

VIEWPOINT

Evolving Workforces

Cybersecurity: Global Talent Spotlight

CBRE INSIGHTS
FEBRUARY 2024



Securing top talent for highly specialized cybersecurity roles has become more challenging than ever for both public and private sector employers. CBRE Consulting formulates talent-based location strategies for companies looking to leverage top talent in both established and emerging markets to help them combat costly cyber threats.

Over the past 10 years, the 115% increase in the U.S. cybersecurity workforce has not nearly kept pace with an 855% increase in job openings for these workers, according to labor analytics company Lightcast. This sizeable supply-and-demand imbalance creates challenges for employers when scaling their cybersecurity workforce, making a thoughtful location strategy essential to any employer seeking to hire and retain this type of talent.

The global cybersecurity industry is expected to grow to \$270 billion in 2026 from \$170 billion in 2020, requiring a corresponding increase in hiring that will be difficult to achieve in this already hyper-competitive talent market. Seventy percent of the almost 12,000 respondents to a recent International Information System Security Certification Consortium (ISC2) poll said they have a severe shortage of cybersecurity workers.

It's critical to study the global cybersecurity talent pool to uncover which industries are employing these workers and which global markets are optimal locations for available cybersecurity talent.



Industry Concentration of Cybersecurity Talent and Fastest-Growing Demand

FIGURE 1: Top 5 Industry Sectors by Share of Global Cybersecurity Talent Pool, Q4 2023

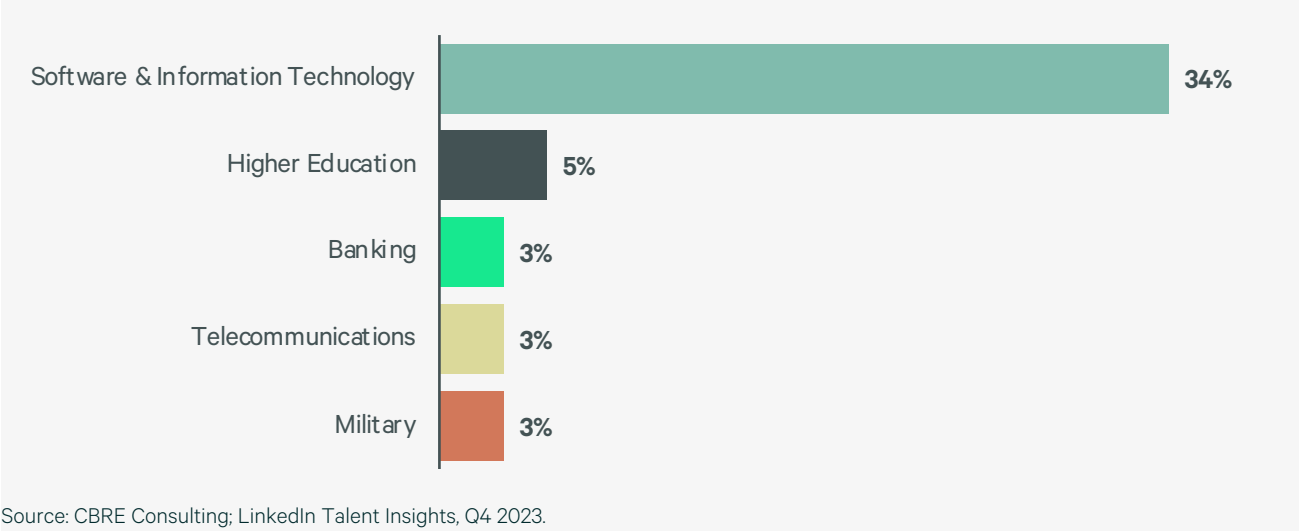
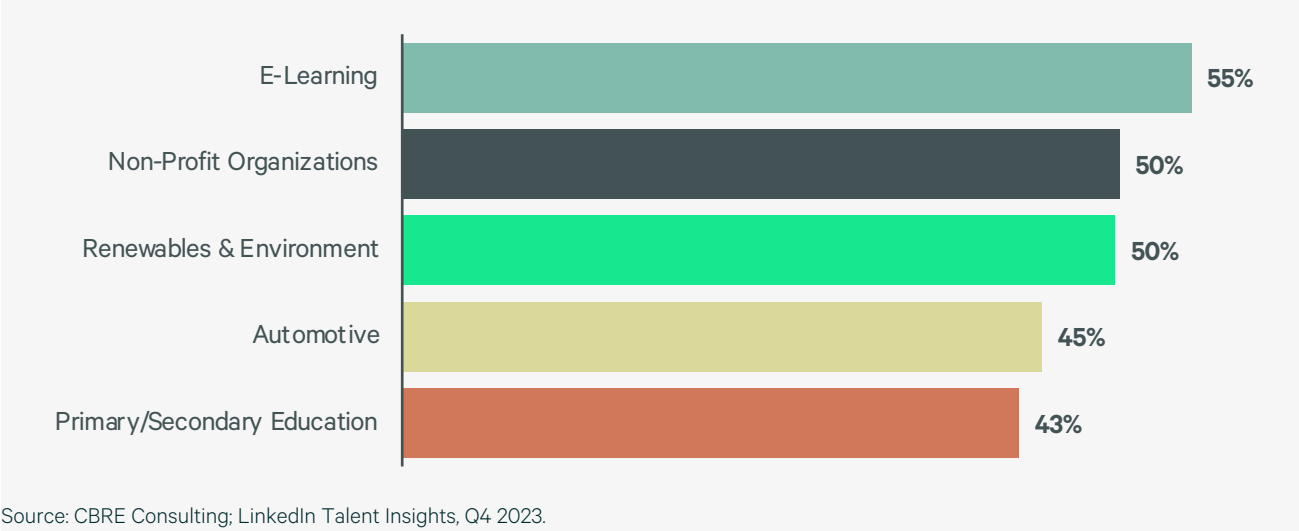


