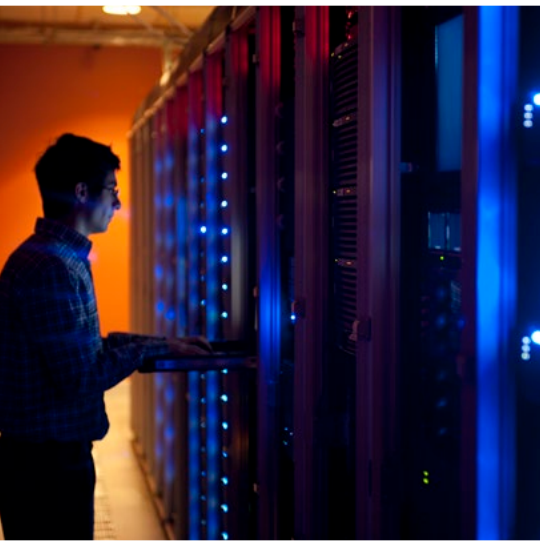
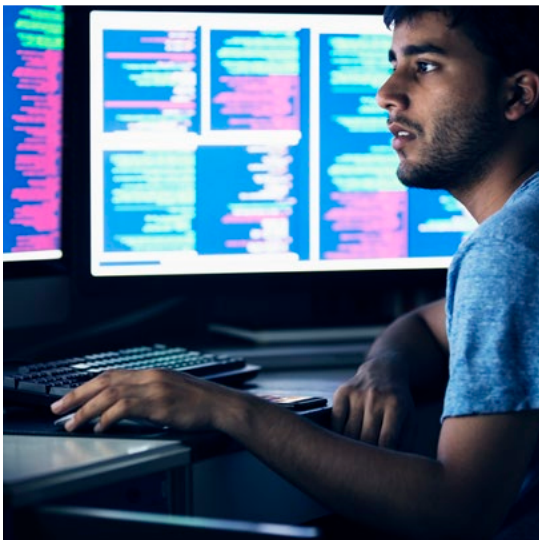
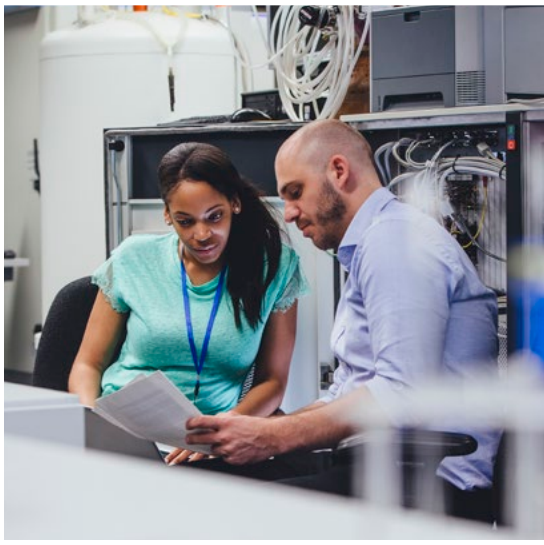
INVEST TO IMPROVE
THE CYBERSECURITY TALENT DEFICIT





BHEF BUSINESS-HIGHER EDUCATION FORUM®

Creating Solutions. Inspiring Action.

ACKNOWLEDGEMENTS

We would like to acknowledge the Office of Naval Research for their significant support for this work.

EDITORIAL TEAM

L. Isabel Cárdenas-Navia
Director of Emerging Workforce Programs
Business-Higher Education Forum

Janet Chen
Associate Director
Business-Higher Education Forum

Karen Elzey
Vice President
Business-Higher Education Forum

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

Ursula Gross
Director, Strategic Communications
Business-Higher Education Forum

Debbie Hughes
Vice President, Higher Education and Workforce
Business-Higher Education Forum

JOIN US IN CREATING SOLUTIONS

INVEST TO IMPROVE: *THE CYBERSECURITY TALENT DEFICIT* provides recommendations for cybersecurity stakeholders—employers, government agencies, and higher education institutions—to enable regional partnerships to meet today's cybersecurity skills needs. This report combines data from a 2017 Gallup survey of business executives and higher education leaders with jobs analyses from Burning Glass Technologies, as well as, for the first time, detailed student demographic and wage data—following them from their college studies to the cybersecurity profession. The findings of this report document the need to develop new approaches to nurture cybersecurity talent in an era in which employers from all sectors must protect their information and systems from extraordinary levels of risk.

The unceasing nature and increasing sophistication of cyber attacks requires expansion of the cybersecurity workforce, from entry level to expert. While many higher education institutions offer cybersecurity programs, the United States faces a significant shortfall in the number of cybersecurity professionals, which is only expected to grow. Closing this talent gap—and providing employers with the workforce they need to protect their organizations—will require the development and expansion of strategic partnerships between business and higher education.

The Business-Higher Education Forum (BHEF) has catalyzed dozens of such partnerships. As the nation's oldest membership organization of Fortune 500 CEOs, college and university presidents, and other leaders dedicated to the education of a highly skilled future workforce, BHEF and our members form strategic partnerships to build new undergraduate pathways, improve alignment between higher education and the workforce, and produce a diverse, highly skilled talent pool to meet demand in emerging fields.

BHEF members have been leaders in developing strategic partnerships in cybersecurity. Members in California, Illinois, Maryland, Massachusetts, and New York—among other regions—have created innovative new pathways in cybersecurity. These pathways reflect the differences in the skills needs and workforce gaps that exist among these regions. Effectively meeting regional talent needs requires a nuanced understanding of the cybersecurity skills requirements in each locale.

Toward this goal, BHEF has developed this assessment of the current state of cybersecurity demand and higher education's response. We hope the following pages will inspire you to take action and join us in building strategic business-higher education partnerships to develop the cybersecurity talent that our economy needs.

Brian K. Fitzgerald, Ed.D.
Chief Executive Officer

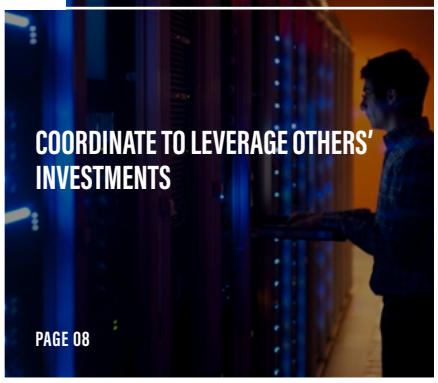
TAKING ACTION TO BUILD WORKFORCE CAPABILITY

This report outlines seven recommendations that stakeholders can pursue to support the development and retention of professionals with the necessary cybersecurity skills. Closing this talent gap will be a significant challenge, but collaborations between employers, educators, and government officials can develop a workforce capable of meeting today's cyber risks.

