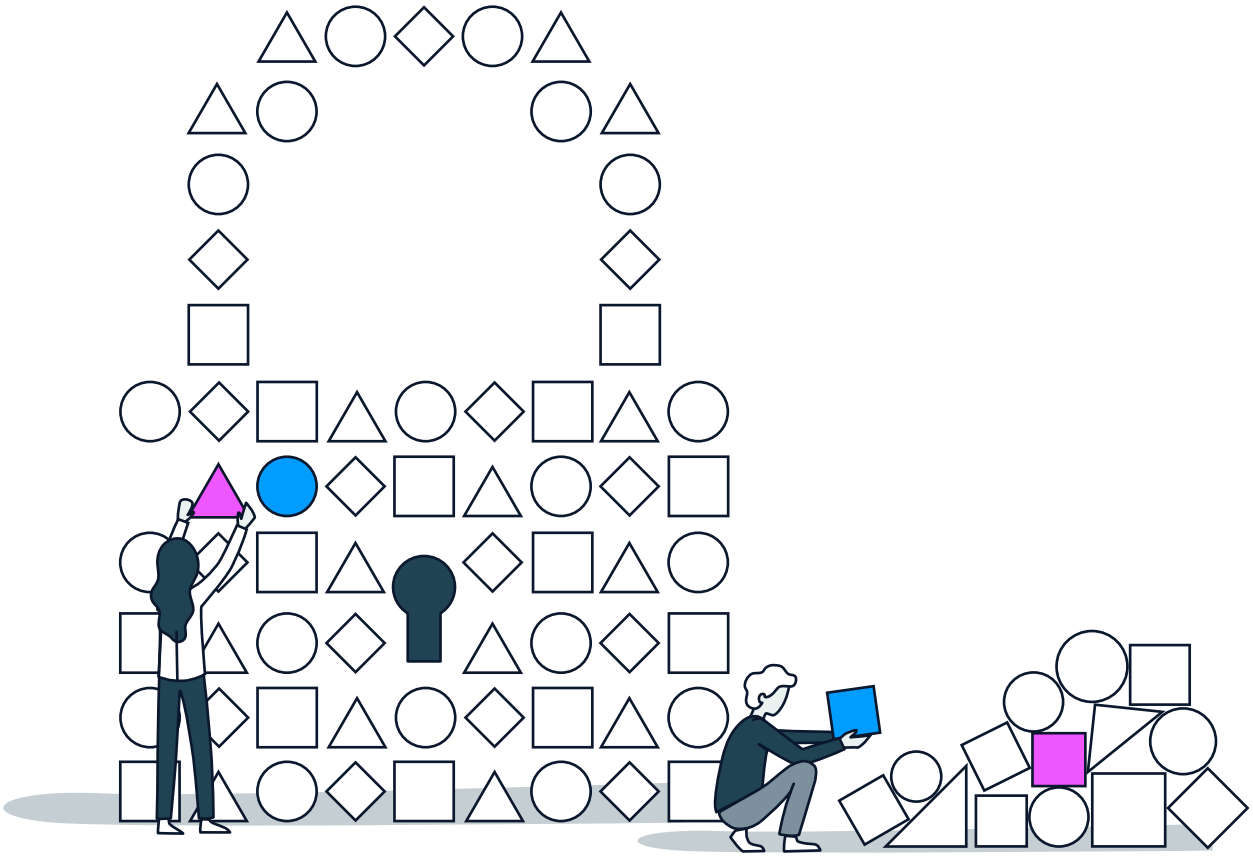
Build

(Don't Buy)

A Skills-Based Strategy to Solve the Cybersecurity Talent Shortage



July 2020

Lightcast

Build (Don't Buy):

Training the Cybersecurity Workforce

Contributors:

Clare Coffey

Gwen Burrow

Rob Sentz

Yustina Saleh, PhD

Levi Law

Lightcast

EconomicModeling.com

Summary

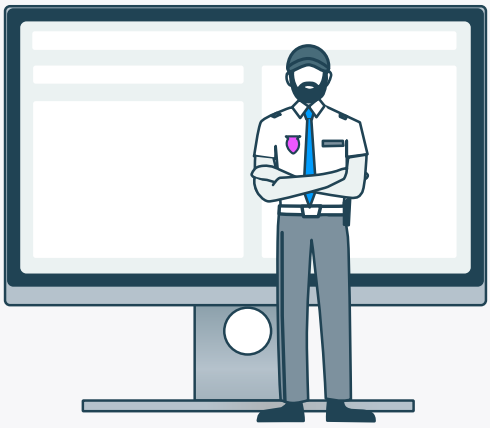
The US has less than half of the cybersecurity candidates it needs to keep up with ever intensifying demand. For every 100 active postings, there are a mere 48 qualified candidates, many of whom are already gainfully employed. So how can we solve the cybersecurity talent crisis? The answer: build, don't buy.[1] Rather than publishing dozens of postings that don't seem to attract the right candidates, companies should focus on re-skilling existing employees. Together, companies and their civic, education, and workforce partners can develop workers with the necessary skills and close the talent gap in this vital industry.

This paper offers suggestions regarding which candidates are ideal for reskilling, as well as which skills companies and regional training and workforce partners should develop.

1 America Needs Cybersecurity Experts Now

Cybersecurity workers were already in high demand (and short supply) before the COVID-19 crisis. Now we need them more than ever as e-commerce skyrockets[2], colleges and universities go digital, and millions of Americans work from home on personal networks. Spam, malware, and scams sabotage the unsuspecting.[3] Cyber attacks against the WHO doubled in March.[4] And the US Health and Human Services Department was hacked.[5]

Right now, it would take a 145% increase in the current cybersecurity workforce to meet global demand, according to a new report by (ISC)2.[6] The digital world plays a profoundly important role in our lives, from apps and social media to banks and the vast sector of defense and national security. Cybersecurity professionals are the safeguards of this vast digital economy. So why aren't there more of them?



The (ISC)2 study offers hints. The report found that the top job concern among cybersecurity employers was the lack of skilled or experienced personnel. In addition, the report discovered that even though cybersecurity professionals with certain critical certifications earn significantly more than their peers ($93,000 vs. $75,000 annually), only 49% of current workers say they have a good idea of how to progress in their cybersecurity careers. The top two obstacles these workers face are, first, the cost of certifications, and second, the lack of clear career path opportunities.

In other words, we have a double-edged talent problem:

1. Employers can't find the professionals they need.
2. Workers don't know how to access the next rung in their careers.

Workers don't know which route will allow them to progress, while businesses—despite the increasing educational focus on STEM—can't find enough people with the highly specific cyber qualifications necessary. These problems cannot be solved without **clarity around skills on both sides.**

In the following report, we use new insight on skills to address this critical problem of the cyber talent shortage. Our data suggests that the talent shortage is a testament to the need for a **"build, don't buy" model** of talent development. Buying talent means searching for and hiring a new employee who has the needed skills. Building talent means helping the employees you already have (and ultimately, the workforce at large) acquire the new skills they need for the job.

As far as cybersecurity is concerned, the "buy" model is clearly less effective, while the"build" model offers more promise. To realize this promise, companies need better strategies to up-skill current employees in roles that might be in lower demand, and to retrain or up-skill displaced workers in need of new employment.