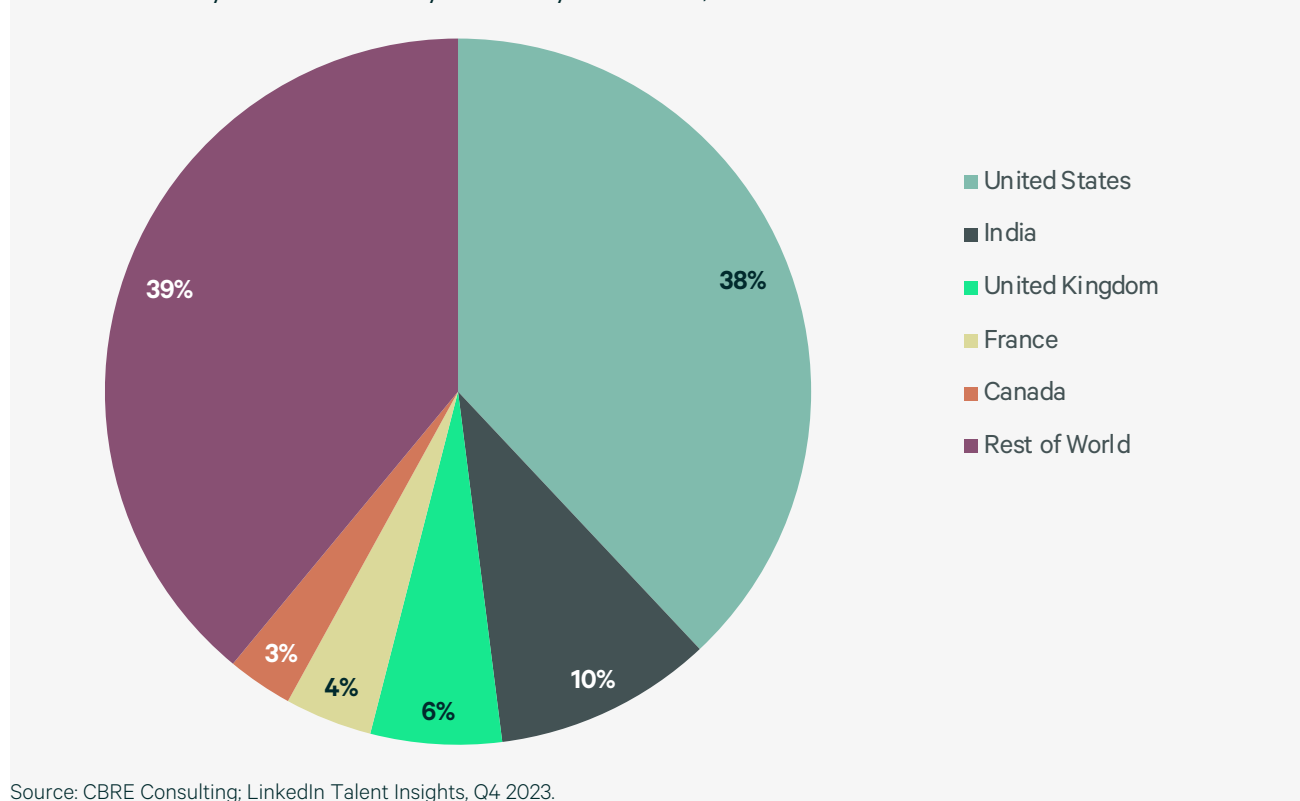
FIGURE 2: Top 5 Industry Sectors by Cybersecurity Talent Growth Rate, Q4 2023



