The National Higher Education and Workforce Initiative

Strategy in Action: Building the Cybersecurity Workforce in Maryland

BHEF BUSINESS-HIGHER EDUCATION FORUM®

BHEF Staff

Brian K. Fitzgerald
Chief Executive Officer

Stephen Barkanic
Senior Vice President and Chief Program Officer

L. Isabel Cárdenas-Navia
Director of Emerging Workforce Programs

Jeanne B. Contardo
Senior Advisor

Karen Elzey
Vice President of Policy

Debbie Hughes
Director of Higher Education and Workforce

Erica Kashiri
Director of Policy and Corporate Innovation

Danielle Troyan
Vice President of External Relations

BHEF BUSINESS-HIGHER EDUCATION FORUM®

Creating Solutions. Inspiring Action.®

The Business-Higher Education Forum (BHEF) is the nation's oldest organization of business and higher education executives dedicated to advancing innovative solutions to U.S. education and workforce challenges. Composed of Fortune 500 CEOs, prominent college and university presidents, and other leaders, BHEF addresses issues fundamental to our global competitiveness. BHEF and its members drive change locally, work to influence public policy at the national and state levels, and inspire other leaders to act.

Business-Higher Education Forum
2025 M Street NW, Suite 800
Washington, D.C. 20036

For more information about BHEF, visit *www.bhef.com*.

The National Higher Education and Workforce Initiative

Strategy in Action: Building the Cybersecurity Workforce in Maryland

BHEF BUSINESS-HIGHER EDUCATION FORUM®

Creating Solutions. Inspiring Action.®

Letter from the CEO

Dear Colleagues,

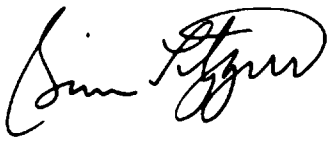
The United States faces two critical challenges that intersect at the nexus of business and higher education: (1) increasing the persistence of students, particularly women and underrepresented minorities, in key fields of emerging importance to U.S. economic competitiveness; and (2) aligning undergraduate education with the demands of the emerging and future work place. The leadership provided by the business and academic members of the Business-Higher Education Forum (BHEF) provides a unique opportunity to address these challenges.

Powerful insights from five years of intensive project development and system dynamics modeling have informed BHEF's work to develop, deploy, and scale a new model of strategic business engagement in higher education that addresses the nation's highest demand workforce needs. The model is operationalized through the National Higher Education and Workforce Initiative (HEWI), which leads business and higher education to move from traditional transactional relationships to collaborations that address high-priority workforce needs in ways that are more innovative, strategic, and mutually beneficial.

HEWI is predicated on the value of investing in coordinated, strategic, long-term partnerships to increase the persistence of undergraduate students toward attaining a degree and entering the 21st century workplace in emerging fields that are critical to the nation's sustained economic prosperity. The power of such partnerships is acutely evident in BHEF's work in Maryland to bring business, higher education, and other key stakeholders together to address the state's need for a workforce highly skilled in cybersecurity. This report documents significant progress to that end, including the creation of major new academic programs at the University of Maryland, College Park, and the University of Maryland, Baltimore County, and the establishment of state and national cybersecurity networks focused on programs and credentials at the undergraduate level.

BHEF is also scaling HEWI through business-higher education partnerships around the country that are addressing critical workforce needs in other fields such as computer science, data science and analytics, engineering, and information technology and in industry sectors such as advanced manufacturing, aerospace and defense, agriculture, energy, and financial services. Through this work, BHEF members and many others are deeply engaged in implementing evidence-based workforce solutions designed to help undergraduates succeed in key emerging fields. We hope this report provides a tangible example of the successful deployment of BHEF's strategy and a blueprint for other organizations to use when creating their own strategic partnerships between business and higher education.

Sincerely,



Brian K. Fitzgerald, Ed.D.
Chief Executive Officer
Business-Higher Education Forum

Executive Summary

The United States faces pressing national security and competitiveness challenges that are rooted in a significant shortage of highly educated and skilled employees, particularly in vital emerging cross-disciplinary fields such as computer science, cybersecurity, data science and analytics, engineering, and information technology. Assuring dynamic growth in the U.S. economy in the 21st century will require a workforce with mastery of core content knowledge and applied experiences in these fields.

To address this challenge, BHEF launched the National Higher Education and Workforce Initiative (HEWI, or the Initiative), deploying a model of strategic business engagement in higher education to meet the highest priority workforce needs. Through the Initiative, BHEF plans, launches, and assesses projects, partnerships, and scaling strategies that are designed to enable business and higher education to move from transactional engagement in low-touch, piecemeal activities to strategic, long-term partnerships that align undergraduate education with workforce needs. A five-year effort, HEWI involves regional projects in many disciplines that are focused on academic-business partnerships as well as a national effort to disseminate insights gained from the regional projects and to adapt and tailor effective practices in other settings and contexts.

With work that started in 2012, BHEF has achieved particular success in operationalizing the Initiative in Maryland around cybersecurity. Leveraging its membership of corporate CEOs, university presidents, and government agency leaders, BHEF partnered with the University System of Maryland (USM) to build a system-wide response to the state's (and nation's) cybersecurity workforce challenges. As a result, BHEF is playing a pivotal leadership role in sparking the innovations that have created and adapted premier undergraduate programs in cybersecurity at four USM institutions with regional businesses, government agencies, two-year colleges, and other stakeholders as partners. Serving as the linchpin in this effort, BHEF began by bringing the right partners to the table. With funding from the Alfred P. Sloan Foundation, BHEF sponsored research, provided vital data analysis, participated in program planning and development, provided convening support and evaluation expertise, and assisted in knowledge dissemination in support of the Maryland efforts.

In addition, USM and BHEF created the USM-BHEF Undergraduate Cybersecurity Network, a coalition of representatives from higher education, business, government, and other stakeholder organizations who are collaborating to create a strategic regional response to the growing need for cybersecurity talent. Focused on the undergraduate experience and the need to increase the recruitment and persistence of students, particularly women and underrepresented minorities, in cyber-related fields, the network seeks to (1) align the cyber workforce requirements of business and government with higher education, (2) develop innovative programs to expand the cyber talent pipeline, and (3) address issues of critical interest to cyber workforce development.

The Maryland activities in cybersecurity validate and underscore HEWI's effectiveness in developing and scaling strategic regional partnerships. In demonstrably powerful ways, the Initiative engages diverse partners in true partnerships that result in the design and implementation of innovative educational programs to meet critical workforce needs on an accelerated timeline. Moreover, the activities inform current BHEF efforts to transfer and adapt the same strategies in other academic disciplines and industry sectors elsewhere across the United States.

Positioning of the strategies in Maryland required (1) commitment to sustained engagement to improve education outcomes; (2) collaboration to develop a shared understanding of academia's and business's interconnected problems, based on research and data that link college readiness and success to workforce requirements; (3) development of a shared vision for systemic solutions; (4) collaboration between USM and BHEF and with other strategic partners to implement solutions; (5) advocacy for public policies needed to achieve goals; and (6) raising of public awareness about the urgency of these issues at the regional, state, and national levels.

BHEF's work in Maryland illustrates that it is indeed possible to effect swift, significant change and innovation in higher education with the goal of better aligning curricula and student outcomes with needed workforce skills. This pace of change hinges on the genuine commitment, expertise, and investment of resources by motivated stakeholders. BHEF's members and partners are encouraged by this track record and believe it can be successfully replicated in BHEF's work elsewhere in the country.

BHEF's work in Maryland has also seeded an important strategy for national collaboration around a top-priority discipline in the form of the National Undergraduate Cyber Network. Sponsored by the Alfred P. Sloan Foundation, the network brings together experts and change agents from business, academe, and government to clarify challenges and shape solutions in bridging workforce needs and undergraduate education around cybersecurity. Finally, in fall 2013, BHEF received a planning grant from the Bill & Melinda Gates Foundation to develop a strategy—*Cybersecurity Undergraduate Pathways (CyberUP)*—for creating and expanding pathways that provide a much broader range of individuals with industry-recognized credentials for careers in cybersecurity, a rapidly growing and highly paid field. As such, the goal is to further expand the knowledge gained in Maryland to other regions and at the national level.

This case study describes how the Maryland regional initiative, as part of HEWI, operationalizes and implements the BHEF strategies.

BHEF's work in Maryland illustrates that it is indeed possible to effect swift, significant change and innovation in higher education with the goal of better aligning curricula and student outcomes with needed workforce skills. This pace of change hinges on the genuine commitment, expertise, and investment of resources by motivated stakeholders.

