# Principles for Growing and Sustaining the Nation's Cybersecurity Workforce

November 2018

ASPEN CYBERSECURITY GROUP

THE ASPEN INSTITUTE

## About the Aspen Cybersecurity Group

The Aspen Cybersecurity Group is a cross-sector public-private forum comprised of former government officials, Capitol Hill leaders, industry executives, and respected voices from academia, journalism, and civil society that have come together to translate pressing cybersecurity conversations into action. At its inaugural meeting in January 2018, the group decided to focus its efforts in three key areas of need as requiring urgent attention by a group that crosses party lines and includes both policymakers and practitioners: (1) improving operational collaboration between the public and private sector; (2) developing the skills and education necessary for a workforce that will increasingly confront cybersecurity challenges; and (3) securing and ensuring confidence in emerging technologies, including the Internet of Things (IoT).

**Co-Chairs:**

**U.S. Representative Will Hurd** (TX-23)

**Lisa Monaco** (Distinguished Senior Fellow, NYU Law School, Center on Law and Security, and Center for Cybersecurity)

**Ginni Rometty** (Chairman, President, and CEO, IBM)

**Members:**

**John Carlin** (Chair, Cyber & Tech Program, Aspen Institute)
**Keith Alexander** (President and CEO, IronNet Cybersecurity)
**Sara Andrews** (CISO, Pepsi)
**Monika Bickert** (Head of Product Policy and Counterterrorism, Facebook)
**Vint Cerf** (Chief Internet Evangelist, Google)
**Greg Clark** (CEO, Symantec)
**Dr. Lorrie Faith Cranor** (Professor, Carnegie Mellon University)
**Michael Daniel** (President and CEO, Cyber Threat Alliance)
**Jim Dempsey** (Executive Director, Berkley Center for Law & Technology)
**Don Dixon** (Co-Founder & Managing Director, Trident Capital Cybersecurity)
**Lynn Good** (CEO, Duke Energy)
**Alex Gorsky** (CEO, Johnson & Johnson)
**Yasmin Green** (Director, Research & Development, Jigsaw)
**Michael Hayden** (Principal, The Chertoff Group)
**Susan Hennessey** (Managing Editor, *Lawfare*)
**Chris Inglis** (U.S. Naval Academy)
**Sean Joyce** (Partner, PwC)
**Dr. Herb Lin** (Senior Research Scholar & Research Fellow, Stanford University)
**Brad Maiorino** (Executive Vice President, Booz Allen Hamilton)
**Chandra McMahon** (Senior Vice President & CISO, Verizon)
**Dr. Gregory Rattray** (Director of Global Cyber Partnerships, JPMorganChase)
**Former Rep. Mike Rogers** (Distinguished Fellow & Trustee, Center for the Study of the Presidency and Congress)
**David Sanger** (National Security Correspondent, *New York Times*)
**U.S. Representative Adam Schiff** (CA-28)
**Dr. Phyllis Schneck** (Managing Director, Global Leader of Cyber Solutions, Promontory Financial Group, an IBM Company)
**Alex Stamos** (Adjunct Professor, Stanford University)
**Dr. Hugh Thompson** (CTO, Symantec)
**Kathy Warden** (President and COO, Northrop Grumman)
**Michelle Zatlyn** (COO and Co-Founder, Cloudflare)
**Jonathan Zittrain** (Director, Harvard Berkman-Klein Center for Internet & Society)
***Jane Harman*** *(ex-officio)*
***Michael Chertoff*** *(ex-officio)*

## Principles for Growing and Sustaining the Nation’s Cybersecurity Workforce

# Abstract

The cybersecurity skills gap is real and it's growing. By 2021, there will be at least 500,000 unfilled cybersecurity roles in the United States if we don't start thinking – and acting – differently about how we identify and develop talent.

We identified four major trends that are contributing to the gap:

1. the growth in demand for skills is significantly outpacing growth in supply;
2. we are leaving large pools of skilled candidates untapped;
3. the complexity of employer requirements means more than 50% of applicants are considered "unqualified"; and
4. there is low awareness of opportunity, fit, and career path for the general population.

The Aspen Institute Cyber and Technology Strategy Group provides eight recommendations for consideration. Alone, no single recommendation will close the gap. Employers will need to build multi-faceted talent strategies to revitalize their hiring, training, and employee development to solution this at scale.

Principles:

1. Widen the aperture of candidate pipelines by adopting New Collar principles (e.g., stop making degrees a mandatory requirement for jobs).
2. Revitalize job postings to be engaging and to focus on the core requirements; don't "over-spec" the requirements.
3. Simplify career models and build transparency; leverage the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework where possible for consistency.
4. Think about new ways of hiring and training, where the adjacent technical and professional skills take priority, and cybersecurity skills can be taught.
5. Launch apprenticeship programs to train candidate pipelines at scale.
6. Commit to employee development – support expanded and focused training in general.
7. Adopt key principles for productive partnerships and programs – maximize impact by partnering with a focus on scale.
8. Make cybersecurity everyone's business – continue to advocate and make cybersecurity education widely available.

## The Cybersecurity Workforce Challenge

The accelerating pace of technology change brings incredible innovation and opportunity. It also brings a new challenge – how do we keep the skills of the American workforce up to date in a world where newly learned skills may be relevant for months or years, not decades? Academia, government, and industry have partnered on the skills gap in technology and STEM, but nowhere are the stakes higher than in cybersecurity, when it comes to protecting our data, our industries, and our nation.

DEFINING CYBERSECURITY SKILLS

When referring to cybersecurity skills, we are referencing the types of skills that are needed for specialized roles, such as cybersecurity specialist, cybercrime analyst, and IT auditor. We are not referring to skills that are needed for more general information technology roles that do not specialize in cybersecurity.

