Building the Cybersecurity Workforce

The Business-Higher Education Forum’s National Higher Education and Workforce Initiative

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 cross-disciplinary fields such as computer science, cybersecurity, data science and analytics, and engineering. Assuring dynamic growth in the U.S. economy in the 21st century will require a workforce with mastery of core content knowledge and experience in these fields. To address this challenge, the Business-Higher Education Forum (BHEF)—Fortune 500 CEOs, presidents of colleges and universities, and other leaders—has launched the National Higher Education and Workforce Initiative (HEWI). This national effort creates partnerships between universities and businesses to help ensure there will be a qualified pool of applicants for jobs in high-skill, high-demand fields. HEWI’s first project focused on cybersecurity.
The Case for a Cybersecurity Workforce

According to a 2014 report from Burning Glass Technologies, from 2007 to 2013 the national demand for cybersecurity professionals grew 74 percent. Some states report demand at more than twice that rate. Additionally, this growth of cybersecurity jobs is more than twice that of all information technology (IT) jobs.¹

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, and threats to U.S. federal data increased by 700 percent from 2006 to 2011.² 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.

Developing a Cybersecurity Ecosystem

BHEF’s work in cybersecurity began in Maryland, with the University System of Maryland (USM), regional businesses, government agencies, and other stakeholders engaged in building a system-wide, multi-level response to the state’s—and nation’s—cybersecurity workforce challenges. The work has evolved to include campus-based projects, expansion to multiple campuses in the system, the creation of a regional network, and the formation of a national cybersecurity network.

With support from Accenture and the Bill & Melinda Gates Foundation, BHEF developed a business plan to expand its cybersecurity work. It focuses on new career pathways that integrate academic experience, industry-approved credentials, and work experience. The business plan also provides the foundation for a broader cyber expansion strategy in the Maryland, D.C., and Virginia region, in which partners will co-create cyber competency maps, multiple academic and career pathways, and new undergraduate cyber programs connecting two- and four-year colleges and universities.

With additional support from the Office of Naval Research, BHEF is addressing the U.S. Navy’s cybersecurity workforce needs by building on-ramps to cyber careers. This effort broadens BHEF efforts with USM by increasing the quality, enrollment, persistence, and diversity of existing USM cyber programs into the broader Washington, D.C., metropolitan area and Virginia, and boosts the number of partnerships with community colleges. It will leverage the growing Naval cyber presence in the Tidewater Virginia region and work closely with local academic institutions to build a 2+2 program and network to build a cyber pipeline to Navy-relevant employees.

Regional Case Study: Developing Maryland’s Cyber Workforce through University Systems and Networks

BHEF’s work in Maryland illustrates that it is possible to affect swift, significant change and innovation in higher education with the goal of better aligning curricula and student outcomes with needed workforce skills. To date, BHEF’s efforts in Maryland include progress throughout USM as well as with a network of partners.

The Advanced Cybersecurity Experience for Students at the University of Maryland (ACES)

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. BHEF was instrumental in helping the University of Maryland, College Park receive a $1.1 million grant from the Northrop Grumman Foundation to support the development of the ACES program.

The program 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. Overall, ACES emphasizes combining classroom knowledge and skills with real-world, flexible, hands-on experience.
Cyber Scholars at the University of Maryland, Baltimore County (UMBC)

As a second major achievement, BHEF supported a partnership between UMBC and Northrop Grumman, which launched the UMBC Cyber Scholars program with a $1 million grant to UMBC from the Northrop Grumman Foundation. The Cyber Scholars program had an initial cohort of nine students, including four women. The program will grow by 15 to 20 new scholars annually, with special emphasis on increasing the number of women and underrepresented minorities.

The program models many of the interventions that BHEF research and modeling have shown to be effective.

■ 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.

The USM-BHEF Undergraduate Cybersecurity Network

The USM-BHEF Undergraduate Cybersecurity Network, comprised of 30 representatives from academia, business, government, and stakeholder organizations, launched in April 2013. The network supports a 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. These stakeholders form a regional ecosystem that identifies, nurtures, and grows the highest-impact cybersecurity learning opportunities for USM undergraduates in alignment with workforce needs.

Future Cyber Leaders Internship Program

A component of BHEF’s Greater Washington Regional Network, the program uses a high-impact cyber recruitment and retention strategy which places undergraduates in corporate and government internships. For eight weeks in the summer, this select group of students will be part of a living learning community that will provide them with cyber academic achievement experiences and leadership building and networking opportunities. BHEF’s anticipated first cohort of 50 interns will be based at George Mason University.

Building a STEM/Cybersecurity Pathway in Massachusetts

Massachusetts is the first expansion site of BHEF’s strategy. Using insights from the Maryland model, the University of Massachusetts System (UMass) will create institution-based projects and launch the Massachusetts Cybersecurity Network. UMass commissioned a high-level task force of representatives from each campus to identify and scope new undergraduate cyber programs. As one of BHEF’s five member sites supported by the $4.5M National Science Foundation award, UMass and its partners will focus on diversity and work with community colleges to establish new pathways for their students to pursue a four-year degree in cyber.

National Cybersecurity Network

As part of BHEF’s efforts to scale insights from the Maryland experience, BHEF convened a National Cybersecurity Network. 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.
Potential Engagement Opportunities with Cybersecurity and HEWI

- Provide placements for summer and academic year research experiences and internships for undergraduate students as early as the freshman year of college
- Co-develop new interdisciplinary courses and materials with college professors
- Support bridge programs for community college students that encourage successful transfer to four-year baccalaureate programs
- Offer incentives and support mechanisms proven effective in attracting and retaining low-income students, underrepresented minorities, veterans, and women
- Participate or support hack-a-thons in cybersecurity
- Provide mentors for undergraduate students
- Serve as speaker in undergraduate courses
- Provide case studies that can be incorporated into undergraduate courses
- Offer seminars to complement undergraduate programs of study
- Support co-op programs, which provide students with academic credit for structured, on-the-job learning
- Conduct workshops and exchanges for faulty, which focus on cutting-edge fields such that faculty can integrate this knowledge into current courses
- Provide data sets that can be used by undergraduate students