RECOMMENDATIONS FOR ACTION

STRATEGIC INVESTMENTS FOR EMPLOYER-HIGHER EDUCATION COLLABORATIONS

1 ALIGN INVESTMENTS TO SUPPORT A CYBER WORKFORCE:



COORDINATE TO LEVERAGE OTHERS' INVESTMENTS

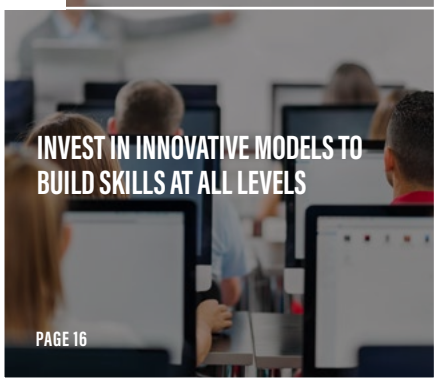
PAGE 08

2 RE-EXAMINE THE ROLE OF CERTIFICATIONS IN HIRING AND CAREER DEVELOPMENT:

MODERNIZE CERTIFICATIONS TO REDUCE CONSTRAINTS ON HIRING TALENT

PAGE 12

3 CREATE NEW MODELS TO DEVELOP TALENT:



INVEST IN INNOVATIVE MODELS TO BUILD SKILLS AT ALL LEVELS

PAGE 16

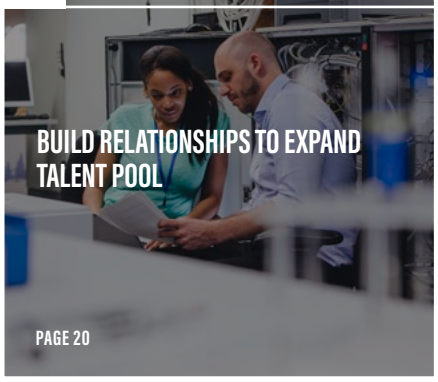
STRATEGIC INVESTMENTS FOR EMPLOYERS

4 FOCUS THE TALENT RECRUITMENT MODEL ON CAREER MISSION AND OPPORTUNITIES:

CAPITALIZE ON THE INCREASED PUBLIC INTEREST IN CYBERSECURITY

PAGE 18

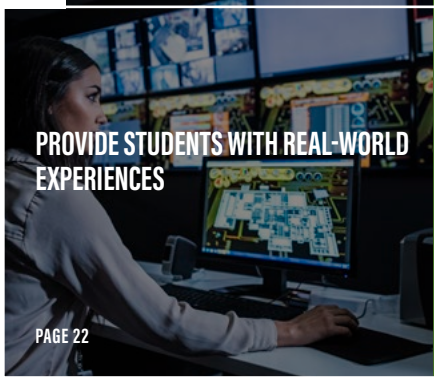
5 INVEST AND RECRUIT AT HIGHER EDUCATION INSTITUTIONS WITH DIVERSE STUDENT POPULATIONS:



BUILD RELATIONSHIPS TO EXPAND TALENT POOL

PAGE 20

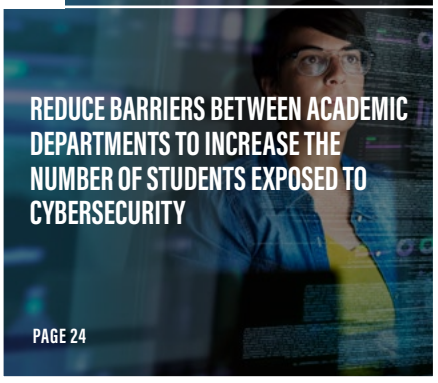
6 GRADUATE STUDENTS WITH PROVEN SKILLS NEEDED FOR A CYBERSECURITY CAREER:



PROVIDE STUDENTS WITH REAL-WORLD EXPERIENCES

PAGE 22

7 DESIGN INCLUSIVE EDUCATIONAL PATHWAYS:



REDUCE BARRIERS BETWEEN ACADEMIC DEPARTMENTS TO INCREASE THE NUMBER OF STUDENTS EXPOSED TO CYBERSECURITY

PAGE 24

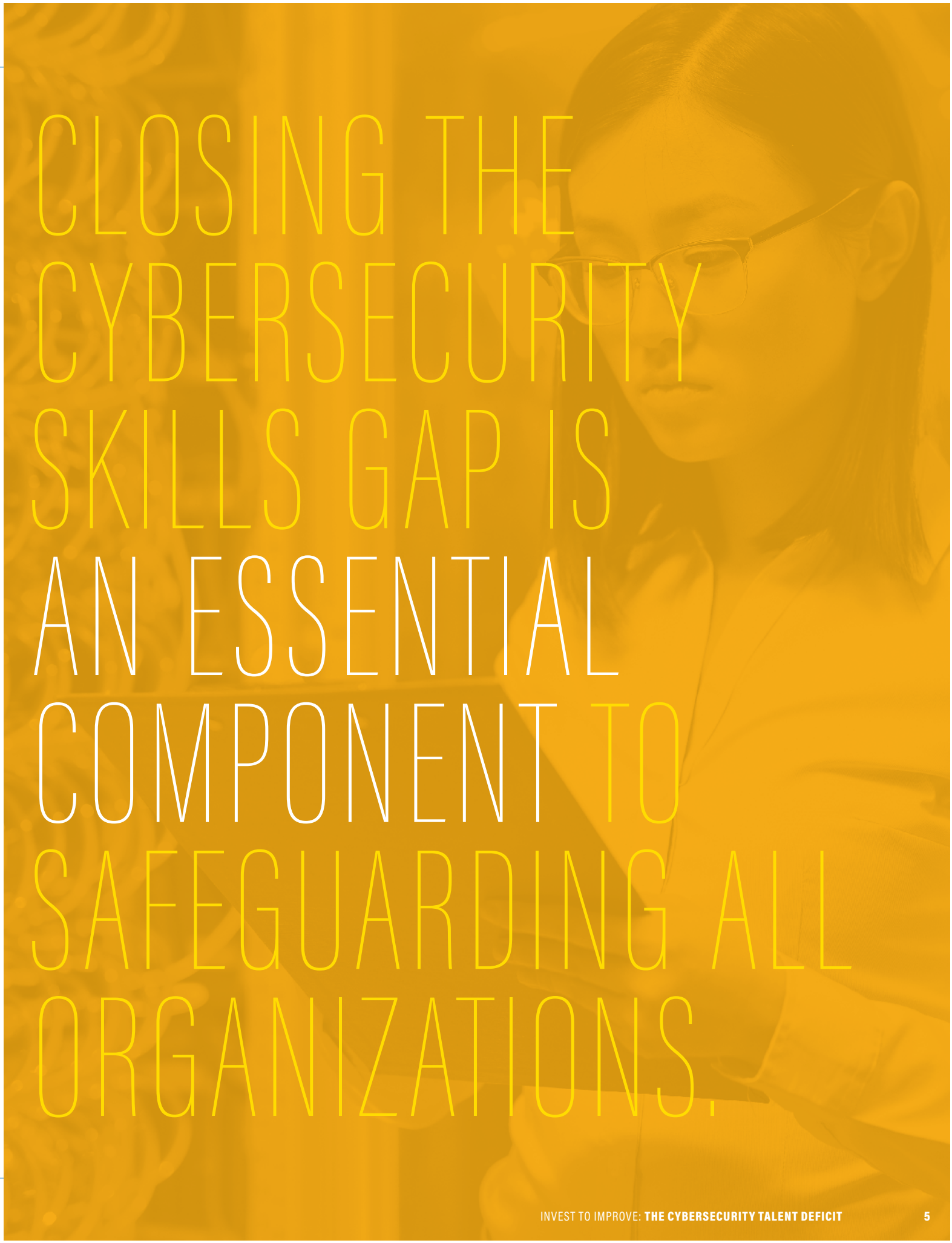
STRATEGIC INVESTMENTS FOR HIGHER EDUCATION

THE TALENT IMPERATIVE: WHAT IS AT STAKE

THE CYBERSECURITY TALENT GAP IS WIDENING.[1]

Approximately 209,000 positions went unfilled in 2015, and demand is expected to continue to grow.[2] This talent deficit directly impacts an organization's ability to protect itself. Seventy-one percent of employers have incurred damages because of this deficit, including data loss and targeting by hackers.[3] Given the daily reports of successful hacks against companies, government agencies, and other organizations, closing the cybersecurity skills gap is an essential component to safeguarding all organizations.

1. The 2015 (ISC)2 Global Information Security Workforce Study, Frost & Sullivan, 2015.
2. Demand to Fill Cybersecurity Jobs Booming, Ariha Setalvad, March 31, 2015.
3. Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills, Center for Strategic and International Studies, 2016.



CLOSING THE CYBERSECURITY SKILLS GAP IS AN ESSENTIAL COMPONENT TO SAFEGUARDING ALL ORGANIZATIONS.

The need to increase investment in cybersecurity talent is high both within the United States and abroad. However, within the United States, the skills gaps and talent needs vary by region. **Burning Glass Technologies examined the demand for cybersecurity talent in the greater New York City metropolitan region, Maryland, Washington, DC, and Virginia, and Massachusetts and found differing certification/skills needs.** The industry sectors with the highest needs for cybersecurity talent also differed by region, reflecting their unique economic strengths. These findings highlight the importance of employers, higher education institutions, and government working together to take action at the regional level.

