ISMG
INFORMATION SECURITY
MEDIA GROUP

TATA
TATA COMMUNICATIONS

THE EVOLUTION OF MANAGED SECURITY SERVICES

Insights from Tata Communications' Avinash Prasad on where he sees the security-as-a-service market heading from a global perspective.

Prasad heads the business area of managed security services globally for Tata Communications. He has a multi-functional focus on customer management, practice and solution development, business development, innovation and partnership. He previously served in leadership roles at Wipro and Infosys.

Tata Communications' Avinash Prasad shares insight on the nuances and differences between what security-as-a-service represents, and what managed security services stands for – the evolution of the space and where it is headed.

In an interview with Varun Haran, associate editor with Information Security Media Group in Asia, Avinash Prasad, vice president and head of business for the managed security services division of Tata Communications, speaks about the nuances and differences between what security-as-a-service represents, and what managed security services stands for. He talks about the evolution of managed security services and shares insight on where he sees the security-as-a-service market heading from a global perspective.

Evolution of Managed Security Services

VARUN HARAN: Avinash, we would really appreciate it [if] you would tell us a little bit about where managed security services has come from? What is the pedigree, and what is the difference and the nuance between what security-as-a-service stands for, and what managed security services represents?

AVINASH PRASAD: Great, very interesting question and it aligns very well with my own experience and the way I've grown in the industry. What I saw was that the initial challenges that started presenting themselves in the IT security industry was really to keep the service at the levels that the enterprises needed to. How to even measure SLA's - there are many times where it's difficult to measure an SLA of an internal function, bring in that level of governance and control, and especially in the cases of, outages and challenges. How does one do any retrospective corrections there?

So what happened was organizations, really as part of the business buying pattern, started stepping out. Initially the search was primarily for the right kind of skills. But in the garb of consulting services, somewhere managed service started taking off, because it was seen as an opportunity by enterprises to bring in some measurability, to bring in some SLA's, and a better understanding, definition and boundaries around the scope; which in the internal function was difficult to set up - there were too many hand-offs, and the issues could always lie in one corner or the other. But with the service contract, with the service provider, one could look at it differently.

However buying security tools, buying technologies, deploying in on-premise was pretty much their DNA. Yes but managing it, operating it, for the benefits of, as I said, much better visibility of service, even cost control in some cases was driving that. So that's where it started, so I remember the time when we used to even talk about a service called SOC-in-the-Box, which was literally take the SOC and deploy it out of a box in the customer environment. From there, then things started evolving more and more, where the customer wanted to look at the possibility of remote shared services also.

> "I remember the time when we used to even talk about a service called SOC-in-the-Box, which was literally take the SOC and deploy it out of a box in the customer environment. From there, then things started evolving."

Clearly the initial moments for more of the Western markets, but then it expanded globally as well. Because of the benefits of what that kind of a more experienced, backed by threat research, that kind of a team could do for customers. And I think that has been one major shift up in the cyclical evolution of MSSP's, whereby they bring in a solid back end of processes, of capabilities, and start providing it in a managed services model to customers. So I think that was one big step up.

Now let's look at what is happening today, when we are talking about security-as-a-service. That's where one is trying to deal with issues of security technology clutter that many customers faced, and they said, "Hey there's too much, I've got way too many point solutions. I need to consolidate, I need to manage all of this, better orchestrate, and I don't know what's going on."

So therefore through an MSSP in a security-as-a-service model, one can achieve some of those benefits also in terms of the kind of consolidation that would be possible, and moving away from a point solution if one wants to do that, or a duplication of solutions also. The second part of it is the fact that these are very distributed organizations - mergers and acquisitions keep happening. The whole digital employment models have other implications. In this you know holding your cards, or in this case a security team close to your chest and being able to extend it, expand it, and create that kind of elasticity as a business model chain is not very viable at all.

So I think those are the natural business drivers which are there, and there's a lot of expectations from the business itself back onto the security teams. Does that mean that there's a lot of agility today in terms of adoption of security services? I'm not saying that either. The fact is there are always these concerns about loss of control. About not knowing whether they will get exactly what they want, or there will be some short cuts here and there. But those are the things that have to be really settled as in any other services contract through appropriate due diligence, through appropriate investigation, through appropriate agreement on the terms.

Managed Security Services vs. Security as a Service

HARAN: Great I think you covered most of it, so when you talk about demystifying security-as-a-service viz a viz managed security services, what are some of the common misconceptions that you hear from people? Also, what is the kind of traction that this particular evolution is seeing on the ground? You'll obviously be having so many people you speak to in the industry - What is the general outlook that you get?