Cybersecurity demand is twice as great as supply

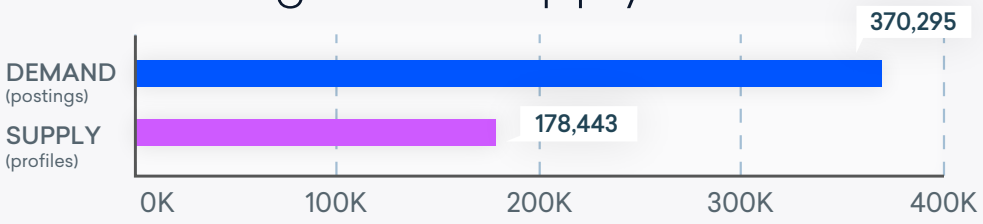
To understand the extent of the cybersecurity shortage, and why the buy model is so problematic, we compared the number of postings for cybersecurity jobs with the number of professional profiles that include cybersecurity experience.

Demand for cyber and information security exceeds supply by a huge margin. For every 100 job postings, we estimate there are only around 48 qualified candidates. This means demand is twice as great as supply. To get the talent they need, businesses are forced to be ultra competitive, recruiting from within other companies. The result is a vicious "zero-sum game"[7] as companies shuffle talent between themselves because there isn't enough to go around.

It should be noted that this data represents a pre-COVID-19 economy. Since it is difficult to know how the crisis may have affected trends in cybersecurity, our analysis draws on data from the fourth quarter of 2019 as a baseline of relative stability. That said, we have confidence that cyber will continue to be very in-demand; perhaps even more so given the dramatic shift to working from home, online school, and a much heavier reliance on e-shopping. Essentially, the coronavirus will likely heighten the need for cyber skills.[8]

FIG 1.1

National cybersecurity demand is twice as great as supply



[5]Source: Lightcast Supply and Demand Estimate*, 2020

*The data is based on estimates of supply and demand using a wide range of labor market data. Lightcast created a unique supply-and-demand index to estimate the demand for various roles vs the supply of qualified workers available to fill these roles. This unique index is based on government sources that help us measure total employment (by industry and occupation), job openings, hires, and separations, and private sources on job postings and professional profiles and resumes.

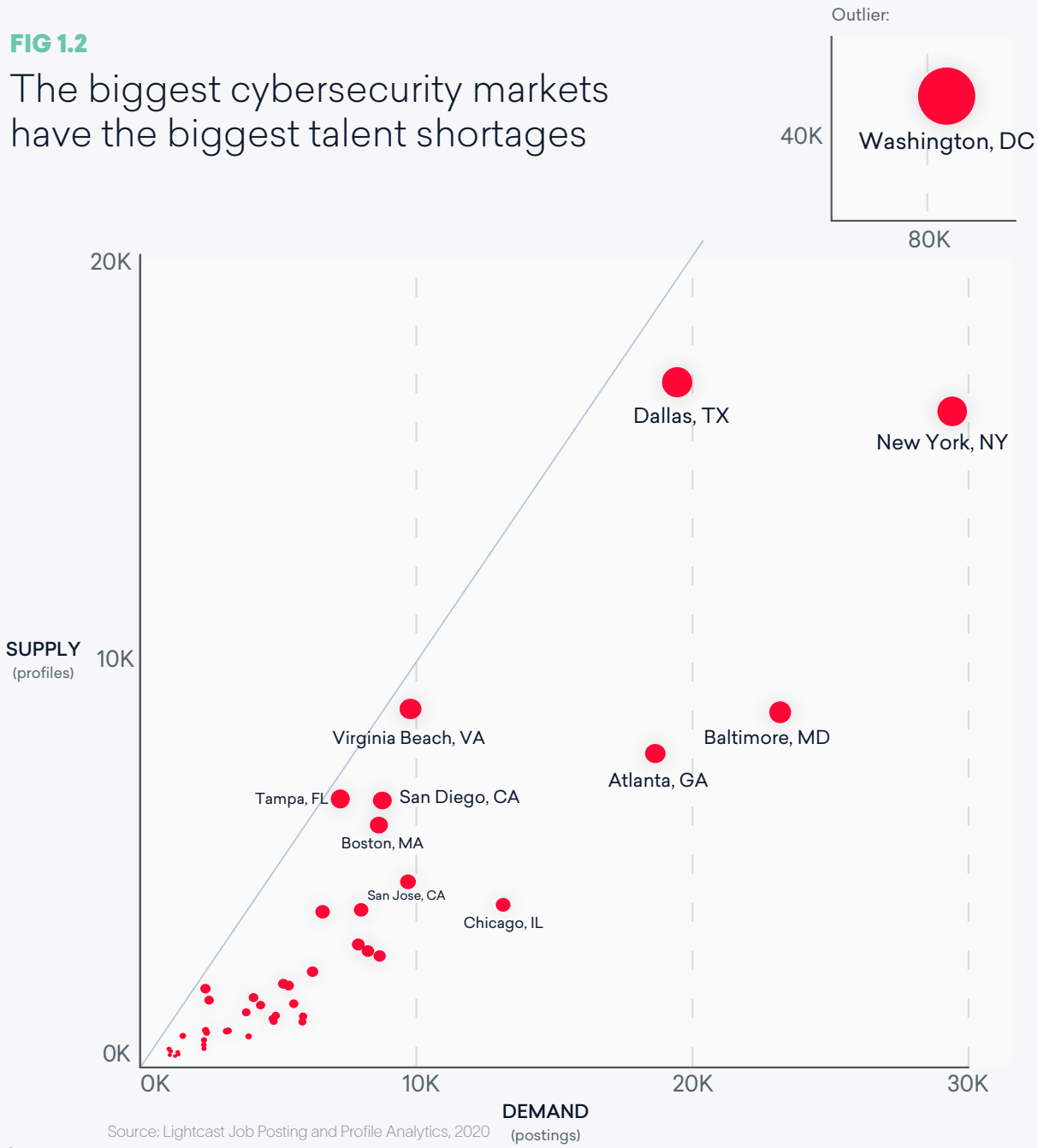
Major cybersecurity markets are hurting the most

Unfortunately, the biggest markets—where cybersecurity is most needed—are among those with the largest talent gaps.

The graphic below shows a city-by-city comparison of people with cybersecurity skills versus companies seeking cybersecurity professionals. The gray line highlights the point where the ratio of postings to profiles is one to one. In other words, it indicates the balance between supply and demand.