REQUIRED CYBERSECURITY CERTIFICATIONS VARY BY REGION

RANK	MD/DC/VA	MASS.	NYC
1	CISSP	CISSP	CISA
2	Security+	CISA	CISSP
3	CISA	CISM	CISM

INDUSTRY SECTORS WITH THE MOST CYBERSECURITY POSTINGS VARY BY REGION

RANK	MD/DC/VA	MASS.	NYC
1	Professional Services & Defense	Professional Services	Finance/ Insurance/ Accounting
2	Public Administration	Manufacturing & Defense	Professional Services
3	Finance	Finance & Insurance	Information

SOURCE: Burning Glass Technologies May 2015 analysis for Maryland, Washington, DC, and Virginia; January 2014 analysis for Massachusetts; and August 2014 analysis for the New York City Metropolitan area.

The cost of not investing in a robust cybersecurity talent pool is high: the average cost of a data breach for a company is $4 million. Costs are higher for companies in highly regulated sectors such as financial services and health care.[4] Only 25 percent of business executives strongly agree that their company can effectively respond to a cyber-attack. Furthermore, companies experience greater difficultly filling cybersecurity roles than other roles.[5] Therefore, the rationale for employers to increase their investment in talent development is strong.

Government institutions and agencies are also highly motivated to invest in and support new models that expand and diversify cybersecurity talent. As leaders in setting cybersecurity policies and regulations, guardians of highly confidential data, and funders of higher education institutions, federal and state governments are not only impacted by the talent deficit, but also well positioned to facilitate and guide investment by other stakeholders.

Although higher education is investing in and growing its cybersecurity programs, a gap remains between the skills graduates possess and the skills employers seek. Only 16 percent of business executives believe that hiring directly from a college or university is a very effective strategy to obtain cybersecurity talent. Less than one-quarter of employers say that education programs prepare students to enter cybersecurity careers. Although employers require cybersecurity employees to hold a bachelor's degree, they rank acquiring hands-on experience and professional certifications as better approaches to gaining cybersecurity skills than a earning a four-year degree. Given the significant competition from alternative education providers, higher education institutions must invest and adapt to better prepare students who pursue cybersecurity careers.

4. 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2016.
5. Understanding Cybersecurity Talent Needs: Findings from Surveys of Business Executives and College Presidents, BHEF and Gallup, 2017.

71%

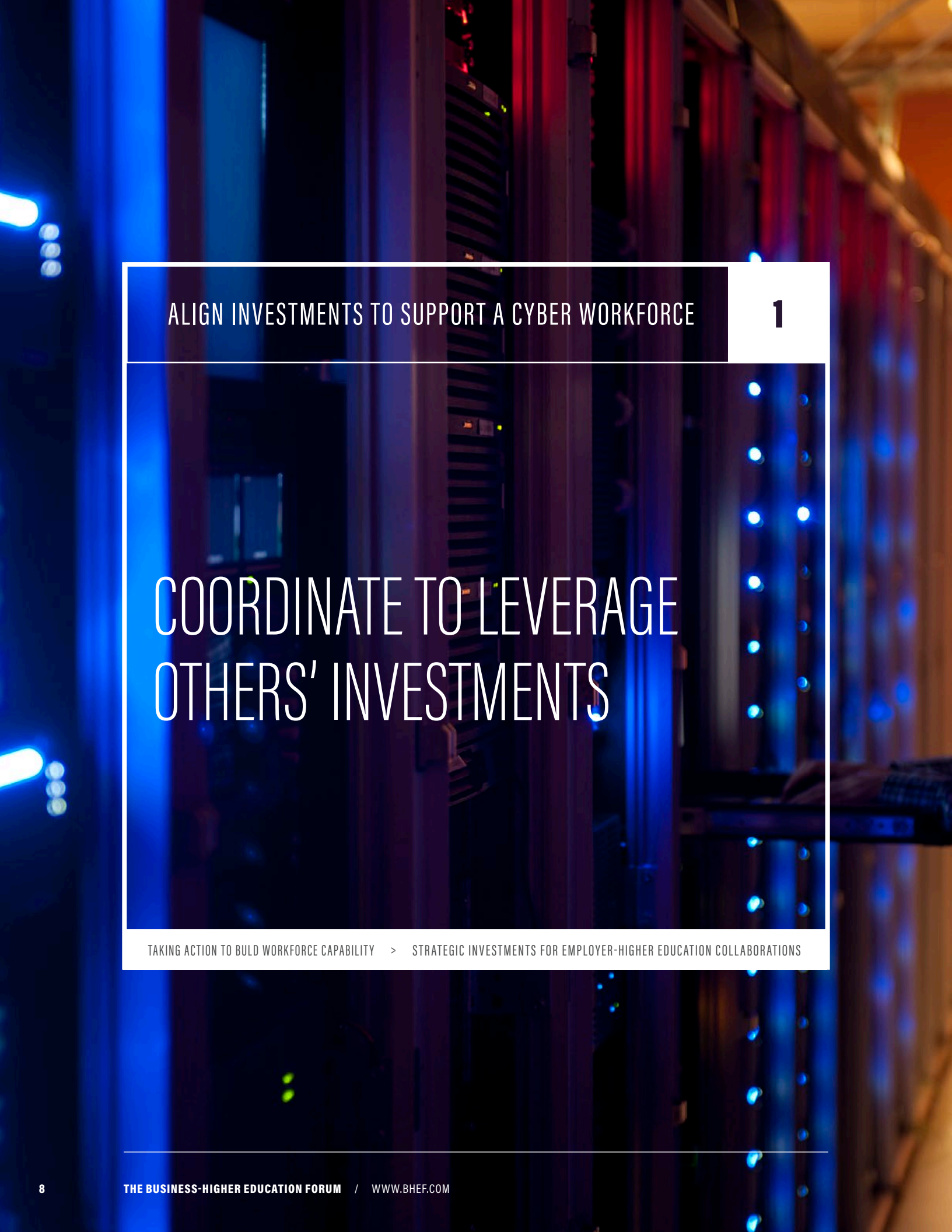
OF EMPLOYERS HAVE INCURRED DAMAGES BECAUSE OF CYBER TALENT DEFICIT

209,000

UNFILLED CYBER POSITION IN 2015

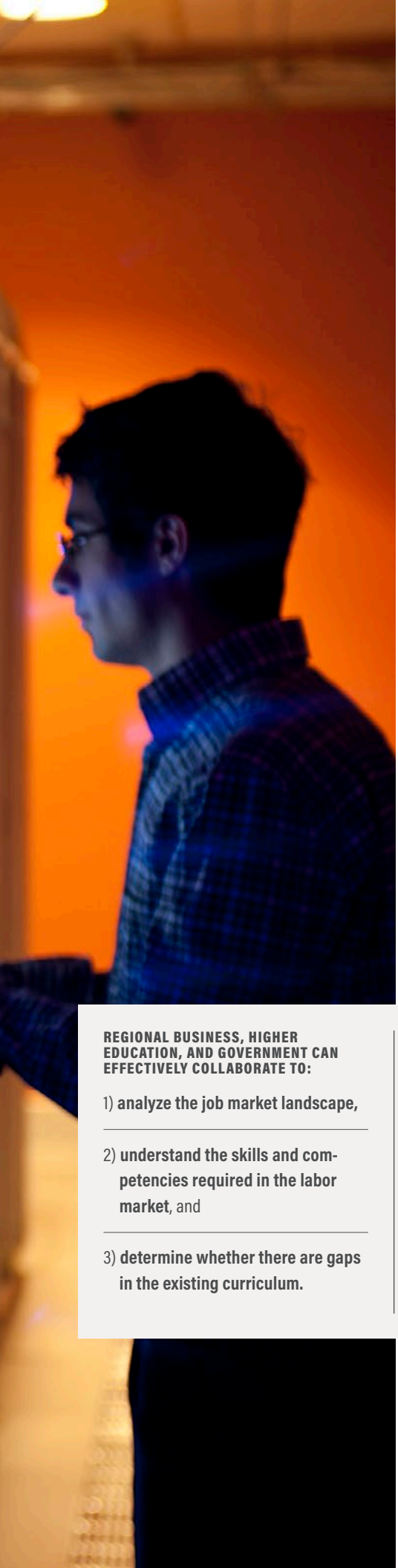
25%

OF BUSINESS EXECUTIVES STRONGLY AGREE THAT THEIR COMPANY CAN EFFECTIVELY RESPOND TO A CYBER-ATTACK



ALIGN INVESTMENTS TO SUPPORT A CYBER WORKFORCE 1

COORDINATE TO LEVERAGE OTHERS' INVESTMENTS



COORDINATING RESOURCES AND INVESTMENTS to meet the demand for cybersecurity workers will reduce costs and facilitate learning for all stakeholders. Higher education institutions primarily self-fund their cybersecurity programs—investing substantial dollars in course development, faculty, and infrastructure. Employers also devote their own funds to provide cybersecurity training to their employees, most of whom already have bachelor's degrees. Aligning these already significant investments will reduce the costs for both higher education institutions and employers.

