TRAILBLAZERS TALK

Ravi Kumar S, President, Infosys, with Jay Chaudhry, CEO, Chairman and Founder, Zscaler

Infosys
Navigate your next

Ravi Kumar

Hello everyone, my name is Ravi Kumar, President at Infosys, and welcome to this new chapter of Trailblazers. As always, this is going to be another exciting chapter on Trailblazers on Cybersecurity, a boardroom conversation in every industry. Today, I'm going to have a visionary in the space, Jay Chaudhry, the CEO, Chair and the Founder of Zscaler, a next-generation Cloud Security Company. A company which, believes in the philosophy of zero trust and is in the mission of making internet a corporate network for enterprises going through digital journeys. Jay is a serial entrepreneur, a technocrat, an innovator and his considerable work in security actually makes him a trusted advisor for many enterprises and partners like Infosys. Zscaler has some amazing traction with enterprises, and it’s reflected in its financial results and the fact that the stock has tripled in the last 12 to 18 months or so. Thank you for joining the session today Jay and thank you for your time today.

Jay Chaudhry

Ravi, thank you for the kind and generous introduction and thank you for your business partnership. It's fun to work together to help many of these enterprises with their secure transformation journey.

Ravi Kumar

Thank you Jay, and I've personally learned a lot from my recent interactions with you. And the first time I met you, I always thought, we have to get you on one of these chapters of Trailblazers for our audiences to know a little more about cybersecurity.

Jay Chaudhry

We all learn from each other every day.

Ravi Kumar

So Jay, you know, let me tee up the first question to you. You know, enterprise security has gained a lot of momentum with significant shifts because of rapid digitization, which was happening even before the health crisis. There is accelerated digitization because ironically, because of the health crisis, more enterprises are doing this. There is digitization and dispersion of sorts in some way as business models are getting dispersed. Unlocking itself out of the physical, physical setups into virtual hybrid setups. Software is getting embedded into products and services, and in a way, it has led to a significant shift on cloud and mobility. And I actually think the key for such acceleration is security and you know, network and security, I would say. And I think you're doing some wonderful work to get us to leapfrog into that space. Tell us a little bit about the advances in this space.

Jay Chaudhry

Ravi, as you said, digitization is happening because more and more digital information can be collected. That means we have better telemetry about customers, we have better telemetry about consumers, what they're buying, where they're going, what's happening, enterprises are collecting better data, and those applications are being built in the cloud. Where all of us are becoming mobile. So providing secure, fast, and reliable access to information, no matter where it sits, becomes extremely important. And that clearly is our focus. Zscaler’s focus was making secure, reliable, and fast access to the internet. If it's not secure, it creates big issues. We have been hearing so many attacks out there ransomware or private information. The challenge is, the security and networking model we had before, where the networking model was called hub-and-spoke network, bringing various branches together and castle-and-moat security is broken. That model said, if you're inside my castle, you’re good, if you're outside my castle you aren’t good. Well, applications have left the castle, users have left the castle. A new model had to be invented. And that’s what Zscaler did. We came up with zero trust architecture, and we're helping customers accelerate the digital transformation, securely.

Ravi Kumar S.

So Jay, thank you so much for that introduction. Tell us a little bit about zero trust. It's a very unique approach. I've heard you every time I've spoken to you. You pioneered this in a way. You also speak about zero trust platforms. You almost start with this assumption that everything is hostile. Establish trust and user identity and context and start from there. So tell us a little bit about how they switch from castle-and-moat to, castle-and-moat kind of gives you a little false sense of security if I may. Tell us a little bit about how that shift is so significant? And what does it take for an enterprise to have that zero trust?

Jay Chaudhry

Sure. If you look at about 30 some years ago when Cisco started as a company. To start networking, we connected various offices to each other so users could access applications sitting in the data center. And we built a moat of firewalls and VPNs around it. This model worked when applications were sitting in the data center and users are sitting in the offices. But that's not true anymore. So the zero trust model says, trust no one. It assumes that applications could be anywhere out there. There could be SaaS applications like Office 365, ServiceNow. There could be applications of the public cloud in Azure, A.W.S., or Google Cloud. And users could be sitting anywhere. If that's the case you can't be extending your castle-and-moat everywhere. It's just broken. The new model said, if you trust no one and you assume that applications are anywhere, users are anywhere. Assume that the zero trust security is like an intelligent switchboard, like a phone switchboard. A user comes and connects with the switchboard. We verify who you are. We verify what applications can you access and we connect a particular user to particular applications, never to the network. Otherwise, if they got on the network, they move laterally and that's when they can cause damage. For example, with the Colonial Pipeline attack, they stole credentials for VPN, got on the network, then laterally moved to find a billing application and held the company hostage. It's like you got in the castle, then you have free access everywhere. That model had to be broken. Legacy security companies who pioneered castle-and-moat, they did the work. It was a useful model. Now companies need to shift to zero trust. Unfortunately, inertia is holding them back. The biggest thing CISO's need to do is wake up and realize that a new model is needed, and that's what we have been advocating from day one.

