Sonya Miller, HR Director, IBM Security and Enterprise and Technology Security

"More Hires, Fewer Hacks: Developing the U.S. Cybersecurity Workforce"

February 11, 2020

Hearing of
the Subcommittee on Research and Technology of the
House Committee on Science, Space and Technology

Chairwoman Stevens, Ranking Member Baird and distinguished Members, I am the HR Director both for our internal security and for our division that helps clients to protect against cyber-attacks.

The House Science, Space and Technology Committee has a critical jurisdiction that supports American technological innovation, research and development, and key agencies to advance U.S. scientific leadership.

Although today's hearing focuses on cybersecurity, the workforce challenges for research are similar. Inclusion, alignment, and attainment are obstacles to both cybersecurity and the research workforce pipeline.

To this end, I would also like to take this opportunity to thank the Committee for its very strong leadership and support of the National Quantum Initiative Act. The NQI is groundbreaking legislation that, once fully implemented, will assure U.S. investment and research in quantum computing remains a priority.

IBM's Security Capabilities

IBM Security is the largest security vendor in the world. IBM manages **over 70 billion** security events **per day** for our clients – one of the largest security intelligence operations in the world. We have 17,500 clients in more than 130 countries, 8,000 employees, including researchers, developers, and subject matter experts focused on security, and more than 10,000 security-related patents.

Since 2015, IBM Security has hired nearly 4,400 additional experts into its Security business and invested more than $2 billion in dedicated R&D. In sum, we "see" a lot of demand for workforce in cyberspace.

To understand IBM Security, it's important to understand the people behind the brand. Our cybersecurity experts have a broad range of skills including researchers analyzing software for

vulnerabilities, incident response teams, analysts who spend hours studying the tactics of cyber criminals, and Security Operation Center staff who guard us in real-time from threats across the globe.

Challenges Companies Face in Recruiting, Training and Retaining Skilled Cybersecurity Professionals

Unfortunately, the U.S. education system is not producing candidates with relevant "soft skills" or even the technical skills for jobs in the cybersecurity space except from a narrow swath of students. The pathways through education include many barriers and often leave students with debt but no degree.

Inclusion: The distribution of bachelor's degrees is low and uneven by income[1], race, age, and gender[2] (in addition to geography). As a result of the variation, higher education graduates are from a much narrower band of students than the US population.

Alignment: Often, higher education institutions simply do not offer cybersecurity majors, minors, degrees, or programs. For example, Michigan State University offers Computer Science or Computer Engineering majors in its College of Engineering, but not cybersecurity as a major, minor, degree, nor program.[3]

Community colleges are offering more and more cybersecurity programs making them an important source of talent. However, fewer than 30 percent of the roughly 1,100 public and independent community colleges across the United States offer a cybersecurity degree, certificate or course.[4]

Attainment: The Higher Education Act does not permit financing for programs of less than 600 hours – exactly the type of education pathway that leads to cybersecurity certifications. Even when a higher education institution offers cybersecurity courses, the bumpy and obstacle-filled pathway of higher education interferes with progress to graduation. End-to-end, only 13% of the 852,439 students who enrolled in community college in 2010 persisted to a

---

[1] http://www.equality-of-opportunity.org/papers/coll_mrc_paper.pdf

[2] https://nscresearchcenter.org/wp-content/uploads/Completions_Report_2019.pdf

[3] https://reg.msu.edu/Courses/Search.aspx

[4] "2016 Fact Sheet." American Association of Community Colleges. http://www.aacc.nche.edu/AboutCC/Documents/AACCFactSheetsR2.pdf; IBM Institute for Business Value interview with Casey O'Brien, Executive Director & Principal Investigator, National CyberWatch Center. February 21, 2017.

bachelor's degree by 2016.[5] The GAO has found that "students who transferred from 2004 to 2009 lost, on average, an estimated 43 percent of their credits."[6]

For example, in 2012, the Michigan legislature included language in the community college appropriations bill calling for improvement in the transferability of college courses. But, Michigan Transfer Agreement (MTA) does not address the transfer of their cybersecurity courses from community colleges (such as Schoolcraft) and only protects the transferability of nine non-security related course such as English composition, social science, fine arts and humanities, to name a few.

