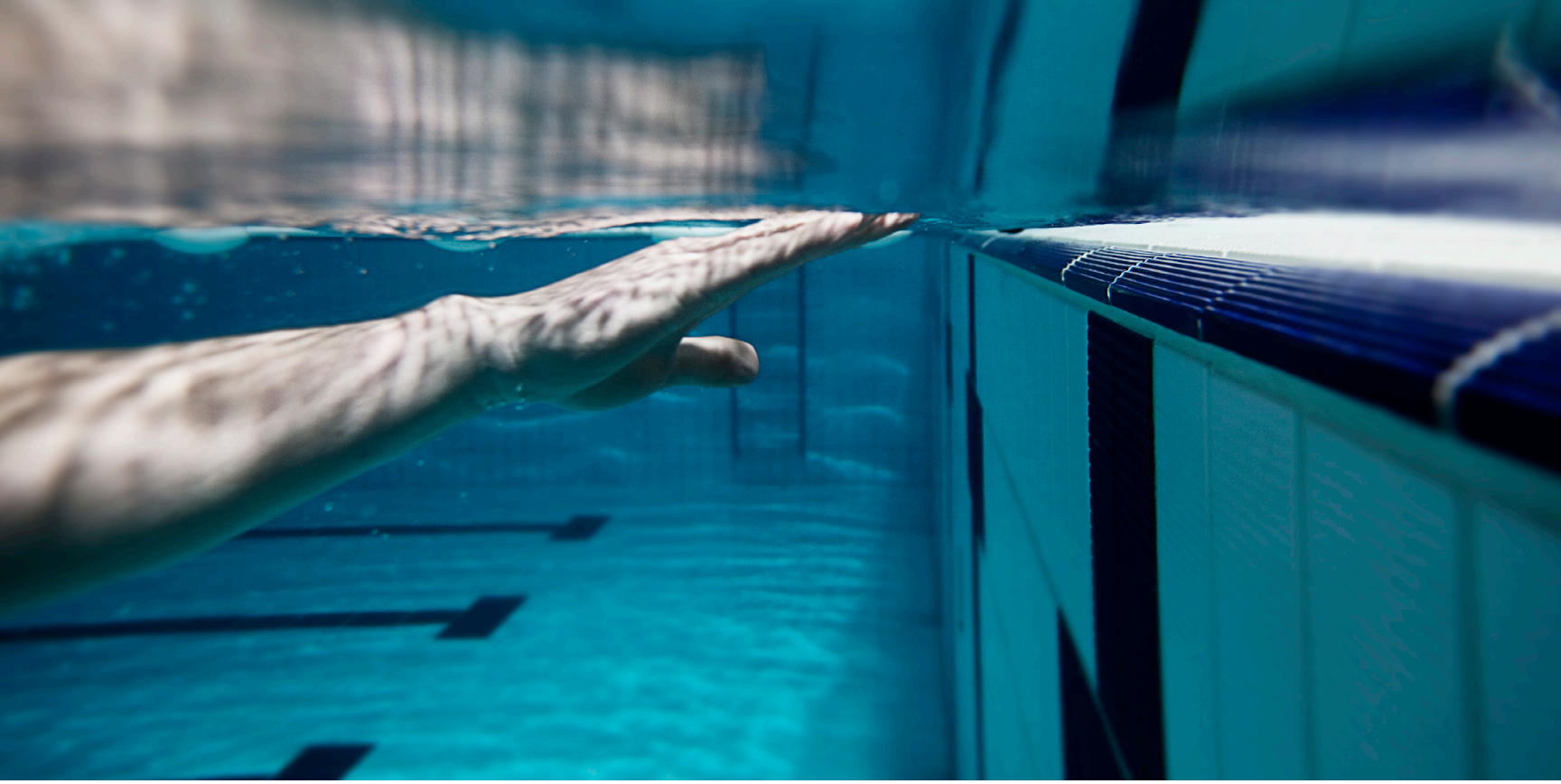


It's not where you start–it's how you finish

Addressing the cybersecurity skills gap with a new collar approach

IBM Institute for Business Value

How IBM can help

Cybercrime is an insidious threat that has reached crisis levels. Though hard to quantify with precision, estimates of its costs to the global economy range from USD 375 to 575 billion per year.[1] No geography or industry is immune. IBM's broad, integrated portfolio is helping organizations outthink threats with an integrated and intelligent security immune system, incorporating the very latest in cognitive, cloud and collaboration technologies.

