Cybersecurity: A new opportunity for India to upskill

Success in a cybersecurity world demands extraordinary levels of discipline, focus, imagination and knowledge

According to various studies, in the next two years, over three million cybersecurity jobs will remain unfulfilled due to lack of availability of qualified talent. That number alone indicates not just the degree of importance that businesses are according cybersecurity but also the level of effort that higher education institutions globally need to put in to cater to this segment. Increasing cyberattacks, loss of critical data and soaring ransom demand for hostage data and infrastructure will together ensure that the demand for skilled cybersecurity professionals will only increase over the next decade.

At the time of writing this article, there were over 3500 open cybersecurity positions posted on a leading Indian job site. Roles like security architect, cybersecurity analyst, threat researcher and information security and incident management are in high demand. The country however faces a critical shortage of trained professionals and this has led to a sharp hike in salaries for these skills. This is despite the fact that India is today home to one of the largest talent pools as far as information technology is concerned.

Success in a cybersecurity world demands extraordinary levels of discipline, focus, imagination and knowledge. Many education institutions have recognized the need to impart cybersecurity education in some form to students. Some are even offering masters and PhD level specializations. However, if one takes a cursory glance at the curriculum an interesting aspect comes to the fore. Most of our courses and in many cases even the certifications offered by training centers are focused on business risk mitigation.

Our higher education approach to cybersecurity needs to consider two factors in addition to risk mitigation. One is to develop real work orientation on cybersecurity roles and the second one is to offer a strong and widespread understanding of technical aspects and strategies to defeat efforts to breach security systems.

The curriculum also needs to bring in an aspect of collaboration to allow cybersecurity professionals to develop skills needed to get a 'buy-in' from their colleagues and management on an enterprise wide cybersecurity effort and to sensitize employees on related aspects. Cybersecurity professionals need to be experts at championing a culture that promotes continuous investments in risk and threat management.

Another important aspect of cybersecurity is prioritizing risks and threats and appropriate resource allocation. Cybersecurity professionals should be able to gauge risks, raise appropriate alerts and inform relevant teams and collaborate to address them. The curriculum followed by Indian technical universities needs to incorporate these aspects.

The Information Security Education and Awareness (ISEA) project launched by the Indian government is a vital step in transforming the cybersecurity education landscape in the country. The agency is working towards increasing awareness at all education levels and conducts periodic workshops in association with other stakeholders. This effort can be amplified through a national platform of connected stakeholders.

To transform India into a cybersecurity hub, a concerted effort from the government, businesses, vendors, campuses and other relevant stakeholders is required. Campuses can play a key role in this endeavor. By enhancing their curriculum, teaching models, industry exposure and laboratory-based gamified learning and aptitude tuning, Indian campuses can start training a new generation of cybersecurity ready students who can turn the tide in our favor in the war on cybercrime.

Vinod Kumar

(The author is Managing Director and CEO, Subex)