From https://www.bloomberg.com/news/articles/2022-03-30/hackers-path-is-eased-as-600-000-cybersecurity-jobs-sit-empty

Bloomberg

Hackers' Path Eased as 600,000 U.S. Cybersecurity Jobs Sit Empty

- Job openings rose at double prepandemic rate in last 12 months
- Cyber professional shortfall could rise to 3.5 million by 2025

By
Olivia Rockeman
March 30, 2022, 7:29 AM EDT *Updated on April 1, 2022, 9:13 AM EDT*

Listen to this article

6:23

Follow the authors @livrockeman

+ Get alerts forOlivia Rockeman

President Joe Biden has urged U.S. companies to "harden your cyber defenses immediately" amid a growing risk of Russian cyberattacks. For many, that won't be easy.

The war for talent has been well-telegraphed throughout the country, but it's particularly acute in cybersecurity. And it's only worsened as competition in the broader labor market has heated up, heightening both companies' potential vulnerability to hackers and the urgency to boost the workforce.

About one million people work in cybersecurity in the U.S., but there are nearly 600,000 unfilled positions, data from CyberSeek shows. Of those, 560,000 are in the private sector. In the last 12 months, job openings have increased 29%, more than double the rate of growth between 2018 and 2019, according to Gartner TalentNeuron, which tracks labor market trends.

"The crunch for cybersecurity talent has definitely gotten a lot worse," said Jamie Kohn, human resources research director at Gartner Inc., a

tech research and consulting firm. “We thought we had five years maybe to get those professionals in the door, and now we’re trying to do it overnight.”

Workers with the technical skills required to respond to cyber threats were already hard to come by before the Covid-19 pandemic forced employees to work from home. But a confluence of events ratcheted up demand even more for positions such as software developers, vulnerability testers, network engineers and cybersecurity analysts.

With so many employees using their home networks and computers, phishing attempts soared, as did ransomware attacks on businesses, schools, hospitals and other organizations.

A ransomware attack on Colonial Pipeline Co. resulted in Americans’ panic-buying fuel, leading to supply shortages on the East Coast last May, while other high-profile incidents were attributed to hackers supported by U.S. adversaries. In Dec. 2020, for instance, investigators revealed a cyber-espionage campaign in which state-sponsored Russian hackers exploited software made by SolarWinds Corp. to infect some customers. Moscow has denied involvement in the matter.

“There are times within cybersecurity when the market even grows faster and when the demand is hotter and I believe we kicked off one of those cycles with SolarWinds,” said Bryan Palma, chief executive officer of Trellix Corp. “Now we have the Russia-Ukraine conflict. We’re seeing cybersecurity grow faster than the normal 16% each year, which therefore is driving the need for even more skills and professionals in that area.”

The cyber worker shortage is a particular problem with smaller organizations, everything from municipalities and law firms to hospitals and businesses, that can’t offer high enough pay to attract high-skilled workers, said Max Shuftan, director of mission programs and partnerships at the SANS Institute, a cybersecurity training organization.

“Most civilian public agencies can’t pay what the public sector can,” Shuftan said. “At the same time, small businesses -- companies that aren’t in an industry that you’d normally worry about this -- they’re probably not going have the staff and that makes them more vulnerable to attacks”

Last year, ransomware attacks affected the operations of organizations including a San Diego hospital system, a nationwide payroll provider and the office network of the Illinois attorney general.

“Our critical infrastructure, our way of life is really under cyber assault all the time,” Jen Easterly, director of the U.S. Cybersecurity and Infrastructure Security Agency said during a speech in mid-March. “And our current geopolitical crisis is only exacerbating this threat.”

If Americans don’t do something about it there will be 3.5 million unfilled cybersecurity jobs by 2025, Easterly said, apparently citing a figure from Cybersecurity Ventures, a research organization.

Cyber Vacancies

A handful of states have the majority of cybersecurity job openings
Source: CyberSeek

The Department of Homeland Security rolled out a new system for hiring cybersecurity personnel in November that would allow federal cybersecurity workers to make as much as $255,800, equivalent to the salary of Vice President Kamala Harris. The new pay scale system was created to help the DHS compete for talent, according to the DHS.

The cybersecurity industry also isn’t immune to the broader macroeconomic trends that are upending the labor market, including a desire for remote work, flexible hours and higher pay. Trellix, for instance, will adopt a hybrid model in which employees balance remote work and work from offices.

In 2020, the annual mean wage for information security analysts was $107,580, almost double the mean for all U.S. occupations combined, according to data from the Bureau of Labor Statistics.

“The competition is real, the great resignation is real, it’s definitely a day-to-day battle.” Palma said. “And compensation is a part of that.” Since the pandemic began, Trellix has grown its overall staff by 5%, but the company is still trying to grow by another 10% or more.

Because cybersecurity skills are in such high demand, workers have room to negotiate and can jump from one company to another relatively easily. But hiring cybersecurity professionals from another company doesn’t address the underlying issue: that there aren’t enough qualified workers, said Stuart Madnick, professor of information technologies at the MIT Sloan School of Management.

Read More: Cybersecurity Pros Name Their Price as Hacker Attacks Swell

Countries like Russia, China and Israel that have compulsory military service have a better talent pipeline of qualified individuals who have been trained in cybersecurity at the government level, according to Palma. He said he’s been communicating with members of Congress to create a AmeriCorps-type program specifically for fostering cybersecurity talent because there aren’t enough Americans being trained via government service.

Other efforts to increase the talent pool include implementing cybersecurity courses in high schools, offering workshops to lower-level IT professionals, running training in rural regions and dropping degree requirements in favor of aptitude tests. Automating some security-related tasks could also be a solution to the hiring problem.

“We have a massive shortage of security experts on the planet, and we want to automate so much of the talent and capability,” Kevin Mandia, CEO of Mandiant Inc., said in a briefing with reporters in early March. “That’s all software’s ever been is the automation of human process.”

But none of those solutions are immediate, and the threats are.

“The worst is yet to come,” said Madnick of MIT. “Not just because things have been getting worse and worse each year, but we’ve concluded that the disruptions we see are nowhere as bad as they could’ve been. We think in many cases these were test runs.”

— With assistance by Nico Grant

(Adds mention of Cybersecurity Ventures, a research organization, in thirteeneth paragraph.)