Below: University of Maryland President Wallace Loh with BHEF Immediate Past Chairs Wes Bush, chairman, CEO, and president, Northrop Grumman Corporation, and William "Brit" Kirwan, II, chancellor, University System of Maryland.

Photo by John T. Consoli/University of Maryland

Introduction to HEWI

Through the collaboration of its business and academic members, BHEF has launched the National Higher Education and Workforce Initiative (HEWI), a six-year effort that involves regional projects focused on business-higher education partnerships in selected states or regions, as well as national efforts to disseminate the knowledge gained from the projects and scale effective practices. HEWI deploys a model of strategic business engagement in higher education to address the highest priority workforce development needs.

Launched on June 11, 2012, HEWI's original projects focused on (1) STEM (science, technology, engineering, and math) undergraduate education and (2) the need for additional college graduates with STEM degrees. As BHEF conducted further research and met with stakeholders across many industry sectors and academia, a third need became evident: an increased demand for STEM skills in non-STEM jobs. These skills include data analysis and interpretation, and complex problem-solving. For example, Burning Glass Technologies reports that advanced manufacturing, finance, and professional services are the leading industries for cybersecurity professionals.[1] Industry sectors need graduates who are both enabled across emerging fields (such as cybersecurity) and well educated in disciplines (such as finance), or who possess work experience (for the advanced manufacturing sector). Thus, BHEF supports a fundamentally new approach to talent development that consults with industry and builds capacity through a combination of academic coursework, professional certifications (where relevant), and work experience. While many employers continue to require cybersecurity professionals be deeply trained in STEM disciplines, HEWI provides a multi-pronged model that allows undergraduates in a variety of disciplines to obtain the STEM skills valued by employers.

Currently, regional projects under HEWI are under way in the fields of computer science, cybersecurity, data science and analytics, engineering, and information technology, and in industry sectors such as advanced manufacturing, agriculture, energy, and financial services (see page 23). Additionally, BHEF plans to expand the scope and number of its projects in the future.

BHEF has implemented a comprehensive strategy to scale this work at the college/university system, regional, and national levels.

- *College/University level* by creating replicable regional workforce projects that build on and support a region's competitive economic advantage. BHEF has more than 20 projects in place or in development across the country.
- *Regional/University System* level by linking multi-campus university system projects or individual higher education institutions, which address emerging trans-disciplinary fields and industry sectors. Evidence-based insights provide the foundation for connecting these efforts to business and government partners and providing broader regional workforce solutions.
- *National level* by strategic partnerships with leading industry and higher education associations. Through these collaborations, BHEF engages its partners in regional projects, disseminates evidence and insights, and supports the scaling of effective practices through field and industry sector networks.

On September 27, 2013, BHEF released its first playbook for HEWI during a National Undergraduate STEM Partnership meeting at the White House.[2] The playbook introduces the Initiative, its evidence base, and the essential steps to develop successful regional workforce projects. It is intended to assist those seeking to understand the potential value of investing in coordinated strategic, long-term partnerships to increase the persistence of undergraduate students, particularly women and underrepresented minorities, toward attaining a degree and entering the 21st century workplace. The intended audience includes businesses, higher education institutions, private philanthropies, membership associations, professional societies, and government agencies.

[1] Burning Glass Technologies. (March 2014). *Job Market Intelligence: Report on the Growth of Cybersecurity Jobs*. Available at *http://www.burning-glass.com/research/cybersecurity*.

[2] BHEF. 2013. *The National Higher Education and Workforce Initiative: Forging Strategic Partnerships for Undergraduate Innovation and Workforce Development*. Available at *http://www.bhef.com/sites/g/files/g829556/f/201308/2013_report_playbook.pdf*.

The Growing Demand for Cybersecurity Professionals

According to a 2014 report from Burning Glass Technologies, the national demand for cybersecurity professionals grew, on average, 74 percent from 2007 to 2013. Some states report demand at more than twice that rate. This growth rate is more than twice the rate of growth of all information technology (IT) jobs.[3] Additionally, on average, cybersecurity jobs pay $15,000 per year more than overall IT jobs.

The growth in demand for cybersecurity workers coincides with the increasing number of cyber-attacks against private and public organizations. Yet employers face competition in recruiting and retaining cybersecurity talent. Businesses and governments are challenged by the lack of clear career pathways into the field and fragmentation of third-party certification, training, and education programs. This is significant given that the volume of data for which companies are responsible is expanding by 35 to 50 percent each year; threats to U.S. federal data increased by 700 percent from 2006 to 2011;[4] and emerging trends such as "bring your own device," cloud computing, the Internet of Things, and social media are spreading sensitive information across a rapidly expanding range of devices. In addition to the small pool of talent, business faces several recruiting challenges, such as security clearances, uncertain government budgets, and intense competition for available candidates. Moreover, the cybersecurity industry has been unable to successfully recruit and retain women and underrepresented minorities.

Efforts are under way at the federal level to develop a national framework for cybersecurity education, training, and careers, such as the National Institute of Standards and Technology's National Initiative for Cybersecurity Education (NICE). However, the industry must become more deeply engaged in building flexible, attractive cybersecurity career pathways for learners. Also needed are efforts to prepare highly skilled, technically trained cyber specialists, whose primary job function will be cybersecurity, as well as managers, policy makers, and broader professionals across a range of sectors who are cyber enabled with foundational skills and awareness of cybersecurity issues.

[3] Burning Glass Technologies, *Job Market Intelligence: Report on the Growth of Cybersecurity Jobs*, March 2014. Available at *http://www.burning-glass.com/research/cybersecurity*.

[4] MIT Sloan Review (2012). *Finding Value in the Information Explosion*. Retrieved from: *http://sloanreview.mit.edu/article/finding-value-in-the-information-explosion* and National Initiative for Cybersecurity Education (2012). *Strategic Plan*. Available at *http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf*.

BHEF's Strategic Business Engagement Model

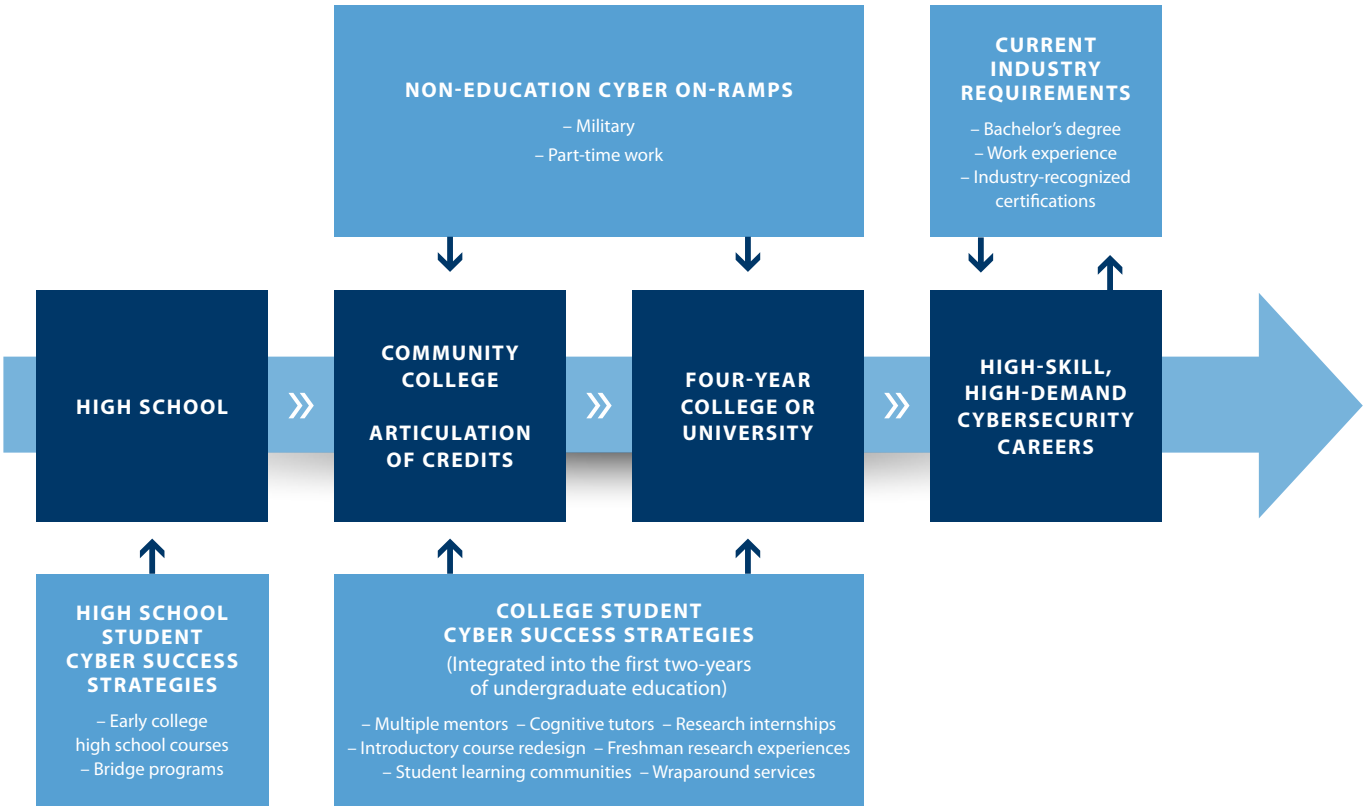
BHEF's approach aligns five levers, or strategies, to drive a shift from transactional relationships to strategic partnerships between business and education to develop a workforce possessing skills vital to competitiveness:

1. Engage and deploy corporate and academic leadership.
2. Focus corporate philanthropy strategically in undergraduate higher education.
3. Identify and tap core competencies and expertise.
4. Facilitate and encourage employee and staff engagement.
5. Expand the focus of funded research to undergraduate education.