To get the latest insights from IBM Security, please visit **ibm.com**/security/ciso.

A new approach for cybersecurity recruiting

There is continued high demand for cybersecurity professionals and an ongoing shortage of talent. Organizations are pursuing numerous ways to close the talent gap in both the short and long term — including new university programs, technical and vocational programs, apprenticeships, certifications, early education and government programs. Many 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. In exploring this approach, we look at IBM as a case study to understand how it is beginning to pursue this path.

The obstacles: State of the skills gap

An organization is only as good as the people that are part of it. For cybersecurity leaders, the challenge of recruiting and retaining the best technical and business professionals is a constant worry. Frost & Sullivan predicts that the growing gap between available qualified cybersecurity professionals and unfulfilled positions will reach 1.8 million by 2022.[2] 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.[3] This cybersecurity talent issue isn't limited to a few sectors; it runs across the board from government to education to industry.

The difficulties don't end at raw numbers. Even though government, industry and education are attempting to address the problem, 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 training and professional development to keep up with evolving technologies and the threat landscape. They are also challenged to find time to properly mentor and train new hires. Academic institutions want to meet industry needs, but they are struggling to evolve 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 rising salaries. Finally, students interested in pursuing the cybersecurity field are faced with defining a career path from myriad options and obtaining the significant education and experience required.

Gap

There will likely be as many as 1.8 million unfilled cybersecurity positions by 2022.[4]

Concept

A "new collar" approach focuses on new employee profiles, roles and partnerships – including leveraging approximately 300 U.S. community colleges with cybersecurity offerings.[5]

Blueprint

There are five steps organizations can take to recruit new and retain the existing 770,000 cybersecurity workers in the United States today.[6]

The obstacles may seem insurmountable, but great challenges inspire great action and creativity. To address the gap, both public and private organizations are experimenting with a multitude of approaches to educate and develop the next generation of cybersecurity professionals at all levels. These include the following:

Creating new education programs

- Exploring new education models like Pathways in Technology Early College High School (P-TECH) in the United States and the National College of Cybersecurity in the United Kingdom.[7]
- Supporting programs at community colleges, vocational institutions, polytechnic schools and career centers (for example, the Community College Cyber Summit).[8]
- Driving early education programs for middle and high schools (Hacker Highschool, for example).[9]

Going beyond the traditional classroom

- Establishing apprenticeships, residency programs and internships (for example, ApprenticeshipUSA).[10]
- Emphasizing certification programs and embedding them into education programs. Examples include CompTIA Security+ certification, Certified Information Systems Security Professional (CISSP) certification and Certified Ethical Hacker (CEH) certification.[11]
- Leveraging code schools and boot camps.
- Sponsoring clubs and competitions like CyberPatriot and CyberTitan.[12]

Making connections and sharing information

- Fostering better collaboration and developing tools for students, educators and industry (for example, CyberSeek and TechHire).[13]
- Actively recruiting underrepresented groups through conferences and organizations like the International Consortium of Minority Cybersecurity Professionals (ICMCP), Hire our Heroes, Women's Society of Cyberjutsu and Women in CyberSecurity (WiCyS).[14]

Navigating the course: A new collar approach

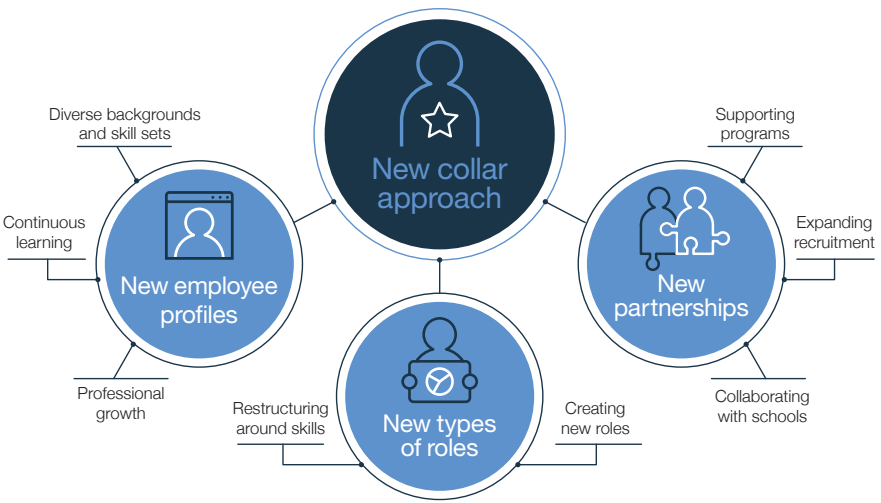
Typically, when any industry is faced with a talent shortage, there are three primary ways to address it. The first is to *change the way work is done* by looking at new operating models. Sometimes that may involve more automation, while other times it might mean utilizing some sort of outsourcing or managed service provider. Another way to traditionally solve a skills gap is to *change the environment.* Attracting a limited resource requires differentiation — making the organization the most desirable place to be either from a challenge, culture, compensation or benefits standpoint. The third way is to *change who the organization pursues*, opening the aperture on the pipeline of candidates.

