Cybersecurity Hiring Slows Even as AI Raises the Stakes

AI Threats Surge, Cybersecurity Hiring Lags, and Cyber Professionals are Rapidly Upskilling in AI Security and Governance

Caroline Liongosari

LinkedIn Economic Research Team

NOVEMBER 2026

KEY FINDINGS

- **Despite an increasing number of cybersecurity incidents, cybersecurity hiring in the U.S. has underperformed relative to overall hiring**, declining 6.3% Y/Y in September 2026 compared with a 1.7% decline in overall U.S. hiring.
- **The bright spot for cybersecurity hiring is outside of tech.** Wholesale was the only industry to grow (+14.4% Y/Y) while cybersecurity hiring in technology declined 14.4% Y/Y[1], and several other industries declining less. This may reflect non-tech industries investing to secure supply chains and close past cybersecurity gaps.
- **AI skills may be becoming an assumed requirement among cybersecurity professionals.** Comparing the periods of 2020–2022 and 2023–2025, the share of cybersecurity talent with an AI Engineering skill increased 362%, while the share of cybersecurity job postings asking for an AI Engineering skill grew by a far smaller 76.4%.

KEY TAKEAWAYS

- **For business leaders:** Given the current threat and security environment, prioritize investment across your organization, which may include hiring more cybersecurity talent. Doing so can help protect your business.
- **For cybersecurity job seekers:** AI skills appear to be becoming part of the job. Highlight AI skills such as AI governance and AI security, even if postings don't list it. Also, consider industries outside tech, where hiring has been more resilient.

Despite growing risk, cybersecurity hiring remains weak

Microsoft's Digital Defense Report 2026[2] finds that AI has enabled "unprecedented speed, scale, and customization" in cyber attacks, with some that once took days now taking only seconds. As generative AI spreads across work, education, and daily life, so do the opportunities for malicious actors

Despite the growing visibility of cyber attacks,[3] hiring for cybersecurity talent has fallen, decreasing 6.3% y/y in September 2026. This deceleration was steeper than for software engineers (-4.2%) and the overall U.S. labor market (-1.7%), suggesting employers may be underinvesting in the talent needed to protect their tech infrastructure, organizational and user data in an increasingly vulnerable environment.

Segment	Hiring Rate (SA*), Sep 2025	Hiring Rate (SA*), Sep 2026	Y/Y Change
Overall US labor market	0.94	0.92	-1.7%
Software Engineer (occupation)	0.89	0.85	-4.2%
Cybersecurity	**0.83**	**0.78**	**-6.3%**

*SA = Seasonally Adjusted, Indexed to 2016

[1] Non-Seasonally Adjusted Hiring Rates

[2] Microsoft. (2026). 2026 Microsoft digital defense report: Executive summary. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/2026-Microsoft-DDR-Exec-Summary.pdf

[3] US companies face rise in cyber attacks. (2026, September 23). Reuters. https://www.reuters.com/legal/government/us-companies-face-rise-cyber-attacks-2026-09-23/

Industries outside of Tech show more cybersecurity hiring momentum

Technology, Information and Media (Tech) is among the largest hirers of cybersecurity talent, representing about 20% of hires in September 2026. With cyber hiring in tech declining 14.4% y/y, it is no surprise that cyber hiring is down overall in the U.S. However, hiring has been more resilient in non-tech industries including Construction, (-4.2%), Education (-8.5%), Manufacturing (-8.9%), and Oil, Gas, and Mining (-8.9%). Of special note is Wholesale, the only industry with positive growth at 14.4%. Non-tech industries such as wholesale, construction, and manufacturing may be hiring more cybersecurity talent to defend their digital supply chains and operations, which have faced increasing attacks[4], and to make up for earlier underinvestment, even as tech hiring pulls back.