In addition, a more strategic approach is needed to address short-term and intermediate demands for skilled cyber workers. Nearly half of all cybersecurity jobs require certifications, which can document an individual's competence and ability ranging from entry-level to more advanced positions. Some of the certifications can serve as an entry point to a career pathway in cybersecurity. However, employers have indicated that certifications alone will not provide individuals with the necessary skills to meet businesses' cybersecurity hiring demands. Many cybersecurity jobs require graduates with a baccalaureate degree and some previous work experience. Additional strategies also are needed to boost the recruitment, retention, and development of cyber faculty. Partnerships with business and government can expand faculty capacity and increase the currency of undergraduate curricula in a rapidly developing field. More than training programs, focused efforts such as these will increase the talent pool and will position students to compete in the open market upon graduation.

The field of cybersecurity is poised to fundamentally reshape IT's traditional reliance on the IT career pipeline and the role of stackable credentials in building new career pathways. BHEF's market research indicates that on-ramps into cybersecurity careers can begin in many academic programs and at many levels—high school diploma plus work experience, sub-baccalaureate certificates, military experience, or an associate's degree—as well as entry through the more traditional four-year college program. A multi-track approach can widen the pipeline to a cybersecurity career, especially for women and underrepresented minorities, lower-income populations, and veterans.

CYBERUP ON-RAMPS AND PATHWAYS



- Illustrative; diagram is not to scale and does not indicate duration to education/career level attainment
- There are many possible combinations of the pathway through each of the CyberUP on-ramps

Building the Cybersecurity Workforce In Maryland

Maryland has been an early and vigorous adopter of the type of program envisioned all along for HEWI. At the time of the Initiative's launch, Maryland had already identified cybersecurity as a strategic focus for education and economic development. Working with its membership, BHEF partnered with USM to build a system-wide response to the state's (and nation's) cybersecurity workforce challenges. BHEF's pivotal leadership role in sparking innovations resulted in the creation of premier undergraduate programs in cybersecurity at two USM institutions and their adaptation at two additional institutions. Together, all partners have created vibrant and relevant educational programs to meet the needs of the cybersecurity industry, which provides proof of principle for HEWI.

Maryland's Business Needs and Supply Analysis

A critical tool in the BHEF model for building business-higher education partnership is a regional workforce assessment, which informs all parties about the unique challenges to the talent ecosystem of a given geographic area. The assessment will: (1) determine whether additional specialists or enabled employees are needed, (2) identify workforce trends in a particular sector, or (3) confirm if a skills gap exists.

Maryland's program grew out a series of planning activities, studies, and regional workforce assessments highlighting the need to sharply increase student graduation rates in STEM fields, particularly among women and underrepresented minorities, to meet the state's rapidly expanding STEM workforce needs, notably in information technology and cybersecurity.

In 2009, the Maryland STEM Task Force, co-chaired by Brit Kirwan, USM chancellor, and June Streckfus, executive director of the Maryland Business Roundtable for Education, submitted its final recommendations to Governor Martin O'Malley in the report, *Investing in STEM to Secure Maryland's Future*.[5] The report noted an anticipated surge in STEM-related jobs in the Maryland region, particularly in critical areas such as cybersecurity, and called for greater collaboration between industry and USM to produce 40 percent more STEM graduates in the state by 2015 to fill these jobs.

This recommendation echoed USM's own 2010 strategic plan, which noted that its annual production of approximately 4,000 STEM graduates (including STEM teachers) was falling considerably short of filling the region's 6,000 STEM openings each year. The plan called for greater collaboration between business and the P-20 system in the state, as well as for increased efforts to align education with workforce needs.

In 2010, Governor O'Malley designated cyber as the state's lead workforce focus. That same year, the Governor's Workforce Investment Board projected that the greatest job growth would be in high-skill occupations, in particular network systems/data communication, computer software engineering, and systems administration.

Following on these efforts, USM Chancellor Kirwan commissioned a Cybersecurity Task Force comprising business, government, and higher education representatives.[6] Its 2011 report detailed the region's need for highly skilled workers in cybersecurity, provided an inventory of USM resources available for cyber education and research, and explored opportunities for partnerships among USM institutions and business and government stakeholders to produce the cyber workforce of the future.

Federal cybersecurity assets are abundant in Maryland and the surrounding region—for example, the National Security Agency, the National Institute of Standards and Technology, the Intelligence Advanced Research Projects Activity, and the Department of Defense. In addition, Maryland anticipates a projected increase of almost 80,000 cyber-related jobs because of the Navy's Cyber Fleet and the relocation of the U.S. Cyber Command to Fort Meade. The Cybersecurity Task Force issued a series of recommendations that included expanding higher education offerings in cybersecurity and information assurance to increase the size and diversity of the regional talent pool, as well as establishing more partnerships among education, government, and business.

[5] *Investing in STEM to Secure Maryland's Future: Final Report of the Governor's STEM Task Force*. Presented to Governor Martin O'Malley, August 2009. Available at *http://www.sciencemasters.com/portals/0/pdfs/Investing_in_STEM_to_Secure_Marylands_Future.pdf*.

[6] *Report of the Cyber Security Task Force to the University System of Maryland, May 2011*. Available at *http://www.usmd.edu*.

In 2012, BHEF received planning and implementation grants from the Alfred P. Sloan Foundation to partner with USM to expand higher education-business collaborations in cyber throughout USM, focusing on Bowie State University, Towson University, University of Maryland, Baltimore County (UMBC), and University of Maryland, College Park (UMD). A key component of this project was to engage regional consumers of cyber talent, namely business and the federal government, as co-developers of that talent with leading higher education institutions. The grants also supported continued and expanded work by the Cybersecurity Task Force as well as extensive research on student migration in and out of STEM fields in the Maryland system.

A 2013 study by the Abell Foundation and CyberPoint International identified Maryland as one of the nation's "hotbeds in cybersecurity," with approximately 20,000 openings in cyber by 1,800 companies, ranking it above such regional powerhouses as Palo Alto and Boston.[7] In parallel with some of USM's activities, BHEF, which has long partnered in workforce development activities with Chancellor Kirwan, began to engage more deeply in Maryland's efforts to grow its cybersecurity workforce.

As HEWI was taking shape in the form of Maryland's cybersecurity programs, BHEF continued to assess industry needs in cyber. Through extensive research with cybersecurity stakeholders, BHEF identified three principal criteria used by employers in hiring entry-level applicants: (1) academic background, notably in courses relevant to cybersecurity, credentials attained through the institution such as certificates, majors, or minors, and level of educational attainment appropriate for the position; (2) professional certifications in cybersecurity by government and industry-recognized third-party providers; and (3) relevant cybersecurity work experience.

Student barriers to such careers begin in K-12 and continue through college and into their professional lives. Further, while work experience is a strong predictor of success in cybersecurity, it is hard to acquire the experience required for entry-level positions. For full-time students balancing work and academic requirements, this is a daunting obstacle. Although half the organizations BHEF surveyed require certifications, they also indicated that there is little industry consensus on the value and relevance of these certifications to the field. In sum, too few clear career pathways into cybersecurity exist despite the sharp workforce demands in the field, due in large part to misalignment of these three industry criteria. BHEF is applying these insights to USM programs and their expansion by broadening the focus beyond STEM disciplines to also include other approaches that prepare undergraduates for a cyber career. Specifically, BHEF will integrate (1) academic credentials, (2) work experience tied to a career goal, and (3) industry-recognized certifications to prepare students for an array of opportunities in cybersecurity.