No one of these techniques alone is going to close the cybersecurity skills gap. Rather, we will see a combination continue to evolve. Many companies, including IBM, are looking at how new technologies can augment security practitioner's skills and change how they work, as well as renewing the focus on their talent pipelines to take advantage of underutilized sources of talent for new types of work.[15] This is the cornerstone of a "new collar" approach and a major component of the overall strategy necessary to address the cybersecurity skills gap. The approach includes:

New employee profiles — 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.

New types of roles — There is a growing realization that new roles focused on emerging technologies require specific skills and knowledge to perform but do not necessarily require a university degree. The approach also involves restructuring work around specific skill sets to create new roles.

New partnerships — Taking a new collar approach requires reaching out and developing new relationships. This includes taking advantage of and supporting federal and state government programs, expanding recruitment at community college programs, collaborating with K-12 school programs and cyber competitions, and linking with veterans training programs.



"The new collar concept recognizes what we at Hacker Highschool have known for years: All you need is a desire to learn and the aptitude for basic computing and networking skills to be a success in the field."

Chris Griffin, Penetration Tester, IBM X-Force Red and volunteer for Hacker Highschool

Training for the race: It's all about skills

Skills are at the center of a new collar approach, and they require a renewed focus. The skills shortage is not limited to cybersecurity talent, as both industry and education face a shortage of workforce skills in general. A recent IBM Institute for Business Value study, "Facing the storm: Navigating the global skills crisis," revealed that a majority of executives surveyed struggle to keep workforce skills current in the face of rapid technological advancement.[16] They fault both their countries' education systems and private industry — 55 percent of executives surveyed said the education systems in their countries don't do enough to promote lifelong learning and skills development, and the same percentage indicated that inadequate investment from industry is the most fundamental challenge around the issue.[17]

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 (see Figure 1). Core attributes can be considered a general disposition beneficial to security professionals — a set of common personality traits and learned behaviors. 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 leadership positions.

Figure 1

Cybersecurity professionals: Core attributes and skills

	Explorer	Problem solver	Student	Guardian	Consultant
Core attributes	Investigative and enjoys challenges	Analytic, methodical and detail oriented	Constantly learning	Protective, ethical and reliable	Can work with others to understand and solve their problems
Skills	An innate understanding of scenarios, risks and "what ifs"	Verifiable hands-on experience with references, certifications and/or micro-credentials Familiarity with and some ability to code—to figure out how to build and take things apart	Specific industry knowledge The ability to adapt to new and emerging security technologies	Familiarity with applicable regulations, laws and policies—and the ability to interpret them	The ability to work in dynamic and diverse teams Effective communication skills—can articulate complex concepts and clearly explain technical issues Experience educating others

"In general, organizations do not go out of their way to hire community college students – even though there are a large number of them and they have great hands-on technical skills. For security, you must be able to 'do it' – it is like being a surgeon: you constantly have to practice, hone your skills, and learn and test new techniques."

Dr. Sujeet Shenoi, F.P. Walter Professor of Computer Science and Professor of Chemical Engineering at the University of Tulsa

Expanding the field: New types of roles

Cybersecurity is just one of many job categories that leverage emerging technologies and require skills and knowledge to perform, but do not necessarily require a traditional four-year university degree. 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.[18]

There are many different security-related roles, ranging from software development, design and sales to consulting and managed security services. Within those areas are dozens of positions requiring different skills and experience, many of which could be filled through a new collar approach. For example, since 2015, IBM Security has hired over 170 people in the United States with less than a university-level education as IT specialists, sellers, software developers and consultants. This accounts for roughly 17 percent of all U.S. hires.

