Statement for the Record
David Jarvis, Security & CIO Lead, IBM Institute for Business Value

"Public-Private Solutions to Educating a Cyber Workforce"
October 24, 2017

Joint Hearing of
Subcommittee on Higher Education and Workforce Development of the House Committee on Education and the Workforce
Subcommittee on Cybersecurity and Infrastructure Protection of the House Committee on Homeland Security

Chairman Guthrie, Chairman Ratcliffe, Ranking Member Davis, Ranking Member Richmond, and distinguished Members, I am honored to appear before both Committees today to discuss the insufficient supply of cybersecurity skills and the increased demand to fulfil important cybersecurity positions to protect the economic and national security interests of the United States and the global digital infrastructure.

In my testimony, I will describe the cyber threat landscape, the skills needed to protect against those threats, what IBM is doing to promote those skills including our "new collar" approach, and finally, what the government should do to improve the supply of cybersecurity skills and jobs.

To set the stage, I work at IBM as part of the Institute for Business Value, which explores and researches emerging business and technology issues impacting a variety of industries. We report insights from that research and provide practical guidance to the market and our clients. I primarily focus on cybersecurity and the various aspects surrounding the discipline - whether it be technical, societal, or economic.

Cybersecurity professionals are not produced by the education system in the United States in the quantities or skill levels needed. This is a problem that isn't going away anytime soon. However, with great challenges come creative solutions that many dedicated individuals and organizations are pursuing. At IBM, we believe that some cybersecurity jobs can be filled through a new collar approach that involves tapping professionals who may not have a traditional college degree but do have the needed technical skills and aptitudes. This approach was outlined by our CEO, Ginni Rometty, at the end of 2016, as a way to address skills gaps across technology-related sectors.[1] By better aligning the education system with industry we can develop the skills needed to fight cybercrime, fill jobs and reduce data breaches.

[1] https://www.usatoday.com/story/tech/news/2016/12/13/ibms-rometty-talk-new-collar-jobs-trump/95370718/

IBM's security capabilities

IBM Security is the largest security vendor selling exclusively to enterprises. IBM manages **35 billion** security events **per day** for our clients – one of the largest security intelligence operations in the world. IBM Security has 17,000 clients in 133 countries, 8,000 employees, including researchers, developers, and subject matter experts focused on security**,** in 36 IBM Security locations around the globe. In sum, we "see" a lot in cyberspace and have also dedicated over $2B in research and development to "out innovate" the cyber criminals.

To understand IBM Security, it's important to understand the people behind the brand. As part of the 8,000 subject matter experts we have on board, IBM Security has:

- **Researchers** analyzing software for vulnerabilities
- **Incident Response teams** (IBM X-Force IRIS) in the wake of a breach conducting forensic investigations and working with law enforcement.
- **Interim CISOs** that help organizations scale and address cyber security planning
- **Malware, spam, and Dark Web analysts**, spending hours understanding the tactics criminals are using to target and infiltrate organizations
- **Security Intelligence analysts** working in and deploying Security Operation Centers (SOCs) across the globe

Since 2015, IBM Security has hired nearly 2,000 additional experts into its Security business, including world-class developers, consultants, and research professionals.

Additionally, IBM Security is developing and using cognitive cybersecurity systems like Watson to augment the skills and capabilities of security teams. With the ability to interpret huge volumes of structured and unstructured data, staff with cognitive tools can better reveal patterns and put security events in context. Using data mining, machine learning, natural language processing and human computer interaction, cognitive systems provide evidence-based recommendations to help cybersecurity experts act with confidence, at speed and scale.

Today's security threats

Today, just about all the breaches we hear and read about involves the exfiltration of data. A cybercriminal breaks into a system, gets access to information, downloads that data and extorts it for profit or influence.

The IBM X-Force Threat Intelligence Index 2017 found in 2016 more than 4 billion records were leaked, more than the combined total from the two previous years, redefining the meaning of the term "mega breach." In one case, a single source leaked more than 1.5 billion records. The industries experiencing the highest number of incidents and reported records breached were

information and communications, government, and financial services. Mega breaches have continued to penetrate all sectors with unabated threats in 2017.[2]

Additionally, late last year IBM and the Ponemon Institute unveiled the results of the annual Cyber Resilient Organization study, which found businesses are continuing to fail when it comes to preparing for and responding to cyber attacks. Companies are being attacked successfully more frequently, they cannot keep business operations going effectively or recover quickly, and most have not done adequate planning or preparation for an incident.[3] Considering the vast digital dependencies for organizations, it is no longer a matter of "if" but a matter of "when" an incident will happen.

