Lightcast

United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

"Expanding the Cybersecurity Talent Pipeline"

Testimony by Will Markow, Vice President of Applied Research, Lightcast

June 22, 2023

Introduction

Chairman Garbarino, Ranking Member Swalwell, and members of the Committee, on behalf of Lightcast, thank you for the opportunity to appear before you today.

As the lines between our physical and digital lives continue to blur, protecting our digital security has emerged as a defining challenge of our time. Although this challenge must be met by a mix of people, process, policy, and technology, the ultimate responsibility for our digital security rests firmly on the shoulders of our cybersecurity workforce. However, this workforce faces persistent talent challenges that choke our cyber talent pipeline and hobble efforts to build the workforce we need to secure our digital infrastructure.

It is against this backdrop that Lightcast researches and quantifies the cybersecurity workforce. We work with institutions across the public and private sectors to arm them with the data and insights they need to expand the cybersecurity talent pipeline and build a world-class cybersecurity workforce.

Lightcast is the Leading Global Authority on the Labor Market – In Cybersecurity and Beyond

Lightcast is the leading global authority on the labor market. We connect people with jobs by providing businesses, communities, and education institutions with the best labor market data and insights possible. Our data-driven insight enables better, faster decisions. To that end, we provide software products, APIs, and consulting services to employers, educators, governments, nonprofit organizations, and other institutions. We collect data from government agencies, online job postings, worker histories, and other sources from over 130 countries across the globe. Lightcast has worked with two thirds of the Fortune 100, 30 states, numerous federal agencies, hundreds of educational institutions, and dozens of nonprofits, among other clients.

Lightcast provides data and insights on all jobs and all industries, but we have been researching the cybersecurity workforce in further depth for over a decade. In 2013, we found that data about cybersecurity jobs were limited, if not missing entirely. This lack of data created an information gap that was exacerbating the cybersecurity talent gap.

Since then, we have released multiple reports on the state of the cybersecurity workforce in an effort to close this information gap. Our research has examined topics such as growth in cybersecurity hiring demand, key drivers of cybersecurity talent shortages, emerging cybersecurity skill requirements, and unique cybersecurity hiring challenges faced by the federal government, among other areas of relevant research.

The Cybersecurity Workforce Faces Two Critical Gaps: A Talent Gap and an Expectations Gap

Lightcast's research over the past 10 years has consistently pointed to a sobering conclusion: the cybersecurity talent pipeline is broken. From May 2022 through April 2023, there were over 660,000 cybersecurity job openings in the United States, but we estimate that the United States only has 69 skilled cybersecurity workers for every 100 that employers demand. This means we are stepping onto the digital battlefield missing nearly a third of our cyber army.[1] In practical terms, this means we need over 460,000 new skilled cybersecurity workers to meet employer demand.[2]

The consequences of the cybersecurity talent shortage echo across the economy. The scale and impact of cyberattacks is well known, but the consequences for companies do not end with digital breaches. Hiring costs for cybersecurity workers have skyrocketed, and cybersecurity salaries are now 10% higher than for other IT workers – despite IT already ranking among the highest-paid career fields. Cybersecurity jobs also take 21% longer to fill than other IT roles,[3] meaning many cybersecurity positions remain empty as our digital threats continue to mount.

The root causes of our broken cybersecurity talent pipeline are varied, but they can be simplified into two critical gaps: a talent gap between supply and demand of cybersecurity workers, and an expectations gap between employer demands and the realities of the cybersecurity talent pool.

The Cybersecurity Talent Gap

The talent gap between supply and demand of cybersecurity workers stem from the rapid growth and evolution in the field. Historically, cybersecurity was not a clearly delineated field and there was limited, if any, training infrastructure in place to prepare cyber workers. As a result, many workers found themselves in cybersecurity by happenstance, rather than intention. As our world became increasingly digital, however, cybercrime flourished. As a result, annual demand for cybersecurity workers has grown 200% in the past 10 years. Such rapid growth is difficult for our education system to catch up with in any field, let alone one as technically demanding and dynamic as cybersecurity.