A new collar approach can be used to help fill both technical and non-technical roles. We have identified some specific roles as suitable places to start.

Builders

- *Integration engineer* — Builds coordinated security solutions using existing components, systems and APIs.
- *Test engineer* — Tests systems and components to ensure they are operating as expected even during misuse.
- *Security device analyst* — Tests end user and Internet of Things (IoT) devices for compliance to policies.
- *Cybersecurity developer* — Writes the code for cybersecurity tools and the rules for security devices (for example, IDS, SIEM).

Operators

- *Threat monitoring analyst* — Monitors computer security events and investigates alerts and incidents.
- *Penetration tester* — As someone who emulates the "bad guys," these red team members attack corporate systems and servers.
- *Security Operations Center (SOC) analyst* — Reports on incidents, assists with incident response and coordinates threat intelligence sharing across the SOC.
- *Command and Control (C2) threat hunter* — Searches through datasets to identify threats and attacks that have evaded automated tools.
- *Cyber operations engineer* — Runs the day-to-day cyber operations of an organization, such as managing firewalls and configuring identity management repositories.

Communicators

- *Cyber help desk analyst* — Provides support and instruction when users experience security incidents and events, such as receiving phishing emails or having their systems locked by ransomware.
- *Technical writer* — Authors manuals and supporting documents for security policies and response plans.
- *Security awareness trainer* — Trains employees and customers on cybersecurity basics and recommended practices. They must translate complex and sometimes scary cyber information into actions that users can remember and implement.

Running with a team: Pushing for new partnerships

The third element of a new collar approach is about establishing and developing partnerships with varied organizations and educational institutions. Many potential partnerships can help improve the cybersecurity talent pool, including those involving government programs, community colleges and veteran's organizations (see Figure 2).

As an example, IBM has numerous internal and external programs that help cast a wider net for cybersecurity talent in both the shorter and longer term:

- Creation and replication of the P-TECH 9-14 School Model (see sidebar: P-TECH School Model)[19]
- Women in Security Excelling (WISE) — an internal group that also sponsors external events like the "Cyber Day for Girls" programs in middle schools[20]
- IBM Veterans Employment Accelerator, which focuses on training and certification programs for military veterans[21]
- Expanding traditional recruiting whenever possible — at military bases, cyber competitions and professional organizations
- Sponsorship of cybersecurity competitions like CyberTitan.

"I grew up and lived only blocks away from Carver High School. I told the students that I wish that I had this type of opportunity to gain knowledge, experience and a degree free of charge. I encouraged them to take full advantage of their opportunity and utilize their mentors to their benefit – that is what we are here for."

Loretta Lemon, Senior Managing Consultant – Security, Compliance and Privacy, IBM

Figure 2

Partnerships to improve the cybersecurity talent pool

P-TECH School Model[22]

Designed to serve historically disadvantaged populations, the P-TECH 9-14 School Model provides U.S. public school students in grades 9-14 a clear path to post-graduate opportunities that might not otherwise be available. IBM, along with the New York City Department of Education and The City University of New York, created the first P-TECH school in Brooklyn, New York, in 2011. Through P-TECH, students, who are not screened for admission, earn both a high school diploma and an industry-recognized two-year postsecondary degree at no cost to them or their families. The students are also first in line for jobs with their industry partner. The model has expanded to over 50 U.S. schools and 300 industry partners, with the goal of expanding to 80 plus schools in 2017.

P-TECH connects high school, college and the world of work to prepare students for STEM jobs of the future. Three P-TECH schools are focused specifically on cybersecurity (see below). Additional schools are expected to follow the model set by these pioneers.

School	Partners	Notes
Excelsior Academy at Newburgh Free Academy (New York)	Partnership between the Newburgh Enlarged City School District, IBM and SUNY Orange Community College	In its third year as a public high school, the program has 150 students. Students develop basic network administration skills, perform computer forensic analysis, demonstrate an understanding of network forensics, develop an understanding of the legal issues associated with cybersecurity and develop an appropriate procedure for handling case evidence.
P-TECH@ Carver (Maryland)	Partnership between Carver Vocational Technical High School, IBM and Baltimore City Community College	The program started in the 2016-17 school year with 50 ninth-grade students, and another 50 are expected in fall 2017. With 87 IBM mentors, many students have two mentors. Students will earn an AAS degree in cybersecurity.
Newport P-TECH (Rhode Island)	Partnership between Newport Public Schools, Community College of Rhode Island (CCRI) and the Southeastern New England Defense Industry Alliance (SENEDIA)	This career and technical education program launched in fall 2016 with 42 students (22 female, 20 male). Mentors come from Rhode Island State Police, the U.S. Navy and defense industry companies.