An effective approach to realize these savings is the formation of regional collaborations between higher education institutions and employers. These partnerships bring regional business, higher education, and government stakeholders together to: (1) analyze the job market landscape, (2) understand the skills and competencies required in the labor market, and (3) determine whether there are gaps in the existing curriculum. Collaborators then use the results of this process to jointly develop new or enhance existing talent pathways that are aligned with the skills needs of employers. Partners take the lead on different tasks and develop strong personal connections with each other. As the collaboration matures, a system is put in place for stakeholders to provide feedback so that the curriculum remains relevant.

REGIONAL BUSINESS, HIGHER EDUCATION, AND GOVERNMENT CAN EFFECTIVELY COLLABORATE TO:

1) **analyze the job market landscape,**

2) **understand the skills and competencies required in the labor market**, and

3) **determine whether there are gaps in the existing curriculum.**

TO BE SUCCESSFUL, THESE COLLABORATIONS SHOULD:

Develop relationships at the individual and organizational levels. Build on strong individual relationships to create champions at all organizational levels to sustain the collaboration.

Tap core competencies and expertise. Use and respect the different intellectual resources, experiences, and skills that the collaborators possess.

Define benefits, roles, and expectations for all stakeholders. Align incentives and clarify responsibilities for each collaborator to ensure appropriate commitment of resources and accountability.

Higher education institutions benefit from these partnerships by developing a strong reputation for graduating cybersecurity professionals with job-ready skills. The competitiveness of graduates in the job market will then lead to increased program enrollment. Higher education institutions also directly benefit from the resources invested in their institution by an employer, such as grants, software, or technical expertise.

Employers benefit by shifting some of the cybersecurity skills development into the classroom, so that they can focus on developing skills specific to their organization. By shaping the curriculum, employers also influence the skills learned by cybersecurity professionals other than their own employees, which could ease future hiring. Equally important, these partnerships provide employers with a reliable source of high quality talent to meet their needs.

> "ACES engages companies at various levels: instructors, mentors, and internship advisors. **Engaging with companies helps to enrich the education for each ACES student** as they gain hands-on learning experiences from professionals in the cybersecurity field."
>
> **MICHEL CUKIER,** DIRECTOR, ADVANCED CYBERSECURITY EXPERIENCE FOR STUDENTS (ACES); ASSOCIATE DIRECTOR FOR EDUCATION, MARYLAND CYBERSECURITY CENTER (MC2); ASSOCIATE PROFESSOR, RELIABILITY ENGINEERING, DEPARTMENT OF MECHANICAL ENGINEERING / UNIVERSITY OF MARYLAND

BHEF has successfully developed a regional cybersecurity partnership in Maryland—the University System of Maryland (USM)-BHEF Undergraduate Cybersecurity Network—with four USM campuses, businesses, government agencies, two-year colleges, and other stakeholders to focus on undergraduate cybersecurity. Through this partnership, members worked to align the cyber workforce requirements of business and government with higher education and to develop innovative programs to expand cyber talent pathways.

Business executives and higher education leaders agree on two collaborative activities to support talent development in cybersecurity: building consensus on security standards and learning from other organizations about security threats. Higher education leaders also believe that a skills framework would help them to prepare students to become cybersecurity professionals.

	BUSINESS EXECUTIVES SAY VERY HELPFUL OR HELPFUL IN BUILDING PIPELINE OF CYBERSECURITY TALENT (N=63)	HIGHER EDUCATION LEADERS SAY VERY HELPFUL OR HELPFUL IN PREPARING STUDENTS WITH CYBERSECURITY SKILLS (N=127)
Consensus between the private and public sector on cybersecurity and online privacy standards	64%	83%
More opportunities to learn from other organizations about cybersecurity threats	83%	86%
A skills framework for cybersecurity that business and higher education can use	BUSINESS EXECUTIVES WERE NOT ASKED ABOUT A SKILLS FRAMEWORK	83%

RE-EXAMINE THE ROLE OF CERTIFICATIONS IN HIRING AND CAREER DEVELOPMENT

2

MODERNIZE CERTIFICATIONS TO REDUCE CONSTRAINTS ON HIRING TALENT

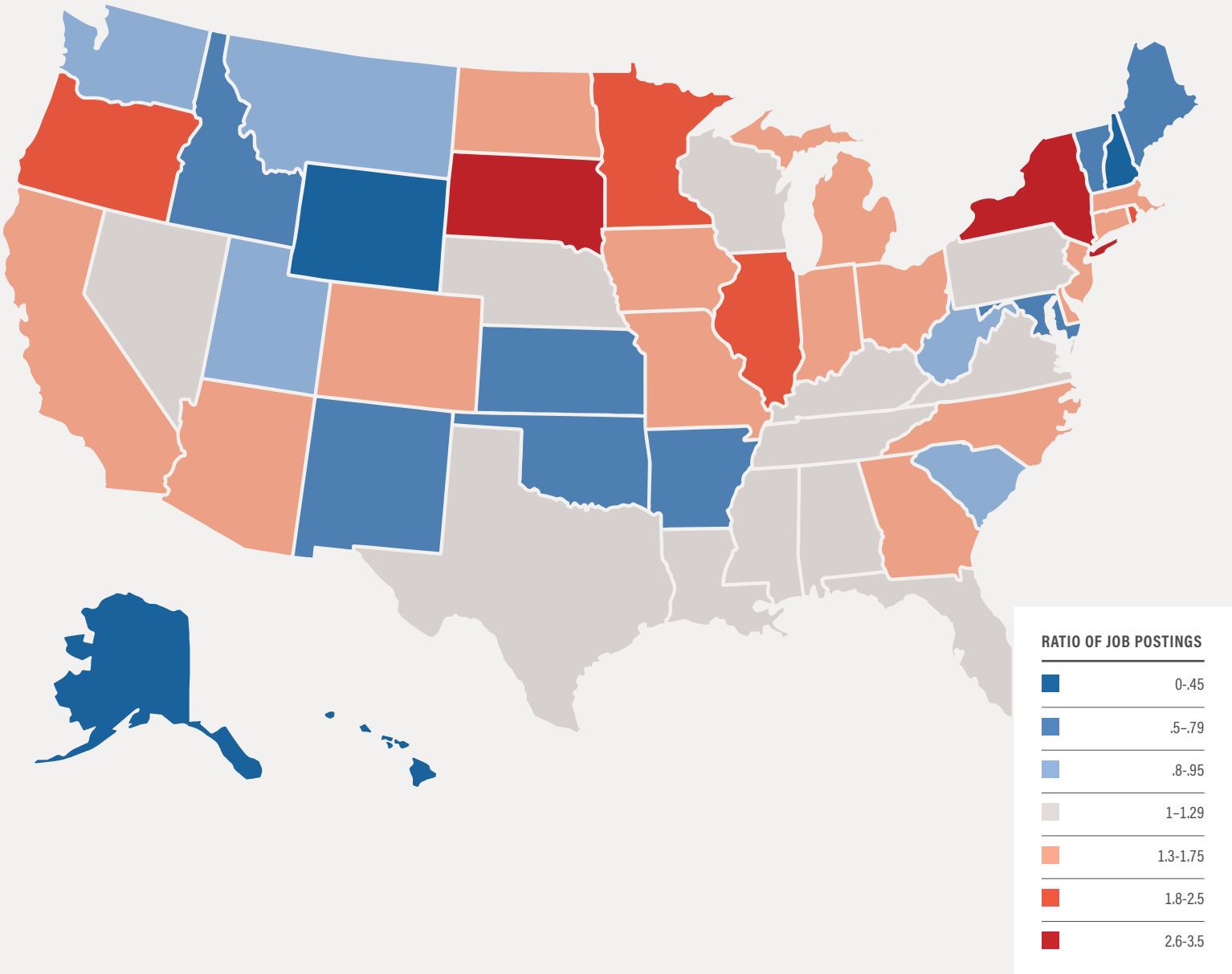
CERTIFICATIONS ARE USED IN CYBERSECURITY AS A PROXY FOR SKILL VERIFICATION. Although a significant number of job postings call for certifications, employers have consistently reported that certifications cannot measure many of the attributes that make individuals successful cybersecurity professionals. For this reason, many employers consider certifications necessary but not sufficient when making hiring decisions.