FIG 1.2

The biggest cybersecurity markets have the biggest talent shortages



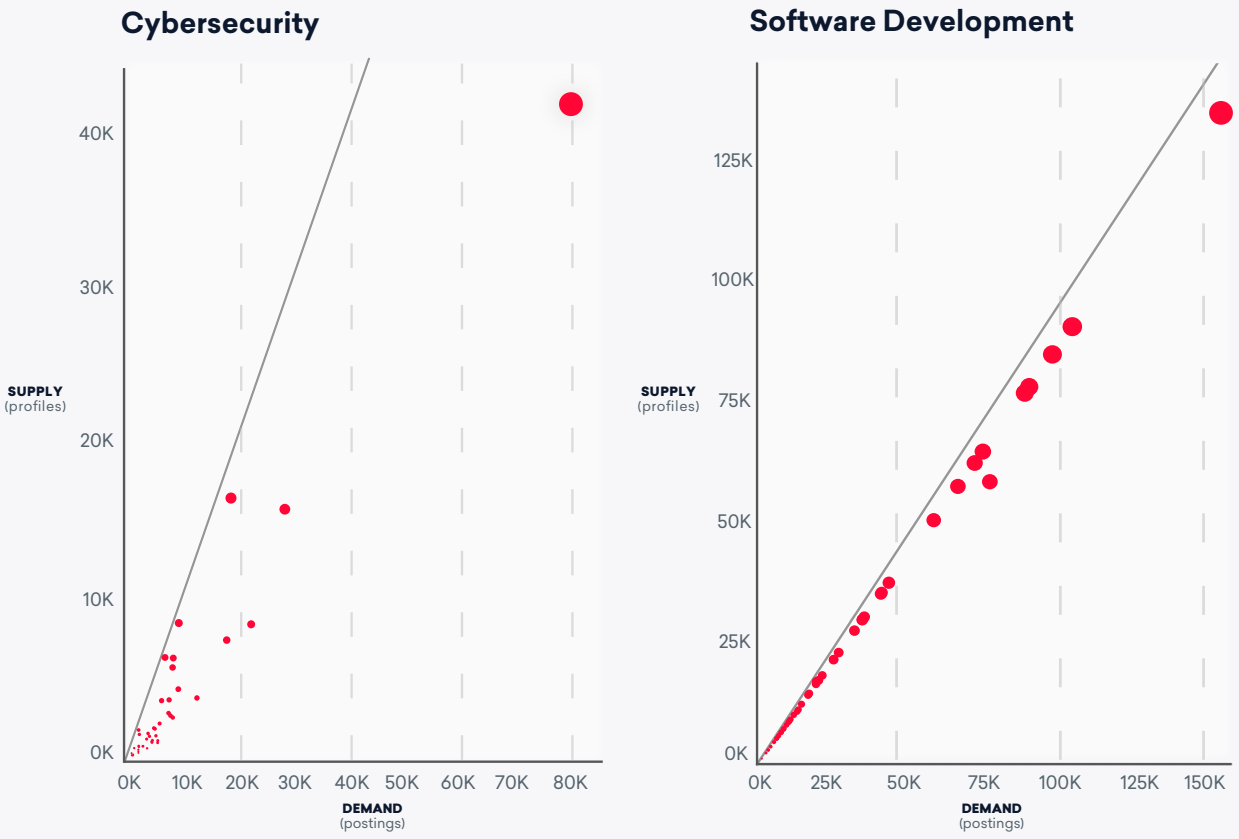
Source: Lightcast Job Posting and Profile Analytics, 2020

The chart illustrates the critical intensity of the cybersecurity problem. Every major US city we explored demonstrates far more cyber demand than cyber supply. The red dots indicate cities that have more demand than supply. The farther below the line a city lies, the greater the gap between the talent it needs and the talent it has.

The national talent shortage in cybersecurity becomes even clearer when we contrast it with the talent needs of software development. We tend to think of software development as being a relatively hard job to fill, but as you can see from the chart below, the market is much closer to filling its needs for software development workers than it is for cybersecurity.

FIG 1.3

The cybersecurity shortage is even clearer when juxtaposed with software development



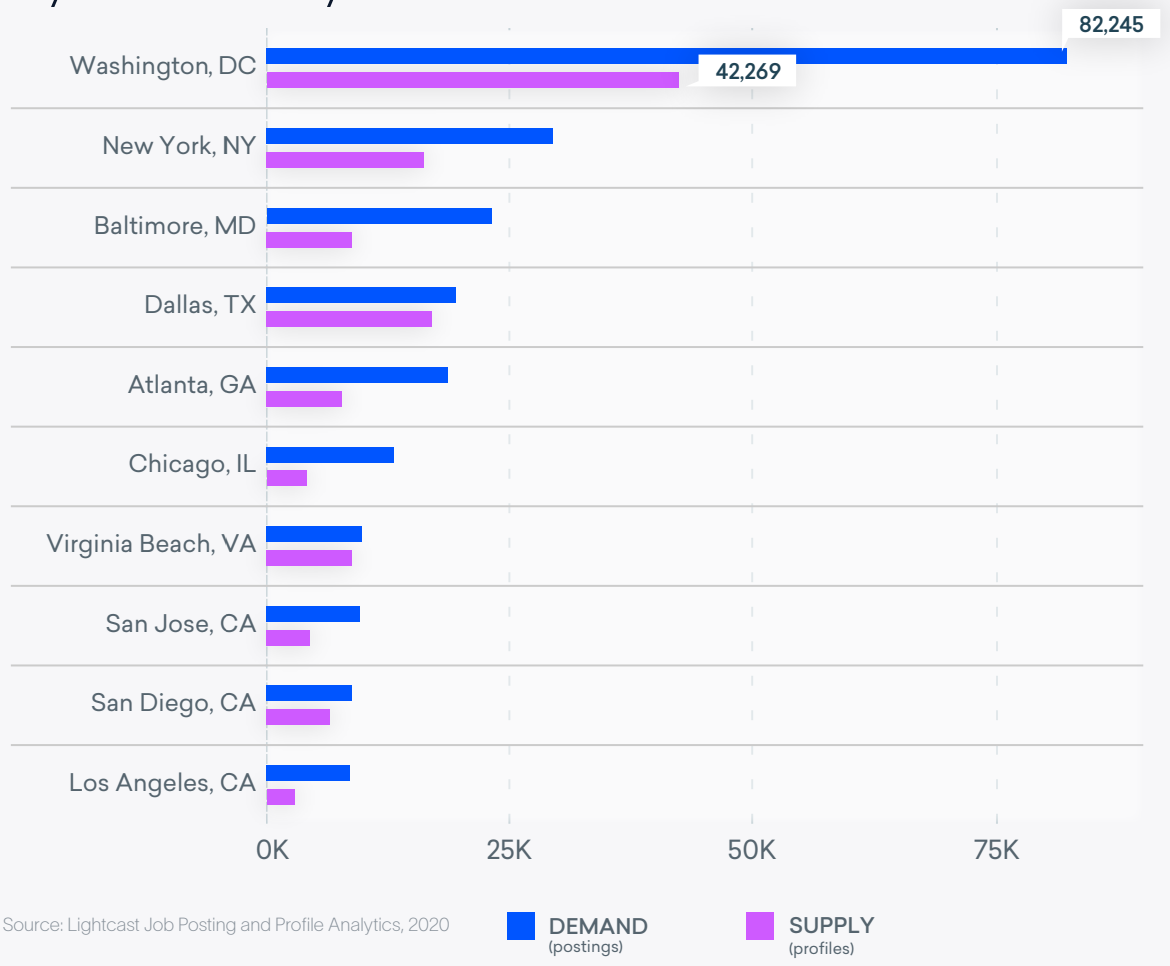
Source: Lightcast Job Posting and Profile Analytics, 2020

Washington, DC: canary in the infosec coal mine

DC towers over other cities in terms of raw talent, with over 80,000 profiles tagged to cybersecurity jobs. The next largest talent hubs, Dallas and New York, have less than half of those cyber-talent numbers. Interestingly, the largest cities for supply aren't necessarily the largest for demand. New York has only slightly less supply than Dallas, but noticeably more demand. And while DC's raw supply is the highest of any American city, the demand is also *that much greater*. For every one profile, there are two jobs open. This situation isn't ideal anywhere, but it particularly needs to be addressed in DC.