"Many organizations are looking in the wrong places and missing untapped pools of talent... for more than ten years, community colleges have created a large network of centers focused on skills development. These networks have powerful and proven talent development and acquisition models, which are scalable across many industry certifications, job roles and verticals."

Casey O'Brien, Executive Director & Principal Investigator, National CyberWatch Center

With growing numbers offering cybersecurity programs, community colleges are another important source of talent. According to estimates, approximately 30 percent of the roughly 1,100 public and independent community colleges across the United States offer a cybersecurity degree, certificate or course. These programs are educating thousands — students, life-long learners and those looking to up-skill or change careers.[23] Community college programs pride themselves on being more adaptable and skills focused than traditional four-year programs. They can typically react faster to market shifts than traditional, research-based university programs by more rapidly adjusting their approach and curriculum. They also have a history of focusing on workforce and skills development. Finally, community college cybersecurity programs tend to be more hands on than university programs.

There are a number of resources supporting community college cybersecurity programs:

- The National Security Agency and the Department of Homeland Security sponsor National Centers of Academic Excellence, including some focused on information assurance and cyber defense, for two-year institutions.[24]
- The National Science Foundation's Advanced Technological Education program supports regional cybersecurity programs at two-year colleges.[25]
- The Community College Cyber Summit, going on its fourth year, is a locus of cybersecurity efforts at community colleges.[26]

At the starting line: Your own new collar approach

If you want to change who you pursue to help address your skills gap, start building your own new collar approach. At a minimum, make it one component of your overall strategy to build and maintain your cybersecurity workforce.

The easiest way to start is to become an advocate of the approach. Look for simple things you can do —places you can speak and information you can share with your peers. For a more robust new collar approach, consider the following:

Re-examine your workforce strategy

- Think about what skills are essential today and in the future for your organization; document them. Use that to help design clear career paths for your security function, focusing on what skills are needed at each level.
- In recruiting, don't focus solely on degrees as prerequisites. Do all your security hires really need four-year university degrees? Don't filter out potential stars before they get a chance to prove themselves — realize that skills and experience can come from a variety of places.

Improve your engagement and outreach

- Expand where you recruit; don't limit yourself to the select set of universities on which you have always focused.
- Start with simple things like learning sessions and demos at community colleges, P-TECH schools and other educational programs and build from there.

"Historically, there has been a lot of talent that is overlooked by many corporations due to formal degrees being the first requirement in many of their job postings. Everyone has a different path, and they may not have attended a four-year college due to cost or life challenges. Sometimes a role may require 'that degree,' but there are other times I believe we may be filtering and scaring off talent without providing them the opportunity to represent their skills and value."

Adam Griffin, Advisory Architect – Manager, Manager Security Services – Infrastructure & Endpoint Security, IBM Security

Build a local cybersecurity ecosystem

- Look to create new partnerships in your region — with regional workforce development organizations, secondary schools, and technical and vocational schools.
- You can also participate on cybersecurity curriculum committees, provide externships for local instructors to keep their skills fresh and relevant, sponsor cyber teams, and work with local middle and high schools to generate interest in the field. These groups are always looking for subject matter experts and mentors.

Provide a robust support program for new hires

- Employ techniques like mentorships, 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.
- Keep them engaged by giving new hires creative freedom to work on different projects and explore new technologies and services.

Focus on continuous learning and upskilling

- Once you have expanded your recruiting aperture and brought new talent in, work to retain the talent. Keep employees engaged by providing opportunities for them to keep skills up to date through classes, certifications, conferences, etc. Cybersecurity is a highly dynamic field, which requires a constant refreshing of skills.
- Additionally, do what you can to support existing employees from other functions who want to move into cybersecurity as a new career.

Are you ready to take a new collar approach?

