While new technologies have brought forward productive gains and opportunity, they have also extended the threat surface, exposing citizens, consumers, companies, and countries to new threats and vulnerabilities. Given that the risk landscape is expanding day by day, ensuring cybersecurity is gradually assuming importance among industry players and the governments of the world. In conversation with senior leadership at Check Point Software Technologies, tele.net discovers how the cybersecurity space is evolving in India and what the future holds...

From left to right: Harsh Marwah, Country Manager, Check Point Software Technologies and Venugopal N, Director, Security Engineering, Check Point Software Technologies)

How has the cybersecurity market in India evolved over the years? What are the emerging trends in this space?

Harsh Marwah- India over the years has evolved tremendously as far as cybersecurity infrastructure mitigation is concerned but it's a very fragmented market. So we see a lot of customers who are extremely mature and who would have really assessed the complete evolved landscape as far as their business is concerned, their larger fraternity is concerned, and they have really taken steps to address it but then there are customers in the small medium enterprises who would typically require lot of hand holding, heavy lifting to be done in terms of taking them on to the next level. Virtually Check Point has been there since the time when cybersecurity evolved, so we have been able to carve out a risk landscape from late 80s till date. At present, we are in Generation 5 of risk landscape and we have done a survey worldwide where we found that customers are typically at around 2.7-2.8 on a landscape of 5.

Venugopal N- In terms of emerging trends and technologies that are going to affect

cybersecurity in the future, we are still at a stage when we are not taking care of the security concerns for the existing trends. So we have to get at that stage where we protect the existing and then look at emerging. While it's important to have this foresight into what will emerge, we are still not actually worried about the existing trends and technologies.

How is the adoption of internet of things (IoT)/machine-to-machine (M2M) technologies likely to impact the cybersecurity space?

Harsh Marwah- Adoption of IoT is leading to millions of devices getting added in a very short duration of time. The amount of data which will get generated is almost 30 times more than all the data at this time put together. So what it is actually doing is it is increasing the risk surface by liberating the data. In such scenario, what we as cybersecurity solutions provider need to do is to bring it together and bring the data to our control.

Venugopal N- Another thing is that the challenges involved with respect to securing the IoT landscape is humongous. There are different types of devices, different operating systems. These might have no space for doing something so basic as encryption because devices are really vast. So the challenge would be how to secure the IoT infrastructure not just at the sensor level but also through the air when the data is travelling through the air from the IoT devices. And this is where we are putting a lot of R&D efforts.

What are the key security solutions being deployed by various industries? What is the outlook for cloud-based solutions?

Harsh Marwah- So till now what has happened is that customers have been looking at fragmented solutions. If there is a problem, the immediate reaction is to safeguard that area instead of deploying a complete overarching solution. But one of the trends which is evolving very clearly is that hackers are looking at paths of least resistance. They will not come from the most fortified infrastructure of yours; they will find loopholes in something which has been unaddressed, maybe an app on a mobile. In the last three years, we have gone to the cloud, the endpoints have started going home, they have travelled all across the world and come back to office, and mobiles have virtually become our twin worker. Further, the way network has evolved; it has gone all over the place. Suppliers, partners, our networks and everything are becoming connected. And over and above if you look at manufacturing space that is where the big vulnerability is. The sector is still using those traditional industrial control systems which have been done for 30-40 years ago.

That is what is important and that's what some of the leaders, such as Check Point, are doing both from the supply side and the demand side.

What are your key offerings in the cybersecurity space?

Venugopal N- Check Point as an organisation is a pure play cybersecurity platform. We do nothing beyond cybersecurity. This includes any kind of security solution for network, cloud and mobility. Besides this we also look at advanced persistent threats which could attack your mobile, your network, your endpoint, or your cloud. So we have our portfolio which comprises all of this. The key thing here is to be able to share the intelligence between all this. And this is where our super glue comes into picture. So if somebody tries to attack your mobile device and you are able to block it, then that intelligence should be immediately passed on to your network or to your cloud because if the attacker is going to come to your organisation through that door, you already have the intelligence to stop it. This sharing of intelligence is also something we do through our portfolio. In totality, Check Point Solutions cover the entire cybersecurity landscape.

What are Check Point's growth targets?

Harsh Marwah- Targets is one aspect. I think at this point in time we can only say that we are growing much faster than the industry. We think this primarily because of two reasons- one is that the industry itself is growing through a typical transformation where every organisation is looking at the phase two of their cyber security readiness and some are typically getting into phase one. The second is that if you look at the depth and breadth of our solutions, there is huge adoption of cloud and mobile apps which creates the need for security solutions. So I think our readiness in terms of some of the emerging technologies is really leading the growth for us. Though the fundamental technologies are absolutely rock solid and doing very well, our work in IoT, cloud, ICS, mobility is really doing exemplary.

What are some of the challenges that you face in India as a cybersecurity solution provider?