FIG 1.4

Washington, DC leads the way in cybersecurity demand

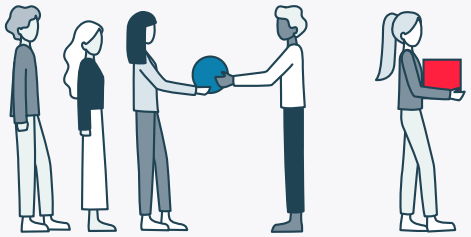


Source: Lightcast Job Posting and Profile Analytics, 2020

DC's predicament underscores the limits of relying on job advertisements as the best method of finding talent (aka the "buy" paradigm). In this case, firms are forced to hire from other firms, and the talent shortage is merely passed around from company to company. Talent becomes increasingly expensive and the shortage is never solved. And since demand continues to grow, without a corresponding increase in the supply of workers, even the few companies that can afford to buy cybersecurity talent will soon feel the pinch.

So since buying cybersecurity talent doesn't work, what does building it look like? In the next section, we will outline the key elements employers and regions need for successful cyber talent development strategies.

2 Building Cyber Talent



The first step in building cyber talent is better understanding the specific skills that need to be developed. A skills-based approach allows us to look beyond the limits of job titles or SOC codes to identify the actual real-time needs of businesses.

In the next three sections, we consider businesses' needs for cybersecurity roles.

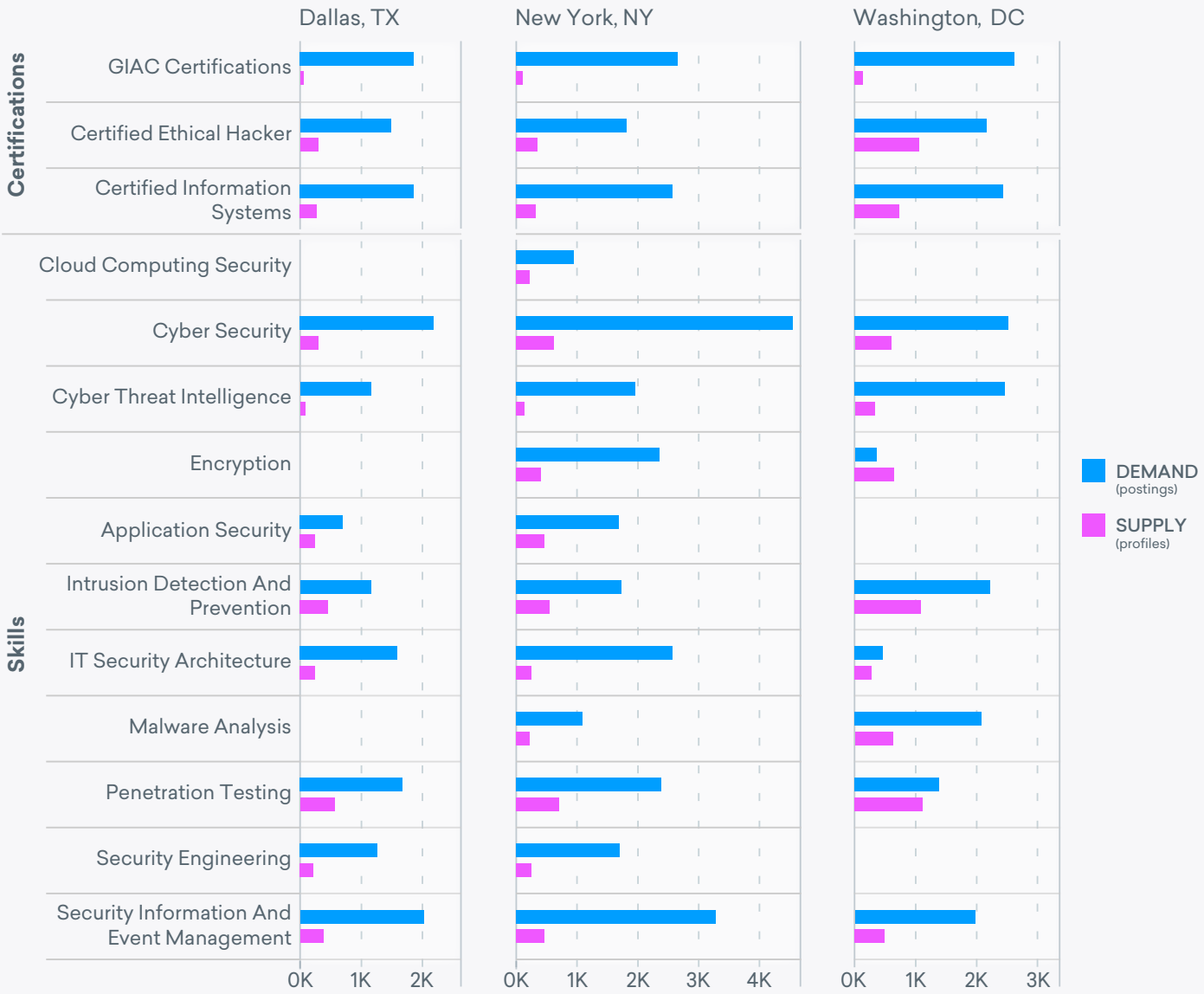
1. Businesses need workers with cybersecurity-specific certifications.
2. Companies should develop this cybersecurity talent by retraining IT, finance, and business operations roles.
3. Domain expertise and local industry needs also shape regional cyber demand, so businesses in one region (or industry) will need to focus on different skills than businesses in another.

GIAC (Global Information Assurance Certifications) is a professional association that offers over 30 cybersecurity certifications. Several of these certifications, such as penetration testing, malware analysis, and data loss prevention, appear as skill gaps in the chart above. In fact, nearly every skill gap shown could be covered by one GIAC-style certification or another. Even skills that do not explicitly mention certifications such as "penetration testing" tend to be covered by various institutional certificates.

These gaps in certifications in DC, New York, and Dallas track with the findings of the ISC2 report, in which unclear career paths and the cost of certification accounted for nearly 60% of self-reported obstacles in pursuing a cybersecurity career.

FIG 2.1

DC, NYC, and Dallas have similar gaps in critical skills



Source: Emsi Job Posting and Profile Analytics, 2020

A lack of professionals certified by GIAC, CompTIA, and other accrediting institutions is the fundamental cybersecurity problem. Who should get these certifications? Where should companies recruit for cyber roles? To gain some insight into these questions, let's look at where cyber talent is already coming from. Then we can determine how existing pipelines can become more robust and efficient.