BHEF's involvement in Maryland's activities proved to be the first major deployment of HEWI. As described below, the Initiative has already realized significant successes on several different fronts in Maryland. Overall, those successes validate the value and efficacy of the Initiative's strategies. Moreover, the experiences in Maryland are informing other BHEF projects under way around the country.

Developing an Evidence Base: USM Student Migration Analysis

A critical early component to deploying HEWI in Maryland was building a foundation of research-based evidence to inform planning and implementation. With the support from the Alfred P. Sloan Foundation to BHEF and USM, through a three-year implementation grant, USM conducted a student migration analysis. Such analyses provide a baseline for higher education partners to understand, at the level of the academic department or institution, the patterns of student enrollment and persistence in the targeted fields prior to the onset of business-driven interventions. The ability to track data over time allows for monitoring and continuous improvement. Moreover, institutions can make informed decisions regarding programmatic offerings, formulate funding requests, and seek partners. Findings can be specific to institutions, even within one education system.

The USM study involved three phases: student data mining conducted by the USM Office of Institutional Research, focus groups with students, and focus groups with campus career services professionals.

The student data were collected in spring 2012 from three cohorts of first-time, full-time freshmen in 2003, 2004, and 2005 at four USM institutions: University of Maryland Eastern Shore, Towson University, UMBC, and UMD. Data were collected across three STEM majors (computer science, mathematics, and engineering; 3,958 students), and business majors were used as a control/comparison group (2,305 students). Students entering STEM majors were more likely to change majors and graduate in a major outside of their entering STEM major than were students entering business majors (26 percent versus 14 percent).

[7] The Abell Foundation and CyberPoint International LLC, January 8, 2013. *Cyber Security Jobs Report*. Available at *http://www.ctic-baltimore.com/reports/Cyber%20Security%20Jobs%20Report-010813.pdf*.

The results showed that STEM students were twice as likely to leave their major for a different major than were business students. And, although computer science majors graduated in their major at somewhat higher rates than other STEM majors, they were least likely to graduate overall. Among STEM majors, engineering majors were the most likely to graduate in their major and least likely to switch to another STEM major. Thus, computer science and engineering majors showed great promise in committing to and sticking with their majors, despite the need for improved outcomes.

Moreover, men and women graduated in their starting STEM major at roughly similar rates—different from the overall national trend of women graduating at higher rates than men. However, women were more likely to graduate in a different major than were men. Thus, women were more likely to migrate out of a STEM major over time. These findings highlighted the need to address the reasons women were disproportionately leaving STEM majors. The analysis also found that an achievement gap persists for underrepresented minorities in both graduation rates and graduation within a STEM major. Specifically, 44 percent of underrepresented minorities within the cohorts of this research study did not graduate.

An assessment of the evidence base yielded insights about the unique goals of participating institutions. UMBC, for example, has a rich tradition of nurturing scholarship for students traditionally underrepresented in the sciences, including women. Although UMD works aggressively to support these student populations, its program development aligns with its distinguished honors program model, which focuses on academically gifted students.

In addition to the migration analysis, focus groups were conducted with students and faculty/administrators in computer science, engineering, math, and business (the control/comparison group) and with career services officers at the four USM institutions. The focus groups have yielded a deeper, on-the-ground understanding of the outcomes from the migration analysis and have informed the development of programs that address unique campus needs across the system.

The student focus groups revealed that prior to the Initiative's work, students in STEM majors were not required to take courses in leadership, communications, or public speaking. Students also reported uneven teaching quality, specifically describing, for example, differences between faculty who worked in industry and those whose work was more research-focused. In general, students said exposure to industry outside of traditional, formal interactions was rare and experiences securing internships were uneven at best.

"The ACES program is the centerpiece of a larger region-wide effort to build the talent that our nation so desperately needs in cybersecurity. What is especially exciting about the program is that it brings exceptional students from different fields together in an exciting living learning environment."

William E. "Brit" Kirwan, II, chancellor, University System of Maryland, speaking at the launch of the UMD ACES program

These findings led to the creation of new university programs explicitly designed to address undergraduate student needs as well the workforce supply-and-demand gaps that the Maryland-based analyses had identified. They also highlighted the need to focus with greater intensity on recruiting and retaining women and underrepresented minorities.

Planning and Deploying Programs that Embed Effective High-Impact Practices

BHEF has conducted extensive research to better understand the interventions and strategies that work best to support the success of undergraduate students. A literature review identified several strategies that have enabled students to increase their persistence in completing degrees, achieve better grades and higher satisfaction, and learn how to apply knowledge in real-world settings. BHEF's research and system dynamics modeling have shown that the following interventions can be particularly effective:

- undergraduate research internships
- freshman research initiatives
- cognitive tutoring
- introductory course redesign
- student learning communities
- scholarships for service
- combined intervention strategies[8]

[8] For a deeper look at BHEF's research and modeling on undergraduate interventions, see *The U.S. STEM Undergraduate Model: Applying System Dynamics to Help Meet President Obama's Goals for One Million STEM Graduates and the U.S. Navy's Civilian STEM Workforce Needs*, available for download at *www.bhef.com*.

> **"For the students, the ACES program represents a competitive advantage in the quest of employment after graduation—employment in fascinating, important, well-paying work."**
>
> Wes Bush, chairman, CEO, and president, Northrop Grumman Corporation, speaking at the launch of the UMD ACES program

Virtually all of these purposeful actions are based on evidence of effectiveness and can be found in the cybersecurity programs developed in Maryland as part of the BHEF Initiative. In fact, they have become the design principles for the USM education programs, first at UMBC and UMD, as described below. In addition, USM and BHEF are in the process of adapting and scaling their collaboration in cybersecurity to two other institutions in the Maryland system, Bowie State University and Towson University.

The Advanced Cybersecurity Experience for Students at the University of Maryland

Building on work undertaken through the Alfred P. Sloan Foundation grants, BHEF was instrumental in helping UMD receive a $1.1 million grant from the Northrop Grumman Foundation to support the development of the landmark Advanced Cybersecurity Experience for Students (ACES) program. Apart from serving as further evidence that business and higher education can partner productively through the Initiative's framework and strategy, the ACES program is distinguished as being the nation's first and only undergraduate honors program in cybersecurity.

ACES educates future leaders in cybersecurity through rigorous, hands-on learning experiences, an intensive interdisciplinary curriculum, collaborative projects, and professional insight from corporate leaders. ACES is based on four central goals. First, students receive a strong underpinning in technical subjects. Second, students learn ethics—an essential consideration given that their future career is likely to involve access to sensitive or private data. Third, students learn fundamental professional skills for the 21st century workplace. Fourth, students "give back" or contribute service to the field.

The ACES curriculum consists of two linked academic programs over the course of four years: (1) a freshman-sophomore living-learning program leading to an Honors College Citation in Cybersecurity and (2) an upper-level course of study in cybersecurity. ACES students take general cybersecurity courses as well as courses on cybersecurity forensics, reverse engineering, secure coding, criminology, and law and public policy, among other topics. ACES seniors complete a yearlong capstone project that addresses a foundational challenge in cybersecurity.

ACES encompasses an interdisciplinary living-learning experience—a high-impact intervention practice modeled by BHEF through its U.S. STEM Undergraduate Model, as described in *The National Higher Education and Workforce Initiative: Forging Strategic Partnerships for Undergraduate Innovation and Workforce Development*. ACES students will live in an honors dormitory that offers state-of-the-art cybersecurity laboratories, giving them the opportunity to work closely and collaboratively both inside and outside the classroom. Prince Frederick Hall, a new honors dormitory, will house ACES students.

The first cohort of ACES students started their studies in fall 2013—less than two years after the program was first conceptualized. Originally, 40 student slots were planned, but the program ultimately elected to enroll 57 students, including 13 women, 2 African-American students, and 3 Hispanic students for its inaugural cohort. ACES students represent a diverse range of majors, including computer science, mathematics, engineering, business, and criminology.

The program's focus on the first two years of undergraduate study further underscores BHEF's findings through system dynamics modeling that (1) a focus on undergraduate education has the highest potential return on investment in developing the STEM workforce and (2) high-impact retention strategies in the first two years of college will have a greater effect on the STEM pipeline than will interventions later in a student's college experience.

ACES emphasizes combining classroom knowledge and skills with real-world, flexible, hands-on experience. Experiential learning opportunities include individual and group research projects with peers and with faculty members of the Maryland Cybersecurity Center, participation on the UMD Cybersecurity Team, and collaboration with the security team responsible for protecting UMD's infrastructure. Students also have internship opportunities during the academic year and in the summer with federal agencies that have cybersecurity expertise, such as the Department of Defense and the National Security Agency, as well as with private corporations such as Northrop Grumman.