The software and information technology industry has the highest share of global cybersecurity talent with 34%, followed by higher education with 5% and banking and telecommunications—both with 3%. Nearly all industries currently employ cybersecurity talent. Sectors with the fastest annual cybersecurity talent growth include e-learning (+55%), non-profit (+50%), renewables & environment (+49%), automotive (+45%) and education (+43%). Many of these industries are rapidly adopting widespread online networks that require enhanced safeguards against cyber threats.

Market Concentration of Cybersecurity Talent

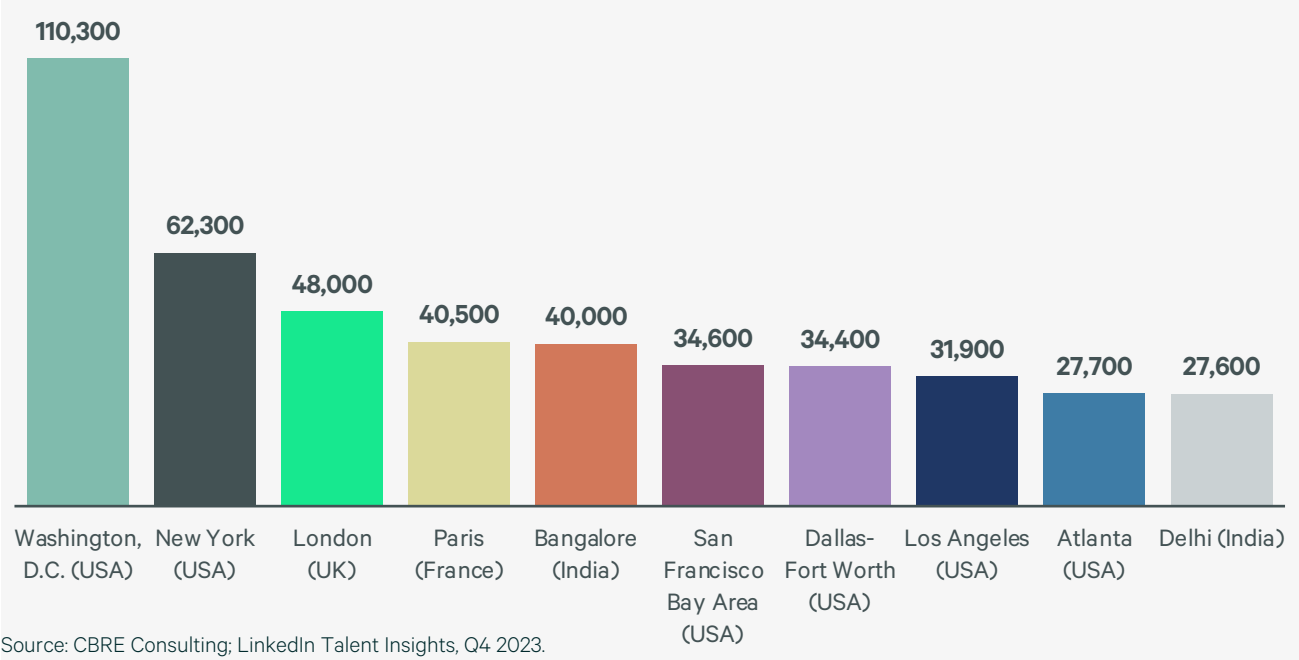
FIGURE 3: Country Share of Global Cybersecurity Talent Pool, Q4 2023



