Authors:

Jairaj Srinivas DG & Founder CIMEI

Dr.Shubhamangala Sunil
CEO-Cyber Security Expert-Certified Anti Terrorism Specialist

Cyber Security Professionals skill gap in India

The sorry state of affairs of just one nation in the cyber-security space, but there is a bigger picture to look at. A shortage of nearly over 2 million cybersecurity professionals in India is a big reason to worry. According to a survey, Israel has the highest skill deficit of cybersecurity professionals. The next few names in this list are first-world countries: Ireland, the UK, and the US and Australia.

It is a global problem and singularly India can solve the problem.

Well, here's the reason for that; India is the home to some of the biggest IT companies that have quite some global reckonings. Now, most recently, some of these IT giants like Wipro, TCS, and Capgemini suffered cyber-attacks. There is no question whatsoever that such cyber -attacks deter the global credibility of this company.

India and the US have been fierce competitors to top the list of countries with the most cyber-attacks. According to a report, the US and India occupy the top two spots on the list. Countries like the UK, Spain, Nigeria is also on the list.

On evaluating both the above factors, it only makes sense that India takes a giant stride in supplying skilled cybersecurity professionals. It is quite intriguing to note that a country that supplies IT professionals, both for home and abroad, has a shortage of cybersecurity professionals. Where does the problem lie? And who is at fault here?

Let us see some of the problems which stifle the growth of cybersecurity professionals.

A government-led model of imparting Cyber security skills

India is a country where providing skills at a reasonable cost lies on the shoulder of the Government. In a country with a majority of middle-class families with meagre incomes, it naturally becomes tough to invest on cyber-security training.

The governments' role in bridging the demand-supply gaps is equivocally undeniable. There is no specific allocation for cybersecurity within India's Union Budget. The finance ministry had allocated Rs 3,750.76 crore in the previous budget but the same was revised downward to Rs 3,212.52 crore. The increase has been mainly due to the budget allocation for various PLI Schemes launched for Electronic Manufacturing which does not promote local value addition and most manufacturers are promoting assembling by importing complete knockdown kits.
If opens up foreign investments for imparting Cyber Skills, then the initiative can be a game-changer in the field of cybersecurity.

Lack of awareness of cyber-security as a potential career option

Suppose you are a student in India who wishes to be a cybersecurity professional. Either of the two factors might have influenced you to consider this profession.

First, you might have seen your friends or relatives earning Pounds or Dollars, so the idea might draw you to this course too. Secondly, you must have been inspired by a movie.

There is no real awareness of the cybersecurity training program from authentic sources. The students are unaware of the salary that cyber-security professionals get in India. This is also a part of the reason why aspiring students move abroad for cyber training for a better ROI, even in a situation where the Indian companies are willing to pay 2-to-10X of the standard salary.
If India needs to meet the demand for cyber professionals, the changes need to come from the grassroots level.

Cycle of outsourcing

The cycle of outsourcing cybersecurity professionals from other countries is a double -edged sword. However, it can be one way to meet the demand for cybersecurity professionals. It can also consume a large portion of the company's budget, which otherwise could have been spent on training employees. It would help if you viewed this factor from a macro level.

There is one other form of outsourcing, which, in a way, allows the organization to shrug off its responsibility of providing training facilities. Lately, companies have been collaborating with foreign clients in acquiring cybersecurity talents on a project basis.

Again, this can only be one of the ways to handle short-term resource deficit. Hence, no effort is made to build the Indian repository of cybersecurity professionals to fill the one million or so vacant jobs.

Lack of educational space of cybersecurity

The educational ecosystem is yet to create a considerable space for the cybersecurity section. The problem here is two-fold, at one level, there aren't enough training facilities to accommodate the number of students who are slowly showing interest in such a course.

Secondly, cybersecurity is a dynamic field of study. It needs learning and relearning. So, the curriculum needs to be regularly updated, which is not just happening. As a result, students who are passing out and getting into the real world fail to deliver.

Some of the private universities like AMITY have started providing cybersecurity courses. But the real change can come from the Edtech start-ups and universities in combination with the likes of industry bodies who can coordinate and motivate with Industries to create new jobs in Cyber space. Ultimately it will monitor the skill gap in this space.

Lack of Edtech Start-up focus on providing programs for cybersecurity

As mentioned before, Edtech Start-up can change the landscape of cyber-security training. Two of the prominent names in Edtech Start-up in the US, Coursera and Khan Academy, have played a key role in US 7% growth in skilled cybersecurity professionals.