Compounding this problem is the rapid evolution of skill requirements in cybersecurity. Cyber threats evolve daily, and the skills needed to defend against these threats must evolve as well. In just the past two years, 24% of the top skills for cybersecurity professionals have changed. Moreover, demand for emerging cybersecurity skills – especially those related to cloud security, automation, and secure application development – have grown faster than virtually any other skills that Lightcast tracks. These skills cost employers even more to fill. Just one emerging skill related to cloud security, for example, can command an annual salary premium of $15,000 or more.

In the face of such rapid skill change and inflated hiring costs, most employers struggle to keep the skills of their cybersecurity teams up to date. This struggle is even more severe for the federal government, and many federal employers lag their private sector counterparts when it comes to adopting emerging skills. Our research finds that cybersecurity teams in the private sector are 87% more likely to request

[1] Reflects the latest data from https://www.cyberseek.org/.
[2] https://lightcast.io/resources/blog/cyberseek-06-06-2023.
[3] Lightcast analysis referenced on https://www.cyberseek.org/.

emerging skills than federal employers. If the skills on our federal cybersecurity teams don't remain current, neither can our cyber defenses.

Lastly, the cybersecurity talent gap extends to cybersecurity leadership as well. Our research found that only 22% of cybersecurity managers have prior managerial experience. This means that nearly 8 in 10 cybersecurity teams are led by someone with no prior leadership experience. We also found that, on average, managers have been out of school for 11 years – more than enough time for their skills to grow stale in such a fast-moving field. This adds another dimension to cybersecurity training challenges and requires employers to invest in training for business acumen and leadership skills alongside technical mastery.[4]

The Cybersecurity Expectations Gap

The second broad cause of the broken cybersecurity talent pipeline is an expectations gap between the requirements employers demand and the realities of the cybersecurity talent pool.

In particular, many employers request inflated education and experience requirements that limit entry-level cyber opportunities. Employers request at least a bachelor's degree in 84% of cybersecurity job openings. Employers also request at least three or more years of prior work experience in, again, 84% of cybersecurity job openings.[5] Such elevated requirements are not aligned with the existing cybersecurity workforce and are rarely needed to perform the duties of a cybersecurity job. As a result, they unnecessarily constrain the pipeline of entry-level workers and limit opportunities to reach a more diverse set of candidates. They also negatively impact employee retention: in 2022, the turnover rate for cyber analysts with at least a bachelor's degree was 64% higher than the turnover rate for cyber analysts with an associate degree.[6]

Inflated certification requirements are also rampant. While certifications can be valuable signals to employers that a candidate has a certain level of knowledge, many employers have overloaded their job requirements with certifications that are unnecessary for the job for which they are hiring. This can artificially filter out otherwise qualified candidates who have the right skills, just not the right credentials.

We also have found a misalignment between the degree levels students pursue and the degree levels employers request in entry-level job opportunities. Every year in the U.S., we graduate around 3,000 fewer students from bachelor's programs in cybersecurity-related fields than there are entry-level cybersecurity jobs requesting a bachelor's degree. At the same time, we graduate over 2,900 more students from associate and master's degree programs in cybersecurity than there are entry-level openings demanding these degrees.[7] If employers reduced their degree requirements in roughly one-third of entry-level cybersecurity openings, this would nearly erase the degree-level misalignment between graduates and entry-level job opportunities.

---

[4] All data in the preceding section, "The Cybersecurity Talent Gap", reflect Lightcast analysis of proprietary Lightcast data. The data related to federal cybersecurity hiring is from Lightcast's report on the federal cybersecurity workforce, titled "Securing a Nation."

[5] Reflects Lightcast analysis of proprietary Lightcast data.

[6] Reflects Lightcast analysis of proprietary Lightcast data.

[7] Reflects Lightcast analysis of 2021 IPEDS data from the Department of Education plus proprietary Lightcast data.

This mix of talent challenges, across both the talent gap and expectations gap, has formed a perfect storm of market failures. As a result, fixing the cybersecurity talent pipeline has become a problem of remarkable complexity.