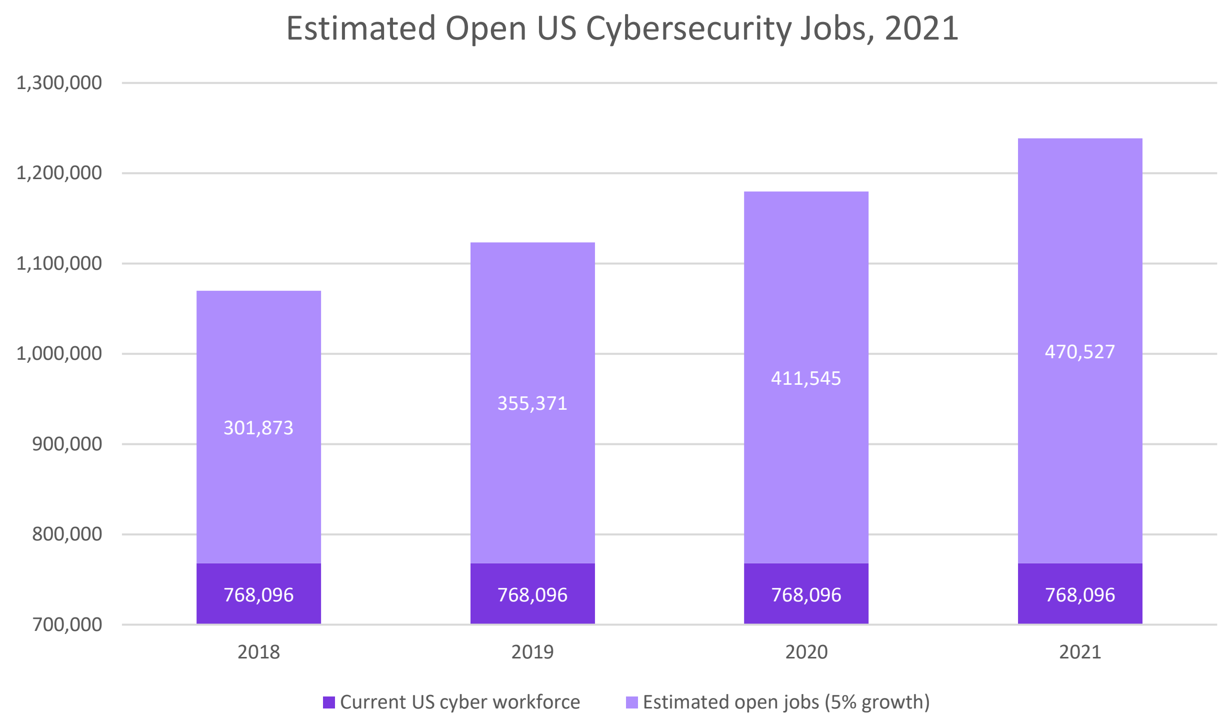
| EXAMPLES OF GENERAL IT SKILLS | EXAMPLES OF CYBERSECURITY SKILLS |
|---|---|
| • Programming languages, like JavaScript, Java, Ruby, Python, Go<br>• Implementing server-side or application logic, developing databases, and designing architectures<br>• Experience with Agile development methodology | • Conducting vulnerability scans and recognizing vulnerabilities in security systems<br>• Assessing the robustness of security systems and designs<br>• Implementing, maintaining, and improving established network security practices |

There are over 300,000 unfilled cybersecurity jobs in the United States.[1] And with the estimated growth rates in the technology and cybersecurity sectors predicted at a minimum of 5%[2] year-over-year – with some estimates even higher – this gap will continue to widen. By 2021, we estimate there will be at least 470,000 unfilled cybersecurity jobs in the United States if we don't start thinking – and acting – differently about how we identify and develop talent.

We need to expand the supply of candidates to fill these roles, and to make cybersecurity as a career more attainable and discoverable to the general population. Cybersecurity must become everyone's business.

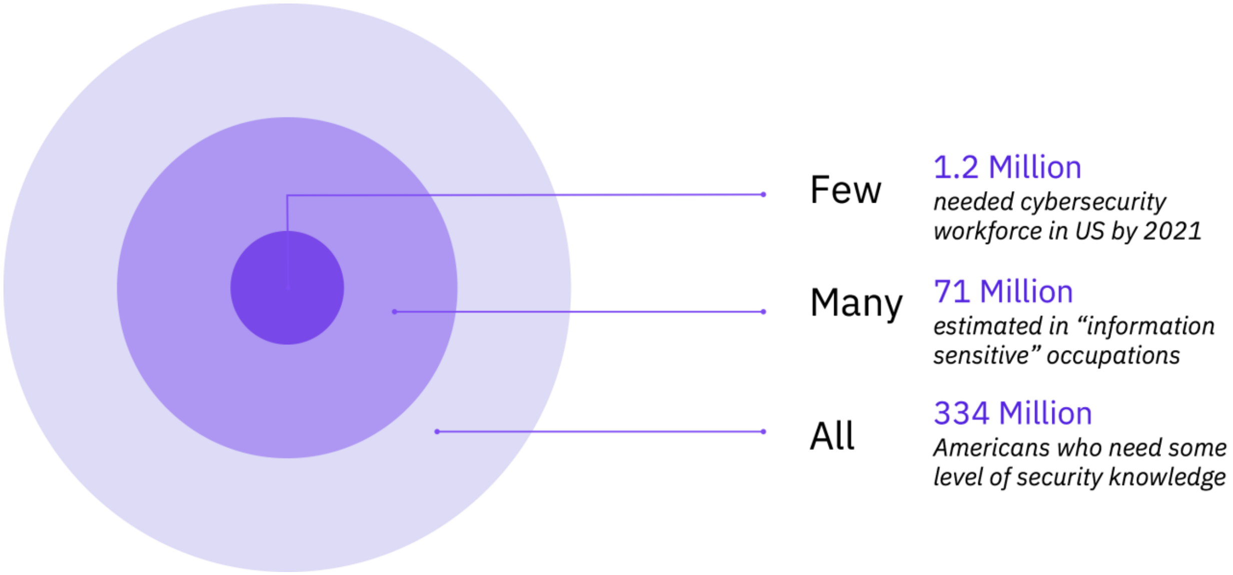
[1] https://www.cyberseek.org/heatmap.html, accessed October 11, 2018

[2] CompTIA, IT Industry Outlook 2018, accessed October 11, 2018



## Cybersecurity is Everyone's Business

While our priority is the estimated 500,000 open cybersecurity roles we will need to fill by 2021, we need to bear in mind that cybersecurity is everyone's business:



Few **1.2 Million** *needed cybersecurity workforce in US by 2021*

Many **71 Million** *estimated in "information sensitive" occupations*

All **334 Million** *Americans who need some level of security knowledge*

The *few* are the cybersecurity practitioners whose jobs focus on digital protection, investigation, analysis, and security-specific responsibilities. However, many Americans will need some level of digital and cyber fluency in their jobs, and we all need general awareness as consumers and citizens.