Harsh Marwah- India is a very fragmented market. We always get the top of the pyramid-customers who typically have the propensity to invest in our solutions. But the bottom part of the pyramid, is still taking a little time to really get ready for this. This is because a lot of these customers feel that since nothing has really happened to them so they are safe. But the way we are seeing the trends, all the breaches are typically very devastating and on a very large scale, you never know whose going to get hit when. So investment by design proactively is something where we feel some of the challenges exist. But as I said the top of the pyramid is absolutely ripe for us to seize the opportunity, the bottom of the pyramid is where we have to do lot of work.

What are your views regarding the existing regulatory and policy framework on cybersecurity in the country? Do you have a regulatory wishlist?

Harsh Marwah- We did see a reasonable document in 2013 but I feel that it has to be a little more comprehensive. We all have to realise that the cybersecurity domain is changing by the hour. We have to keep evolving from a framework perspective also. Even in this space the market is fragmented. Some of the regulators are doing a phenomenal job, especially in the BFSI space, but the rest have to catch up. So a lot of comprehensive work has to be done. Also, thinking one step ahead of the framework is important. Once the framework is there, the guidelines are out in the open, organisations and various sectors know what is to be done, execution becomes key. I think that is something which is fundamental to overall readiness.

In terms of a regulatory wishlist, I feel regulators in each industry vertical must compel the organisations and enterprises to think through what kind of risks they are carrying in terms of their business. The moment they have assessment of the risks, the rest all will come. I think it’s more about awareness, giving that message in terms of sensitising the entire industry is something that regulators must do.

With increasing focus on enterprise mobility, what are the rising threats and how telecom providers can contribute to a safer environment?

Harsh Marwah- Just to give you perspective let’s see some numbers, the spend globally on mobility is 35 times less than the spend which we do on our endpoints. But the malwares that hackers created are typically ten times more than what we see in the endpoints. This is sweet spot for the hackers, this is a path of least resistance, and they will simply get into it. It’s very easy for hackers to get into a mobile and in order to curb it responsible behaviour has to

happen.

Venugopal N- Anitivirus alone is not enough. If you look at attacks which happen on mobility, every attack is a zero day, it's an unknown attack. What will antivirus do is it will stop known viruses but all the attacks that you see are more or less unknown. The second aspect is that if you connect to a free WiFi, an antivirus is not going to help stop or clean the traffic that goes from your mobile phone through the free WiFi. So you need to look at a holistic mobility solution. The third aspect is, I could get a phishing email, and an antivirus won't be able to stop it. The nature of mobile security is also changing; we need to look at mobile security more than just as antivirus security solution.

Telecom service providers are bundling anti-virus products for consumers, is it enough to secure applications running online? What more can be done?

Harsh Marwah- The telecom players are doing a good job in terms of bringing awareness that you have to do something on your mobile, at least start with the antivirus. But it's not good enough. I think they really need to understand themselves the risk landscape that mobility carries. And then perhaps tie up with the right set of partners and build it as part of managed services. This way they can actually serve a large customer base within short duration of time because finally at the end of the day the biggest challenge we have is that we are 1.2 billion mobile subscribers, obviously the smartphones are much lower, but still their size and scale is huge. So I think they need to start aligning with cyber security partners more comprehensively and give more comprehensive solutions.

With increasing deployments in enterprise hybrid cloud environment, what are the rising security concerns?

Venugopal N- In enterprise cloud environment, what we are seeing is that a lot of our data is in the cloud. And the biggest concern we are seeing is the mindset of the people to think that the cloud service provider is providing all the security. You are putting all your data and applications on the cloud, it is also your responsibility to ensure that the data is secure while the infrastructure is something the service provider would take care of. I think we are getting to a stage where we are beginning to educate people that it's no longer just about relying on the security provided by the service provider but also realising that it's your data that has to be secured by you. Why because we are seeing a lot of account takeovers happening. For something as simple as having your mail on the cloud, people are able to take over your

account. The second aspect is that we are no longer connected to the cloud just through a laptop, we are connected to cloud through a mobile device and you could have a weak link from your mobile to your cloud as well. So, it is a shared responsibility model between the enterprises which is hosting the data on cloud as well as the cloud service provider that needs to be taken into consideration for security needs.

What role would you like to see telecom services providers play in securing connectivity within enterprise hybrid cloud component?

Harsh Marwah- I think the telecom alone cannot do anything; it has to be a very well defined comprehensive role all across. So from a telecom service provider perspective, what they have to do is that they have to ensure the infrastructure is rock solid. By giving a cloud infrastructure doesn't mean everything is secure, you put your crown jewels on top of it, you are the custodian; your service provider doesn't really know what you are putting in terms of data and information on top of cloud. Now telecom players have a bigger challenge to tackle. Whether it is mobile apps, whether it is IoT devices, whether it is all other devices, it all rolls back into cloud. Now it is not only about safeguarding that, perhaps installing clean pipe into those cloud infrastructure is something they have to do. So just giving an antivirus on a mobile or something very fundamental is just ticking the box, they have to think much beyond that.