One qualification not addressed by cybersecurity certifications is hands-on experience with real-world problems. Although certifications commonly screen for years of experience as a proxy for hands-on experience, in some cases this proxy measure has become a significant hiring constraint. This is readily apparent with the CISSP certification, which requires five years of full-time paid work experience in cybersecurity to take the exam. The ratio of job postings requiring a CISSP certification to certification holders averages 1.2:1 across all 50 U.S. states, ranging from a low of 1:2.7 in Hawaii to a high of 3.2:1 in South Dakota.[6] South Dakota would require 167 new CISSP certifications to meet the demand identified in job postings. Even in Hawaii, without a significant number of new CISSP certifications, 37 percent of the 651 existing certification holders would need to switch jobs to fill the current postings.

6. See http://cyberseek.org/heatmap.html.

To address its cybersecurity workforce challenges, the Department of Defense (DoD) is transitioning to a new approach to cybersecurity certifications based more on practical skills and less on theoretical knowledge. Although still in development, the manual for the new DoD Directive 8140 is anticipated to emphasize hands-on simulations of scenarios and situations developed from the real-world. Other federal, state, and local government agencies will likely follow the DoD's lead.

RATIO OF JOB POSTINGS REQUIRING A CISSP CERTIFICATION TO CERTIFICATION HOLDERS



The role of cybersecurity certifications should be re-examined, with the goal of developing a more comprehensive approach to vetting the skills of qualified cybersecurity professionals. This re-examination must recognize the important role that certifications play in providing professionals with a system to signal their skillsets to their peers. In addition, the new approach must be flexible, to ensure its adoption by the different types of education providers that interact with cybersecurity professionals throughout their careers. For example, a new strategy might blend a traditional test with participation in a relevant cybersecurity competition as evidence of hands-on application of the tested subject. Another option would be to have an expert body evaluate topic-specific professional portfolios submitted by individuals.

Developing an inclusive approach to vetting cybersecurity skills will require (1) a common understanding of skills relevant to the cybersecurity professional, including technical *and* nontechnical skills; (2) recognition of the many different types of relevant hands-on experience in cybersecurity (e.g., internships, capstone projects, full-time work); and (3) models, in addition to certification exams, for professionals to showcase their skills.

Many organizations that lead the cybersecurity field—Computing Technology Industry Association (CompTIA), National Initiative for Cybersecurity Education (NICE) led by the National Institute of Standards and Technology (NIST), and Center for Cyber Safety and Education (ISC)[2]—are able to convene stakeholders to re-examine the role of certifications. In addition, significant research is being conducted on new models to showcase skills, including a national effort from the Lumina Foundation.[7]

7. See https://www.luminafoundation.org/credentials..

1:2.7

HAWAII HAS THE LOWEST RATIO OF JOB POSTINGS REQUIRING A CISSP CERTIFICATION TO CERTIFICATION HOLDERS

1.2:1

AVERAGE RATIO OF JOB POSTINGS REQUIRING A CISSP CERTIFICATION TO CERTIFICATION HOLDERS ACROSS ALL 50 U.S. STATES

3.2:1

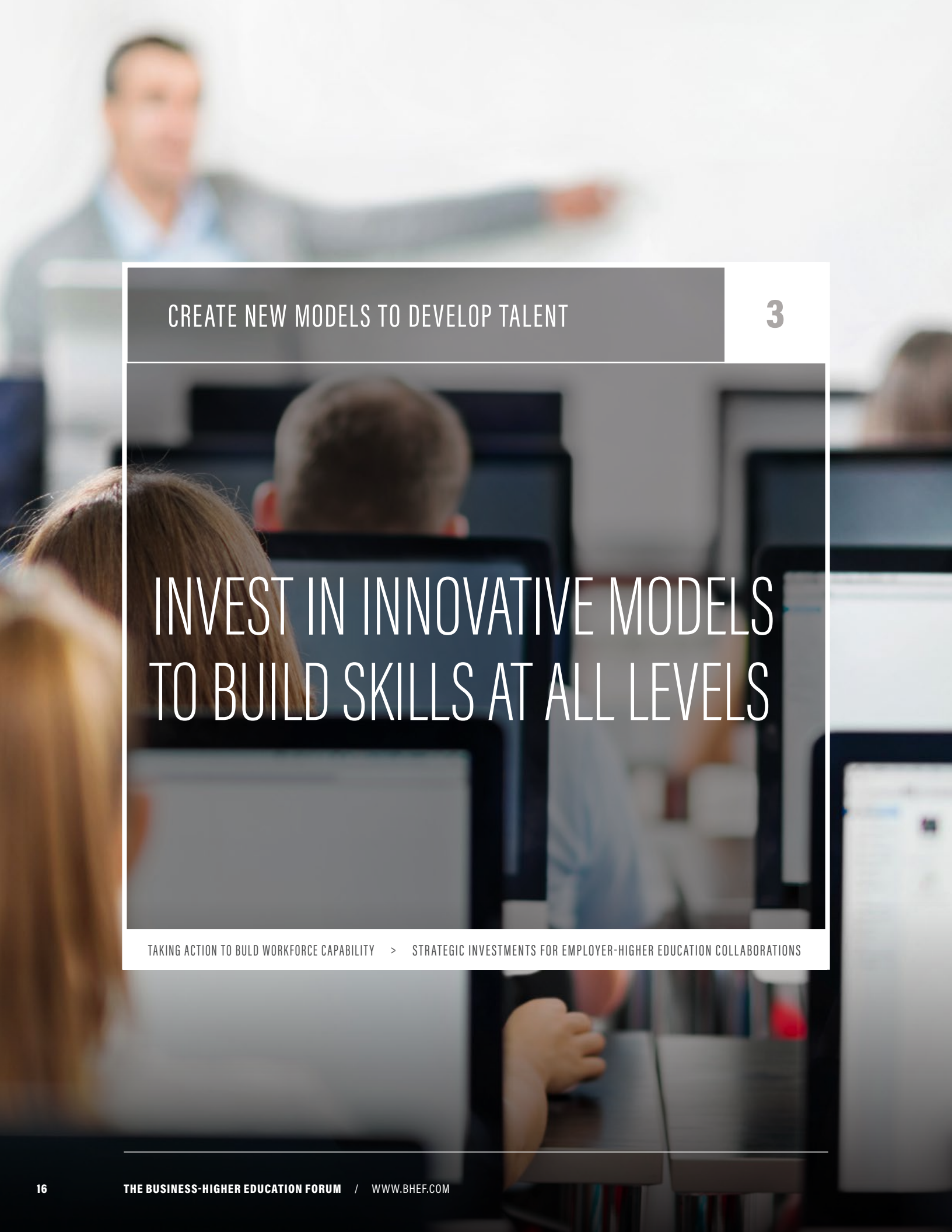
SOUTH DAKOTA HAS THE HIGHEST RATIO OF JOB POSTINGS REQUIRING A CISSP CERTIFICATION TO CERTIFICATION HOLDERS

DEVELOPING AN INCLUSIVE APPROACH TO VETTING CYBERSECURITY SKILLS WILL REQUIRE:

A common understanding of skills relevant to the cybersecurity professional, including technical *and* nontechnical skills

Recognition of the many different types of relevant hands-on experience in cybersecurity (e.g., internships, capstone projects, full-time work)

Models, in addition to certification exams, for professionals to showcase their skills.



CREATE NEW MODELS TO DEVELOP TALENT

3

INVEST IN INNOVATIVE MODELS TO BUILD SKILLS AT ALL LEVELS

ADDRESSING THE CYBERSECURITY TALENT DEFICIT will require a comprehensive approach that targets new graduates, reskills incumbent workers, and upskills information technology, networking, and cybersecurity professionals. The resulting broadening of the workforce will greatly benefit all employers in their recruitment of qualified professionals, regardless of size, sector, or mission.