We are seeing security attacks and techniques continue to evolve across skill level, geography, and sectors. It is now estimated to be one of the largest illegal economies in the world, costing the global economy more than $445 billion dollars a year[4]. To put this in perspective, $445B is greater than the GDP of more than 160 different countries, including Ireland, Malaysia, Finland, Denmark, and Portugal, among many others.

The most sophisticated thieves operate like a well-oiled global business. They build development tools and collaborate on software. They share knowledge about targets and vulnerabilities. They recruit, educate, promote, and reward their workforce. In fact, each successful attack proliferates the skills, tools and ecosystem because hackers often reuse malware and other vulnerabilities that they know are proven to work. Think of it as on-the-job education.

As the threat emanates from a variety of angles, we need to respond with innovative cyber defenses including a workforce with a diverse set of skills that are constantly updated. Persistent and well-funded cybercrime organizations are constantly probing a range of vulnerabilities. They look for simple misconfigurations of installed software, but also have the capability to carry out sophisticated brute force, phishing, and malware conflicts. The spread of attacks from simple to complex requires a broad set of skills and capabilities to respond – across skill levels, information technology defenses, organizations, and geographies.

Due to the current lack of skills, cybercrime creates chronic infections of government, enterprise, and individual systems that take months (if not years) to heal, and are corrosive to the economy and public trust.

[2] https://www.ibm.com/security/xforce/research.html
[3] *"The 2016 Cyber Resilient Organization"*, Ponemon Institute and IBM, November 2016
[4] Net Losses: Estimating the Global Cost of Cyber Crime, Center for Strategic and International Studies, June 2014

The skills challenge and needed capabilities to defend against cyber threats

An organization is only as good as the people that are part of it. The challenge of recruiting and retaining the best technical and business professionals is a constant worry for any organization, even more so in the cybersecurity field.

The cybersecurity talent issue isn't limited to a few sectors; it runs across the board from government to education to healthcare and all industries. Strong talent is needed in all communities from rural farms that increasing rely on information technology to financial service companies in large urban areas.

There are many estimates as to the size of the shortage of cybersecurity professionals. Frost & Sullivan predicts that the growing gap between available qualified cybersecurity professionals and unfulfilled positions will reach 1.8 million by 2022.[5] While the size of the gap certainly indicates the severity of the problem, the bigger point is that unless we change and improve our approach dramatically, the gap will be an elusive thing to catch up to and close.

Many leaders believe that not enough is being done about the shortage. According to a report by the Center for Strategic and International Studies and Intel Security, three out of four security professionals surveyed believe their government is not investing enough in cybersecurity talent.[6]

The inherent complexities that make cybersecurity challenging have created this severe skills shortage. Even though government, industry and education are attempting to address the problem through many different initiatives, the entire supply chain of talent is stressed. Industry is facing a shortage of qualified candidates with the necessary hands-on skills and product experience. Those working as security professionals today are under constant pressure, as they need continuous education and professional development to keep up with evolving technologies and the threat landscape. They are also challenged to find time to properly mentor and educate new hires.

Academic institutions want to meet industry needs, but they are struggling to evolve and develop curriculum to keep pace with industry shifts and technological advances. There is also a shortage of qualified teachers and professors at both the university and community college levels, as many are lured away to industry by competitive salaries. Finally, students interested in pursuing the cybersecurity field are faced with defining their own career path from a myriad of options and then obtain the significant education and experience required.

---

[5] "The 2017 Global Information Security Workforce Study: Women in Cybersecurity." Frost & Sullivan. March 2017. https://iamcybersafe.org/wp-content/uploads/2017/03/ WomensReport.pdf

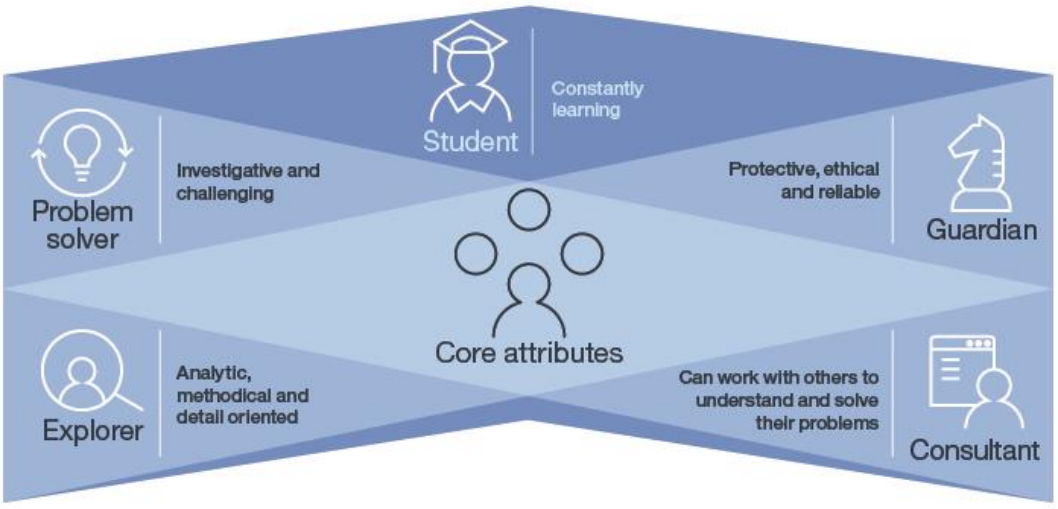
[6] "Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills." Center for Strategic and International Studies and Intel Security. 2016. https://www.mcafee. com/ca/resources/reports/