Industry involvement plays a vital role in ACES' success and broader impact. As an extraordinarily active partner in ACES, Northrop Grumman helps shape the curriculum for the program, works regularly onsite with program planning, and provides guest lecturers, program advisors, paid internships, and mentors for students throughout their four-year experience. Northrop Grumman representatives also participate in the program's industry advisory board, experts serve as adjunct faculty, and representatives provide regular opportunities for students to visit company facilities and meet employees. Although Northrop Grumman played a lead role in the launch and development of the ACES program, additional companies are involved by serving as advisors as well as providing experts, internships, and scholarships.

In particular, additional support for the program comes from Parsons, a leading firm that provides technical, engineering, construction, and management support throughout the world to federal, regional, and local government agencies as well as private industry. Over three years, Parsons is supporting partial scholarships, based on student need, for 24 high-achieving ACES students. Parsons also provides professional insight to students and advises them about career options in cybersecurity.

Upon graduation, students receive a designation on their transcript indicating their participation in the ACES program. This citation will be recognized by employers as a meaningful credential in the hiring process.

"There are two main goals for ACES. One is to show that you need interdisciplinary approaches to cybersecurity; it's not purely technical. The other focus is to have a very diverse group of students, including a high percentage of women and a representative population of all students—essentially, to have diversity at all levels."

Michel Cukier, director, ACES and associate director for education, Maryland Cybersecurity Center

Cyber Scholars at the University of Maryland, Baltimore County

As a second major achievement in its cyber-related work in Maryland, BHEF supported a partnership between UMBC and Northrop Grumman, which resulted in the launch of the UMBC Cyber Scholars program with a $1 million grant to UMBC from the Northrop Grumman Foundation.

Below: Past Chairs Wes Bush, chairman, CEO, and president, Northrop Grumman Corporation, and William E. "Brit" Kirwan, II, chancellor, USM, join the inaugural cohort of ACES for its class portrait.

Photo by John T. Consoli/University of Maryland

"At UMBC, we're working to accomplish three related goals. First, we provide a supportive living-learning community, leveraging existing programs, to support student success and retention, two factors that have traditionally been challenging in STEM and computer science education and with underrepresented minorities and women. Second, UMBC Cyber Scholars receive both specific technical classes and considerable practical preparation, such as internships and practicums, for work in cybersecurity careers. Third, from day one we connect students, even first-year students, with research mentors."

Anupam Joshi, director,
UMBC Center for Cybersecurity and
UMBC Cyber Scholars program

The program draws on significant insights gained through UMBC's nationally renowned Meyerhoff Scholars program, which is widely considered to be at the forefront of efforts to increase diversity among future leaders in STEM fields. Designated for undergraduate students, with a focus on women and underrepresented minorities pursuing STEM degrees, the Meyerhoff program combines financial aid, student learning communities, summer bridge programs, mentoring, personal advising, and counseling into a comprehensive program that has proven extraordinarily successful and is widely touted as a national model.

Informed by the successes of the ACES and Meyerhoff programs, the Cyber Scholars program models many of the interventions that BHEF research and modeling have shown to be effective, and strategically engages business to assist in the persistence of women in cybersecurity, a need that companies have highlighted as extremely important toward their continued success. Launched in fall 2013, the Cyber Scholars program had an initial cohort of nine students, including four women. The program is in the process of increasing participation to 15 to 20 new scholars annually, with special emphasis on increasing the number of women and underrepresented minorities preparing for cybersecurity careers. For example, the program plans to enroll 50 percent women. Cyber Scholars can major in computer engineering, computer science, or information systems.

The Cyber Scholars program is also modeled in some respects on the scholars program run by UMBC's Center for Women and Information Technology, housed in the university's new Cybersecurity Center, and is run in partnership with the Center. In addition, the program is an extension of an already strong partnership in cyber-related activities between UMBC and Northrop Grumman, which includes the Cync program, a start-up business incubator for companies developing innovative solutions to counter the global cyber threat.

Like the ACES program, the Cyber Scholars program charts new ground in the delivery of effective undergraduate education in cybersecurity. Scholars receive financial awards with special opportunities for advanced research, directed internships, and other forms of academic and social support. They are matched with a faculty research mentor as well as an industry mentor. The program fosters a cybersecurity-focused community through common on-campus living-learning housing, events, and activities. Each week, scholars engage in a cyber practicum that includes talks from field practitioners. Scholars also have the opportunity to visit government agencies and industry laboratories that engage in cybersecurity.

Cyber Scholars take a combination of management-oriented and technically focused courses. All scholars are required to take an introductory seminar in their freshman year and at least one cybersecurity course in their junior year.

As with UMD and its ACES program, Northrop Grumman has enthusiastically partnered with UMBC and its Cyber Scholars program. Northrop and UMBC built on relationships established during development of the Cync program to collaborate on the Cyber Scholars program. Throughout program development and launch, Northrop advised UMBC representatives on how to best shape a program that meets industry's needs. Beyond financial support, Northrop also provides regular consulting, speakers, and opportunities for students to interact with industry representatives.

Networking and Scaling the Programs in Maryland

To disseminate the learning, insights, and outputs from its regional projects, BHEF is pursuing strategies that adapt and scale successes at the college/university system, regional, and national levels. These strategies build on each other and, together, provide a coherent and transparent framework for growing and improving individual regional projects and the Initiative as a whole. Maryland has implemented scaling strategies at the multi-campus and university system levels.

Through their engagement in the USM-BHEF Undergraduate Cybersecurity Network (see discussion below), Bowie State University and Towson University are connecting with business and government partners to develop undergraduate cyber programs unique to their institutional missions, resource base, and faculty and student interests (see *Scaling the Effort to Other USM Campuses* on page 16). The Network provides a framework for sharing experiences from program development at UMD and UMBC, and a forum for potential business and government partners to express their workforce needs and identify opportunities for collaboration.

The USM-BHEF Undergraduate Cybersecurity Network

The USM-BHEF Undergraduate Cybersecurity Network, comprising 30 representatives from academia, business, government, and stakeholder organizations, was launched during its inaugural meeting in April 2013. The network supports an overarching system-wide goal of significantly increasing the number and diversity of graduates in cybersecurity fields. It supports projects aimed to strengthen business-government-higher education partnerships; focus on key policy challenges, such as accelerating student security clearances; share curricula and other resources; and develop a clearinghouse on effective cyber education practice and tools.

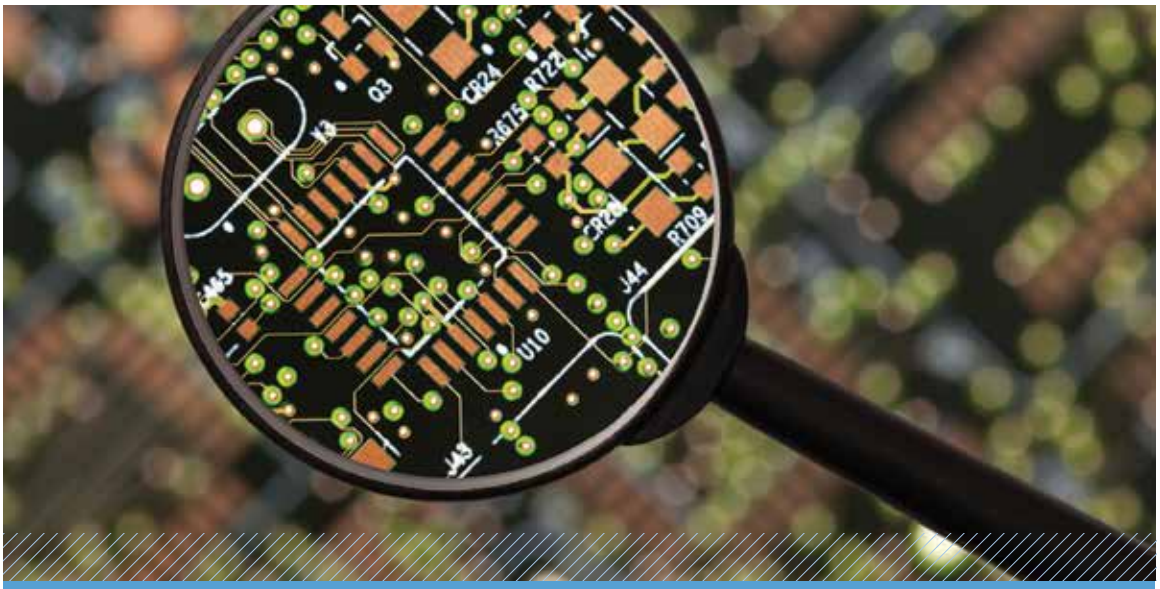
The network's development has been vitally important to BHEF's work. This coalition of stakeholders comprise a regional ecosystem that identifies, nurtures, and grows the highest-impact cybersecurity learning opportunities for USM undergraduates in alignment with workforce demands.