Ravi Kumar S.

And Jay, would you now believe that your workloads on the cloud are much safer than on-prem? With this, you know, significant switch from a castle-and-moat to a zero trust architecture. Do you really believe that the transition has happened?

Jay Chaudhry

It is in process. It is happening. Progressive companies are already there, but many companies are coming along. I think it'll take some time. Take, for example, 35 percent of the Fortune 500 companies are Zscaler's customers. They're gone through this journey. But there's a long way to go. And part of that challenge ends up happening when new technology is invented, is that it disrupts incumbents. What we are doing with networking security is it's disrupting some of the traditional service provider models. It is disrupting some of the networking models and, of course, security model. So incumbents kind of like security vendors, they try to claim that they've become zero trust overnight. I like to say it's easy to build PowerPoint and claim stuff. It's much harder to build a cloud service that works. So it is work in progress. The changes, such as pandemic with COVID, it accelerated all of that stuff because we had to work from home. Some of the recent hacks on attacks and ransomware, is raising visibility that things must change. If you're spending billions of dollars on traditional firewalls and VPNs, why should attacks be happening? Well, the model is broken, so, I think it's our duty for all of us to raise awareness and visibility. And Biden administration has actually done a good job, through its EO to say you must embrace zero trust.

Ravi Kumar S.

And Jay, just a tee up on this conversation, of course, this is a technology-led transformation to secure workloads, users, applications on the cloud. How much is it to do with the other two keys in this transformation, which is process and people? And what do you tell us a little bit about, what is the people cultural renewal needed in enterprises? Are there those two or three big items which, you believe enterprises have to be aware of? Sure. On the people side.

Jay Chaudhry

You know, I was talking to the CIO of NOV, National Oilwell Varco, a sizable gas and oil company. The CIO said, 'it was easier for me to get budget for digital transformation than to convince my team that it's a good thing'. What he was talking about, the fact that the change of mindset, the change of culture is much harder. It's a change. Any time there's a significant change, it creates discomfort, especially as you go down the food chain. So education, finding progressive leaders, progressive people who actually can drive the transformation, it becomes a hard part. So people change from mindset and culture is important. Though COVID helped making that change because COVID showed that things can be done. The other part is process, now process always plays an important role, especially for larger companies. Things need to be done systematically. You can't change your enterprise network and security that you built over the last 30 years in days. It's going to take time and you do it in phase journey. Phase one, phase two, phase three. It also gives the leadership confidence. You do a good phase one. You get confidence. You've got people behind you and you move on to phase two and phase three. So technology, people, process all three things play a very important role.

Ravi Kumar S.

And, Jay, you know, that's very well said. In fact, one of the other things, a recent conversation of mine with the CIO and a CISO together was about, how clockspeed for businesses is so important? And tying security with static identity management makes them a little lesser on agility in terms of speed. And there's this concept of dynamic, dynamic identity management and dynamic security, which is kind of being evolved. How much do you think that is important in a digital world where you have to dynamically, intuitively, and intelligently drive policies across applications, data, and infrastructure?

Jay Chaudhry

Yeah, the two aspects. Your question is very good. The first part, in today's network centric security world, you deal with IP addresses. For example, an enterprise will say, my user, can go from this IP address at my headquarters to Salesforce. That model was OK when people sat in a couple of offices and they could put a list of IP addresses from which you could go to Salesforce. In today's world, when you work from everywhere, what IP addresses are you going to put? You try to bring the traffic back to the data center, a choke point to do this, IP address based authentication. It's silly. It needs to go away. The next level is it's user base authentication. That's where identity has been playing a big role in companies like Microsoft Azure AD. Companies like OKta have done a good job in building cloud based identity. It uses a standard called SAML. We at Zscaler, integrate with it so that changes from network-based security or IP address based security to user base security. You can have users and groups, that's being done widely today. All Zscaler's customers, whether it's Siemens or Shell or DHL or PNG or United Airlines they all use, user based identity not network-based. But there's a next level where we need to go. Identities can be stolen, so user identity alone is not enough. You need to check a few more contexts and the system should be smart to do that. What are those contexts? Well, maybe user location is good. Why should I allow someone coming from North Korea and do some of those things? It could be easily part of the policy to stop it. There could be other context, for example, managed device. You could have one set up policy access on, managed be another one. Maybe if you're trying to send information, that's confidential. The policy could be adapted. It can be sent to certain parties, it can't be sent to other parties. And all this can be automatically done based on behavior and using AI/ML. And those technologies are making it easy to operate these things and make them more smart. And those are the type of things we are driving along with our partner ecosystem.

Ravi Kumar S.

That's fascinating. In fact, I had a question, a very different direction but, and I'm sure you have a view on this. How much do you think we can syndicate across an interconnected, interdependent ecosystem with hyper scalers, with complementary players, and leverage data and AI to identify breaches, and to actually support, you know, threat identification in a way. How much do you think that is happening? How much do you think we could potentially do more, bringing the community together to deal with these issues?