The population of *many* are at least the 71M Americans[3] in information-sensitive professions who require some level of expertise. These employees handle sensitive information as a key part of their daily responsibilities and may need additional skills and knowledge based on their discipline (professions like lawyers, law enforcement, bankers, healthcare providers, securities traders, engineers, educators, and scientists) or based on their role (corporate board members, law enforcement, educators). While their knowledge may not need to be as technical or deep as the cybersecurity practitioners, a need still exists.

The population of *all* represents all Americans -- because we all have a requirement to have some level of digital fluency and awareness. By building a minimum skill level across America, we establish a sort of "herd immunity" that allows the larger population to help protect all our data through better hygiene and behaviors.

## New technologies – challenge or opportunity?

The pace of technological change makes it more challenging to develop cybersecurity practitioners fast enough to meet demand. But could advances in artificial intelligence, machine learning, and data science form part of the solution? According to IBM research, on average, security teams sift through more than 200,000 security events per day with more than 20,000 hours per year wasted chasing false positives. AI and other new technologies will be critical to keep up with the anticipated doubling of security incidents over the next five years.

When considered against the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework categories, the potential exists for technology advances to create efficiencies that may address some of the cybersecurity skills gap.

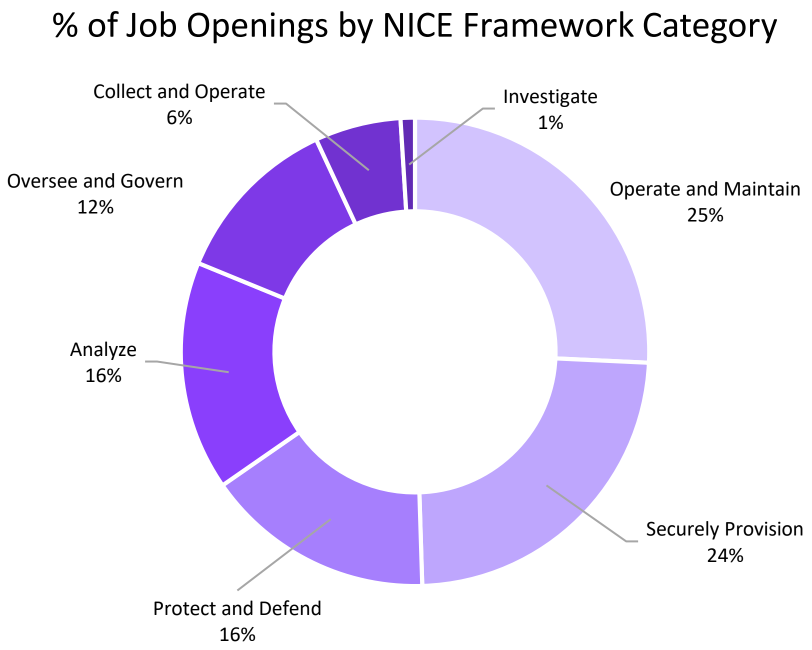
[3] The 71M number is based on current workforce volumes in "information sensitive" occupations, which is currently 69M. BLS is estimating a 0.7% increase annually in the labor market through 2026, so 71M is a projection based on that growth rate. Our list of "information sensitive" occupations includes: Computer and Mathematical; Business and Financial Operations; Management; Healthcare Support; Legal; Education, Training, and Library; Office and Administrative Support; and Sales and Related occupations.

| NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY | DESCRIPTION |
|---|---|
| SECURELY PROVISION | Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development |
| OPERATE AND MAINTAIN | Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security |
| OVERSEE AND GOVERN | Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work |
| PROTECT AND DEFEND | Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks |
| ANALYZE | Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence |
| COLLECT AND OPERATE | Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence |
| INVESTIGATE | Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence |

Workforce categories such as *Securely Provision* or *Oversee and Govern* need higher order human capability, relationships, and engagement, and are less likely to be significantly impacted by automation. However, workforce categories such as *Analyze* and *Collect and Operate* involve the collection and categorization of large quantities of raw data, and may benefit from advancements in data analytics, machine learning, and artificial intelligence.

New technologies will impact the work of cybersecurity practitioners across the individual categories by providing decision-support and foundational capabilities such as data collection, analytics, data representation, correlation, and reporting. This will shift the workforce needs from manual tasks to higher-order work only accomplished through human intervention. Further exploration into the impact of technology advances, within the context of the NICE Workforce Framework, is warranted.

Analyzing the relationship between the percentage of job opening by workforce category shown below and technology advances may inform prioritization of the solutions pursued. For example, the *Operate and Maintain*, *Protect and Defend,* and *Analyze* workforce categories represent a large portion of the job openings and will likely benefit most from technology advances and automation. Closing the gap in these categories might best be addressed through investment in data analytics tool suites. Job openings in *Securely Provision*, which is identified as an area requiring higher-order human capabilities, may be addressed through other means such as targeted upskilling in secure systems architecture, secure network design, and systems development. This analysis should be used to develop more focused approaches to the cybersecurity workforce challenge; specific solutions can be developed to optimally address an organization's business needs and current workforce situation.



[4]

The numbers associated with cybersecurity workforce supply and demand are already fluid based on a number of factors and adding new technologies into the equation makes specificity in future projections even more difficult. We should continually reevaluate the forces impacting the cybersecurity workforce to adjust to changing dynamics.

[4] https://www.cyberseek.org/heatmap.html, accessed October 11, 2018

## Root causes behind the cybersecurity skills gap

Four major trends emerge as root causes behind the skills gap.

