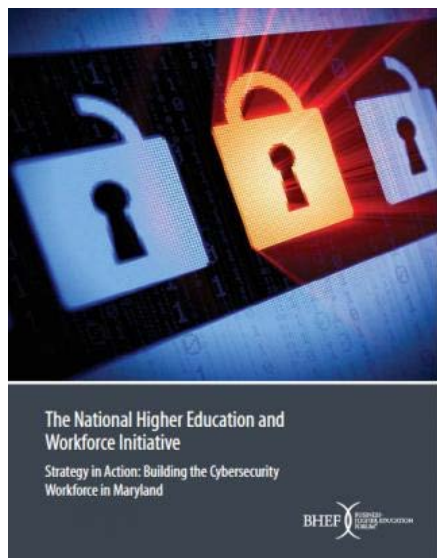
UMBC Cyber Scholars Program

The goal is to prepare the next generation of cybersecurity professionals, with a focus on increasing the participation of women and other underrepresented groups.

- Launched in 2013
 - Directed by the UMBC Center for Cybersecurity and run in partnership with UMBC's Center for Women in Technology
 - Goal to support 15-20 students annually
 - \$1 million grant from Northrop Grumman Corporation provided major start-up support for the program
- Program features
 - Fosters community through common on-campus living-learning housing, events, and activities
 - Special introductory practicum/seminar in freshman year and technically focused cybersecurity courses in addition to computing sciences courses over next four years
 - Participation in at least one cybersecurity internship at a local company or government organization
 - Assigned a faculty mentor who is pursuing cybersecurity-related research of their own
 - Opportunity to carry out original cybersecurity research in their field early in their academic careers

BHEF Cybersecurity Reports

BHEF captures and disseminates findings and key insights through the development of publications and case studies.



Case Study Background

Working closely with the USM and institutions within the System, as well as with corporate and government partners in their undergraduate cyber programs, BHEF developed a comprehensive case study of USM's response to Maryland's cyber workforce needs.

- Documents the ongoing development of undergraduate cybersecurity pathways on multiple campuses within the USM
- Provides third-party validation of USM's commitment and impact on Maryland's cyber workforce, which can be used with the Governor, legislators, members of the Board of Regents, and benefactors
- Conducted background research and gathered information and insights from over 20 individuals to inform the case study
 - Business and government partners included The Greater Washington Partnership, The MITRE Corporation, National Institute of Standards and Technology, National Security Agency, Northrop Grumman Corporation, and the State of Maryland
 - University System of Maryland campuses included Bowie State University, University of Maryland, Baltimore County, University of Maryland, College Park, and University of Maryland University College
- Scheduled for release in March 2018

Challenges in Cyber Workforce Development

USM is surrounded by a dense network of businesses and government agencies that urgently need access to a larger pool of highly skilled cybersecurity professionals.

- In 2017, employers in the Washington, DC metro area posted more than 40,000 job openings in cybersecurity-related positions, and this number is only expected to grow.
- Furthermore, cybersecurity jobs request significant experience and advanced credentials, which can drive talent away from the region.
 - 84% of cybersecurity jobs postings request a Bachelor's degree or higher
 - 84% required at least 3 years of experience and 45% of cybersecurity jobs request at least 6 years of experience
 - 48% of cybersecurity jobs request an industry certification. CISSP and Security+ are the most commonly requested.
- Meeting demand at this scale will be impossible unless many more people, including women and underrepresented minorities, pursue careers in cybersecurity.
- Pathways into this relatively young field are not yet clearly defined.
- This picture is further complicated by rapid evolution in the field.

Work-Based Learning

Through its cybersecurity programs, USM seeks not only to prepare graduates for successful careers in the field, but also to address the shortage of cybersecurity professionals in the region. Work-based learning experiences, and internships in particular, play a critical role in meeting both of these objectives.

- Internships are a high-impact practice in higher education that provide students with opportunities to apply their emerging knowledge and skills in real-world settings.
- They also serve as opportunities for students to explore potential employers—and for employers to evaluate potential full-time employees.
- USM and its campuses frequently communicate with partner organizations about internships, to learn whether students are demonstrating the expertise that employers expect and to use that feedback to make any needed adjustments in the curriculum.
- For employers, internship programs are a valuable strategy for recruiting future full-time employees.
- Interns build relationships with colleagues and become familiar with the organizational cultures at their internship sites.

Recommendations for University Leaders

These lessons learned through USM's ongoing efforts may be helpful to university leaders interested in developing new cyber pathways on their campuses.

- 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 win-win
- Invest in efforts to attract and retain students from underrepresented groups
- Identify and remove barriers to collaboration

Recommendations for Business Leaders and Policymakers

These lessons learned through USM's ongoing efforts may be helpful to business leaders and policymakers who may be interested in supporting similar efforts.

Business Leaders

- Commit to deep engagement with academic partners
- Be open to talent from nontraditional pathways

Policymakers

- Engage academia and industry in efforts to understand workforce needs and opportunities
- Use convening power to set a workforce development agenda in motion
- Fund public higher education to enable strategic workforce development

Contact Information



Thank you. If we can provide additional information, please contact us:

Steve Barkanic

Senior Vice President and Chief Program Officer |
Steve.Barkanic@bhef.com | 202-367-2422

Janet Chen

Director | Janet.Chen@bhef.com | 202-367-2350