At the most basic level, employers must ensure that software, networks, and cyber defenses are correctly installed and configured. Skills for these broadly needed services are low- to middle but required throughout the economy in large numbers.

At the other extreme, Chief Information Security Officers (CISOs) for large enterprises and government agencies are required to orchestrate a broad set of defensive capabilities and respond to a bewildering array of breaches. CISOs are highly skilled positions with significant education and experience who must balance managing their own security operations with advising, guiding and educating their C-suites and boards of directors.

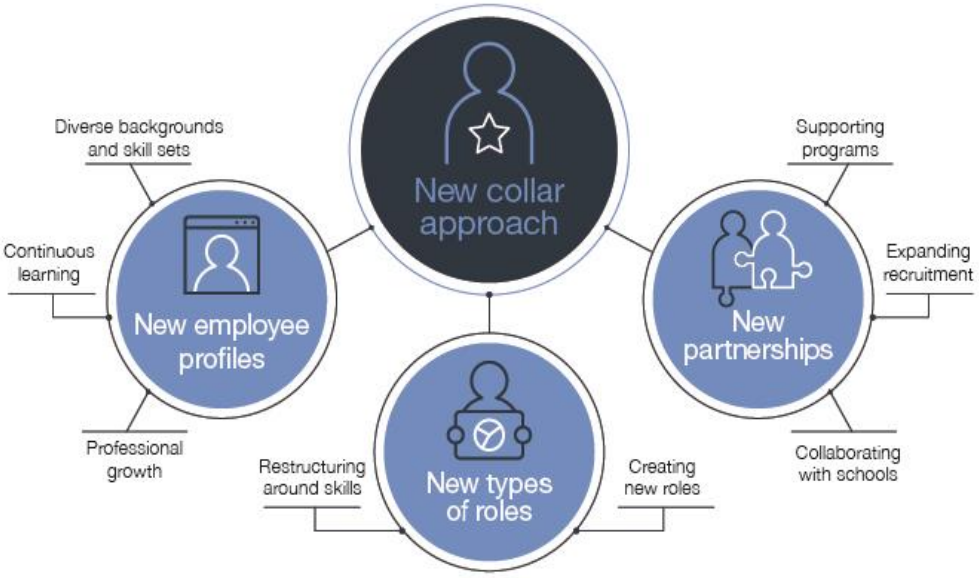
What skills should new cybersecurity professionals focus on? No matter the educational background of the professional, there are some essential elements. These elements can be classified into two groups: core attributes and skills.

Core attributes can be considered a general disposition beneficial to security professionals — a set of common personality traits and learned behaviors. This includes being investigative, methodical, analytical, ethical, reliable, constantly learning, a good communicator, and able to team with others to solve challenging problems. Skills include both technical and workplace-related abilities. A new security professional may not have all these skills at first, but focusing on them over time will provide greater career path flexibility and the foundation for technical or business-focused security leadership positions.



Developing cybersecurity skills: The IBM new collar approach

IBM's new collar approach focuses on skills — not degrees earned - and emphasizes work-based learning and core skills like teaming and adaptability.



The cornerstone of a new collar approach and a major component of the overall strategy necessary to address the cybersecurity skills gap is to seek new sources of skills that may not have been pursued in the past, due to a lack of traditional academic credentials.

A new collar approach is used at IBM to fill both technical and non-technical jobs. We have identified some specific cybersecurity jobs as suitable places to start. This includes "builders" such as integration engineers and cybersecurity developers, "operators" such as threat monitoring analysts and security operations center analysts, and "communicators" such as technical writers and security awareness educators.