- Are you overlooking potential cybersecurity talent by focusing solely on candidates with four-year degrees?
- What cybersecurity roles in your organizations are well suited for a new collar approach?
- How and with what organizations can you build partnerships to expand your cybersecurity ecosystem?
- How can you improve support for cybersecurity new hires?
- What additional opportunities could you offer cybersecurity employees to encourage continuous learning and improve talent retention?

For more information

To learn more about this IBM Institute for Business Value study, please contact us at iibv@us.ibm.com. Follow @IBMIBV on Twitter, and for a full catalog of our research or to subscribe to our monthly newsletter, visit: **ibm.com**/iibv.

Access IBM Institute for Business Value executive reports on your mobile device by downloading the free "IBM IBV" apps for your phone or tablet from your app store.

To learn more about IBM Security, please visit **ibm.com**/security/ciso.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value

The IBM Institute for Business Value, part of IBM Global Business Services, develops fact-based strategic insights for senior business executives around critical public and private sector issues.

About the authors

Marc van Zadelhoff is the General Manager, IBM Security, one of the largest enterprise security companies in the world. With 20 years of experience in cybersecurity, he works with clients across industries to help them develop their security strategies and determine the best technologies to meet their needs. Marc can be reached on Twitter @mvzadel and at marc.vanzadelhoff@us.ibm.com.

Lindsey Lurie is the Chief Marketing Officer for IBM Security. Lindsey's 15 plus years of experience with IBM spans marketing and communication roles across multiple businesses. Her areas of expertise include demand generation, product marketing, digital and channel marketing, advertising and event execution. She can be reached on LinkedIn at linkedin.com/in/lindseylurie and at llurie@us.ibm.com.

David Jarvis is the Security and CIO Lead at the IBM Institute for Business Value. He is responsible for developing and executing a research agenda that explores emerging business and technology topics for those areas. David can be reached on LinkedIn at linkedin.com/in/davidajarvis, via Twitter @dajarvis and at djarvis@us.ibm.com.

Contributors

Diane Delaney — Worldwide Talent Manager, IBM Security
Lisa van Deth — Campaign and Thought Leadership Strategy Manager, IBM Security
Kelli Jordan — Talent Leader, New Collar Initiatives, IBM Human Resources
Diana Kelley — Global Executive Security Advisor, IBM Security
Ivo Klaassen — Global Professional Development Leader, IBM Security
Heather Ricciuto — Transformation and Academic Initiatives Leader, IBM Security

Acknowledgments

Cliff Archey — Program Manager, Education, IBM
Lee Christian — Senior MSIEM Analyst, U.S. MSIEM Analyst Team Lead, IBM Security
Ashleigh Cooper — Program Manager, Education, IBM
Sean Davis — Security Services Senior Security Engineer, IBM Security
Matthew Dombrowski — MSS IES Engineer, IBM Security Services, IBM Security
Adam Griffin — Advisory Architect, Manager, MSS: Infrastructure & Endpoint Security, IBM Security
Michael Kelly — Chair, Computer Studies & Information Processing Department, Community College of Rhode Island
Valinda Scarbro Kennedy — Worldwide Skills Program Manager, IBM
John Kuhn — Manager, IBM X-Force Services, IBM Security
Linda Larsen — Director, Education Outreach, Southeastern New England Defense Industry Alliance
Loretta Lemon — Senior Managing Consultant, Security, Compliance, and Privacy, IBM
Molly Magee — Executive Director, Southeastern New England Defense Industry Alliance
Bill McDonald — Director, Human Resources, IBM Security
Casey O'Brien — Executive Director & Principal Investigator, National CyberWatch Center
Cecelia Schartiger — Jr. IA Compliance Officer, Cyber & Biometrics, IBM Global Business Services
Ken Shade — MSIEM Monitoring Manager, IBM Security
Dr. Sujeet Shenoi — F.P. Walter Professor of Computer Science and Professor of Chemical Engineering at the University of Tulsa

Notes and sources

1 "Net Losses: Estimating the Global Cost of Cybercrime." Center for Strategic and International Studies and McAfee. June 2014. https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

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

3 "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/

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

5 "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.