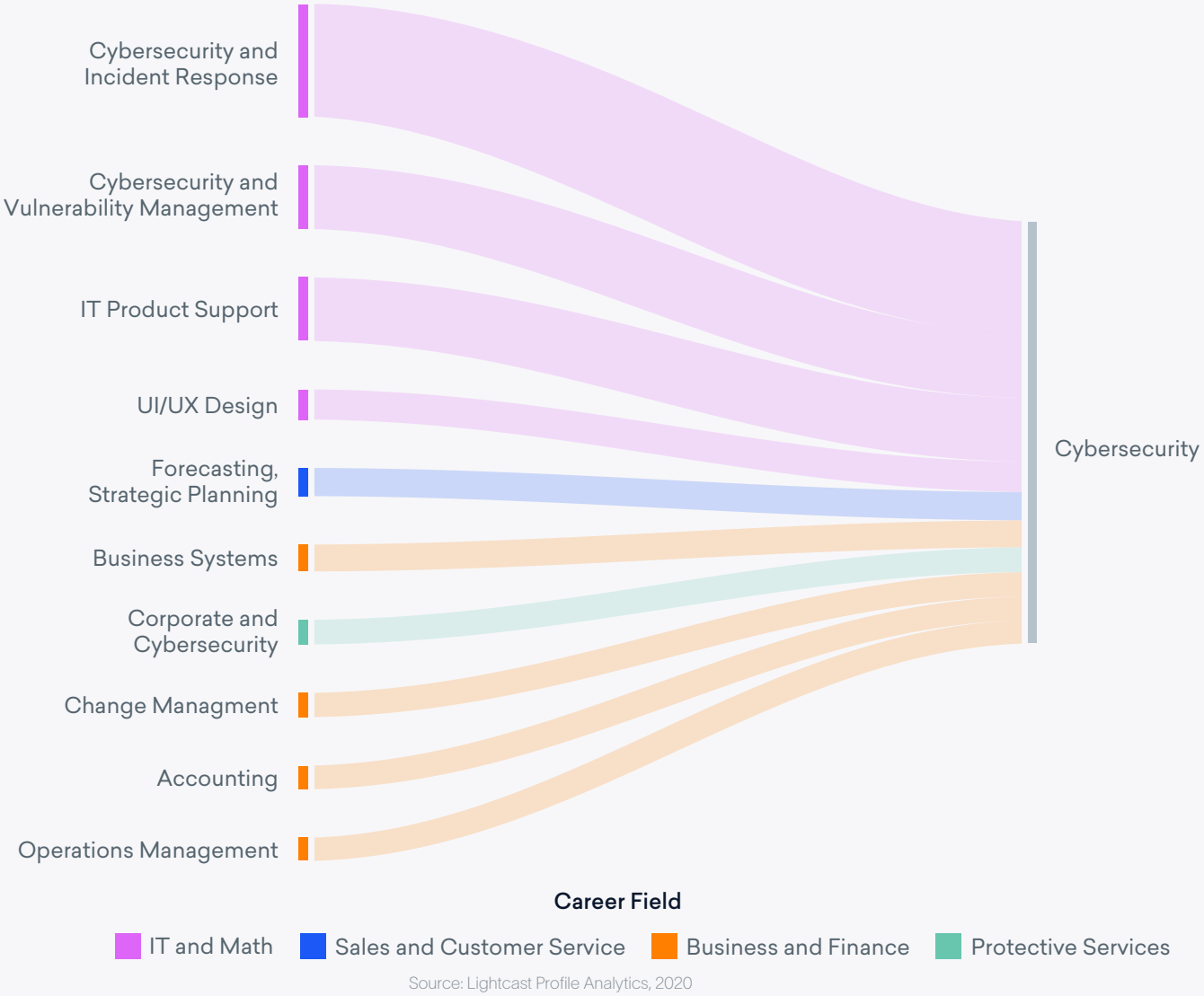
While certifications are not the only gap faced by various cities, they represent a notably consistent problem from city to city (and in fact, are common to a wider range of cities than we visualize here). Thus, in aggregate, they represent probably the single most important cybersecurity skills gap.

Companies need to develop cybersecurity talent by retraining IT, finance, and business operations roles

When we break down the top transitions into cybersecurity by occupation, the biggest subgroups are within the cybersecurity field: incident response and vulnerability management. In other words, the largest feeder occupation for cybersecurity is...cybersecurity. (See the graph below.) This pattern reflects the primary problem occuring in the market. When companies need cybersecurity talent, they post for candidates who *already have cybersecurity experience*.

FIG 2.2

Common occupations that transition into cybersecurity

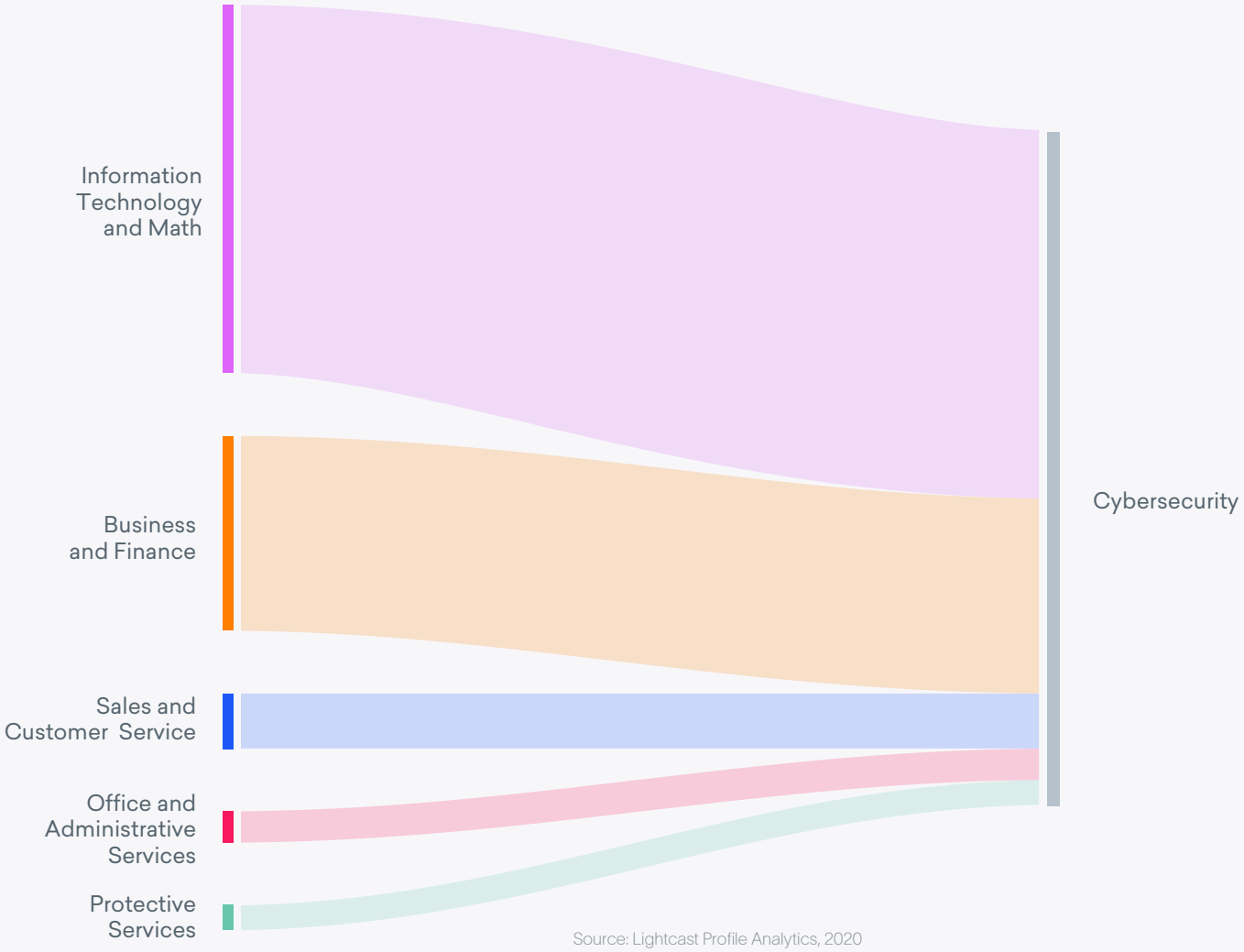


Source: Lightcast Profile Analytics, 2020

Existing cybersecurity workers may be the top source for talent, but there's a diverse array of jobs that send smaller numbers of workers into cyber roles. Business and finance are two other notable cyber talent pools. Knowing this immediately helps us to broaden our ideas about who could be trained and transitioned into cybersecurity roles.