Higher education institutions will also benefit from new talent development models. Currently, few companies hire cybersecurity talent directly from higher education institutions—partially because they use other approaches to build their talent pipelines. However, this situation presents an opportunity for higher education institutions to collaborate with employers to develop cybersecurity pathways that better meet industry needs. Higher education institutions can tap into employers' current investment in upskilling the existing cyber workforce. Programs for non-traditional students may need to be expanded, as many employers are looking for their employees to gain skills while continuing to work fulltime. Higher education institutions should also consider developing and implementing more pathways for individuals with nontechnical backgrounds.

Business executives and higher education leaders also report that learning about cybersecurity threats from other organizations is an effective way to build a talent pipeline. At the national level, there is a role for professional societies, associations, and nonprofits to coordinate information sharing among organizations. At the regional level, higher education institutions can build strong relationships with local employers through models that more formally bring this sharing into the classroom.

> "State Farm and our neighbor Illinois State University both recognized the growing need for cybersecurity skills in today's world, so we worked hand-in-glove to develop a higher education cybersecurity curriculum. We're very excited to see the program launch this year, because we believe in its value in developing talented cybersecurity professionals—not only for future employment with our company, but across all industries."
>
> **DUANE FARRINGTON,** EXECUTIVE VICE PRESIDENT, TECHNOLOGY, DIGITAL AND INNOVATION / STATE FARM MUTUAL AUTOMOBILE INSURANCE COMPANIES

Upskilling of the incumbent information technology and cybersecurity workforce is especially important. If cybersecurity professionals do not possess the necessary skills, then security tasks are not performed or are performed sub-optimally, which places organizations at risk. This skills gap is most evident when the abundance of professionals with the entry-level Security+ certification relative to the number of jobs requiring that certification is compared to the scarcity of professionals with the advanced-level CISSP certification relative to the number of jobs calling for that certification. Filling the cybersecurity skills gap is also critical at the managerial level, where application of technical expertise is blended with coordination of security initiatives and broader organizational goals.

FOCUS THE TALENT RECRUITMENT MODEL ON CAREER MISSION AND OPPORTUNITIES

4

CAPITALIZE ON THE INCREASED PUBLIC INTEREST IN CYBERSECURITY

"Cybersecurity is an important part of Parsons' business and, because of the global cybersecurity skills gap, we're constantly on the hunt for new talent. We employ many approaches to attract and retain our talent. We start by developing relationships with our candidates and highlighting important factors such as our unique mission to help our clients address threats to our nation's critical assets, our innovative culture, and our talented and diverse workforce. Internships are also a significant piece of our recruitment strategy, which allows our employees to mentor students interested in careers in cybersecurity. Finally, **another key component of our recruitment strategy is partnering with colleges and universities that directly engage undergraduate students in cyber academic enrichment, leadership building, and networking opportunities.**"

BIFF LYONS, EXECUTIVE VICE PRESIDENT AND SECURITY & INTELLIGENCE DIVISION MANAGER / PARSONS CORPORATION

With rising wages and a growing cybersecurity talent deficit, employers must seek solutions that address the churn in incumbent cybersecurity professionals (20 percent in 2014) and that attract new talent to the profession. Such solutions must move beyond competitive compensation to focus on the opportunities, impact, and learning that are unique to the organization.

At all levels, employers should emphasize the value of a cybersecurity career at their organization beyond salary and benefits. One strategy is to highlight educational opportunities and potential career advancement. Another strategy is to highlight the organization's mission—particularly if unique, such as for government agencies. For example, young adults are increasingly aware of cyber-attacks and have a growing interest in cybersecurity careers. Although 90 percent said that a high salary was either important, very important, or extremely important to them, 96 percent said it was either important, very important, or extremely important to feel personally connected to their employer's goals.[8]

This sense of mission in cybersecurity can be a particularly strong lure for students with a previous interest in science, technology, engineering, and mathematics (STEM) disciplines. Cybersecurity programs and employers often recruit from this pool of students, and focusing on the important mission supported by cybersecurity professionals can offer a competitive advantage with this student population.

At universities within USM, which strongly promote their cybersecurity degree programs, cybersecurity graduates are growing at a faster rate than STEM graduates. This disproportionate growth is not explained by post-graduation wages, which are very similar for graduates from both programs. One explanation could be the proximity of USM campuses to major cybersecurity employers such as Deloitte, the National Security Agency, and Northrop Grumman Corporation and the impact of hearing regularly about these high-profile organizations.

8. Securing Our Future: Closing the Cybersecurity Talent Gap, National Cybersecurity Alliance and Raytheon, 2016.

INVEST AND RECRUIT AT HIGHER EDUCATION INSTITUTIONS WITH DIVERSE STUDENT POPULATIONS

5

BUILD RELATIONSHIPS TO EXPAND TALENT POOL

With women estimated to compose 11 percent of the cybersecurity workforce and minorities less than 12 percent,[9] meeting the talent deficit must include expanding the talent pool. This will require employers to look beyond current recruitment strategies and develop new relationships with higher education institutions with diverse student populations.

There is good news for employers who are committed to developing these relationships: existing institutions are graduating students from diverse backgrounds with cybersecurity-related credentials. USM campuses and the Virginia Community College System (VCCS) both serve diverse student populations, as reflected in the demographics of graduates from their information technology and cybersecurity programs. Graduates from these programs work for many of the leading employers in the region, including Booz Allen Hamilton, Capital One, Ernst & Young, and Inova.

Although the percentage of female students graduating with a cybersecurity-related degree or certificate does not mirror the percentage enrolling in these systems, it is much greater than the estimated 11 percent. One-quarter (25 percent) of the cybersecurity-related degree/certificate USM graduates from 2015 were female. Of the students enrolled in cybersecurity-related degree/certificate programs at VCCS in the 2016 calendar year, 52 percent were female.

The percentage of VCCS students enrolled in cybersecurity-related programs who are underrepresented minorities (34 percent) matches the percentage of underrepresented minorities in the general student population. Interestingly, the student populations at USM graduating with cybersecurity-related degrees are more diverse than the student populations graduating with a STEM degree. Broadening the cybersecurity talent pool does not require stakeholders to first solve the STEM diversity challenge. Although it does rely heavily on STEM majors and graduates, the cybersecurity pathway also offers pathways for nontechnical majors, such as post-baccalaureate and master's programs.

Employers seeking cybersecurity candidates from diverse backgrounds should actively invest in higher education institutions with diverse student populations through internships, guest lectures, or other engagements. These efforts will build new relationships with faculty and students and broaden opportunities to find qualified talent.

9. Women, Minorities Largely Absent from Cybersecurity Jobs, Dinah Brin, January 30, 2017.

STUDENTS WITH CYBER-RELATED DEGREES OR CERTIFICATES

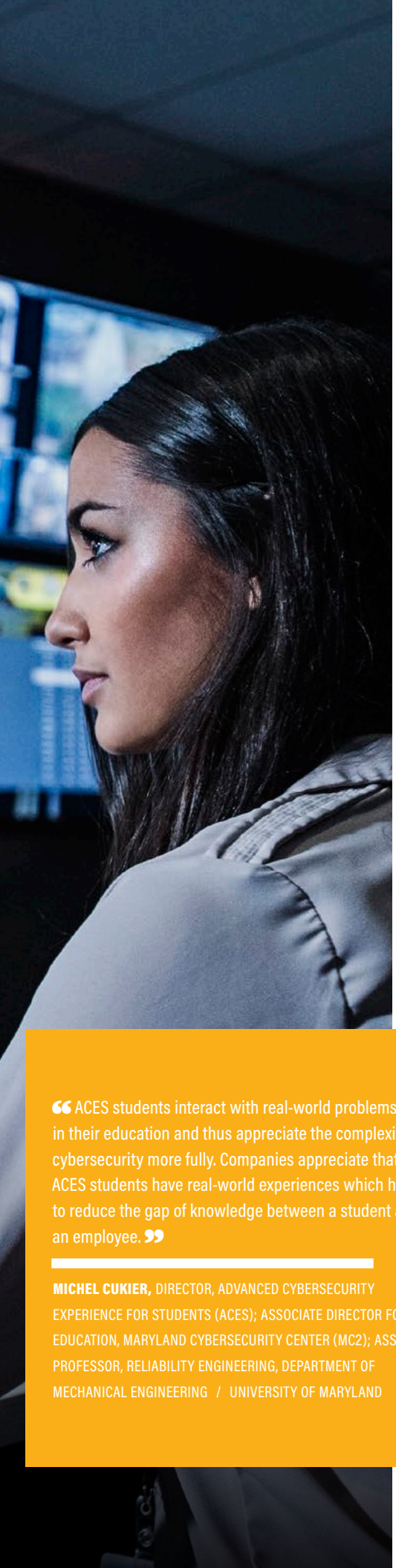
	VCCS (2016 CALENDAR YEAR ENROLLED STUDENTS)	**USM** (2014–2015 ACADEMIC YEAR GRADUATES)
Male	48%	75%
Female	52%	25%
White	52%	44%
Black/African-American	19%	27%
Hispanic	9%	9%
Asian	14%	9%*
Other	6%	n/a

*This number reflects students who self-identified as Asian/Pacific Islander / **Note**: Numbers may not sum to 100% if information was not provided.