### FIRST: The growth in demand for skills is significantly outpacing growth in supply.

The rate of growth for cybersecurity jobs is at least in line with the growth of IT jobs overall, but may be as high as 3x that rate. Exacerbating the situation is that all domains - government, industry and academia - need to add cybersecurity practitioners to their workforce regardless of the products or services they provide. This in turn leads to increased competition between public and private sector for scarce skills. If these trends continue, the gap between supply and demand will continue to grow. There is no evidence that the supply of candidates for these jobs will grow in parallel with the demand, which means that we need to think differently about both sides of the equation – modernizing our approaches to role design and hiring (the demand) and finding new ways to build and grow our pipeline (the supply).

### SECOND: We are leaving large pools of skilled candidates untapped.

Women are severely under-represented in cybersecurity, with representation at only 11%[5] -- compared to 26% of the workforce in general IT. There is evidence that this is improving, with some reports that women now compromise 20% of the global cybersecurity workforce.[6] Regardless, these percentages still indicate that that there is a significant untapped pool of talent, since women make up 43% of the full-time labor force in the United States.[7]

Military veterans, including those recently transitioning back to civilian life, are another significant pool of candidates to be tapped. There are approximately 10.1 million veterans in the labor force today, including 5.9 million who have served since the start of the Gulf War era.[8] In addition, there are approximately 200,000 veterans transitioning back to the workforce each year,[9] which accounts for a significant net new supply of talent. Veterans provide a ready supply of talent with key skills aligned to many cybersecurity roles, simply by the nature of the work they performed while serving. Additionally, more than 10% of cybersecurity jobs require that employees hold some type of security clearance or undergo a background investigation. Many military veterans completed these requirements while serving and bring those credentials to the civilian work.

Third, the geographic locations of traditional “tech hubs” and the continued assumption around bachelor’s degree as a requirement for employment serve to exclude a large population of potential candidates. Brookings found that 17% of workers in thirteen different computer and mathematical occupations did not have a bachelor’s degree, and that many of these “mid-tech” or new collar jobs can

[5] https://www.techrepublic.com/blog/it-security/gender-gap-why-information-security-needs-more-women/
[6] https://cybersecurityventures.com/women-in-cybersecurity/
[7] https://www.dol.gov/wb/stats/NEWSTATS/latest/parttime.htm#one
[8] https://www.bls.gov/news.release/vet.t01.htm, accessed October 11, 2018
[9] https://www.jpmorganchase.com/corporate/news/stories/gen-odierno.htm

be found in areas outside the traditional coastal hubs, in cities like Springfield, IL; Ames, IA; and Raleigh, NC.[10]

## THIRD: The complexity of employer requirements means more than 50% of applicants are considered "unqualified."

In general, job postings show that cybersecurity roles often require more experience, education, and certifications than IT roles. 84% of postings studied required a bachelor's degree; 83% required at least three years of experience. More than 35% required certification, with the top three desired certifications requiring a minimum of five years of experience. Security clearances can delay the hiring process further, with more than 10% of cybersecurity jobs requiring them.[11]

Most employers do not provide a sufficient distinction between the roles of various cybersecurity practitioners across the continuum of engineers, scientists, developers, operators, and defenders, because they are not specifying clear tasks and corresponding knowledge, skills, and abilities (KSAs). Not all roles require the same amount of education and training, though jobs are posted as if they do.

## FOURTH: There is low awareness of opportunity, fit, and career path for the general population.

Among the general population, there is a lack of awareness of cybersecurity as a profession -- only 37% of students were advised of cybersecurity as a career.[12] There is insufficient outreach aimed at raising awareness among diverse populations, though a number of diversity-focused student and professional organizations have emerged in the cybersecurity domain. Information about the cybersecurity career path is not easily discoverable or consumable, with Cyberseek.org and the National Initiative for Cybersecurity Careers and Studies (NICCS) being leading providers. In general, careers aren't well-understood either, even once a possible candidate has found out about jobs, they simply don't understand how to navigate the myriad options or what could be possible for them.

[10] https://www.brookings.edu/blog/the-avenue/2018/06/20/could-mid-tech-jobs-elevate-more-people-and-non-coastal-places/

[11] https://www.burning-glass.com/research-project/cybersecurity/

[12] https://www.raytheon.com/sites/default/files/2017-12/2017_cyber_report_rev1.pdf

# Solving the cybersecurity workforce challenge

With no single reason behind the skills gap, the adoption of key principles is a common starting point for solutions. The key principles outlined below, while rooted in the need to develop solutions to solve the skills gap in the United States, are extensible to the global market that is facing similar challenges.

## No degree?  No problem!  Widen the aperture of your candidate pipeline

Employers can immediately begin to expand candidate pipelines by thinking about their job opportunities through the lens of New Collar roles. The concept of New Collar, a term coined by IBM CEO Ginni Rometty, is that there are many opportunities in the technology industry that don't require a four-year degree, but rather, they require some level of knowledge or skill.  These skills can be earned in a variety of ways – from traditional education including community colleges, to bootcamps, on-the-job learning, or apprenticeship.

By thinking about open jobs through the lens of New Collar, employers can immediately begin to expand applicant pools. This also has the benefit of creating more diverse and inclusive candidate pipelines, which is especially important for a field like cybersecurity, where diverse teams are beneficial to solving complex challenges.

How do employers apply a New Collar focus to their job postings?  It's simple.  Remove degree requirements from job postings whenever they are truly not required.  Shift the mindset from recruiting like it has always been done in the past, and challenge the assumption that a degree is required for every role.  As shared previously, a study undertaken by Brookings found that half a million workers in high-tech – 17% of the workforce - lack a bachelor's degree.[13] Educational pedigree isn't a non-negotiable requirement.

Adopting this principle means an internal review of job descriptions. An employer may have to conduct a job analysis to clearly understand the qualifications for a role, but after completing that exercise, will be able to clearly post opportunities that state only true role requirements, and will be able to bring in more qualified candidates for every opening.

[13] https://www.brookings.edu/blog/the-avenue/2018/06/20/could-mid-tech-jobs-elevate-more-people-and-non-coastal-places/

## Stop focusing on all the ways a candidate doesn't measure up

Most job descriptions today don't provide a candidate-centric experience. Rather, the long and tedious list of over-qualifications, certifications, and years of experience in multiple areas of expertise really serves to tell a candidate that they can't measure up to exceedingly high expectations.