FIG 2.3

Common career areas that transition into cybersecurity



Source: Lightcast Profile Analytics, 2020

With this in mind, companies can consider a large array of workers—including their own employees—especially those who already have a background in IT and math (specifically IT support roles) and/or business and finance (specifically accounting, operations, and change management roles.

For one thing, a huge number of cybersecurity incidents revolve around financial transactions, computing, or some combination of the two: a fact reflected in the level of regional demand

around, say, finance in New York, or machine learning in Dallas. For another, both accounting and IT support are—in their current iteration—relatively narrow roles that involve a high number of repetitive tasks. These are the types of roles especially vulnerable to obsolescence in the wake of technological change. By helping such workers gain highly-demanded cyber skills (particularly the certifications), companies are giving them a stronger footing in the labor market and filling their own skill gaps at the same time.

Further, by cross-training finance and IT employees, companies will acquire cyber professionals at a rate almost certainly cheaper and quicker than paying to recruit people from other companies. They will also gain cybersecurity workers with irreplaceable insights given their experience at the company and creative solutions derived from years of experience.

The future of a firm's corporate structure may not be accounting, IT, and cybersecurity siloed away in separate departments, but hybrid roles exercising key skills from all three. In fact, there's good reason to think that finance and IT workers may be particularly helpful in solving another element of the cybersecurity shortage: the regional demand for domain expertise. We'll get into that in the next section.

Domain expertise and local industry needs also shape regional cyber demand

In New Geography of Skills, Lightcast and the Strada Institute for the Future of Work found that various industries—and the communities wherein those industries reside—manifest unique and highly nuanced skill needs, or what we call "skills shapes." Regional skill shapes are driven by local industry demand. When we apply this principle to cybersecurity, we gain two important perspectives.

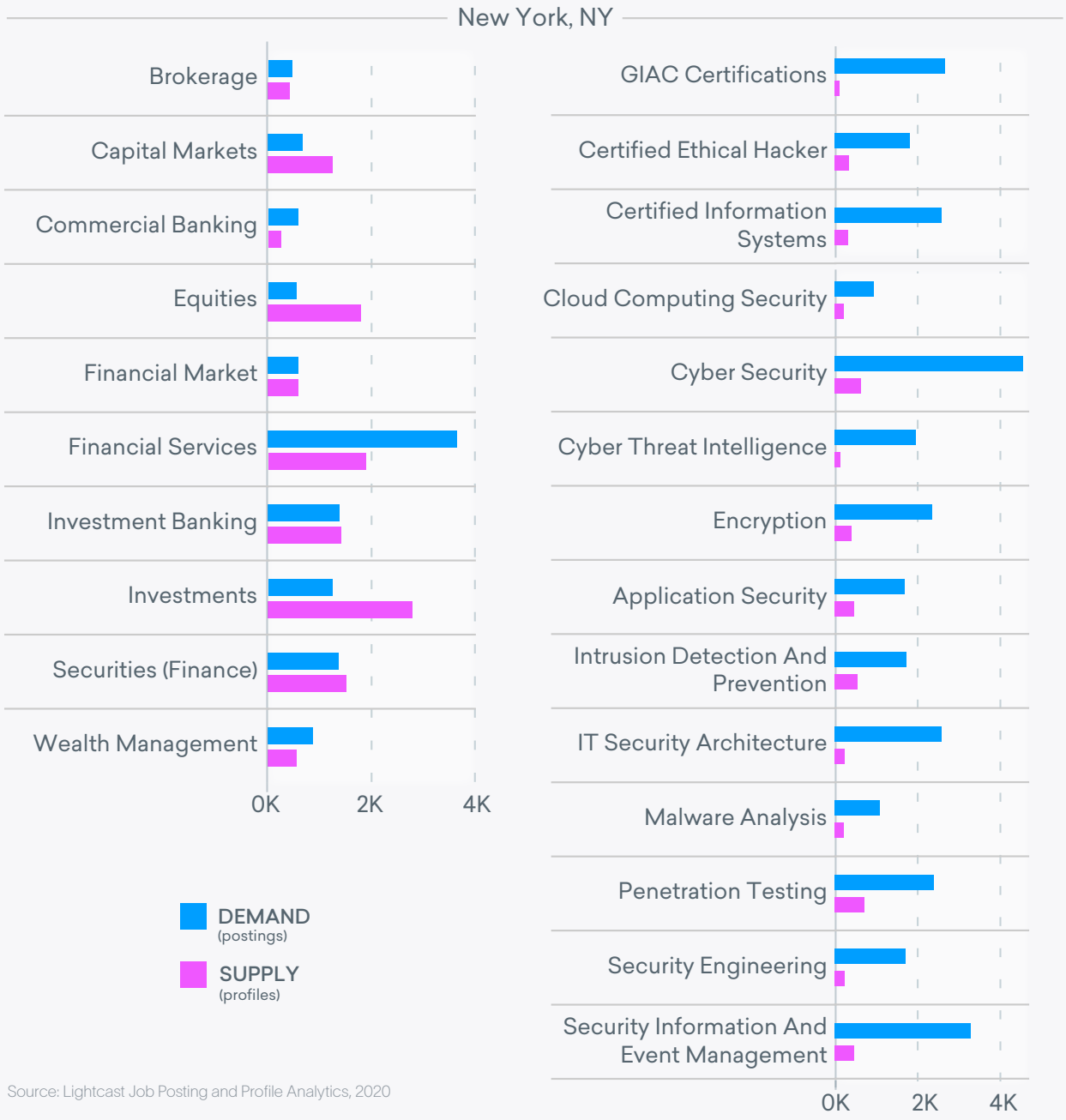
First, at the national level, we see the overarching need for cybersecurity certifications. Second, as we zoom in on specific industries or regions, we also see the local shape of cybersecurity demand. These localized skill shapes include both the broadly-needed cyber qualifications as well as the specific skills needed by that particular industry and region.

This dual perspective—national and local—helps regional development organizations and learning providers create niche, tailored strategies for programs that meet local demand. It also gives businesses key insights that help them understand the nuances of their own needs.

Let's apply this principle to NYC. NYC's massive financial sector needs cybersecurity professionals who understand the banking world in particular. Workers must have expertise in areas such as brokerage, commercial banking, wealth management, and financial services. In order to upskill employees for these roles, companies should obtain both general cybersecurity training (GIAC certifications and certified ethical hacking) and specific training in finance. Upskilling current employees within their finance department can give companies a powerful leg up as they fill those cyber talent gaps.

