uberknowledge

# Ajit Sancheti, Co-founder and CEO, Preempt Security

## The Challenge of Identity in Security

Ajit asks where enterprise CISOs are finding their biggest challenges. He discusses the often-overlooked role of cybersecurity in the M&A process and suggests CISOs tell the board how they will manage risk post-transaction. He believes cooperation is the future of cybersecurity and sees mature technologies on platforms and bleeding-edge technologies as point solutions.

1:01 The network perimeter change means enterprises have to deal with many moving parts, but they often don't understand how to identify threats
1:37 There are an overwhelming number of threat alerts, 90 percent of which are suspicious but not malicious. The talent shortage means we are seeing enterprises chasing down suspicious threats with resources they don't have.
2:46 The principles of Preempt: maintain security, allow the business process to take place, don't use up scarce resources.
4:23 Customers aren't satisfied with detection alone they want to see response too.
6:45 Organizational structure. Enterprises are not monolithic. They have very clear security groups
7:21 Identity has been part of the infrastructure team and the IT team, not the security team.
09:02 Cybersecurity is simply not considered enough in M&A.
09:49 80 percent of dealmakers uncover data security issues in at least a quarter of their transactions.
11:31 What the CISO needs during M&A is visibility. Crucially, put in the tools to gain insight; do not rely on the security team of the acquisition.

13:06 CISOs do not have a veto in the M&A process so they need to tell the board how they intend to manage risk.
15:34 Identity is becoming a big deal for security because we have seen so many transformations in the workplace.
16:32 There's only two ways you can think of where security can be really effective. One is around the assets and applications. The other is around your identity.
19:03 There is no single pane of glass. You can't go to war with just tanks or just soldiers or just airplanes.
19:35 Maturing technologies will be platforms and emerging technologies will be point solutions.
20:34 Can't use just platforms or point solutions, CISOs will have to judge where to use which.
21:24 If CISOs can walk away from RSA 2019 having seen vendors being open with their technologies and each other, then the industry will be winning.

Ashwin Krishnan: [00:00:00] So welcome to another edition of the UberKnowledge podcast. I have the pleasure of talking to Ajit Sangcheti today, who is the CEO of a really interesting security company called Preempt Security. So over to you, Ajit. Can you tell the audience a little bit about when and why you decided to solve the problem that Preempt is trying to solve?

Ajit Sancheti: [00:00:23] Thanks for having me, Ashwin. A few years ago, in about 2014, as we started to look at the importance of cybersecurity, cyber became very, very important. We'd gone through some of the breaches like the Target breach. Security started to rise up on everybody's radar, especially in enterprises. What we noticed, my co-founder Roman Blachman and I, was that as we started to think about the network perimeter change when starting to go from static enterprise networks to hybrid to cloud to private data centers to an on-prem infrastructure, what was happening was that enterprises had to deal with a lot of these moving parts and they didn't really understand how to identify threats. That was the first challenge. The second challenge was how do you respond to that. A lot of times what we noticed was many solutions were

coming using analytics — you have behavior analytics, you have user profiling, things like that, most of those were trying to tell you if there was a problem. We all know that in many cases you have suspicious activity, but it's not malicious.

Ashwin Krishnan: [00:01:37] Right.

Ajit Sancheti: [00:01:37] And that might be up to 90 percent of the time. In fact, if you look at a lot of breaches, 90 percent of the time it's suspicious not malicious. You combine that with the fact that you're starting to see more and more of a lack of security talent. So now you have enterprises that are chasing down threats, and those threats may not be real, with resources that they can't really find.

[00:01:58] So what we said was if that is true, then how do you go and solve a problem not only to help with identifying and surfacing these issues but also verifying them in real time? If we as a security team can identify these threats and force a verification of that user, of that behavior, all that activity in real time, then you get three benefits. One, you verify. Two, you allow the business process to take place because you confirmed it. Once you confirm it, you know that the person is who they say they are, doing things that they are supposed to do. Three, you don't use up these scarce resources. So, you maintain security, you allow the business process to take place, you don't use up the scarce resources, and that's what we set out to do. How do you build a solution that can not only detect but also respond including inside the enterprise, inside the perimeter? Most of the time is focused on the perimeter itself. But once you get inside, nobody wants to be the person who's stopped the CEO from doing his job.