In essence, the network creates not only campus-specific responses in cybersecurity, but also an overarching action agenda for meeting the state's cybersecurity workforce needs. The network enables USM to connect its campus-based regional workforce projects and provides a forum for the campus programs to learn, adapt, and adopt evidence-based practices. It uses USM as an effective scaling mechanism for extending learning while meeting the state's challenges in cyber. To these ends, the network pursues the following specific goals:

- **Co-development of strategic undergraduate interventions.** Drawing on the core competencies of its business and government partners, the network supports the establishment of highly efficacious interventions at partner universities, such as early research internships, courses and curricula redesigned around active learning principles with industry participation, cohort and team-learning experiences, co-op programs, and mentoring.
- **Clear articulation of industry and government cyber workforce needs.** A number of companies (e.g., Battelle, Northrop Grumman, Raytheon) have engaged with faculty and administrators at UMBC to create a cybersecurity Professional Science Master's degree program. The process by which this program was created, and the materials and learning arising from it, is informing the development of undergraduate cyber programs and providing a back map for identifying the content knowledge, competencies, and skills the cyber industry is seeking in its employees.
- **Focus on key policy challenges in undergraduate cyber education.** Security clearance for undergraduates has been identified as a critical issue in the successful implementation of undergraduate cyber programs and a potentially major barrier for students contemplating cyber careers. The USM network is playing an important role in providing on-the-ground opportunities to address such challenges.
- **Engagement with community colleges and K-12.** The network is creating partnerships with K-12 and community colleges to build the cyber workforce pipeline and a scaffolded set of opportunities for students into four-year cyber programs. Programs such as *CyberPatriot* provide a potential source of connections, programmatic ideas, and students to fuel the USM network and its activities.

The network has created three working groups focused on specific areas of interest. The first group is identifying challenges to students acquiring the security clearances needed to work in cybersecurity, which is critical to the successful implementation of undergraduate programs. The second group is developing a clearinghouse of cybersecurity resources relevant to undergraduate education. The third is focusing on curriculum development and sharing.

The network plays a pivotal role in scaling cyber activities across Maryland. Focused on the undergraduate experience and the need to increase the recruitment and persistence of students, particularly women and underrepresented minorities, in cyber-related fields, the network is an invaluable tool for aligning the cyber workforce requirements of business and government with higher education, developing innovative programs to expand the cyber talent pipeline, and addressing issues of critical interest to cyber workforce development.



Scaling the Effort to Other USM Campuses:
Cybersecurity Education at Bowie State University and Towson University

The Center for Cybersecurity and Emerging Technologies at Bowie State University provides educational, research, and training opportunities in network and information security to both students and faculty. Through a grant from the National Nuclear Security Administration, Bowie State professors can train in cybersecurity techniques, including cyber forensics, which they can then apply in the classroom. In addition, Bowie State can build cyber-related technological capacity in its laboratories and other facilities, and students can hone their practical skills in summer internships at Sandia National Laboratories and other Department of Energy facilities. Bowie State is in talks with potential partners to extend these activities and develop new initiatives in cybersecurity. BHEF has reached out to Boeing, Lockheed Martin, and Raytheon, and has initiated discussions with other business members to foster collaboration with Bowie State. The university has strong ties to local community colleges, notably Prince George's Community College, and, as a historically black institution, has strong potential to increase the representation of minorities in cyber-related fields.

Towson University was one of the first universities in the nation and the first in Maryland to offer a computer security track in its curriculum, and it has offered an undergraduate track in cybersecurity since 2003. Today, its cyber programs are growing. Since 2002, the National Security Agency and the Department of Homeland Security have designated Towson as a Center of Academic Excellence in Information Assurance. The university has been exploring a new cooperative program with Raytheon that would enable cyber students to participate in internships and paid co-op opportunities. Additionally, Raytheon engineers and other cyber professionals would work with Towson faculty to review and validate the cybersecurity curriculum, thus ensuring that the program benefits from the most leading-edge thinking in the field. In turn, Raytheon would benefit from more direct access to students skilled and experienced in cybersecurity.

Insights Gained through HEWI in Maryland

In the case of BHEF's efforts to coalesce engagement by business and higher education around cybersecurity in Maryland, program leaders offer several preliminary observations about the strategies behind program development and the impact of the current initiatives.

Choose the right partners. When business and academic partners collaborate strategically, the development of new academic programs that align with workforce needs can occur rapidly. As evidenced by the partnership between Northrop Grumman and USM—and contrary to commonly held perceptions—deep, systemic change in the way academic programs are designed to meet workforce needs can be conceptualized and implemented relatively quickly when the right parties are at the table.

In Maryland, for example, Northrop Grumman and other corporations have immediate needs for increasing the pipeline of top cybersecurity talent. At the same time, USM has identified a strategic objective to better align its educational programs to meet state cybersecurity workforce needs. Through conversations brokered by BHEF, Northrop and USM recognized the extent to which their interests intersected. These common interests and synergies motivated the two parties to design and implement the ACES program in less than two years, a pace of change that outstrips the more traditional and slower-paced track of programmatic change in higher education.

Execute strategies based on a solid base of evidence. Anecdotal information often frames the nature of challenges, but if solutions are to be truly effective, then they must be based on evidence that apprises decision makers about the root causes of problems and the strategies that are likely to address them. In this regard, research has been a vital underpinning of the Initiative from the start. A significant body of evidence that was collected before any students enrolled in either program, for example, informed planning for the ACES and Cyber Scholars programs. As described above, evidence collected by the Maryland STEM Task Force and the UMD Cybersecurity Task Force primed policy decisions about starting the programs at UMD and UMBC and influenced the development of program curricula. This evidence was enhanced by analyses and focus groups conducted by USM of the major migration, retention, and graduation patterns of STEM students. Other organizations seeking to model some of the Initiative's strategies should build their own body of evidence that is tailored to their specific issues and environment.

Leverage existing partnerships between business and higher education to spark and drive change. The corporate and university partners observed that their success in pushing from a concept to an operating program relatively quickly hinged on their ability to capitalize on existing relationships. They advise business and higher education partners seeking to pursue a similar strategy to look to existing partnerships before investing time and energy to create new ones. Often dormant partnerships can be energized and expanded with relatively little effort.

Establish proof points from which further program development can occur. Programmatic innovation is iterative. That is, the program can be enhanced over time even while it is delivering on its mission. Especially in the case of the reforms reported on here, it would be counterproductive to expect to design the perfect program because environmental factors that affect cybersecurity are extremely fluid and evolve rapidly. Rather, the goal ought to be to establish proof points along the evolutionary cycle on which further program enhancements can be developed. In the case of the ACES program at UMD, for example, all partners considered it imperative to get the program up and running. Therefore, they decided to address some of the program details, such as the identification of metrics to access success, after the program launch. Now, in the program's first year, program leaders and advisers are defining metrics and the methods by which data will be collected and analyzed. Metrics under consideration include student enrollment, diversity, career choices, and direction after graduation. Longitudinal data will inform future program innovations and design.

Build from existing academic structures. A vital strategy in forming programs is capitalizing on existing structures. Each USM institution discussed in this report had existing computer science departments and curricula. Therefore, new programming in cybersecurity could be constructed and implemented relatively quickly by building on existing academic structures, staff, and relationships with business. In the case of UMD, which opted to make cyber an honors program, a robust structure of honors-level education provided a rich framework on which the new program could be developed.

Plan for and build networks. Networks, such as the USM-BHEF Undergraduate Cybersecurity Network, are vitally important proving grounds for strategic partnerships. Through these networks, stakeholders can share ideas, develop innovations (including curricular innovations), and address critical policy questions through a mechanism that no single institution or entity could muster on its own. For example, the network is making solid progress statewide in finding ways for cybersecurity students to obtain the security clearances needed for internships in business and government settings.

Encourage and facilitate deep corporate engagement. Dedicated corporate engagement enhances corporate philanthropy. The ACES and Cyber Scholars programs have been successful because Northrop Grumman, the corporate partner in both programs, has brought far more than money to the table. Northrop representatives have been deeply and consistently engaged in shaping the design and implementation of the programs on a monthly, weekly, and sometimes daily schedule.

