Skill gap in cyber security hobbles IT industry

Hunt for professionals with right skills pushes up salaries; makes hiring unaffordable for many firms

VARUN AGGARWAL
Mumbai, April 23

Cyber attacks on Wipro, Infosys and Capgemini have brought to the fore the challenge of filling the skills gap in the cyber security space in India, even as demand continues to outweigh supply.

This in turn has led to a sharp increase in the pay package of such professionals, who end up earning two to 10x the average salary of an IT engineer.

According to a recent workforce development survey, 59 per cent of organisations have vacant cyber security positions, with Frost & Sullivan forecasting a shortfall of 1.5 million by 2020 globally.

That presents a huge opportunity for India and its IT services industry to reskill and fill the gaps.

But it seems easier said than done. The acute shortage and the consequent spike in salaries are making professionals with just 2-3 years of experience unaffordable.

"We are seeing people with just six months to a year of experience in information security demanding 2-10 times a normal engineer's salary. In most cases, we are even willing to pay the amount, since we have big projects lined up and can't hold on to hiring," said Trishneet Arora, CEO at TAC Security, a cyber security start-up.

Experts believe the situation will continue till the skill gap is bridged.

A 2019 Gartner survey shows the global talent shortage is now the top emerging risk facing organisations.

The expansion of the digital marketplace has generated more jobs than the current supply of security professionals can meet.

Focus on Careers & Education

Recent cyber attacks on IT firms have brought security gaps to the fore ISTOCKPHOTO.COM

Investment in training

"Big corporate investment is not going in cyber security training. It is more according to immediate requirements," said Pareekh Jain, founder at Pareekh Consulting.

"One reason why large corporates don't want to invest heavily in cyber security training (unlike IT services training in the 1990s and early 2000s) is that these trained professionals will leave for better job prospects," Jain added.

There is also a lack of cyber security training institutes of scale, though some institutes, such as Lambada School are coming up.

These institutes train professionals on emerging technologies — including cyber security — based on an income-sharing agreement.

This could reduce the risk for both students and corporates, and improve supply situation.

"Engineers are very reluctant to spend on cyber security training and certification. Cost is one of the main barriers, despite the cyber security field having a zero per cent unemployment rate with very good compensation," Michael Joseph, Regional Director, System Engineering, India and SAARC, Fortinet, said.

"Not just individuals, even organisations remain unwilling to invest in cyber-security training programmes or hire entry-level candidates without prior experience. Investments in training programmes for IT professionals are considered a waste of resources, pushing companies to hire candidates with experience and training already under their belts," Joseph added.

Even the Big Four consulting firms are ramping up their cyber security teams.

"There is a mismatch in what clients look for, and the skills the industry offers. Companies are doing whatever they can to plug this gap. The industry is spending about ₹10,000 crore a year on training and development," said Amit Aggarwal, CEO of IT/ITES, Sector Skill Council, Nasscom.