Just two countries—the U.S. and India—account for nearly half (48%) of the global cybersecurity talent pool. The other three of the top five countries for cybersecurity talent share account for just 13%.

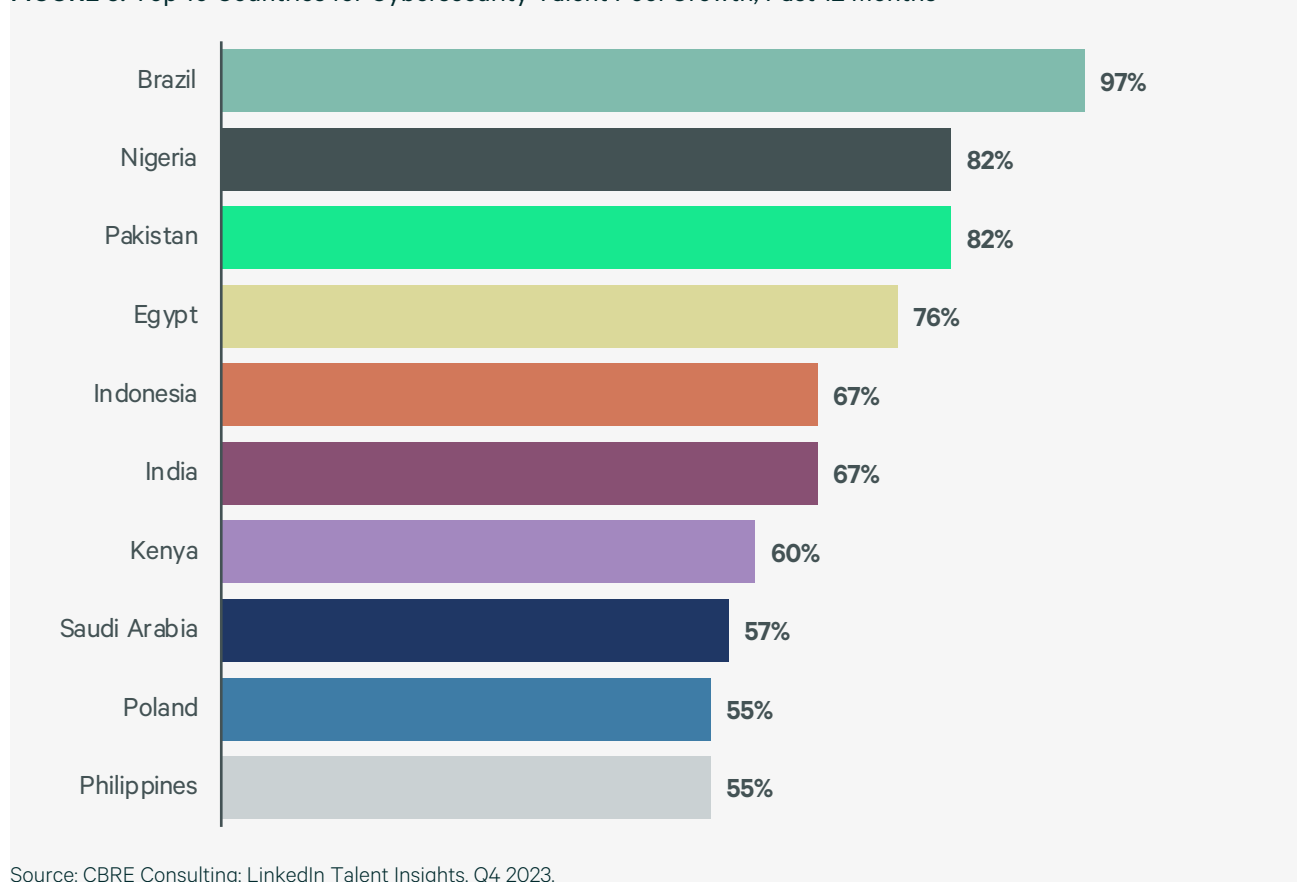


FIGURE 4: Top 10 Global Cybersecurity Talent Markets (Metro Areas), Q4 2023



The Washington, D.C. metro area is the world’s top market for cybersecurity talent with a 5% global share. If it were a country, Washington, D.C. would be the world’s fourth largest for cybersecurity talent. This heavy concentration is largely attributable to the U.S. federal government and its many security and defense contractors. Other top metro markets are major technology and government centers, including New York, London, Paris, Bangalore and the San Francisco Bay Area.