PRASAD: Right, so first thing, I think in terms of demystifying security-as-a-service, because it's still, in a way, on one hand, dominated by starts-up - more of newer players who have come up in this space. New players and start-ups address some specific aspects or areas, again I don't want to name it but if you look at some of the magic quadrants and other things you'll find out, where some elements of security [are] being offered there. So security service doesn't mean that you could get all, any and all capabilities there.

So that's one part of it, the second part of it is somewhere the association of that with cloud service itself. Meaning that since there are very big brands and platform providers in the cloud services model, who are kind of driving adoption, and are really making customers move. I mean classic examples being Office365, and various other such applications, which have really made enterprises move, who all of them are doing it otherwise in-house deployed models. They have a direct influencing aspect also in security-as-a-service. Meaning that a lot of the evolution has happened to upport these

> "If business transforms, security has to transform all with it, and that elasticity and that agility provided by security-as-a-service."

initial workloads, these initial environments that are coming up live.

So even if you look at [a] security-as-a-service model today, many providers would pick up the value proposition that "Hey you're going to Office365, you know we can secure you. Don't worry all your data will be secure, and this is how we'll do it." So I think there have been certain catalysts and influencers for where security-as-a-service is going. So it is still an area, which is expanding, there are certain slices of the market, which get covered, maybe not everything is getting covered today in that way. Managed services from where it has come, obviously can cover pretty much everything for you, because there the options are, a fully managed to a co-managed model, customer-owned infrastructure versus provider-owned infrastructure. So it's much more of a hybrid play there, right? So, that's one part of it.

Where do I see things going though? I believe that things are going to go clearly in the favor of security-as-a-service. It's for no other reason but for the fact that if every other service that is going to be utilized, right, whether it is intelligence, getting data from the external environment, using applications, knowing more about your customers, everything else is also being leveraged with external sources and in a model of as-a-service - security will have to tie to that.

The customer challenges that I see in terms of lack of visibility, possibly lack of control, potential contract omissions, which could later on expose them to issues and threats and all of that. These are indeed certain things that I see and of course the fact that you know the concept of trust. Can I really trust the provider? Those issues are there, it's clearly a case of evolution, a case of maturity cycle as to how far it will go.

It'll be supported by industry bodies, by the other certifying bodies, others who are there, who will come in and help assess the broad-based shared environment and give certifications around that. So customers will have to rely more on that rather than doing their own separate independent assessment, which they may not be able to do.

So I think that's where some of those concerns will get addressed. But I still think business will be the biggest driver. If business transforms, security has to transform all with it, and that elasticity and that agility provided by security-as-a-service. I think that's the main reason why it could be a winner.

Is Security-as-a-Service for Everyone?

HARAN: I think what I hear you saying is security-as-a-service is to security as [the] cloud has been to IT. Something along those lines, right?

PRASAD: At this time from where I stand pretty much yes.

HARAN: Okay, but you know obviously there are, there is a business case to be made for it and the whole idea that it can help you cut down the technology stack that you have right now, which is growing with all these point solutions. It can help you slice that down and if you just push it over to somebody else. But does it make sense for every organization? Or is it going to be on a case-by-case basis?

PRASAD: Yeah, you know of course as we say, firstly the customer is king, and the second saying as it goes is, buyer beware. So I think some of those principles will come [into] play. Customers will make up their own minds, some customers will not want to go for it. I think that the whole aspect of it, doing separate due diligence, applying due care around how you sign up security-as-a-service contracts, these are the things which are coming into it. One obvious thing that we all tend to think of is, it's only for small and medium businesses. I would say that's still kind of a myth, right? Because if I were to just take your previous question, that would [be what] the cloud

"The customer challenges that I see in terms of lack of visibility, possibly lack of control, potential contract omissions, which could later on expose them to issues and threats."

has been to IT services, right? Security-as-a-service could be to security. Then I'd be saying that only small and medium businesses are going to the cloud or utilizing the cloud. But you already know the answer to that.

So if that parallel is going to broadly hold, then one myth is that only small and medium size of businesses would be doing, no. It will probably extend because of the complexity that large enterprises have, and yet the more transformational IT programs that they have to do, that they will have to align with.

So I think the whole market would be there, there could be issues, regulators, other worries on customers' minds, which will of course play into how they buy it. But it's for the entire market, absolutely and I think the future is only bright.

For more information, please visit us at:

https://www.tatacommunications.com/products-services/enterprises/managed-security-services

Full Interview: http://www.inforisktoday.in/evolution-managed-security-services-a-10037

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

91-22-71011500 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification.

ISMG INFORMATION SECURITY MEDIA GROUP

C-704 Marathon Innova, G.K Marg, Lower Parel (W) • Mumbai • 400013 • www.ismg.io