To be blunt, we are "over-spec'ing" cybersecurity roles, to the point where even so-called entry-level jobs often require 3 – 5 years of experience!

Stop signaling to candidates that they aren't qualified for roles, and re-write position descriptions to focus on the knowledge, skills, and abilities (KSAs) necessary to complete tasks. This could start with the job analysis recommended in the previous solution, but another great starting point for employers would be to align position descriptions to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), developed by the US Department of Commerce's National Institute of Science and Technology. The NICE Framework is a robust, searchable framework of cybersecurity roles, KSAs, and tasks. Organizations can use this tool to identify the key skills, tasks, and activities they are looking for, and align them to an industry-recognized job title.

### CASE STUDY

As part of the Aspen Cybersecurity Group, IBM undertook a three-week project sprint to improve their cybersecurity job postings. The Talent Acquisition team identified five job profiles where they had large recruiting needs and/or challenges finding the right candidates, and matched up the IBM terminology with data from the NICE Framework. Simultaneously, the team rewrote more engaging descriptions of the general IBM experience, and also put a candidate-centric spin on the job description, through the use of personalization and words like "you" and "your" instead of "the incumbent." Finally, they also leveraged tools like Textio to augment their writing and assess overall tone. Examples of the new job descriptions can be found in the appendix.

## Simplify, streamline, and standardize your career model

It can be challenging to understand the differences in job roles between, and even within, companies, as job titles, skills, and tasks can be inconsistently named. Employers may have their own in-house terminology and job titles, which makes it hard to compare opportunities, or understand progressive career paths.

Focus on making your career paths understandable and accessible to current employees and possible job seekers by simplifying, streamlining, and standardizing them. If you're taking action to rewrite your position descriptions as recommended, you're already part of the way there.

1

Rewrite your position descriptions, leveraging the NICE Framework, and eliminating jargon and company-specific phrases.

2

Create clear career roadmaps, showing common career progressions between roles, as well as parallel or adjacent roles that might feed into the roadmap with additional training. The Career Pathways map on cyberseek.org is a great place to draw inspiration.

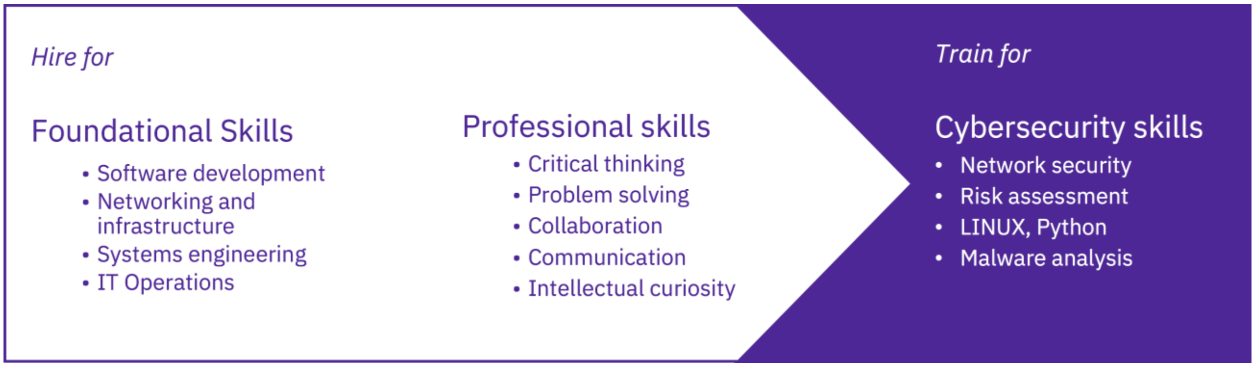
3

Share information openly and transparently. Advertise your career paths, share stories of career progression, and provide links to the NICE Framework so that employees and job seekers can understand the linkages and explore more.

## Flip your model – hire with the intent to train

Today, companies tend to rely primarily on technical skills fit when hiring. The depth of cybersecurity skills takes top priority, with foundational skills and professional skills prioritized lower in candidate evaluations – the assumption being that those skills can be learned on the job.

However, experience has shown that flipping that model may be beneficial, especially as we look for new ways to close the skills gap. More often, employers are finding it difficult to train for foundational skills and professional skills. By focusing hiring efforts on those skills as the priority, with the intention to deliver the deeper cybersecurity skills in on-the-job learning, employers can open up the aperture of their candidate pool and start to bring in more New Collar, diverse, talent, and create new opportunities for work-based learning through apprenticeships.



*Hire for*

Foundational Skills

- Software development
- Networking and infrastructure
- Systems engineering
- IT Operations

Professional skills

- Critical thinking
- Problem solving
- Collaboration
- Communication
- Intellectual curiosity

*Train for*

Cybersecurity skills

- Network security
- Risk assessment
- LINUX, Python
- Malware analysis

Think critically about what you look for in your hiring, especially in entry level roles.  By identifying candidates with the broader foundational skill sets, not only will you expand your candidate pool, you may also find that you have an existing in-house pool of talent with the basic skills needed and who are eager to be retrained and upskilled for emerging cybersecurity roles as the next step in their career.

## “Learn and earn” with apprenticeship programs

Apprenticeship is a “learn and earn” model that combines on-the-job training with job-related instruction, tied to the attainment of national skills standards. It’s a proven model dating back hundreds of years in the skilled trades, and is seeing significant growth and adoption across the tech industry today.

Apprenticeship provides opportunities to hire talent eager to learn, and for employers to hire new employees who can be trained in the exact way needed for their open roles. It’s highly scalable and can help to build the talent you need, through structured education and hands-on learning.

This model can also be highly effective for workers who already have foundational knowledge and experience in relevant areas. It creates the opportunity to train on the needed cybersecurity skills while providing the time needed to gain on-the-job experiences.

### CASE STUDY

In October 2017, IBM launched a Department of Labor Registered Apprenticeship program.  IBM had identified a need for an apprenticeship program as a talent pipeline solution based on increasing competition in recruitment, as well as the need to support knowledge transfer for retiring workforce segments.  In the course of 12 months, the program grew from 7 apprentices to 190, in occupations like Software Development, System Administration, Project Management, and of course, Cybersecurity.