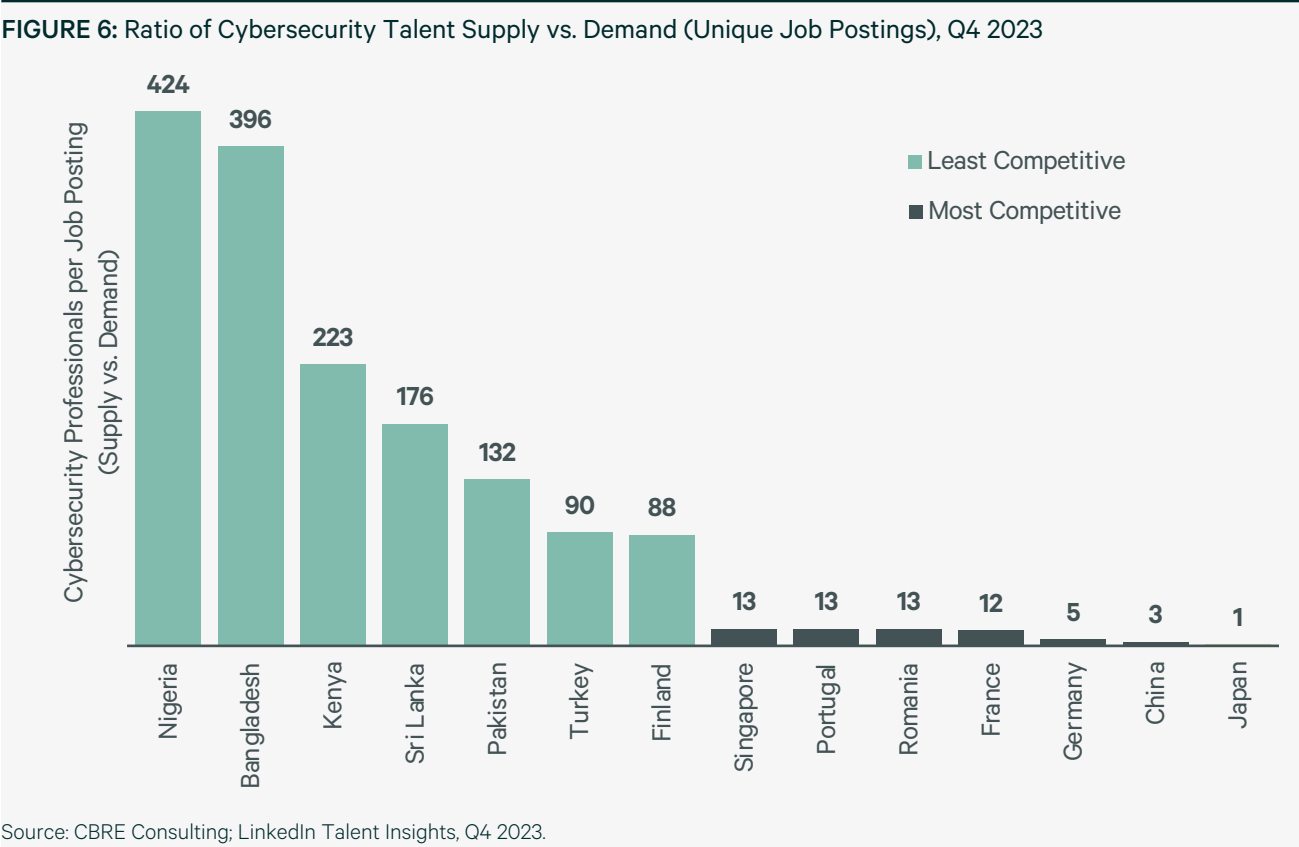


FIGURE 5: Top 10 Countries for Cybersecurity Talent Pool Growth, Past 12 Months

While the largest cybersecurity talent pools tend to be in major global gateway markets and technology hubs, the countries with the fastest growing talent supply tend to be in developing economies in the Global South. Among countries with cybersecurity talent pools of more than 10,000, the top five for talent pool growth over the past 12 months were Brazil (+97%), Nigeria (+82%), Pakistan (+82%), Egypt (+76%) and Indonesia (+67%).

Other smaller countries with rapid talent growth rates include Costa Rica, Portugal, Sri Lanka and Peru. Many multinational companies have pivoted their hiring to these emerging markets amid the highly competitive environment in more mature markets. These companies are typically hiring talent to work remotely to realize substantial cost savings.

Cybersecurity Talent Acquisition and Retention Risk (Select Countries)



The ratio of cybersecurity talent supply to demand (job openings) is a primary indicator of the hiring risk or competitive environment in any talent market. Many of the most competitive markets for cybersecurity talent are more established and mature markets in Asia and Europe. China and Japan, for example, are extremely favorable job markets for workers. Major European markets like Germany and France also have tight talent markets, as do lower cost European countries like Romania and Portugal. These markets are more likely to have increased talent attraction and retention risk that will likely lead to above average wage growth.

On the other hand, many emerging and fast-growing cybersecurity talent markets have less hiring risk due to fewer job openings. Two of the countries with the fastest rates of supply growth (Figure 5)—Nigeria and Bangladesh—also have among the lowest competitive risk. These markets have more employer-favorable labor conditions, making them more attractive for multinational companies to hire remote workers.

The Big Picture