A new collar approach focuses on skills — not degrees earned— as a prerequisite to find and attract nontraditional candidates with diverse backgrounds and skill sets. Once hired, these new employees are expected to strive for continuous learning and professional growth. A new collar approach recognizes there are alternative ways to learn the skills needed. For example, respondents from a CSIS and Intel Security study ranked hands-on experience and professional certifications as better ways to acquire cybersecurity skills than a degree.[7]

To expand new collar skills, IBM is experimenting with a multitude of approaches to educate and develop the next generation of cybersecurity professionals. These include creating and developing new education programs, going beyond the traditional classroom and making new connections and sharing information.

[7] "Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills." Center for Strategic and International Studies and Intel Security. 2016. https://www.mcafee. com/ca/resources/reports/rp-hacking-skills-shortage.pdf

IBM is utilizing the new education model Pathways in Technology Early College High School (P-TECH) in the United States and other countries specifically for cybersecurity. Currently, we are working with Excelsior Academy at Newburgh Free Academy in New York (a partnership between the Newburgh Enlarged City School District, IBM and SUNY Orange Community College) and P-TECH@Carver in Baltimore, Maryland (a partnership between Carver Vocational Technical High School, IBM and Baltimore City Community College) on cybersecurity specific pathway programs.

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

P-TECH model could be adopted by federal agencies to create job opportunities for students, and as an approach for their workforce needs. Over 60 P-TECH schools exist throughout the US including in my home state of Rhode Island and there are many more on the way.

We are partnering with community colleges to build the skills of the future through our Community College Skills Accelerator. This program provides access to documented skills roadmaps, access to free IBM tools, including platforms, services, and software, access to IBM mentorship and subject matter expertise, including collaboration on curriculum review and creation and pathways to employment, including internships and apprenticeships.

With growing numbers offering cybersecurity programs, community colleges are 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.[8] Those that offer cybersecurity classes have difficulty updating the content and finding the needed teaching staff. The additional demands of accreditation, distributional requirements, and financial aid requirements make cybersecurity education very challenging for educators.

Programs like the National Security Agency and the Department of Homeland Security sponsored National Centers of Academic Excellence and the National Science Foundation's Advanced Technological Education program that supports regional cybersecurity programs at two-year colleges, are very important resources for these community college programs.

---

[8] "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.

IBM is also driving education programs for middle and high schools. This includes an initiative with ISECOM, a non-profit organization which produces the Hacker High School project - open cybersecurity courses designed specifically for teenagers to develop critical thinking and hands-on, technical skills. As part of this collaboration, IBM is providing sponsorship, expert guidance and IBM Security tools for new Hacker High School lessons focused on the skills needed for an entry-level security operation center (SOC) analyst – a position that is in demand. IBM also hosts "Cyber Day for Girls" events nationwide to provide middle school-aged girls with the opportunity to learn more about cyber security careers, reaching them at a critical age.

IBM partners with hundreds of universities and colleges world-wide to develop the next generation of cyber talent. Through our Academic Initiative program, we provide access to skills and software at no charge. We also sponsor and recruit at key university cyber-competitions, including ones at the Rochester Institute of Technology, New York University and the National Collegiate Cyber Defense Competition.

Military veterans bring unique talents, mindset and skills that are attractive to the technology industry, and even more so to cybersecurity positions. The mission focus mentality and professionalism are attributes needed to protect and defend networks. IBM recently announced it will hire 2,000 U.S. Veterans over the next four years as part of the company's broader pledge to hire 25,000 workers by 2020. Veterans are a natural fit for the new collar approach. We developed the IBM Veterans Employment Accelerator to focus on education and certification programs for military veterans and participate in Veteran recruiting events and transition summits.[9]

Women are globally underrepresented in the cybersecurity profession at 11%, much lower than the representation of women in the overall global workforce. In 2016, women in cybersecurity earned less than men at every level.[10] 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 group that also sponsors external events like the "Cyber Day for Girls" programs in middle schools and provides scholarships to attend security conferences.[12]

---

[9] "Citizen IBM Blog – Veterans Employment Accelerator." IBM website, accessed March 19, 2017. https://www.ibm.com/blogs/citizen-ibm/tag/ibm-veterans-employment-accelerator

[10] 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/

[12] "How IBM Supports Women Building their Careers in Cyber Security." IBM Jobs Blog, November 7, 2016. https://blog.ibm.jobs/2016/11/07/how-ibm-supports-women-building-their-careers-in-cyber-security/

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 2,000 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.

Our success provides some guidance to efforts to create policies around building a cybersecurity workforce, but in many ways, is dependent on the willingness to address the overall challenges in the education system.

