Wanted: Millions of cybersecurity pros. Salary: Whatever you want

By Clare Duffy, CNN Business Updated 3:48 PM ET, Fri May 28, 2021

New York (CNN Business) — A series of major digital security breaches over the past year are serving as a wake-up call to Corporate America about the need to invest in cybersecurity.

Friday brought yet another reminder of the risk of cyberattacks, when Microsoft (MSFT) said the hackers behind the 2020 Solar Winds breach launched a new attack on more than 150 government agencies, think tanks and other organizations globally.

But perhaps the most striking recent example is the Colonial Pipeline ransomware attack, which forced the company to shut down the pipeline temporarily — resulting in gas shortages and price spikes in multiple states over several days. The debacle cost Colonial at least $4.4 million, the amount its CEO admitted to paying the hackers.

In the weeks before the attack, the company had posted a job listing for a cybersecurity manager.

"As far as I know, this is the first cybersecurity incident that has led to a measurable economic impact on the American population," said Jonathan Reiber, senior director for cybersecurity and policy at AttackIQ and the chief strategy officer for cyber policy under the Obama administration's secretary of defense.

"It should be something that triggers people," he said.

The takeaway from such security breaches, according to experts, is that it's high time for companies to start investing in robust controls and, in particular, adding cybersecurity professionals to their teams.

The only hitch: There's a massive, longstanding labor shortage in the cybersecurity industry.

"It's a talent war," said Bryan Orme, principal at GuidePoint Security. "There's a shortage of supply and increased demand."

Millions of unfilled jobs

Experts have been tracking the cybersecurity labor shortage for at least a decade — and now, a new surge in companies looking to hire following recent attacks could exacerbate the problem.

The stakes are only growing, as technology evolves and bad actors become more advanced.

In the United States, there are around 879,000 cybersecurity professionals in the workforce and an unfilled need for another 359,000 workers, according to a 2020 survey by (ISC)^2, an international nonprofit that offers cybersecurity training and certification programs.

Globally, the gap is even larger at nearly 3.12 million unfilled positions, the group says. Its CEO, Clar Rosso, said she thinks the need may actually be higher, given that some companies put off hiring during the pandemic.

The needs range from entry-level security analysts, who monitor network traffic to identify potential bad actors in a system, to executive-level leaders who can articulate to CEOs and board directors the potential financial and reputational risks from cyber attacks.

The US Bureau of Labor Statistics projects "information security analyst" will be the 10th fastest growing occupation over the next decade, with an employment growth rate of 31% compared to the 4% average growth rate for all occupations.

If demand for cybersecurity professionals in the private sector increases dramatically, some experts say talented workers could leave the government for more lucrative corporate jobs — a risk that is especially acute for smaller, local government agencies that manage critical infrastructure in their communities but have limited budgets.

"Think of the criticality of what your local government does: water purification, waste treatment, traffic management, communications for law enforcement, public safety, emergency management," said Mike Hamilton, chief information security officer at Critical Insight. "But Amazon is out there waving around bags of cash to protect their retail operation."

Hamilton — who was the former chief information security officer for Seattle, Washington, from 2006 to 2013 — added that local governments "cannot attract and retain these people when the competition for them is so high, which is why we've got to make lots of them."

'Not a short term solution'

A variety of education, training and up-skilling programs are already working to address the shortage.

GuidePoint helps train veterans leaving the military for cybersecurity careers. And Critical Insight's Hamilton runs a nonprofit called Public Infrastructure Security Cyber Education Systems, through which students at five universities get hands-on experience by doing security monitoring of real-time data on local government networks, providing a crucial service for small cities and counties that might not otherwise be able to afford it.

Experts say there's also an opportunity to bring new talent into the industry by focusing on diversity. Just 25% of cybersecurity professionals are women, so (ISC)2 launched a diversity, equity and inclusion program this year aimed at recruiting and keeping more women in the profession, Rosso said.

"We need to recognize that there is this huge diversity of people that can actually do ... this job very well," Hamilton said, referring to security analysts who monitor traffic on a network to look for behavior that might indicate a bad actor has accessed the system. "As a country, we are not taking very good advantage of the resources that we have."

In the meantime, as the industry works to grow its labor force, it could be a huge opportunity for service and software provider companies that can help firms beef up their cybersecurity protocols without hiring their own teams.

Because even with existing training programs, the global cybersecurity labor gap is expected to grow by 20% to 30% annually over the next several years, (ISC)^2's Rosso said. Experts say both the public and private sectors must invest more in growing the industry's workforce.

Portions of President Joe Biden's $2 trillion American Jobs Plan could help. The infrastructure proposal includes $20 billion for state, local and tribal governments to update and improve cybersecurity controls for their energy systems.

Still, experts say more needs to be done, suggesting a broad rethinking of education systems from

elementary school through higher education to include more cybersecurity training.

"Sadly, there's not a short-term solution," GuidePoint's Orme said. "I think we need to take a long-term view of it — as a lot of our adversaries do — to say, how can we systematically build the next generation and the generation after that and create a flywheel of qualified security talent that will be entering the workforce over the next 50 to 100 years?