While the global supply of cybersecurity talent is growing rapidly, demand is increasing at an even faster pace. Many more companies are employing highly skilled workers who are dedicated to combating cybersecurity threats. The extremely tight cybersecurity talent markets means that companies must develop and implement talent-driven location strategies that go well beyond just the depth of a local talent pool. They must evaluate a growing number of factors that affect cybersecurity talent availability, including competition, cost and the operational environment's alignment with each company's broader business practices and objectives.

Contacts

Chris Volney

Managing Director
CBRE Consulting
chris.volney@cbre.com

Udit Sabharwal

Head of APAC Labour & Location
CBRE Consulting
udit.sabharwal@cbre.com

© Copyright 2024. All rights reserved. This report has been prepared in good faith, based on CBRE's current anecdotal and evidence based views of the commercial real estate market. Although CBRE believes its views reflect market conditions on the date of this presentation, they are subject to significant uncertainties and contingencies, many of which are beyond CBRE's control. In addition, many of CBRE's views are opinion and/or projections based on CBRE's subjective analyses of current market circumstances. Other firms may have different opinions, projections and analyses, and actual market conditions in the future may cause CBRE's current views to later be incorrect. CBRE has no obligation to update its views herein if its opinions, projections, analyses or market circumstances later change.

Nothing in this report should be construed as an indicator of the future performance of CBRE's securities or of the performance of any other company's securities. You should not purchase or sell securities—of CBRE or any other company—based on the views herein. CBRE disclaims all liability for securities purchased or sold based on information herein, and by viewing this report, you waive all claims against CBRE as well as against CBRE's affiliates, officers, directors, employees, agents, advisers and representatives arising out of the accuracy, completeness, adequacy or your use of the information herein.