The depth of corporate engagement in the Maryland cyber activities has been notable. Corporate advisors have helped to shape the educational components—from curricula to credentialing—to ensure that what is taught aligns with business needs. Moreover, they recommend adjunct faculty with practical experience, host on-site visits, as well as find corporate mentors and internships for students.

Recognize and honor culture and traditions. Corporate participation works best when it is consistent with corporate policies and traditions. Partnerships should be designed to respect the corporate partner's unique traditions, practices, and cultures. For example, Parsons continued its decades-long tradition of supporting educational institutions and organizations in the communities where it operates by providing scholarships for 24 students in the ACES program.

Build strength through multi-level partnerships. The successes of the ACES and Cyber Scholars programs are also attributable to the commitment of individuals at multiple levels and points throughout the process. Engagement at the CEO level assisted in conceptualizing the program and in driving expectations about ongoing progress. At the same time, partnerships among corporate representatives and university faculty and administrators were essential to completion of the day-to-day work to operationalize the concepts and bring the programs online.

Strengths of small businesses. Business-higher education partnerships can and should create opportunities for smaller companies to participate. Although many of the major stakeholders in the cybersecurity industry are large, well-established companies, the nature of the industry is such that many of the innovative companies in the field are smaller firms, including start-ups. Current participants in the BHEF Maryland initiative cited the importance of providing gateways for some of these smaller firms to partner with universities around cybersecurity academic programs. Although smaller firms likely are not able to make large financial contributions or provide extensive operational support, they can participate in other ways, such as serving as adjunct faculty, providing speakers for student programs, and offering students paid internships.

Below: The female members of the first ACES cohort.

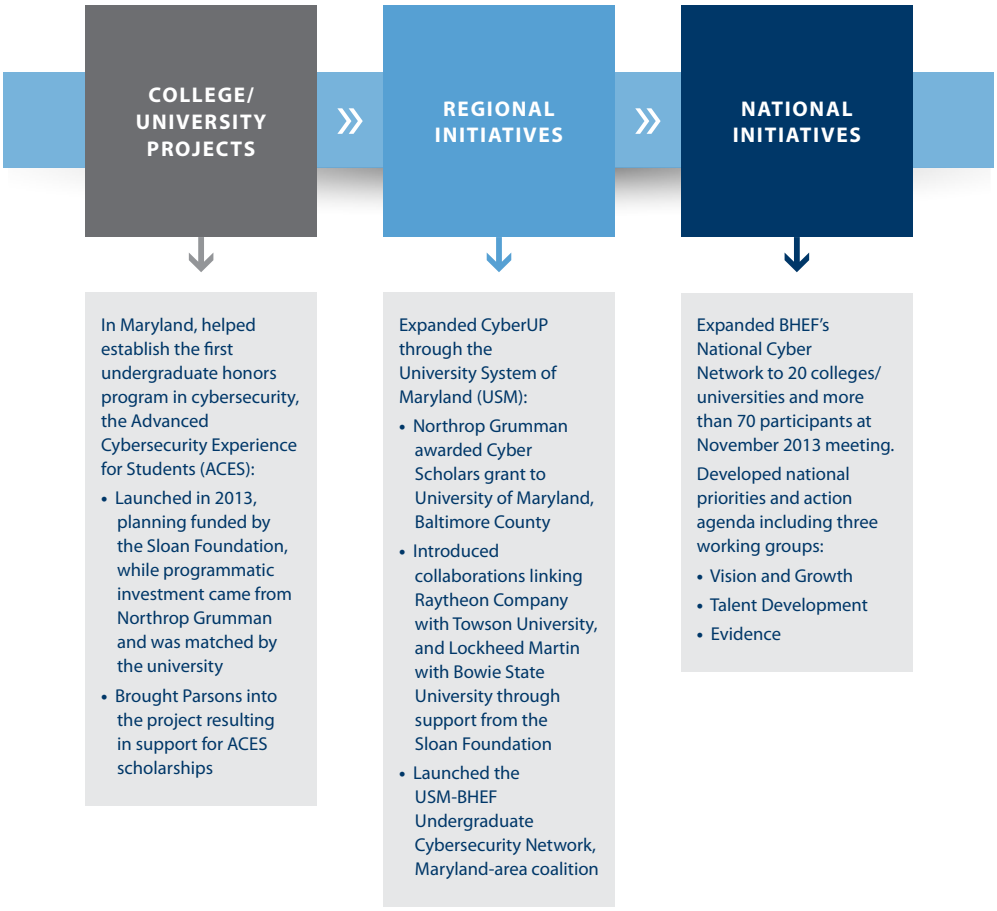
Photo by John T. Consoli/University of Maryland

Next Steps: Further Scaling the BHEF Initiative

BHEF has played a central facilitating role in the Maryland cyber initiative by identifying and convening potential academic, public, and private partners. BHEF works to sustain relationships among partners and to maintain overall enthusiasm for the project from conceptualization through implementation. Moreover, BHEF aims to gather and analyze insights from the Maryland experience, document them, and disseminate them broadly. BHEF has considerable experience in this regard and has gained insight into how to most effectively scale Maryland's activities at the national level. Going forward, BHEF has identified a number of steps that will be necessary to further consolidate the gains that have already been realized in the Maryland initiative and to adapt, translate, and disseminate what has been learned from projects in other regions.

BHEF has begun to characterize the practical steps that constitute effective cybersecurity partnerships between business and higher education. The insights gained through the Maryland initiative, as well as other regional projects, are invaluable in informing strategies that are being considered and implemented in other disciplines. It will be important to further understand the roles of all relevant stakeholders—universities, philanthropies, businesses, industry and professional associations, government agencies, community colleges, and others—in such partnerships. A vital future step, therefore, will be to document these processes more formally and to further tease out insights from the Maryland initiative.

EXPANSION CHANNEL STRATEGY, CYBER ILLUSTRATION



National Cybersecurity Network

As part of its efforts to scale insights from the Maryland experience, BHEF convened a National Cybersecurity Network in December 2012. BHEF's vision for this dimension of its work is to sustain a national network of experts from higher education, business, and government who can serve as the intellectual hub of undergraduate cybersecurity and promote cooperation around cybersecurity education among the academic, business, and government sectors.

In practical terms, the national network serves as a platform for information sharing, discussions, and collection of undergraduate cybersecurity resources. It provides a forum for dialogue between business and higher education about persisting gaps in cybersecurity workforce skills and provides a venue for establishing the groundwork and developing the strategies needed to address these gaps. The network also provides a scaling and dissemination vehicle for BHEF regional projects and a channel through which regional projects can both learn from and inform national efforts.

The second meeting of the network took place in November 2013, involving more than 70 representatives from business, higher education, government, and other stakeholder organizations. Over the course of one year, the network grew from 15 to 70 academic, business, and government organizations. The 2013 gathering highlighted the continuing need for industry and government to address major challenges in recruiting and, increasingly, retaining cybersecurity talent. Higher education institutions are a critical partner in solving this challenge.

However, skills and competencies need to be better defined. Fortunately, NIST's NICE initiative is developing a framework for a common lexicon for the cyber workforce, which will provide an important structure for current and future partnerships. Furthermore, meeting participants agreed that the intersection of cybersecurity and data science is one of increasing importance given the rapidly expanding volumes of data in cyber. Both cyber specialists and cyber-enabled professionals will need to be equipped with skills and competencies in these areas.

CyberUP

In fall 2013, BHEF received a planning grant from the Bill & Melinda Gates Foundation to develop a strategy—*CyberUP*—for creating or expanding pathways that provide students with industry-approved credentials as they pursue their postsecondary education. BHEF, in partnership with Accenture, has designed a plan to leverage the work underway in Maryland and to expand undergraduate cybersecurity programs in different geographic areas that will unlock the potential of industry-recognized cybersecurity credentials.

As described above, BHEF's research indicates that appropriate undergraduate academic coursework, combined with work experience and third-party validated professional certifications, are essential to meet industry cybersecurity needs. *CyberUP* will leverage industry and government partners to define cybersecurity pathways in specific regions and nationally by developing industry-recognized credentials and bridging the three areas of academic coursework, professional certifications, and work experience. Particular focus will be placed on underrepresented minorities, women, and veterans.

Five expansion strategies are underway: (1) scale and strengthen existing USM programs, (2) strengthen the BHEF-USM Cyber Network and expand to more institutions, (3) expand throughout the Greater Washington, D.C. regional area, (4) establish a cyber network in a new geographic area: Massachusetts, and (5) implement the National *CyberUP* Network and plan for future growth. Each strategy has explicit goals that, when combined, create a disruptive approach to developing a diverse talent pool in an emerging and important field, with plans for scaling and sustaining projects.