Developing Cybersecurity Skills: The IBM New Collar Approach

IBM's New Collar approach focuses on skills first — not degrees earned - and emphasizes work-based learning and core skills like teaming and adaptability. It is a pathway to finding and attracting nontraditional candidates with diverse backgrounds and skill sets.

Around two-thirds of the U.S. working age population does not have a bachelor's degree. Additional education pathways can provide cybersecurity opportunities to the two-thirds of the country that haven't graduated with a bachelor's degree – and those additional students that are ending their education early, with debt but no degree, each year.

IBM Security seeks New Collar employees with learning agility, skills, and experience who will seek continuous lifelong learning and professional growth.

To expand new collar skills, IBM is experimenting with a multitude of approaches to educate and develop the next generation of cybersecurity professionals

P-TECH -- Over 220 Pathways in Technology Early College High Schools (P-TECH) are educating students in 24 countries with the participation of over 600 companies. Through P-TECH, public high school students can earn both a high school diploma and an industry-recognized two-year postsecondary degree at no cost to them or their families, while working with industry partners like IBM on skills mapping, mentorship, workplace experience and internships.

The P-TECH model of schools has four key elements:

- Alignment of the Program of Study for grades 9-14 with the skills needed by an employer
- Mentors for all students from the employer
- Internships for students from the employer

[5] https://nscresearchcenter.org/wp-content/uploads/SignatureReport13_corrected.pdf
[6] https://www.gao.gov/products/GAO-17-574

- A commitment that graduating students will be first in line for a job with the employer.

Apprenticeship: IBM launched our Department of Labor Registered Apprenticeship Program in October 2017. It's a program for the 21st century, focused on building skills in cybersecurity, data scientist, software development and more. This 12-24-month program pairs apprentices with an IBM mentor to work on actual IBM projects, along with traditional classroom learning, in technology's fastest-growing fields.

Apprentices are paid while in the program, avoiding student loan debt and earning the skills to work in the tech industry right away. We hired as many as 500 apprentices by the end of 2019, and we expect to hire 450 apprenticeships each year moving forward for the next five years with some being in such roles as cyber security analyst and hardware hackers. Apprenticeship programs are great opportunities for mid-career workers to build new skills or break into new industries without having to leave the workforce to be a full-time student. It's a chance to earn while you learn.

Outreach: Women are globally underrepresented in the cybersecurity profession at 24%, much lower than the representation of women in the overall global workforce. In 2016, women in cybersecurity earned less than men at every level.[7] IBM is actively recruiting underrepresented groups through conferences and organizations like the International Consortium of Minority Cybersecurity Professionals (ICMCP), the Grace Hopper Celebration and Women in CyberSecurity (WiCyS).[11] Additionally, we have an internal network called Women in Security Excelling (WISE), an IBM professional development community that also sponsors and hosts external events like the "Cyber Day for Collegiate Women" programs for college women.

IBM's efforts to build a cybersecurity workforce prove to be working – as mentioned, we have built a business of over 8,000 experts including an additional 4,400 since 2015 – although job openings at IBM Security are still plentiful. That workforce is a result of reaching new sources through our New Collar recruitment – in fact, nearly 20% of our security hires since 2015 have fit into this "new collar" category.

What Should the U.S. Government do to Address Cybersecurity Skills and Capabilities?

IBM urges the Committees to examine four areas for changed government activity that will improve the cybersecurity workforce. Those four areas are listed below and then discussed in more detail:

---

7 https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf 11 International Consortium of Minority Cybersecurity Professionals website, accessed April 3, 2017. https://icmcp.org/; Women in CyberSecurity website, accessed April 3, 2017. https://www.csc.tntech.edu/wicys/

- **Introduce and Enact Companion Legislation to S. 2775, the HACKED Act of 2019** as passed by the Senate Commerce Committee, and work closely with your colleagues in the Senate to pass a bipartisan proposal that will strengthen America's cybersecurity workforce and align education and training with the cybersecurity workforce needs.
- **Higher Education Act Reforms** including Passage of the HR 3497, the JOBS Act of 2019 to extend federal Pell Grant Eligibility of Short-Term Programs, removal of restrictions that prevent students from using their Federal Work Study with cyber-related internships in the private sector and support additional pathways to careers.
- **Explore P-TECH Model** -- Federal agencies should explore the P-TECH model for workforce development strategies they can implement.
- **Expand New Collar Hiring** -- The federal government should adopt a New Collar approach to reach and expand sources of labor.