6 "Interactive map." CyberSeek website, accessed May 3, 2017. http://cyberseek.org/heatmap

7 "P-TECH 9-14 Model." P-TECH website, accessed April 3, 2017. http://www.ptech.org/; Coughlan, Sean. "Bletchley Park: 'Codebreakers school' planned for site." BBC News. November 24, 2016. http://www.bbc.com/news/education-38065563

8 "2017 Community College Cyber Summit (3CS): Strengthening our cyber IQ." 3CS website, accessed April 3, 2017. https://www.my3cs.org/

9 "Hacker Highschool: Security Awareness for Teens." Hacker Highschool website, accessed April 3, 2017. http://www.hackerhighschool.org/

10 "Apprenticeship USA." United States Department of Labor website, accessed April 3, 2017. https://www.dol.gov/featured/apprenticeship

11 "CompTIA Security+." CompTIA website, accessed April 3, 2017. https://certification.comptia.org/certifications/security; "CISSP – Certified Information Systems Security Professional." (ISC)2 website, accessed April 3, 2017. https://www.isc2.org/cissp/default.aspx; "Master the Core Technologies of Ethical Hacking." EC-Council website, accessed April 3, 2017. https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

12 "Air Force Association's CyberPatriot: The National Youth Cyber Education Program." CyberPatriot website, accessed April 3, 2017. https://www.uscyberpatriot.org/; "CyberTitan: Now launched." Information and Communications Technology Council website, accessed April 3, 2017. http://www.ictc-ctic.ca/cybertitan/

13 "About this tool." CyberSeek website, accessed April 3, 2017. http://cyberseek.org/; TechHire website, accessed April 3, 2017. http://techhire.org/

14 International Consortium of Minority Cybersecurity Professionals website, accessed April 3, 2017. https://icmcp.org/; "Veterans Training." Hire our Heroes website, accessed April 3, 2017. https://hireourheroes.org/veterans-training/; Women's Society of Cyberjutsu website, accessed April 3, 2017. http://womenscyberjutsu.org/; Women in CyberSecurity website, accessed April 3, 2017. https://www.csc.tntech.edu/wicys/

15 Barlow, Caleb. “Artificial intelligence makes cybersecurity the ideal field for ‘new collar’ jobs.” The Hill. March 22, 2017. http://thehill.com/blogs/pundits-blog/technology/325067-artificial-intelligence-makes-cybersecurity-the-ideal-field-for
16 King, Mike; Anthony Marshall; and David Zaharchuk. “Facing the storm: Navigating the global skills crisis.” IBM Institute for Business Value. https://www-935.ibm.com/services/us/gbs/thoughtleadership/skillsstorm
17 Ibid.
18 “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
19 “IBM and P-TECH.” IBM press kit. IBM website, accessed April 3, 2017. https://www-03.ibm.com/press/us/en/presskit/42300.wss
20 “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/
21 “Citizen IBM Blog – Veterans Employment Accelerator.” IBM website, accessed March 19, 2017. https://www.ibm.com/blogs/citizen-ibm/tag/ibm-veterans-employment-accelerator
22 “P-TECH Schools.” P-TECH website, accessed March 19, 2017. http://www.ptech.org/schools; “IBM Equips Youth with Tech Career Skills in Nationwide Network of High Performing P-TECH Schools.” IBM press release. January 5, 2017. http://www-03.ibm.com/press/us/en/pressrelease/51327.wss; “Case study: Preparing students at Excelsior Academy for Careers.” P-TECH website, accessed April 3, 2017. http://www.ptech.org/case-study/preparing-students-at-excelsior-academy-for-careers; “Two Baltimore high schools first to join P-TECH program in Maryland.” Johns Hopkins University, University News. June 16, 2016. http://hub.jhu.edu/2016/06/16/p-tech-schools-announced-dunbar-carver/; “Newport P-TECH.” P-TECH website, accessed April 3, 2017. http://www.ptech.org/schools/000000000000049; “P-TECH.” Rogers High School webpage. Newport Public Schools website, accessed April 3, 2017. https://www.npsri.net/ptech
23 “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.
24 “NSA/DHS Current National CAE Designated Institutions.” Information Assurance at the National Security Agency website, accessed March 19, 2017. https://www.iad.gov/nietp/reports/current_cae_designated_institutions.cfm
25 “ATE Centers – Security Technologies.” National Science Foundation’s Advanced Technological Education centers website, accessed March 19, 2017. http://www.atecenters.org/st/
26 “Community College Cyber Summit 2017.” Accessed March 19, 2017. https://www.my3cs.org/

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
May 2017

GBE03830USEN-01