What should the 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:

- **Reauthorize Perkins CTE** -- The government needs to improve the alignment between the education system and the skills needed for today's jobs through reauthorization of the Perkins Career and Technical Education Act and the Higher Education Act.
- **Explore P-TECH Model** -- Federal agencies should explore the P-TECH model for workforce development strategies they can implement.
- **Remove Obstacles to Cybersecurity Skills** -- Broad reforms to higher education appear necessary due to poor performance on inclusion, graduation rates, defaults, and alignment with today's jobs. A good starting point is to eliminate existing regulatory obstacles imposed between individuals and cybersecurity careers.
- **Expand New Collar Hiring** -- The federal government should adopt a new collar approach to reach and expand sources of labor.

Alignment through Reauthorization of Perkins Career and Technical Education: The education system is poorly connected to the job market. Schools and colleges often do not offer students relevant classes in emerging areas such as cybersecurity and do not emphasis core attributes like teaming and communication in a program of study. Aligning the education system with the skills needed for today's jobs would more effectively spend federal dollars to help our nation's students acquire the skills that they need and employers are demanding

Recently, the House passed a reauthorization of the Perkins Career and Technical Education Act. Although the Senate has failed to take up the legislation, recently 59 Senators sent a letter to the Chair and Ranking Member of the Senate HELP Committee urging action. The letter called for:

- Align CTE programs to the needs of the regional, state, and local labor market;
- Support effective and meaningful collaboration between secondary and postsecondary institutions and employers;

- Increase student participation in work-based learning opportunities; and
- Promote the use of industry recognized credentials and other recognized postsecondary credentials.

IBM urges the Senate to move forward on reauthorization of the Perkins Career and Technical Education Act, and to incorporate these principles into its reauthorization of the Higher Education Act.

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.

Eliminate Obstacles on the Critical Pathway to Cybersecurity Skills: The education system has appalling key performance metrics in areas relevant to cybersecurity workforce development – first generation entrants into higher education are scarce, completion rates are low, misalignment of skills and jobs is high, and default rates on student loans are astronomical.

Adopting the critical pathway approach used in healthcare to improve quality can help improve the cybersecurity workforce by highlighting the most problematic steps in the education process.

For example, work-based learning is a critical source of skills – particularly in cybersecurity. However, the federal work-study program prohibits more than 25% of funds administered by a college or university from use for off-campus for relevant internships or other work-based learning with private-sector employers.

Eliminating the restrictions would increase the flexibility of students and institutions of higher education to use their federal work study allocations for part- and full-time off-campus cooperative education and other work-study purposes. Rather than forcing work-study grants to be used for dining hall jobs, students could get internships that were relevant to their majors and provided critical work experience and skills.

IBM urges Congress to return flexibility to students and higher education Institutions in their use of work study funds.

New Collar Approaches: Finally, IBM recommends that organizations expand their recruitment of 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:

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

Document the skills and experience that are essential today and in the future. Use that skill map to help design clear career paths for security functions, focusing on what skills are needed in different cybersecurity roles at each level. In recruiting, substitute the skill map for degrees as prerequisites. The skill map should determine when academic degrees are included in hiring requirements. Do all security hires really need four-year university degrees? Do not miss a potential star by imposing arbitrary degree requirements before job candidates they get a chance to prove themselves — realize that skills and experience can come from a variety of places.

Recruit new collar workers from sources beyond traditional higher education sources. Seek students who are earning cybersecurity certificates, AAS, and Associate degrees at community colleges; don't limit efforts to a select set of four-year and research universities. As mentioned earlier, Veterans and separating service personnel are another new collar workforce that has critical skill attributes such as leadership, teaming, and adaptability. IBM has specific recruitment programs for veterans and separating armed services personnel that allow their skills to be mapped against IBM job roles.

To address the different skill and education needs of new collar workers, employers need to build a local cybersecurity ecosystem that provides a robust support program for new hires and focuses on continuous learning and upskilling. Employers need to participate in regional partnerships — with workforce development organizations, secondary schools, and technical and vocational schools. Examples of partnerships between employers and educators include joint cybersecurity curriculum committees, externships for local instructors to keep their skills fresh and relevant, the sponsorship of cyber teams, and programs with local middle and high schools to generate interest in the field. These groups are always looking for subject matter experts and mentors that employers can provide to improve the cybersecurity pipeline.

Work-based learning and "earn and learn" strategies are critical for new collar career pathways. Employ techniques like mentorships, internships, rotational assignments, shadowing and other opportunities for new cybersecurity hires to gain experience and learn. Allow them to explore their options and opportunities —not everyone knows what they want to do right away.

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 five 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 both Committees for the opportunity to present IBM's thoughts, strategy and activities on improving cybersecurity education and your consideration of this testimony.