FIG 2.4

Financial skills define the NYC cybersecurity cluster

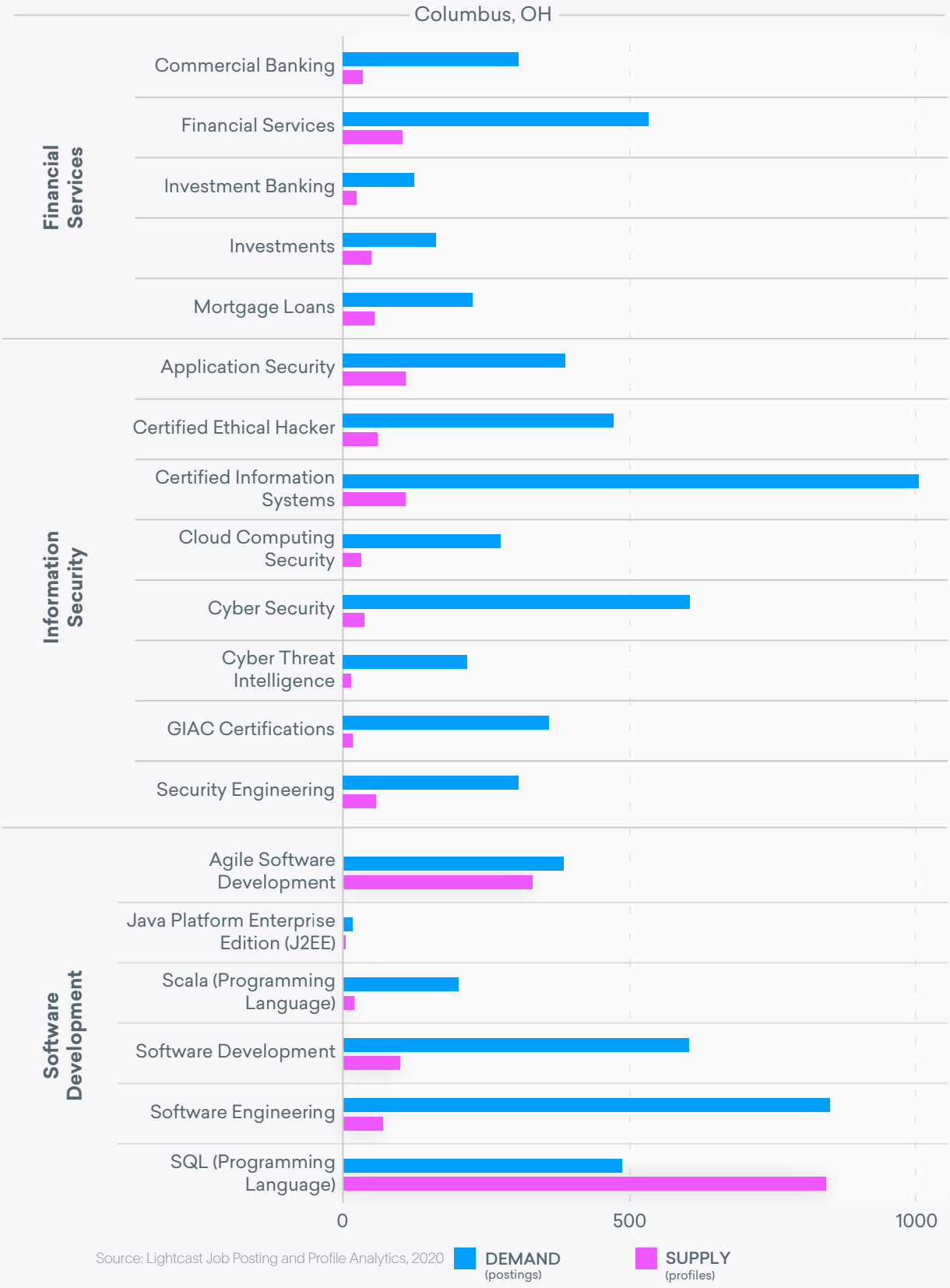


Source: Lightcast Job Posting and Profile Analytics, 2020

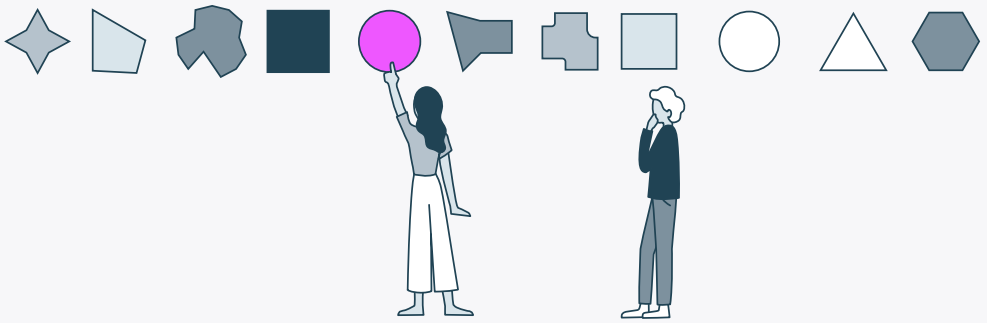
In Columbus, employers need people in its finance sector as well as its burgeoning tech sector. But unlike NYC, Columbus lacks a large base of finance skills. As a result, we see several sizable domain expertise gaps (like commercial banking and financial services) and a few smaller gaps (like investments and mortgage loans). Further, tech skills are particularly in demand, with large gaps in software development, software engineering, and Scala, as well as notable gaps in cloud computing and application security. With these wide-ranging gaps, companies in Columbus need to combine tech and finance skills with their cyber training.

FIG 2.5

Cybersecurity gaps run across domains in Columbus



Source: Lightcast Job Posting and Profile Analytics, 2020



3 Building the right programs

Microcredentials for in-demand skills

To solve the cybersecurity shortage, we need the right programs for the right people.