IBM Cybersecurity Analyst apprentices complete a 12-month training program that includes over 400 hours of structured learning, coupled with mentorship and on-the-job activities like performing network and wireless intrusion detection, security activity monitoring, incident response processes, scans of databases, web applications, anti-virus and others.  IBM also built a Cyber Learning Lab to train apprentices on how to set up and maintain a cybersecurity lab and how to install, use and troubleshoot cybersecurity tools and technologies like QRadar, Guardium, McAfee, Tenable, and others.  In addition, apprentices complete required learning and exam preparation for the CompTIA Security+ Certification.

More information on the IBM Cybersecurity Analyst apprenticeship can be found in the appendix.

## Commit to employee development

While efforts to contemporize the talent acquisition process are a good start, focusing on your existing employee population and their skill development will also be key.  As an employer, you need to prioritize employee access to learning, and support employee efforts to reskill and upskill.

As you build out your new career model, consider how you can incorporate employee learning into the roadmaps.  Are there clear learning journeys or activities that an employee can undertake to help support their career progression?  If yes, share those publicly.  And if not, consider building these out, either internally or with third-party training partners.

Remember that many mechanisms beyond external hiring exist to help address the skills gap.  Many employees will be eager to progress their career through reskilling and upskilling, so make a point to offer opportunities for things like stretch assignments and shadowing, so that employees can begin that journey in an easily accessible way.

A model for cybersecurity reskilling can be found in the appendix.

## Adopt key principles for productive partnerships and programs

Because there are multiple root causes behind the skills gap, a variety of solutions will be needed, and employers will not be able to solve the challenge in a vacuum. Partnerships – with academic institutions, non-profit organizations, and government – will be part of how we address this challenge at scale.

The more successful programs and partnerships have something in common. These common design points have been distilled into five key principles that we recommend all companies adopt as part of their programmatic and partnership efforts.

1. Collaboration is key. Successful programs don't do it alone. Industry, academia, and government collaborate and share best practices to leverage successes, maximize the value of efforts, and achieve results at the scale necessary.
2. Inclusion is a must. Successful programs engage under-represented populations or expand the aperture of candidate profiles. With so many unfilled cybersecurity positions, we must attract everyone to this profession. By being more inclusive, we can build the more diverse teams so critical to solving complex cyber challenges. Diverse teams – in education, experience, exposure, problem-solving approach, and perspective – lead to better solutions and business results.
3. The ecosystem of skills development should address all skill levels and types. Education efforts must address the needs of the *few*, the *many*, and the *all* - with specific programs unique to each segment. Think of it as a pyramid – by building a qualified base of *all*, we can draw from a broader pool of talent. It will also help us to increase awareness, with everyone becoming an advocate for cybersecurity.
4. Programs must be highly scalable. Scale is essential to drive impact and close the gap. This is a no-brainer. The numbers shared earlier in this white paper are enormous. We need to design scalable programs – and share them widely. We also need to invest commensurate with the magnitude of this challenge and sufficiently to close the skills gap within our own organizations and, through collaboration, across the national landscape.
5. Programs should include some level of outreach. Challenges around perception, awareness, and discoverability must be addressed while providing new skills. This principle also focuses on building that pyramid base – that by addressing all levels of the *few*, the *many,* and the *all*, we can increase the likelihood of crafting a sustainable and accessible solution.

## Partnerships & Programs

| | | | | |
|---|---|---|---|---|
| IBM Cyber Day for Girls | P-TECH | University of Maryland Baltimore County Cyber Scholars Program | Air Force Association’s CyberPatriot National Youth Cyber Education Program | GenCyber |

- IBM Cyber Day for Girls: Launched in 2016, #IBMCyberDay4Girls helps to build knowledge of cybersecurity through a fun day of learning, games and giveaways! Girls are exposed to opportunities in STEM (science, technology, engineering, math) while they learn about protecting their online identities and securing the Internet of Things. They also learn about exciting careers in cybersecurity and are introduced to female role models studying and working in the field. The program has already had over 660 participants to date, and IBM has committed to impacting 1,000 students in 2018.

- P-TECH: Pioneered by IBM, P-TECH is an innovative public schools model spanning grades 9 to 14 that brings together the best elements of high school, college, and career. Within six years, students graduate with a no-cost associates degree in applied science, engineering, computers and related disciplines, along with the skills and knowledge they need to continue their studies or step easily into well paying, high potential new collar jobs in the information technology arena for multiple industries. This model was designed to be both widely replicable and sustainable as part of a national effort to reform career and technical education. Two of IBM’s existing partner schools offer degrees in Cybersecurity for their students. More information is available at http://www.ptech.org.

- University of Maryland Baltimore County Cyber Scholars Program: This collaborative partnership, launched and sustained through a grant from the Northrop Grumman Foundation, is preparing the next generation of cybersecurity professionals in an increasingly digital age, with a focus on increasing the participation of women and other underrepresented groups in this fast-growing field. Launched in 2013, it supports 15 – 20 scholars annually. More information is available at https://cybersecurity.umbc.edu/cyberscholars/.

- Air Force Association’s CyberPatriot National Youth Cyber Education Program: The premier national youth cyber education program created to inspire youth toward academics and careers in cybersecurity and related disciplines critical to our nation's future. The core of the program is the National Youth Cyber Defense Competition for middle school and high school aged youth. Additional program elements include the Pre-K Cyber Literature Series, the Elementary School Cyber Education Initiative (ESCEI), and the CyberCamps program for youth aged 12 - 18. The Northrop Grumman Foundation is the presenting sponsor of CyberPatriot. Top winning teams in high school-aged divisions are eligible for scholarships from Northrop Grumman totaling over $50,000 annually. Any CyberPatriot participant aged 16 and older is eligible for a paid internship opportunity at Northrop Grumman and other government and industry organizations. The program has reached nearly a quarter-million students, with 27% female participation and 41% ethnic diversity participation. More information is available at https://www.uscyberpatriot.org.