CyberSeek.org: Deciphering the Cybersecurity Job Market

Fixing the cybersecurity talent pipeline requires solutions for both the underlying talent gap and the expectations gap. To solve the talent gap, we must motivate more workers to enter the field and build the training infrastructure to support them. To solve the expectations gap, we must provide employers with the resources they need to make informed hiring decisions.

These solutions require tight coordination across employers, educators, government, students, and many other groups throughout the country. Aligning this patchwork of stakeholders is impossible without shared visibility into cybersecurity workforce needs within communities across the country.

It was this need for shared visibility that catalyzed the development of CyberSeek.org, a cybersecurity workforce analytics and career pathway platform that is freely available to the public. CyberSeek was developed in 2016 through a partnership between Lightcast, NICE, and the technology industry association CompTIA. It is funded by a grant from the National Institute for Standards and Technology. The platform provides actionable, accessible, and up-to-date information about the cybersecurity workforce in communities across the country.

CyberSeek is a unique tool that provides best-in-class data and interactive visualizations to connect the dots between employer needs and career opportunity. It includes a supply and demand heatmap, cyber career pathways, skill-based job descriptions, and a map of local training providers – all of which are completely free and open to the public. To promote additional efforts to grow the cybersecurity talent pipeline, CyberSeek also includes links to other resources on the cybersecurity workforce – including those from CISA and the National Initiative for Cybersecurity Careers and Studies.[8] CyberSeek data are aligned with the NICE Workforce Framework for Cybersecurity[9] and are updated multiple times throughout the year.

Since its release, CyberSeek has become widely used within the cybersecurity community – from students and professors to policy makers and hiring managers. Data from CyberSeek are routinely mentioned in media outlets across the country, and CyberSeek has been publicly cited by multiple presidential administrations. Many educators now develop assignments for their students to visit CyberSeek and learn more about cybersecurity careers. Inspired by the success of CyberSeek, Lightcast has helped develop two sister websites, AUCyberExplorer[10] in Australia and CyberSeek Indiana.[11] The latter is a state-level version of CyberSeek with even more localized information.

---

[8] https://niccs.cisa.gov/

[9] The NICE Cybersecurity Workforce Framework details seven key categories of cybersecurity work, as well as dozens of specialty areas and specific work roles included within each of these categories. It also includes information about the tasks performed within each work role, as well as the knowledge, skills, and abilities required to perform these tasks.

[10] https://www.aucyberexplorer.com.au/

[11] https://www.cyberseekin.org/

We are continuously soliciting feedback on CyberSeek, and we hope to continue to improve the platform so we may arm stakeholders across the country with the tools and data they need to build a world-class cybersecurity workforce.

Lightcast Supports Stakeholders Across the Cybersecurity Community

In addition to CyberSeek, Lightcast works directly with employers, educators, government agencies, and other stakeholders across the cybersecurity community. We provide best-in-class labor market data and insights through software, APIs, and consulting services. To the best of our knowledge, we are the only organization that has mapped external worker supply and employer demand data to the NICE Framework at scale.

Educators use Lightcast tools and data to inform cybersecurity program development and align their curricula with the skills that employers demand. This helps educators keep their cybersecurity programs current, and ensures their students graduate with the skills they need to secure a job. Similarly, Lightcast works with many cybersecurity certification providers to help them align their credentials with employer needs. By linking credentials with in-demand skills, we help these certifying organizations develop credentials that hold value in the eyes of both workers and employers.

Lightcast also works with employers to inform their talent decisions related to strategic workforce planning, talent acquisition, employee training, and more. We help organizations implement a skills-based approach to cybersecurity hiring, which can help expand the talent pipeline, increase candidate diversity, and improve hiring outcomes. For example, we have found that organizations taking a skills-based approach to hiring entry-level cybersecurity workers, rather than a degree-based approach, can save an average of over $15,000 per hire and expand their skilled candidate pool by over 60%.[12]

Lastly, Lightcast also works with government agencies – both at the federal level and the state, local, and tribal level – to support cybersecurity workforce development. At the federal level, we have worked with multiple departments and agencies beyond our work with NIST and NICE. In particular, we have provided information and data to the Office of the National Cyber Director and the Cybersecurity and Infrastructure Security Agency. We have also shared research findings and data on multiple interagency webinars, in meetings with federally convened working groups, and in discussions with individuals across federal agencies.