Industry	Cybersecurity Hiring Rate Y/Y% (not SA*)
Wholesale	+14.4%
Construction	-4.2%
Education	-8.5%
Manufacturing	-8.9%
Oil, Gas, and Mining	-8.9%
Technology, Information and Media	**-14.4%**

*not SA = not Seasonally Adjusted

AI skills are critical to cybersecurity, but cybersecurity job postings aren't keeping up

The cybersecurity workforce is rapidly adapting to the AI landscape. Comparing the periods of 2020-2022 and 2023-2025[5], the share of the cybersecurity workforce with an AI engineering skill[6] grew 362% while the share of cybersecurity job postings requesting such skills grew just 76.4%.

One explanation is that employers are updating requirements more slowly than the workforce evolves. Another, offered by Lea Kissner, LinkedIn's Chief Information Security Officer, is that AI is becoming a baseline requirement in cybersecurity: *"AI has changed the job for every security professional, whether they asked for it or not and so knowing the technology has become table stakes. Often, we don't bother writing it into the job description. For business leaders, that means the work is changing so fast that nobody has a perfect resume for it, so the most important thing is hiring people who can adapt. I also look for strong technical skills, comfort with ambiguity, and a willingness to keep learning. A good place to start can often be inside your own company as there may be engineers and IT folks who already know how your systems work and can make great security people with the right training."*

AI security and AI governance, which rank among the top five fastest-growing skills among cybersecurity professionals in the past year, are consistent with Kissner's view. This suggests that AI upskilling is increasingly part of the job, whether or not job postings ask for it.

Conclusion

While AI is accelerating the cyber threat landscape, cybersecurity hiring in the US has been decreasing, faster than overall U.S. hiring. Some non-tech industries, led by Wholesale, appear to be shoring up their defenses even as tech hiring pulls back. Meanwhile, cybersecurity professionals are upskilling in AI security and governance, suggesting AI fluency is increasingly part of the job, whether or not postings ask for it.

Workforce upskilling alone may not be enough. Business leaders should evaluate whether their investment in cybersecurity talent is sufficient to protect their organizations and user data against evolving threats, and whether their job requirements reflect the skills their security teams now need.

For cybersecurity job seekers, AI skills appear to be becoming part of the job. Highlight AI skills such as AI governance and AI security, even if postings don't list them. Also, consider industries outside tech, where hiring has been more resilient.

[4] Cybersecurity and Infrastructure Security Agency & Federal Bureau of Investigation. (2026, September 23). Considerations for critical infrastructure operators working with third-party ICS integrators. https://www.cisa.gov/resources-tools/resources/considerations-critical-infrastructure-operators-working-third-party-ics-integrators

[5] 2020-2022 and 2023-2025 are the three-year periods before and the launch of ChatGPT

[6] An AI Engineering Skill is a skill associated with a building and implementing AI systems

Methodology

Data and Privacy: This body of work represents the world seen through LinkedIn data, drawn from the anonymized and aggregated profile information of LinkedIn's 1+ billion members around the world. As such, it is influenced by how members choose to use the platform, which can vary based on professional, social, and regional culture, as well as overall site availability and accessibility. In publishing these insights from LinkedIn, we want to provide accurate statistics while ensuring our members' privacy. As a result, all data show aggregated information for the corresponding period following strict data quality thresholds that prevent disclosing any information about specific individuals.

Skills: LinkedIn members self-report their skills on their LinkedIn profiles. Currently, more than 42,000 distinct, standardized skills are identified by LinkedIn.

AI Engineering Skill: A skill associated with building and implementing AI systems including Large Language Models (LLMs), Machine Learning, and Artificial Neural Networks

Cybersecurity Talent: A LinkedIn member is considered a cybersecurity talent if they have listed at least 2 cybersecurity skills on their profile. Cybersecurity skills include cybersecurity incident response, vulnerability assessment, and cloud security.

Hiring Rate: The hiring rate is the percentage of LinkedIn members who added a new employer to their profile in the same month the new job began, divided by the total number of LinkedIn members in the U.S. This number is indexed to the average month in 2016. For example, an index of 1.05 indicates a hiring rate that is 5% higher than the average month in 2016.