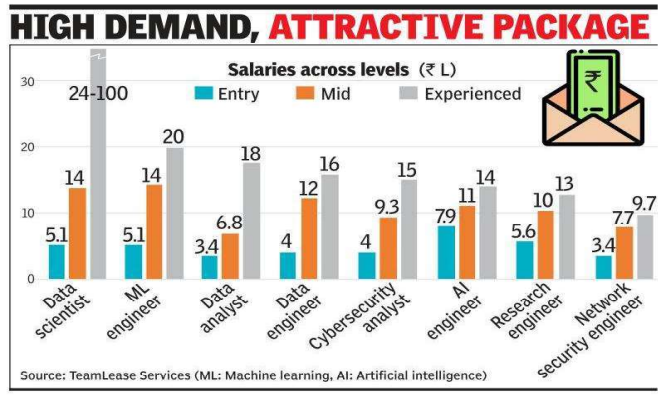
In India, BYJUS and a handful of other tech start-ups are focusing on proving the cybersecurity training program. The numbers have to increase; otherwise, we will be reeling in improvements, while other countries like the UK and the US will make improvements.

The government allocation of 99,300 crores on the education, of which little over Rs. 3000 crores would go into skill development, is a promising sign of change that we can see soon. Also, the ISEA (Information Security education and Awareness) website, which is run by the Department of Electronics and Information Technology, has listed some training courses on their website. But that hardly meets the scale of solution which is needed right now. The call now is for big moves and bold changes.

6 Reasons Why Women Should Consider a Career in Cyber Security

There is a massive labour shortage in the cyber security field. It has been estimated that, on a global scale, there are over 1 million unfilled cyber security jobs—and if history is any indicator, that number is likely to increase. Between 2010 and 2014, cyber security job postings grew by 74%. As cybercrime intensifies in both scale and sophistication and our society becomes increasingly reliant on technology, think the Internet of Things and Electronic Medical Records, the magnitude of this worker blight is becoming more and more threatening, posing serious risk to the safety and security of individuals, corporations and the nation as a whole. So how do we solve the labour shortage in the cyber security industry? Think women. Right now, women in cyber security represent a mere 11% of the industry worldwide. That means that the cyber security industry is missing out on almost half of the population's talent pool, during a period in history when cybercrime poses one of our most menacing threats.

The women representation in workforce globally 2021 at the highest rate of work-force participation since March 2020, which is, at 57.8 percent. Whereas in India the percentage is only 20.3% representation of total workforce and in Tech Jobs. There are plenty of reasons why they should opt for tech jobs.



Job Security

Because demand is far outpacing supply in the cyber security sector and cyber-attacks aren't going away anytime in the foreseeable future, job security in this sector is strong. According to the 2015 (ISC)2 Global Information Security Workforce Study, there will be 1.5 million unfilled jobs in cybersecurity by the year 2020. So, if you want a career you can rely on and that will offer opportunity for growth, cyber security is the place to be.

High Pay

Thanks in part to the extreme drought in cyber security talent and the skills required to work in the field, salaries in cyber security are high. According to **CNBC**, the average annual salary for a cyber security professional with a bachelor's degree is $116,000. And for the more advanced positions that typically require a master's degree, the salaries almost double:

- Lead software engineer-$233k
- Chief security officer-$225k
- Global information security director-$200k
- Security consultant-$199k
- Chief information security officer-$192k

Scholarships and Incentives for Women

President Barack Obama remarked in 2013, "One of the things that I really strongly believe in is that we need to have more girls interested in math, science, and engineering. We've got half the population that is way underrepresented in those fields and that means that we've got a whole bunch of talent…not being encouraged the way they need to."The realization that women are hugely underrepresented and direly needed in the field of cyber security has spurred the creation of many programs aimed at attracting and promoting women in this largely male dominated industry."

Companies are Eagerly Seeking Women in Cyber Security to Diversify Their Workforce

Corporations as well as governmental agencies have recognized the lack of diversity in the cyber security talent pool as well as in their own cyber security departments. Not only is it beneficial from a public image standpoint to employ a diverse workforce, but more importantly, a diverse workforce drives innovation. The author feels, "Diversity encourages a culture where divergent opinions can be brought together to develop innovative solutions for some of the toughest problems our nation faces today.

NEXT PAGE

Companies are Eagerly Seeking Women in Cyber Security to Diversify Their Workforce

Corporations as well as governmental agencies have recognized the lack of diversity in the cyber security talent pool as well as in their own cyber security departments. Not only is it beneficial from a public image standpoint to employ a diverse workforce, but more importantly, a diverse workforce drives innovation. The author feels, "Diversity encourages a culture where divergent opinions can be brought together to develop innovative solutions for some of the toughest problems our nation faces today."

Help Break Down Stereotypes and Advance Equality for Women

Women are sorely underrepresented in cyber security and often don't see the occupation as a viable option due to a number of factors such as a lack of female role models within the industry, stereotyping and pay gaps. Yet, in order to change the industry and remove barriers for women, women need to enter the field in higher numbers and work to remove these stereotypes, demand equal pay and act as role models for other women hoping to enter the field.

Make a Real Impact on Individual, Corporate and National Security

Cyber security experts are in desperate need. According to The Centre for Strategic and International Studies' an estimated $100 billion is lost every year in the U.S. alone and roughly 508,000 jobs in the U.S. are lost every year due to cybercrime. Today's wars are being fought online and as such there is an urgent need for both women and men who have the technical skills and understanding required to combat persistent and malicious cyber-attacks.