Ashwin Krishnan: [00:03:10] [Laughing] Right. Yeah.

Ajit Sancheti: [00:03:12] So we had to build a solution that could do the analytics and could also do the response. There are a couple of things you have to do. One, you have to do the analytics, and we chose to do it with identity behavior

and risk because that gives a good profile of what someone is. On the other side, we had to make sure that the responses were not just "allow" or "deny" because that's too coarse on the inside of the enterprise. So, you need a really nice fine-grained set of responses, allow, deny, multifactor, reauthenticate, isolate, SMS, text and then, like every other large enterprise where different rules apply to different people, you need a policy engine to tie the two together. And that's the genesis of how we started working on Preempt and here we are.

Ashwin Krishnan: [00:03:53] This is a great segue into the second question. A lot of what you're talking about here is something that I'm sure every CISO is nodding their head at vigorously. You talk about lack of security talent and the overwhelming number of alerts that they get and the alert fatigue that sets in. There were certainly a lot of assumptions that you put in place when you started Preempt. Name a few that got resoundingly validated, even to your own surprise.

Ajit Sancheti: [00:04:23] Well, one of the biggest risks we took was we assumed that people would allow response to happen in real time. And without naming names, one of the analysts that we talked to initially said the only place where you should expect to see response happening is at the end point because people will be willing to do some kind of automated response at the endpoint. And because we were sitting on the network itself that would be a bridge too far for a lot of customers. And in the beginning, yes, we felt that way in 2015, maybe 2016, but now a lot of customers are asking us when we tell them you can do detection with our product, they say I like the detection but show us a response, we want to build a response.

[00:05:07] Now for us, the ultimate validation and the assumption — getting to your point of how the assumptions get resoundingly validated — we thought went pretty far when Gartner came out with the framework called Continuous Adaptive Risk and Trust Assessment (CARTA). What that framework suggests is every digital transaction has risk, and the more you can do instantaneous and real-time verification, the more likely you are to be secure. And that's really what

we're doing. If someone's doing something, we'll be able to force them to do a multifactor authentication. If a service account is misbehaving, you can block it, allow it, have someone else respond to it. You start to get the insights and the responses. To us this validation means zero trust is along that path, CARTA is along this path. So those assumptions that we made are being validated. Also, the customer success we are seeing.

Ashwin Krishnan: [00:05:58] Got it. So along the same lines, what were some of the new learnings along the path that you maybe did not have in your sights when you set out? Suddenly you had new target personas and started thinking that's interesting for me. What were some of the things that that you discovered along the way that have made the offering more compelling? You mentioned one, which I'll just repeat for the sake of the audience, it's usually pretty coarse grain — allow or deny — but having this wider variety where you can pick and choose the response based on the kind of activity and the kind of suspicious malicious graft that somebody is or may be. What are the others that that you think recently emerged, whether it's IoT or AI. I mean, I don't want to put words in your mouth.

Ajit Sancheti: [00:06:45] I think I would put it in terms of the organizational structure. Enterprises are not monolithic. They have very clear security groups. They have very clear enterprise infrastructure groups. One of the key things that happened for us, and it took us some time to figure out, was the fact that we're using identity in a security-centric way.

[00:07:06] In many organizations, security has a play with identity. In some organizations, that I think are further along, identity is part of the security organization. In many cases identity is in an active directory.

Ashwin Krishnan: [00:07:20] Yes, it's IT.

[00:07:21] It's been part of the infrastructure team, the IT team and not about security. We did not acknowledge that strongly enough in the beginning. So,

what would happen is we would talk to the security team and they would say, "Oh, this is wonderful, this is something we want to do. We get this instantaneous response and we don't have to worry about chasing threats. You've improved our security, our SoC operations by 20 to 30 percent." I mean those are the numbers we heard. But then the IT team would say, "You're going to do what in front of my domain controllers? You're going to do what on my domain controllers?" And so we learned that we had to build capabilities for the active directory teams, the single sign-ons — Okta, the cloud infrastructure teams. We had to build capabilities for them, and we had to build in an enterprise capability that made us not a single point of failure, so that companies could go in and deploy us confidently. So, I felt that initially we did not, to our disadvantage, but at least we figured it out. In the early days we did not figure out how much we needed to cater to infrastructure as much as we needed to cater to security, and that was much harder than expected.