GRADUATE STUDENTS WITH PROVEN SKILLS NEEDED FOR A CYBERSECURITY CAREER

6

PROVIDE STUDENTS WITH REAL-WORLD EXPERIENCES



> “ACES students interact with real-world problems early in their education and thus appreciate the complexity of cybersecurity more fully. Companies appreciate that the ACES students have real-world experiences which helps to reduce the gap of knowledge between a student and an employee.”
>
> **MICHEL CUKIER,** DIRECTOR, ADVANCED CYBERSECURITY EXPERIENCE FOR STUDENTS (ACES); ASSOCIATE DIRECTOR FOR EDUCATION, MARYLAND CYBERSECURITY CENTER (MC2); ASSOCIATE PROFESSOR, RELIABILITY ENGINEERING, DEPARTMENT OF MECHANICAL ENGINEERING / UNIVERSITY OF MARYLAND

EMPLOYERS VALUE HANDS-ON EXPERIENCES when recruiting cybersecurity talent. Eighty-three percent of cybersecurity job postings ask for at least two years of experience, and more than one-third ask for six or more years of experience.[10] Providing students with real-world experiences elevates their cybersecurity skills beyond theoretical knowledge and hones problem-solving skills. It also provides opportunities to practice blending technical and other skills—such as communication, leadership, and teamwork—within a security context.

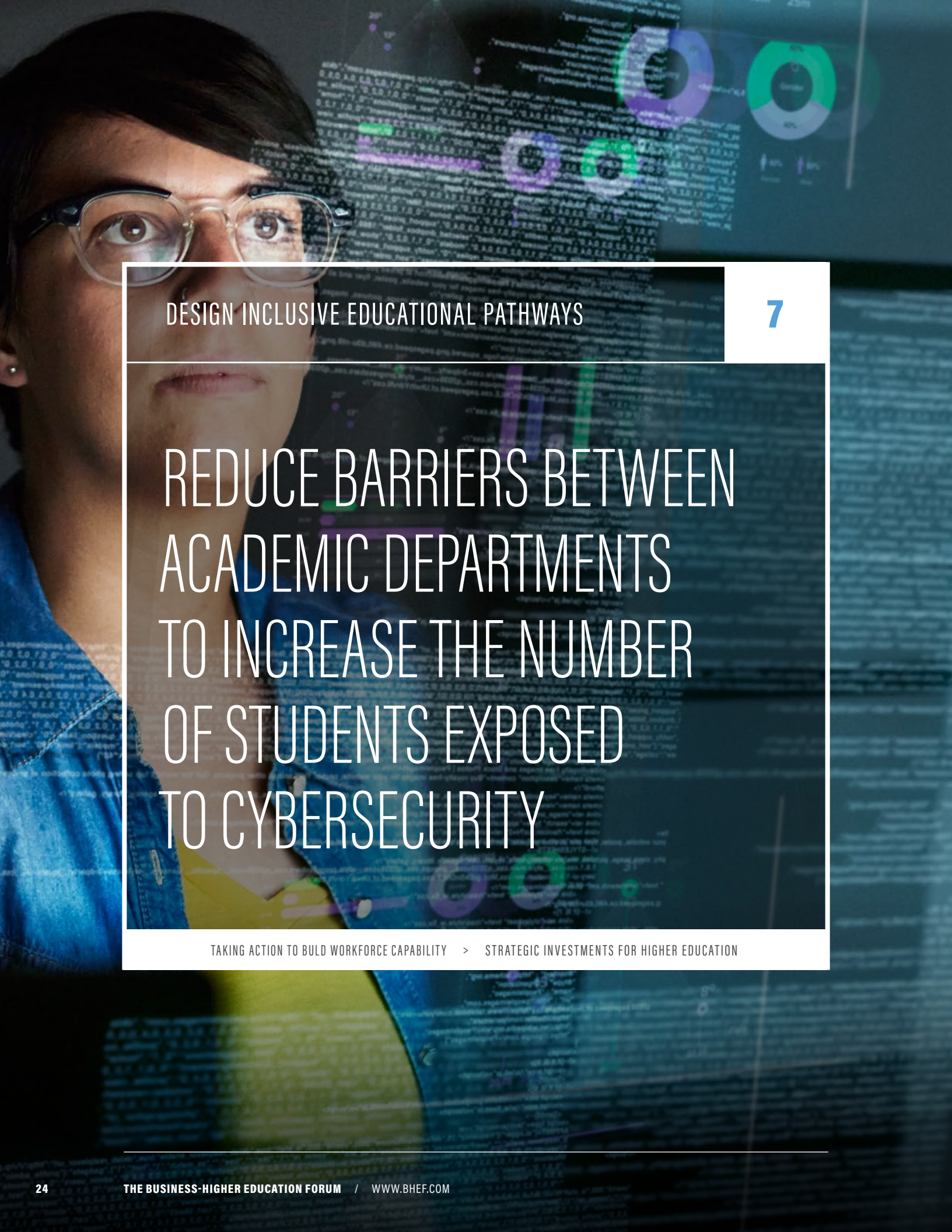
Because nearly all cybersecurity job postings require at least a bachelor’s degree, higher education institutions have the extraordinary ability to ensure that every graduate has encountered and grappled with real-world experiences as part of their education.

Employers are willing to develop partnerships with higher education institutions to support hands-on experiences. A small group of students enrolled at Northern Virginia Community College (NOVA) performed a security assessment for Community Lodgings in Alexandria, Virginia, a small nonprofit whose mission focuses on lifting families from homelessness and instability to independence and self-sufficiency. As part of their project, students developed a security assessment plan, a security assessment report, and an acceptable use policy. Community Lodgings plans to continue to work with students from NOVA to perform security awareness training about the acceptable use policy and other security best practices.

Different approaches have been used to bring real-world experiences into the classroom, such as introductory courses, independent study courses, and capstone projects. Many higher education institutions also offer co-ops or internships for which students receive academic credit. More informally, the cybersecurity community has embraced hacking (e.g., capture the flag) competitions as an approach to develop applied skills. Higher education institutions can host these competitions for their students and invite local employers to design and lead the competitions.

Real-world experiences should also be incorporated into educational offerings for cybersecurity professionals who are deepening their skills, or executives who are building their knowledge of the impact of security on business. These professionals may require different models to gain real-world experience, such as weekend boot camps.

10. How to Get a Cybersecurity Job in Three Charts: a Degree, a Certification, and a Clearance, Dan Restuccia, May 13, 2016.



DESIGN INCLUSIVE EDUCATIONAL PATHWAYS

7

REDUCE BARRIERS BETWEEN ACADEMIC DEPARTMENTS TO INCREASE THE NUMBER OF STUDENTS EXPOSED TO CYBERSECURITY

THE NEED FOR CYBERSECURITY TALENT spans all industry sectors. Although certain core competencies are required knowledge for any cybersecurity professional regardless of industry sector, some skills are specific to an industry sector. For example, security in the financial services, aerospace and defense, and health care sectors is highly regulated, and practitioners working within these sectors require specialized knowledge.

Most higher education institutions coordinate their cybersecurity programs within a single department, with only 25 percent of programs coordinated by multiple departments. Ninety-four percent of community colleges house their cybersecurity programs within a single department. This centralization of cybersecurity within a single department too often focuses on the technical knowledge specific to cybersecurity and disregards the broader skill set and domain-specific knowledge required in the workplace. Centralizing a cybersecurity program can also make it difficult to engage faculty members from other departments, such as business or communications, and to weave those competencies throughout the cybersecurity curriculum.