Introduce and Enact S. 2775: The Hacked Act of 2019. Multiple education pathways to cybersecurity careers are a goal of IBM and central to the HACKED Act. Under the legislation, the Director of NIST is directed to target identified skills gaps and ensure that existing education programs, partnerships, and regional alliances lead to specific tasks found in the NICE Cybersecurity Workforce Framework. Our experience with P-TECH has shown that collaborations with government, education systems, and employers are very productive.

The Hacked Act will facilitate: "local and regional partnerships—

> (A) to identify the workforce needs of the local economy and classify such workforce in accordance with such framework;
>
> (B) to identify the education, training, apprenticeship, and other opportunities available in the local economy; and
>
> (C) to support opportunities to meet the needs of the local economy.

IBM is strongly supportive of these goals due to our experience with P-TECH and apprenticeships.

Higher Education Act Reforms including Passage of HR 3497, the JOBS Act of 2019 and other additional pathways.

IBM urges the House to move remove obstacles in the Higher Education Act to inclusion, alignment, and graduation by allowing students to use their Pell Grants for shorter education programs that lead to certifications. Under existing law, students who need short-term programs of 150 to 600 hours length in order to get certifications are required to sign up for longer education programs or forgo federal financial assistance.

- We want the Pell grant program to allow part-time students and mid-career professionals to get financial support to acquire new skills — including certifications, apprenticeships, other job-related classes. Pell Grants need to work harder for everyone with need, not just full-time students.

- Education pathways should be revised so grants and loans can support more career pathway opportunities. Student aid should support the attainment of degrees *and* the attainment of industry recognized credentials and licenses, and support apprenticeships, certificate programs, or other mid-career re-skilling.

- We want the federal Work-Study Program revised to remove restrictions on student use of funds for off-campus work experiences like internships at companies. These funds should not be restricted to supporting jobs in campus cafeterias and libraries.

Explore P-TECH Model Participation by Federal Agencies: The P-TECH model is based on a collaboration between employers and educators to improve alignment of the existing education system with needed job skills. Developing programs of study and educational materials is the responsibility of our nation's educators, but P-TECH employers play a vital role by telling what skills are necessary "to be first in line for a job". Defining skills needs, providing mentors, internships, and committing that graduates will be "first in line for a job" are all employer responsibilities in the P-TECH model.

Federal agencies are major employers and should explore the workforce development strategies developed and tested by the private sector through the P-TECH model schools. Federal agencies could join other P-TECH employers that provide information to workforce boards and educators on needed-job skills. Federal agencies could provide work-based learning opportunities including mentors and internships. Both student and potential federal employers benefit from enhancing skills learned through improved alignment and work-based learning.

New Collar Approaches: Finally, IBM recommends that "Skills First" approach to recruitment expand the New Collar cybersecurity workforce. For a more robust New Collar approach, employers need to create new collar career pathways in their workforce strategy with five components:

- Agility Centered Recruitment
- Skill Maps
- Broader Recruitment
- Education Ecosystem
- Work based Learning
- Retention

With an expanded recruiting aperture bringing new talent in, there must be comparable efforts to work to retain the talent. Keep employees engaged by providing opportunities for them to advance and keep skills up to date through classes, certifications, conferences. Cybersecurity is a highly dynamic field, which requires a constant refreshing of skills. Additionally, support existing New Collar employees from other functions who want to move into cybersecurity as a new career.

Conclusion

With the four approaches above, IBM believes New Collar workers can add an important component of the nation's overall approach to tackling the cybersecurity skills gap. It is applicable across industry and government and has tangible benefits for both employers and potential employees. By not tapping into underutilized sources of talent across the country and supporting and nurturing it, we are doing a disservice to everyone and not securing ourselves as well as we could. There are many innovative approaches to improving cybersecurity education happening all across the country, but to truly address the cybersecurity skills gap we need to scale these approaches, including new collar ones.

Thank you, Members of the Committee for the opportunity to present IBM's approach to improving cybersecurity education and your consideration of this testimony. I look forward to your questions.