- GenCyber: The GenCyber program provides summer cybersecurity camp experiences for students and teachers at the K-12 level. The goals of the program are to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation, help all students understand correct and safe on-line behavior and how they can be good digital citizens, and improve teaching methods for delivery of cybersecurity content in K-12 curricula. To ensure a level playing field, GenCyber camps are open to all student and teacher participants at no cost. Funding is provided jointly by the National Security Agency and the National Science Foundation. More information is available at https://www.gen-cyber.com.

## Make cybersecurity everyone's business

While most of our recommendations focus on actions that can be taken now to address the supply and demand of skilled candidates to close the gap, we would be remiss if we didn't focus on the broader issue of cybersecurity and the general population.

Cyber-related risks are everywhere – from malicious emails and social media posts, to more innocuous tasks many of us face in the workforce today, such as communicating with external customers, managing financial matters, and delivering services. Even for those not directly involved in what we would call cybersecurity jobs, everyone has a responsibility to understand their role and take responsibility for mitigating risk to themselves and their organizations.

For anyone who develops or delivers training, education, or certifications, there are implications to consider with regard to our digital infrastructure, responsibility, and ethics. Think about what information is important and include this in your programs. Review and share publications such as "Cybersecurity is Everyone's Job," from the National Initiative for Cybersecurity Education. Continue to play your part in helping to protect our workforce, our data, our businesses, and our nation from cyber risk.

For **employers**, this means taking actions to train all employees, regardless of role, on cybersecurity policies and guidelines. For example, at IBM, every employee is required to complete annual training covering cybersecurity threats and how to securely protect email, data, and passwords from attacks.

For **academia**, this means expanding course offerings to include new cybersecurity courses or degree paths, and to provide cyberfluency courses to all incoming students.

For **certifying bodies or affiliations**, this means expanding advocacy and awareness efforts by launching new public awareness campaigns around internet protection and good cyber hygiene, or making new, free, learning content available via public sources like school districts, libraries, and other non-profit learning providers.

# Conclusion

The cybersecurity skills gap is real and it's growing. While we estimate a shortage of at least 500,000 cybersecurity practitioners, the gap could be even larger.

We've presented eight principles for employers, in partnership with academia and government, to consider to solve the cybersecurity workforce challenge.  Given the size of the gap, implementation of a single recommendation won't be enough to move the needle – employers will need to reimagine their approaches to hiring, training, and employee development to drive measurable change.

But this is not an insurmountable challenge.

We have identified some big ideas that could be the key to closing the gap.

## Open the aperture of your talent pipeline

As of September 2018, the civilian US workforce has 36M participants age 25 and over who have completed high school but no college, and an additional 37M who have completed some college or an Associate's Degree.[14]  That's 73M potential candidates who might be able to apply to cybersecurity jobs if degree requirements are loosened or removed entirely. If just half of a percent of that 73M has the relevant skills for employment, we have immediately added more than 350,000 candidates to our employment pipelines.

## Identify new sources of talent

We've heard from many companies that veterans and transitioning service members are a great source of cybersecurity talent due to the nature of the work they have performed for our country.  Did you know that there are over 200,000 service members that transition to the civilian workforce each year?

If we target 10% of those transitioning service members, that would be an additional 20,000 workers to add to our cyber workforce each year. And with collaboration across industry, government, and academia, we could greatly increase that number through expanded training and educational opportunities.

## Focus on employee reskilling and upskilling

According to the BLS, as of May 2017, more than 4.2M were employed in the Computer and Mathematical Occupations,[15] which includes roles such as Computer Systems Analysts, Information

[14] BLS, Labor Force Statistics (CPS), accessed October 19, 2018
[15] https://www.bls.gov/oes/current/oes150000.htm, accessed October 19, 2018

Security Analysts, Network and Computer Systems Administrators, and Computer Network Architects. These roles should be prime focus areas for employee reskilling and upskilling.

If just 1% of the current workers in these occupations were targeted for retraining, we'd have a ready market of 42,000 new cybersecurity workers.  If we retrained 10%, the gap would almost close completely, with 420,000 new cybersecurity workers.

When thought about with this lens, it is feasible that working together, we have the means to build a bigger and stronger cybersecurity workforce to protect our data, our companies, and our nation.

# Appendix

- Example revised job description
- IBM Cybersecurity Analyst Apprenticeship overview
- Getting started with reskilling: a high level model

For more information, additional appendix materials, and tips for how to get started with growing and sustaining your cybersecurity workforce, please visit our website at

http://aspencyberworkforce.mybluemix.net/

## Case Study Example: Revised Job Description

### Cyber Threat Hunter

Are you a security guru who loves a challenge? We are looking for highly-skilled and dedicated cyber threat hunters to help find and fight threat actors attempting to harm our clients. Our Managed Detection and Response Threat Hunt team is a best-in-class squad of malware reverse engineers, forensics and incident response analysts, and SOC analysts charged with performing threat hunt activities on our clients' MDR deployments. Our client base is global and in nearly every industry.

### Your Role

You will bring confidence and peace of mind to your clients by using your skills to develop, perform, and analyze the results of proactive and reactive host and network-based investigations to figure out whether previously undetected malicious activity exists on a network. You'll build customized threat hunts tailored to critical assets on networks, research malware, and develop detections based off numerous input vectors.

### Your Responsibilities

- Actively develop hunts, translate them into an iterative process, and deploy them in numerous EDR solutions.
- React to EDR based alerts.
- Define client relationships and understand the critical assets in their environment to develop advanced detections and reporting.
- Develop and mature new and existing solutions for threat hunting detection capabilities.
- Fully document and communicate findings to an array of audiences which includes both technical and executive teams.
- Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).

## Your Abilities & Skills

- Apply programming languages and scripting to new or existing processes.
- Pivot off indicators within networks to identify the scope and breadth of attacks.
- Developing threat hunts based on various inputs.
- Actively developing hypotheses for hunting.
- Performing both host and network-based investigations.
- Reviewing logs to identify evidence of past intrusions.

## Your Knowledge

- Computer networking concepts and protocols, and network security methodologies.
- Laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- Cyber threats and vulnerabilities.

## Required Expertise

We believe you are a good fit for this role if you are someone that can analyze alerts, proactively hunt for malicious activity, and develop new detection methods. From a technical expertise perspective, you will succeed in this position if you have 1 year of experience in:

- Understanding granular details about network flow, operating systems internals, and threat actor intentions.
- Correlating anomalous behavior, intelligence, and statistical outliers in the environment to hypothesis driven hunts.
- Applying programming languages and scripting to new or existing processes.