To prepare students for the breadth of cybersecurity careers and to address the variety of talent needs in cybersecurity, higher education institutions should structure cybersecurity programs in a way that facilitates inclusion of faculty from multiple departments. This facilitation will benefit two complementary student populations: (1) students with a primary academic interest in cybersecurity and (2) students with a primary interest in a field relevant to cybersecurity.

> "In order to address the astounding workforce gap, **cybersecurity education needs to expand beyond traditional disciplines and skill levels** to include a broad range of vocational and professional degrees across a wider base of students from engineering, science, business, and policy."
>
> **CHARLES CLANCY,** DIRECTOR, HUME CENTER FOR NATIONAL SECURITY AND TECHNOLOGY; ASSOCIATE PROFESSOR, BRADLEY DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING; L-3 COMMUNICATIONS FACULTY FELLOW IN CYBERSECURITY, COLLEGE OF ENGINEERING / VIRGINIA TECH

Students primarily interested in cybersecurity will gain access to faculty who can help them understand the specialized skills needed for different cybersecurity sectors and roles. Students will understand the breadth of career opportunities they can access with a strong grounding in cybersecurity and will gain industry knowledge within a classroom setting.

Students primarily interested in fields such as business, systems engineering, or political science will gain a basic understanding of how cybersecurity is relevant in their discipline. Faculty members can teach case studies about a data breach in a business class, which will inform students' understanding of the broad impacts of security on an organization's finances. Similarly, the Internet of Things necessitates that engineering students understand how security is critical in design. Reducing the barriers in the structure of cybersecurity programs and faculty will increase the number or students with cybersecurity knowledge.

Recognizing the importance of cybersecurity to a variety of academic disciplines—including business-oriented studies—Baruch College's Zicklin School of Business offers a minor program in cybersecurity and information assurance. Undergraduate business majors interested in cybersecurity can enroll in this program. Students will develop a practical understanding of information security and assurance issues that face organizations. The minor consists of three courses: networks and telecommunications issues, cybersecurity, and information technology audit.


ALL STAKEHOLDERS
MUST EMBRACE
THE SHARED
RESPONSIBILITY
TO DEVELOP THE TALENT
NEEDED TO PROTECT
OUR INFORMATION.

CONCLUSION

THE ONGOING SHORTAGE OF CYBERSECURITY TALENT is impacting large and small employers throughout the United States. What has been hacked cannot be unhacked. Proper protection of information is critical to the mission of many of these organizations. An immediate and significant commitment from all of the stakeholders to increase or accelerate their efforts is required to adequately build the cybersecurity talent pipeline.

This commitment is one of both individual and collective action. Stakeholders can individually pursue actions to build a cybersecurity talent pipeline. Regional partnerships bring together the resources of multiple stakeholders to impact a broad population. All stakeholders—employers, higher education institutions, and government agencies—have strong incentives to make both types of commitments.

Although the focus of this paper is on aligning cybersecurity stakeholders to broaden the talent pipeline, stakeholders recognize that the security threat is ever-evolving and ever-increasing in this digital age. The response, both from a technical and talent perspective, must be equally dynamic. Educators must structure cybersecurity courses and programs that can easily and nimbly adapt. Employers must emphasize their commitment to lifelong learning as a recruitment and retention strategy. And all stakeholders must embrace the shared responsibility to develop the talent needed to protect our information.

This report proposes actions for stakeholders to take for immediate impact in their region. We also invite those who are invested in these actions and partnerships, or wish to invest in these actions and partnerships, to collaborate with BHEF and its members as part of a national effort to meet this critical talent need.

ABOUT THE SURVEYS

Gallup conducted 63 phone interviews from October 31, 2016, to February 27, 2017, with business leaders. The sample consisted of 25,683 chief executive officers, chief information officers, chief technology officers, human resources officers, and vice presidents of human resources and operations at oil and gas, finance, insurance, computer systems, manufacturing, information, biotech, health care (HMO medical centers, hospitals, and diagnostic labs), retail trade, and transportation and warehousing companies with annual revenues of $10 million or more. The sample of business leaders was obtained from Dun and Bradstreet and is not nationally representative of U.S. companies in these industries, although it is comprehensive.

Gallup also conducted 127 phone interviews from October 31, 2016, to January 5, 2017, with college and university presidents, chancellors, provosts, and deans from public, private, two-year, and four-year institutions. The sample consists of 2,450 U.S. college and university leaders. The sample of higher education leaders was obtained from Higher Education Publications, Inc. and is not nationally representative of U.S. presidents of colleges and universities, although it is comprehensive.

Question wording and practical difficulties in conducting surveys can introduce error or bias into the poll findings.

ABOUT THE JOBS MARKET ANALYSIS

All jobs data in this report are drawn from Burning Glass's database of online job postings, which includes nearly 100 million worldwide postings collected since 2007. Each day, Burning Glass visits more than 38,000 online jobs sites to collect postings. Using advanced text analytics, more than 70 data fields are extracted from each posting including job title, occupation, employer, industry, required skills and credentials, and salary. Postings are then de-duplicated and placed in a database for further analysis.

DEFINITIONS USED IN THE REPORT

Geographical Areas used in Analysis: The analysis for the states of Virginia and Maryland, as well as the District of Columbia, reflects the 2014 calendar year. The analyses for the New York City metropolitan region and the state of Massachusetts reflect the 2013 calendar year. The New York City metropolitan region was defined as the New York-Newark-Jersey City, NY-NJ-PA Metropolitan Statistical Area.

Cybersecurity Jobs: This report classifies cybersecurity jobs as those with a cybersecurity-related title, require a cybersecurity certification, or request cybersecurity-specific skills. Cybersecurity-related titles used to define the roles analyzed in this report include network security, information security, information assurance, and penetration tester. Cybersecurity skills include information assurance, cryptography, computer forensics, forensic analysis, 800-53, Federal Information Security Management Act, computer network defense, network security, and ArcSight.

Pipeline Roles: This report classifies pipeline roles for cybersecurity as jobs within a set of networking occupations that do not require cybersecurity-specific skills or certifications, but with additional training could transition into cybersecurity roles. These roles occupations are Network/Engineer Architect, Computer Systems Engineer/Architect, Systems Analyst, Network/ Systems Administrator, Network/ Systems Support Specialist, and Computer Support Specialist.

ABOUT THE STUDENT ANALYSIS

University System of Maryland (USM): Student-level data were provided by USM through a secure transmission to the Jacob France Institute via an Excel spreadsheet. Graduation years of Cybersecurity and STEM graduates ranged from 2000 to 2015. Student data fields included: graduation year, institution ID, social security number (SSN), degree level, program of study, gender, race, and a cybersecurity flag.

The final analysis file contained approximately 50,000 records. Students were matched by their SSN longitudinally with Maryland unemployment insurance wage records and the Quarterly Census of Employment and Wages database. In addition, wage matches with the District of Columbia's Department of Employment Services and the federal Office of Personnel Management were conducted.

Virginia Community College System (VCCS): CEB TalentNeuron was the primary tool used in the analysis of labor market information. The intelligence behind CEB TalentNeuron relied on several data sources such as the National Center for Education Statistics. The software could estimate the number of job positions available based on data from the Occupational Employment Survey of the Bureau of Labor Statistics and several other data sources compiled by TalentNeuron.

Student-level data were collected through the VCCS Institutional Research and Effectiveness department using student data sources from each college in the system and from unemployment insurance data from the Virginia Employment Commission. To examine enrollments and graduates in specific CIP codes (programs of study), a cohort of 6,526 students who started in fall 2008 was selected. The variables selected for this report included age, race/ethnicity, military status, grade point average, and credits earned. Wage data for graduation years 2013/2014 were selected and analyzed. Wage data were collected on a quarterly basis. The data were compiled in both Excel and SAS spreadsheets.

CREATING SOLUTIONS. INSPIRING ACTION.

BHEF BUSINESS-HIGHER EDUCATION FORUM®

Creating Solutions. Inspiring Action.

© 2017 Business-Higher Education Forum / 2025 M Street NW, Suite 800 / Washington, DC 20036
p: 202.367.1189 / info@bhef.com / www.bhef.com