Benefits to students include: increased opportunity for all students to pursue and complete industry-recognized credentials through academic programs and professional certifications; expanded access to applied and relevant work experiences while pursuing a degree; and increased access to mentors and wraparound services, such as financial support for low-income students.

Universities and community colleges benefit from the development of new and expanded programs and courses in cybersecurity; increased enrollment and persistence of underrepresented and low-income populations, leading to high-skill, high-demand careers; recognition as a leader in cybersecurity; and development of clear pathways from community college to a four-year institution.

Business benefits through access to a pool of cybersecurity talent that meets its needs; increased quality of work-ready students persisting in higher education; increased diversity in the talent pool, including low-income and underrepresented populations; and deeper alignment of higher education credentials with industry needs.

BHEF and *CyberUP* partners will employ a strategic approach that includes the following elements: needs analysis and asset mapping, competency mapping, strategic meetings, webinars and conference calls, and business plan development. This process will allow BHEF to develop and scale solutions that forge strategic links between higher education and business to drive innovation needed for regional and national economic competitiveness. *CyberUP* leverages BHEF's national footprint in cybersecurity, and insights from the Maryland initiative will inform scaling efforts in other regions.

Left: UMBC Cyber Scholars students. Right: BHEF Immediate Past Chair and Northrop Grumman Corporation Chairman, CEO, and President Wes Bush. Below: UMBC Cyber Scholars with Stephanie C. Hill, Lockheed Martin (second from right), and program director Dr. Anupam Joshi (far right).


Photo by JMarlayna Demond for UMBC


Photo by John T. Consoli/University of Maryland


Photo by JMarlayna Demond for UMBC

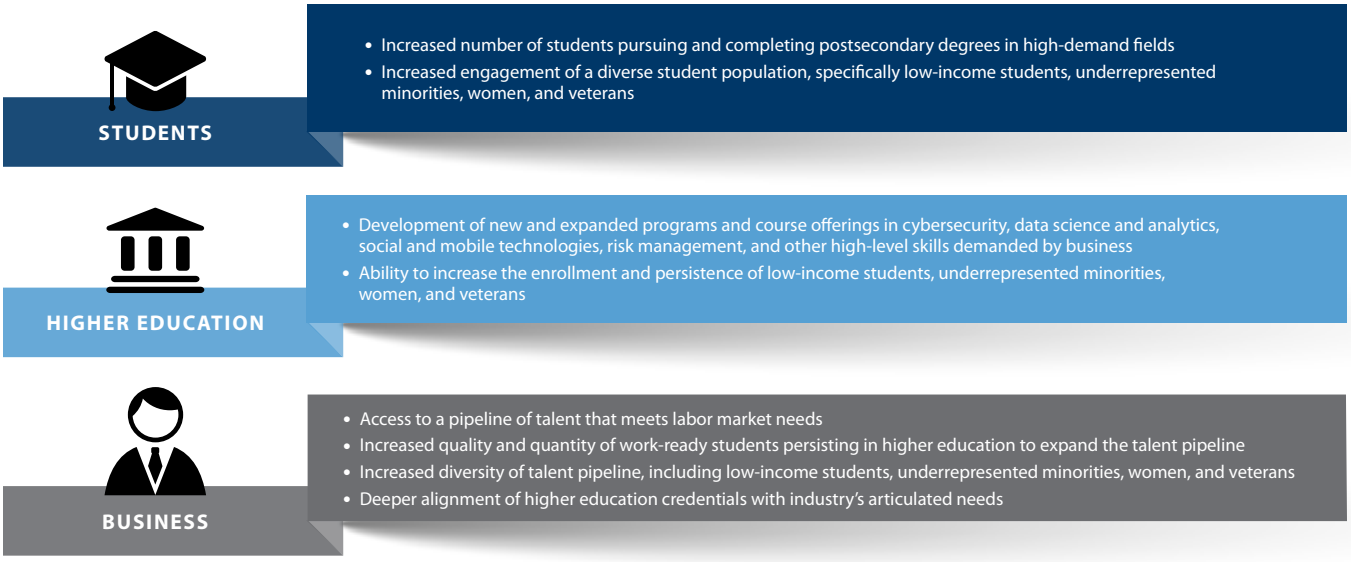
Conclusion

Maryland's cybersecurity education initiative is still developing and will be closely watched and studied by others contemplating similar efforts in their region. Importantly, it encapsulates BHEF's vision for HEWI, in terms of its planning and deployment as well as how it can be modified and implemented across the country.

BHEF's specific successes in Maryland are significant. Students are now enrolled in robust new undergraduate cybersecurity programs at UMD and UMBC. New curricula have been developed in cybersecurity, particularly at UMD. The groundwork has been established to expand cybersecurity programs at both Bowie State University and Towson University. In those processes, BHEF developed new strategies for engaging partnerships in Maryland, especially between business and higher education, which can increase the recruitment and persistence of students in key STEM fields and other vital disciplines. By developing the USM-BHEF Undergraduate Cybersecurity Network, BHEF has created a learning ecosystem of expertise and resources that will expand its current knowledge throughout the greater Washington, D.C. area, and derive and codify strategies to scale BHEF's work nationally to new market-driven locations, such as Massachusetts.

BHEF's work in Maryland illustrates that it is possible to rapidly effect significant change and innovation in higher education with the goal of better aligning curricula and student outcomes with needed workforce skills. This pace of change hinges on the genuine commitment, expertise, and investment of resources by motivated stakeholders. BHEF is encouraged by this progress and believes these outcomes can be successfully scaled elsewhere in the country to the benefit of students, business, and higher education.

BENEFITS TO STUDENTS, BUSINESS, AND HIGHER EDUCATION



Beyond Maryland: Sampling of BHEF's Regional Higher Education and Workforce Projects

Cybersecurity and Information Technology

- **Case Western Reserve University** and **Eaton Company**: Increasing the persistence and transfer of community college students in information technology.
- **Cal Poly San Luis Obispo**, **Northrop Grumman Corporation**, and **Raytheon Corporation**: Building a new undergraduate cybersecurity curriculum and laboratory.
- **Miami Dade College** and **NextEra Energy**: Developing a new bachelor's degree program for students with associate's degrees in information technology and cybersecurity.
- **San José State University** and **Bay Area Council**: Creating a Silicon Valley Center for Cybersecurity focused on cyber hygiene for computer science students.
- **The University of Massachusetts**, **Massachusetts Competitive Partnership**, and **Advanced Cyber Security Center**: Launching regional projects and a network to respond to the high demand for cyber-enabled professionals, principally in commercial sectors.

Data Science and Analytics

- **Case Western Reserve University**, **Accenture**, **Eaton**, **FirstEnergy**, **IBM**, **KeyBank**, and **Medtronic**: Creating a distinctive undergraduate degree program in data science with a focus on specific domain areas of health, energy, and manufacturing and production.
- **The City University of New York (CUNY)** and **IBM**: Building pathways for CUNY undergraduates and community college students in energy sustainability and large-data analytics.
- **The Ohio State University** and **Battelle Memorial Institute**: Developing new undergraduate courses in large-scale data analytics and data science.

Engineering and Computer Science

- **Washington University in St. Louis** and **The Boeing Company**: Increasing the transfer of students from St. Louis community colleges and the University of Missouri-St. Louis into bachelor's engineering programs.

Higher Education-Workforce Alignment Around High-Demand Clusters

- **Drake University** and **Principal Financial Group**: Strengthening the education-workforce pipeline in high-demand fields such as biosciences, financial services, and health professionals.
- Louisville's **Business Leaders for Education**: Addressing the skills misalignment to strengthen the education-workforce pipeline in high-demand fields such as advanced manufacturing, food and beverage manufacturing and innovation, value-added logistics and distribution, and lifelong wellness and aging care.

Water Science

- **The University of Wisconsin System** and the **Milwaukee Water Council**: Expanding opportunities in water science for undergraduates across the system, and recruiting and retaining students from community colleges into four-year programs.

National HEWI Scaling Partners

Aerospace Industries Association

American Council on Education

Association of American Universities

Association of Public and Land-grant Universities

Business Roundtable

National Defense Industrial Association

Office of Naval Research


Product

BHEF BUSINESS-HIGHER EDUCATION FORUM®

Creating Solutions. Inspiring Action.®

2025 M Street NW, Suite 800 • Washington, D.C. 20036
Phone (202) 367-1189 • Fax (202) 367-2100
www.bhef.com