The Federal Government Can Strengthen the Cybersecurity Talent Pipeline Through Three Broad Levers: Information, Incentives, and Standards

Lightcast's work with stakeholders across the cybersecurity ecosystem gives us a unique vantage point on opportunities for the federal government to help strengthen the cybersecurity talent pipeline. In our view, there are three broad levers that Congress, CISA, and other federal actors have at their disposal: information, incentives, and standards.

[12] Reflects Lightcast analysis of proprietary Lightcast data.

Lever 1: Information

The federal government – and CISA in particular – are in a unique position to provide actionable information for stakeholders across the cybersecurity workforce ecosystem. There are multiple avenues through which this can be accomplished, but key opportunities include the following:

- **Become an exemplar for innovative, skills-based cybersecurity hiring practices.** This means shifting to a skills-based approach to hiring for cybersecurity roles and cataloging and promoting best practices for the private sector to emulate. Examples of skills-based best practices that CISA and other federal agencies can take include the following:

    - ***Reduce education, experience, and certification requirements in job openings.*** This can have dramatic impact toward reducing hiring difficulty and expanding the size and diversity of the government's candidate pool. For example, Lightcast data show that removing a bachelor's degree from early-career cybersecurity job postings can reduce the average cost to hire by over $15,000 and increase the candidate pool by over 60%.[13]

    - ***Prioritize training for high-growth, high-value skills.*** Lightcast projects that demand for many emerging cybersecurity skills will grow 50% or more in the coming years, and many of these skills command salary premiums of $10,000 or more.[14] In most cases, these skills cost considerably less to train. Focusing training on these high-growth, high-value skills – such as cloud security, DevSecOps, and others – can help the federal government maximize the return on its training investments.

    - ***Build career pathways to enhance career advancement potential for cybersecurity workers.*** CISA and other federal agencies may develop clear cybersecurity career pathways that communicate the roles that individuals may target at different stages in their careers, possible transition opportunities between each role, and the skills or other attributes workers can develop to progress between roles within a career pathway.

- **Educate employers as well as practitioners.** In addition to providing education materials for practitioners and managers, CISA or other federal actors may provide training resources for employers that outline talent management best practices for cybersecurity workers. Providing quality training resources that are accessible and targeted to personas on both sides of the hiring process can help address the dual talent and expectation gaps plaguing the cybersecurity workforce.

- **Expand and enhance access to tools and resources that support cybersecurity workforce development and hiring.** This could include the development of new tools and resources or the expansion of existing tools – such as CyberSeek, current resources from CISA and NICE, or others. These may be accomplished through either of two vehicles: increasing funding or increasing awareness.

[13] Reflects Lightcast analysis of proprietary Lightcast data.
[14] Reflects Lightcast analysis of proprietary Lightcast data.

- ***Increasing Funding:*** First, additional federal funding directed internally towards CISA or other federal agencies, or externally through grants or other mechanisms, would enable the development of new tools, functionality, and resources. For example, this may include tools providing more data on emerging cybersecurity skills, resources for employers to easily adopt skills-based hiring best practices, or even tools that directly connect individuals to open jobs or relevant training opportunities.

- ***Increasing Awareness:*** Second, expanding knowledge and promotion of existing resources can maximize their impact and help reach a larger pool of users without requiring much, if any, additional investment. For example, resources could be developed by CISA or others that provide additional "how to" guidance and case studies that demonstrate how to use existing tools and implement best practices – such as skills-based hiring. Various federal actors can also aid in the promotion of existing resources through public announcements, webinars, speaking engagements, op-eds, or other activities.

Lever 2: Incentives

The federal government is also in a singular position to influence incentives for individuals, educators, employers, and other stakeholders to help strengthen the cybersecurity talent pipeline.

For employers, this could take the form of incentivizing employer-sponsored training to upskill and reskill existing employees. These incentives may take the form of tax credits or stipends which can partially or fully offset the costs of training employees. This could improve the economics for employers to invest in training. This, in turn, may help employers strengthen the skills of existing workers and reduce the cost of hiring entry-level workers to upskill. Numerous states have developed similar programs, and the state-level experimentation and outcomes associated with these types of programs may inform similar federal programs.