## About Managed Security Services

We offer the industry-leading tools, technology and expertise to help secure your information assets around the clock, often at a fraction of the cost of in-house security resources. IBM Security Operations Center Portal, a single window into your entire security world, is included in every managed security service.

Learn more at: https://www.ibm.com/security/services/managed-security-services

## Your life at IBM

We come to work thrilled knowing it will never be the same day twice. At IBM, you have access to a rare combination of experiences that together build a powerful, rewarding career for you. These experiences consist of:

- Opportunity to do work that impacts not just your team but often the very lives of millions of people. You're not just joining a big company, at IBM you're joining a bigger cause.

- Ability to discover the exact career you were meant to have by trying different roles, industries, technologies even locations, right within IBM. No other company gives you the career Infinence (infinite experiences) like IBM.

- A company with a progressive and inclusive heritage based on leadership and a history of taking stands on things that matter.

## EO Statement

IBM is committed to creating a diverse environment and is proud to be an equal opportunity employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, gender, gender identity or expression, sexual orientation, national origin, genetics, disability, age, or veteran status. IBM is also committed to compliance with all fair employment practices regarding citizenship and immigration status.

# IBM Cybersecurity Analyst Apprenticeship Overview

## Duration: 12 months

## WORK PROCESS

*This section delineates the general outline of basic, high-level requirements that each participant will need to satisfy including projects, coaching, job shadowing, and training.*

**Principles and Practices**

1. Apply security fundamentals
2. Apply security best practices

**Cybersecurity Fundamentals**

3. Perform network and wireless intrusion detection
4. Perform security activity monitoring
5. Execute incident response processes
6. Perform scans of databases, web applications, anti-virus and others

**Tools and Technologies**

7. Use various cybersecurity tools and technologies
8. Perform Application maintenance and troubleshooting
9. Perform Application maintenance and troubleshooting

## COMPETENCIES

*In support of this competency-based apprenticeship model, this section identifies what technical knowledge and professional behaviors will be evident as a product of achieving proficiency in these areas.*

**Principles and Practices**

1. Demonstrate knowledge of Security best practices
2. Demonstrate knowledge of organizational security offerings
3. Demonstrate knowledge of basic security fundamentals

**Security Fundamentals**

4. Demonstrate knowledge and ability to conduct network intrusion detection
5. Demonstrate knowledge and ability to conduct wireless intrusion detection
6. Demonstrate ability to perform security activity monitoring
7. Demonstrate ability to initiate incident response processes
8. Demonstrate ability to maintain and troubleshoot applications
9. Demonstrate ability to perform scans of databases, web and mobile applications

## RELATED TECHINCAL INSTRUCTION (411 HOURS)

*This section outlines specific formal training that each participant will be required to complete.*

**Professional Foundations**

- Employee Onboarding
- Professional / soft skills

**Principles and Practices**

- Security best practices / information security principles
- Security offerings including DoD and Federal offerings
- Security fundamentals, including networking protocols, scripting, troubleshooting

**Cybersecurity Fundamentals**

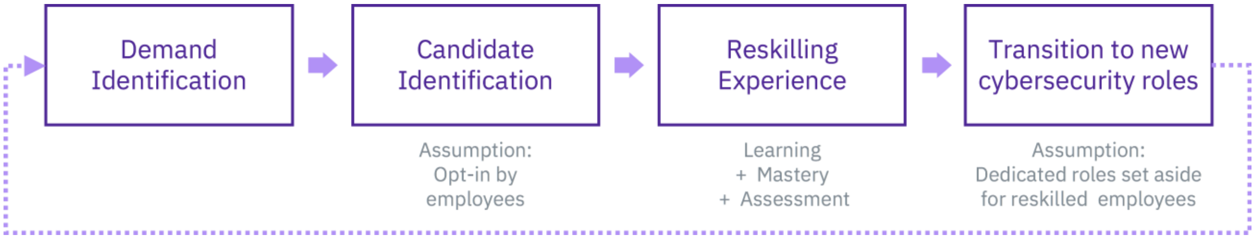
- Network Intrusion Detection
- Wireless Intrusion Detection
- Security Activity Monitoring
- Incident Response Management
- Scanning

**Tools and Technology**

- Various cybersecurity tools and technologies like Qradar, McAfee, Tenable and others
- Reporting
- Application maintenance and troubleshooting

## Getting started with reskilling: a high-level model

Below is reskilling with tactical actions that can be followed to implement a reskilling model in any organization.  While the genesis of this model focused on reskilling employees for roles in cybersecurity, the principles can apply to all roles.


Demand Identification
Candidate Identification
Reskilling Experience
Transition to new cybersecurity roles
Assumption: Opt-in by employees
Learning + Mastery + Assessment
Assumption: Dedicated roles set aside for reskilled employees

**Step 1: Demand Identification**

1. Identify demand for reskilling
    a. Consider roles with highest hiring needs or roles lacking significant candidate pipeline.
    b. Consider roles with high attrition or planned retirements.
2. Identify critical skills needs, including required, preferred, and soft skills

**Step 2: Candidate Identification**

1. Identify target candidate population
    a. Consider roles that are declining in need or that may have adjacent, related skills
2. Select candidates for participation through application and assessment process

**Step 3: Reskilling Experience**

Accelerated Learning

1. Transition employees out of current roles for agreed-upon time period to focus 100% on reskilling learning
2. Employees complete custom learning journeys aligned to employee starting points (assessment process from Step 2)

Project and Skills Mastery

3. Employees complete projects or on-the-job experiences to demonstrate skills mastery

Competency Assessment

4. Managers and mentors assess competency mastery through completion of learning curriculum, project and on-the-job experiences, attainment of digital badges, credentials, and/or certifications

**Step 4: Transition to new cybersecurity roles**

1. Implement transfers to new roles for employees who have successfully reskilled
2. Begin reskilling cycle again, as needed

Principles for Growing and Sustaining the Nation's Cybersecurity Workforce

November 2018