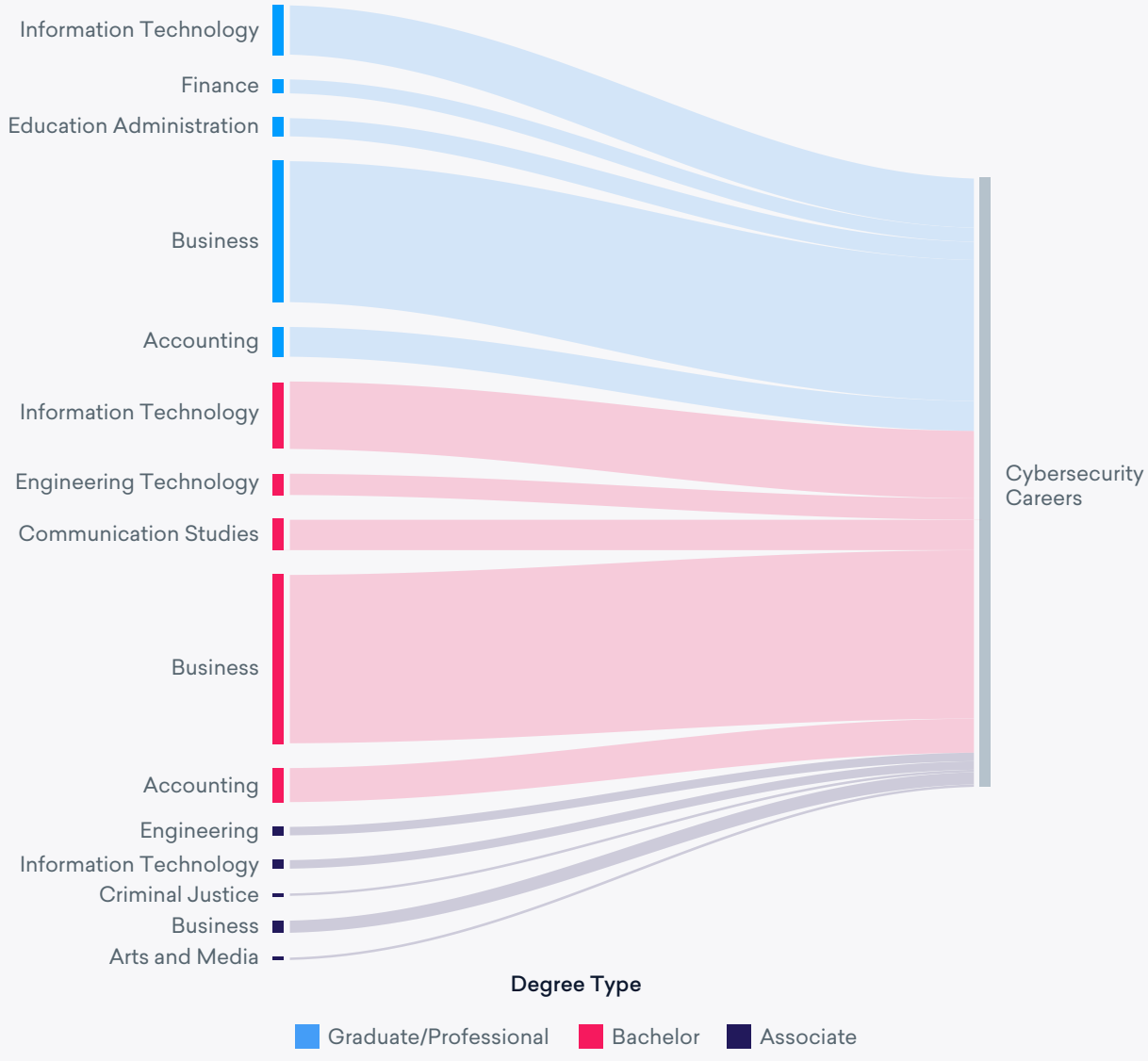
But a national, one-size-fits-all model for cybersecurity microcredentials will not solve the hyper *localized* nature of the cybersecurity shortage. Thus, economic development and educational institutions should do the following in this order:

1. Identify the regional skill shape of cybersecurity.
2. Discover whether key regional industries offer a sufficient talent pool from which to recruit.
3. Design short microcredentials that combine GIAC certifications in tandem with other skills needed by key industries.

To expound on item No. 3, businesses should focus on upskilling their employees through short-term, skills-based programs rather than four-year programs or advanced degrees in cybersecurity. The hard skills that cybersecurity workers need can be gained through microcredentials, which are quick and relatively inexpensive to obtain. Part of our problem is that currently, the majority of cybersecurity professionals hail from bachelor's and master's degrees, which take much longer to complete.

FIG 3.1

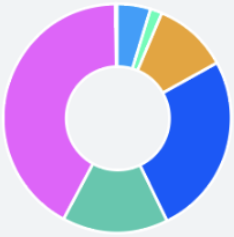
Cybersecurity workers hail from a variety of degrees—most of them at the bachelor's and master's levels



Source: Lightcast Data 2020

FIG 3.2

83% of cybersecurity completions are at the bachelor's level or above



Award Level	Completions (2018)	Percent
Award of less than 1 academic year	89	4.9%
Award of at least 1 but less than 2 academic years	27	1.5%
Associate's Degree	190	10.6%
Bachelor's Degree	463	25.8%
Postbaccalaureate Certificate	274	15.2%
Master's Degree	754	41.9%

Source: Lightcast Labor Market Analytics, 2020

Several institutions are already blazing the trail by offering shorter cybersecurity certifications. TheUniversity of Pennsylvania and FullStack Academy now have cyber boot camps, and the University of Idaho recently announced a computer science-based cyber defense curriculum ranging from advanced degrees all the way down to certificates. Such programs and boot camps, which generally cost between $5,000 and $20,000, offer significant possible savings for employers who pay to upskill current employees rather than slogging through layoff/hire cycles.

As we saw earlier, NYC is in particular need of cybersecurity professionals with experience in finance. Therefore, local learning providers should offer microcredentials that focus almost exclusively on cyber skills and certifications like encryption and security architecture.

Columbus, on the other hand, should offer GIAC certifications combined with courses in financial services and commercial banking. It should also offer another set of programs focused on its tech industry by offering credentials specifically focused on application security, cloud computing security, COBIT (an IT management system), and the programming language Scala.

Finally, in addition to recruiting students from regionally important industries, institutions should work with local businesses to identify workers facing redundancy or obsolescence who could reskill into cybersecurity roles—particularly workers within business operations, finance, or IT.

Conclusion: Building a secure future

The data presented here provides clear evidence for a "build, don't buy" strategy for solving America's cybersecurity talent shortage. Everyone has a role to play:

- **Employers** should invest time and money in understanding their own critical gaps and using that knowledge to better understand where current employees can acquire new cybersecurity microcredentials to fill these new roles.
- **Colleges, universities, and other training organizations** can focus on the key skills needed at the local or regional level and help upskill the many working adults who might be looking for new employment, plus a generation of new grads hungry for good opportunity in a disrupted labor market.
- **Regions and cities** have a vital role in addressing the crisis as they broker between local businesses and higher education to fill the talent gap. Such data will help them address specific regional needs.

Collaboration is key. Together, employers, workforce development organizations, and higher ed institutions can reduce the cost of cybersecurity certifications, and communicate the value of these qualifications to a wide range of students in diverse programs.
The cybersecurity crisis presents major opportunities for all: an opportunity for companies to save jobs while meeting real needs, an opportunity for workers to unlock the next level in their careers, and an opportunity for regions to coordinate innovative programs that meet the needs of both.

Endnotes

1. Josh Bersin, "Rethinking the Build vs. Buy Approach to Talent: How Savvy Employers Are Building Tech Skills from Within," https://josh-bersin.com/wp-content/uploads/2019/10/Build_vs_buy_Bersin_1.0.pdf (accessed June 24, 2020).

2. Footwear News, https://footwearnews.com/2020/business/retail/online-retail-sales-coronavirus-1202949538/ (accessed April 27, 2020).

3. Sentinel Labs, https://labs.sentinelone.com/threat-intel-update-cyber-attacks-leveraging-the-covid-19-coronavirus-pandemic/ (accessed April 27, 2020).

4. SecurtyWorldMarket.com, https://www.securityworldmarket.com/int/News/Business-News/during-covid-19-no-one-is-immune-to-cyber-attacks (accessed April 27, 2020).

5. Bloomberg, https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response (accessed April 27, 2020).

6. (ISC)2, https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study (accessed April 27, 2020).

7. Bersin.

8. Jim Boehm, James Kaplan, and Nathan Sportsman, "Cybersecurity's Dual Mission During the Coronavirus Crisis" https://www.mckinsey.com/business-functions/risk/our-insights/cybersecuritys-dual-mission-during-the-coronavirus-crisis# (accessed June 24, 2020).

9. Robert Half, "Hybrid Jobs: What Are They (and How Can You Get One)?," https://www.roberthalf.com/blog/job-market/hybrid-jobs-what-are-they-and-how-can-you-get-one (accessed June 24, 2020).

10. Strada and Lightcast, "The New Geography of Skills," https://www.economicmodeling.com/geography-of-skills/ (accessed April 27, 2020).

This page intentionally left blank.


Lightcast