The federal government may also incentivize private employers to invest in hiring entry-level workers through public/private partnerships, talent sharing, or related initiatives. This may take multiple forms, but some examples include the following:

- **Expanding shared training resources between CISA or other federal agencies and private employers.** This could reduce the cost to employers to train entry-level workers. Ideally these resources would be focused on high-value, high-growth skills – such as cloud security, DevSecOps, secure application development, and others.

- **Providing funding to local communities to support grassroots innovation.** Providing funding to state and local governments, or directly to other local institutions or consortia, can support local collaboration between employers, educators, and other local workforce development stakeholders working to grow the cybersecurity workforce. An existing example of this is the RAMPS program from NICE.[15]

[15] https://www.nist.gov/system/files/documents/2017/08/18/ramps_one_pager_032017.pdf8u_tpo.pdf

- **Providing resources, tax credits, or other financial incentives to employers to develop cybersecurity apprenticeship programs.** These programs can help students build on-the-job experience and develop diverse talent pipelines for employers. Improving the economics of apprenticeships can help more employers adopt them for entry-level cybersecurity roles.

- **Developing public/private talent sharing programs.** Under these programs, a worker can spend time working in both the public and private sector, which helps them gain new skills and on-the-job experience. CISA has already experimented with similar programs on a limited scale. These talent sharing programs could support greater information and resource sharing between the public and private sector and would help workers in all sectors build new skills. It may also reduce hesitancy for employers to hire entry-level workers if they are able to share the training of those workers with federal employers.

Lever 3: Standards

Lastly, the federal government can develop standards and frameworks that support consistent application of best practices related to workforce development, training, and hiring. Already, NIST and NICE are providing valuable standards and frameworks related to cybersecurity. This also extends to cybersecurity education and workforce development, which is most prominently achieved through the NICE Framework.

The NICE Framework has become a valuable resource that is used widely in the cybersecurity community. Educators use the NICE Framework to inform their training content and align it to the needs of the workforce, employers use it to assess gaps in their cybersecurity workforce, and individuals use it to identify the types of work they can prepare for within the cybersecurity field, among other stakeholders.

Building off the success of the NICE Framework, the federal government may take additional steps to provide standards and frameworks that will strengthen the cybersecurity talent pipeline. Some of these steps may include the following:

- **Provide frameworks and standards that outline best practices for cybersecurity employers.** This may include standards describing best practices for adopting skills-based hiring, optimizing job descriptions, building career pathways, maximizing the value of learning and development, developing apprenticeships, engaging with educators or other stakeholders, and related activities. This will help to address the expectations gap that creates misalignment between the needs of employers and the realities of the existing cybersecurity talent pool.
- **Continue to update and refine the NICE Framework.** The rapid evolution of cybersecurity skill requirements necessitates frequent updates to the NICE Framework to ensure it remains current. Moreover, additional data collection and industry input can help NICE continue to further align the Framework with the language and needs of employers.
- **Provide frameworks and standards for educators to build training content that is up-to-date and aligned with employer needs.** This may take the form of baseline standards for curriculum development, suggested steps for data collection and analysis on market job and skill demand, recommendations for strengthening employer engagement, tools for embedding hands-on

learning opportunities into curricula, resources for developing co-ops and internship opportunities with local employers, and related activities.

Conclusion

Expanding the cybersecurity talent pipeline is, undoubtedly, a complex issue. It requires coordination across a constellation of disconnected, yet interrelated, educational institutions, employers, and individuals. Aligning this diverse ecosystem of stakeholders requires a shared understanding of the problem, and clear, level-headed guidance on how to solve it.

Thousands of stakeholders – both in the public and private sectors – are already facing this challenge head on. Lightcast is committed to working with these stakeholders, and we welcome collaboration with anyone interested in creative, data-backed solutions to cybersecurity's pipeline challenges.

Thank you again for the opportunity to participate in this hearing an I look forward to further engagement with the Committee.

Respectfully,

William Markow

Will Markow
Vice President of Applied Research
Lightcast