Jay Chaudhry

I think it's happening at a small scale, but the world is waking up and it has to happen. Because otherwise this is a game with bad guys and they are getting in. Remember if they try 100 times, they need to get in only once, they can fail 99 times and they're still in. If we fail once, it's a big deal. So, while all of us are doing a whole range of security policies and whatnot, the best thing we can do is understand and analyze the data and traffic. For example, Zscaler collects all the logs when a user goes to Salesforce, Office 365 or SAP, wherever. The logs can be now analyzed with machine learning and AI to look for unusual behavior. And that unusual behavior can uncover compromised machines sitting inside the enterprise. That's a big deal. We are teaming up with vendors like Microsoft. They are able to share things such as failed authentication attempts. Before they try to compromise, they try to go in and try to crack passwords. Combining some of those logs with our logs, becomes very useful. Companies like CrowdStrike, they can share with us posture data, device posture. You combine these things, it becomes extremely useful, and machine learning allows us to go through tons and tons of data and look for some of those weird, unusual traffic patterns of applications and destinations and users. And that's how, more and more threat detection will be done. And I think it's great idea and we are driving that initiative with many of our ecosystem partners.

Ravi Kumar S.

Thank you, Jay, for that response. In fact, we are very excited about leveraging the hyperscalers ecosystem, with a community of players to see how security can be dealt with. You know, one of my passionate topics I've researched upon is, how do you mainstream you spoke about the bad, the bad player. How do you mainstream bug bounty programs? In a way, vulnerability disclosure policies, good hacker communities, and actually divert a lot of this talent and a lot of this concerted effort in supporting our networks, our enterprise networks instead of actually joining the bad players. I think there's a lot of work which can be done. And I don't know what your views on this topic are.

Jay Chaudhry

Absolutely. In fact, companies like yours, Infosys, can play a big role as you work with all of the key partners as well. In fact, even your previous even about the previous question. You are collecting logs from various parties. There's an important role Infosys can play. Analyzing and coming up with meaningful information. The data is sitting there, converting it becomes an important part in some of these other programs. Bug bounties of the world. I think, they are very useful. We actually use them to take advantage of it. But, the more important part is, information sharing about all these things we're learning from each other is extremely important. There are some programs in place for information sharing among vendors. I think a lot more could be done. FS-ISAC is a financial services nonprofit body that actually encourages it. We love to work with bodies like that. And the U.S. government is trying to encourage more and more threat information sharing. I think, which is very important because the bad guys come in, take a new phishing attack. There are millions of attacks coming every day. The damage gets done in the first 30 minutes. The sooner we can share that information, the sooner we can protect our customers.

Ravi Kumar S.

Thank you, Jay,That's wonderful. In fact, I'm going to squeeze in one last question. This is such an exciting and interesting topic. I can go on for hours with you. Tell us a little bit about how do boards assess the readiness of the enterprises they represent? This is a boardroom agenda. Many board members keep asking this question. In fact, I'm on one of the external public boards and we're always debating, how do we, what are those leading indicators for assessing whether we're doing okay on cybersecurity? Would you be able to give some pointers on this?

Jay Chaudhry

Of course, it is actually a big agenda, and I have talked to several boards in the past six to nine months. Especially after Solarwinds happened, and it didn't stop then Microsoft Exchange happened. Then we had Colonial Pipeline and whatnot. So, it's an interesting topic that actually boards are trying to learn and understand this topic. Which is wonderful, because that's where it all starts. In the past, the boards never thought this was an important topic. Now it is! That's the starting point. Number two, I think most boards are looking at saying, first of all, having people who have responsibilities, having a CISO, for example, in every company who actually reports directly many times to the CEO, has an important role to play. The boards are creating a risk committee now. And the risk committee actually works with the management team and external parties, to make sure they understand the risk that needs to be done. More and more boards are asking for doing what's called 'let's do risk assessment' by third parties, to see what is my risk posture, so I understand that needs to be done. And generally auto risk posture. There are some of the key steps that need to be taken. They are being taken. But if there's one message I'll leave with companies is, if you embrace cloud, if you sorry embrace traditional castle-and-moat; if your business depends upon firewalls and VPNs and the like, no matter how much money you spend, you will always have risk. The sooner you embrace zero trust, the better you will be from a security point of view because you're trusting no one.

Ravi Kumar S.

Thank you, Jay. That was, as always, a conversation where I've learned significantly. Every time I speak to you, I come back with some learning and some reflection about how corporate landscapes have to gear up for digital journeys. Thank you again. I'm sure my audience would have learned a lot, and therefore, they have some very important insights to carry forward. Thank you again for your time today and looking forward to our partnership with Zscaler.

Jay Chaudhry

Ravi, we thank you for the partnership. The last word I'll say is, CISO's shouldn't think about security as security. They should look at security as a business enabler because digital transformation has to be done securely. And CISOs are playing a more and more important role. IT is playing a more and more important role. And you and I both are there to help them. Thank you.

Ravi Kumar S.

Thank you, Jay. Thank you again for your time today.