Ashwin Krishnan: [00:08:28] What you're saying is absolutely resounding in my head because this has happened to so many different companies. We start off with a single target persona in mind, and you don't realize the chasm that might exist within an organization and you target one. Once you leave the meeting, you don't know what's happening in the background. Kudos to you to actually be able to figure that out and realize that there's a different group within the same target customer that needs to be addressed.

Ajit Sancheti: [00:08:57] I wish we'd learned it sooner, but we didn't.

Ashwin Krishnan: [00:09:02] I want to focus on an article that your CMO authored, which I found to be amazingly intuitive as well as incisive, on M&A. When we think of mergers and acquisitions, we don't think cybersecurity, and this article put those two together in sharp focus. So, give us a flavor as to why this could be one of those weakest links that companies fail to see. In fact, I was reading the Momentum Cybersecurity 2018 report and the funding for cybersecurity companies was about $6.8 or $7 billion, and the M&A was $15

billion. So, I look at it purely from a numbers' perspective, this is where you need to be focused on cybersecurity. I mean, what's your viewpoint on that?

Ajit Sancheti: [00:09:49] Yes. There's great research. PWC had an article that was using research from Donnelley Financial Services where they actually, I think the numbers were in the range of 80 percent, 80 percent of dealmakers, the people who actually go do the big deals, they uncovered data security issues in at least a quarter of their transactions.

Ashwin Krishnan: [00:10:09] Wow.

Ajit Sancheti: [00:10:09] Okay, and that's just at a very global level. You dive down one step deeper, you look at the Verizon-Yahoo acquisition which, I think, ultimately ended up being in the range of $925 million. The fact that they had the breach delayed the transaction, it reduced the price of the transaction. And these numbers are really startling when you think about the fact that initially when people looked at acquisitions they focused on their business fit, their market fit, can we sell more, can we sell to the same customer, and on getting efficiencies of scale. Nobody ever said what are my risks that I don't understand, the risks were typically financial. Now the risks are also from the security standpoint.

[00:10:54] What we do notice is ... here's some very basic things that we see when people are doing M&A. They have this timeline that says we're going to start to do the integration. We're going to close the deal and then we're going to do the integration. And the first thing that happens is the IT security teams look at what they have to integrate, and they don't know what is there. They have absolutely no idea what legacy decisions that other company made, what the impact will be. They're always helping you but when you've institutionalized certain things in the target company, they don't think of that as unusual. But for the acquiring company these may be a no-go.

Ashwin Krishnan: [00:11:30] Right.

Ajit Sancheti: [00:11:31] So the first thing that from a security standpoint the CISO needs to think about is how do I get visibility into that other organization. How do I understand who's doing what? How do I understand where the identities are stored, are they disparate, are they combined? Are people doing things they shouldn't be doing? Is the security hygiene of the entire organization good or poor? What does that scale look like? I think for CISOs to get some level of comfort before they start to combine these networks together, they need visibility. And once they have the visibility they can start to do this.

[00:12:06] I'll give you an example. We saw two relatively small companies get together over 2,000 employees in the acquiring company and about 1,000 in the company that was being acquired. But the company that was acquiring only had six or eight domain controllers. The company that was being acquired had four domains and 46-48 controllers. They had no idea what was going on in that and why they had chosen to build the architecture that way. And so, the M&A aspect is pretty significant.

[00:12:35] If you don't have enough visibility, you will pick up long-term security risks without understanding it. So, the most important thing for CISOs to do is to first get the visibility and an understanding. Don't do it by asking the CISO or the security team of the other side, put in some tools to get the visibility. Once you have the visibility you can start to make some concrete decisions with data not with what maybe an out of date plan that you pick up when you look to diligence materials. So that's very important.

Ashwin Krishnan: [00:13:06] Yes. The other thing that struck me is it's getting more prevalent for CISOs to report to the board about the overall cyber-risk posture of an organization. This could be again one of those tools where post-M&A your risk might have actually gone up because I don't think we're at a point right now where a CISO has a veto power when it comes to M&A. Unlike a VP of R&D or a VP of Products who can look at it and say the talent isn't there or the product is

not mature enough. But at least you can talk about the risk profile changing post-acquisition and what you can do to get it back to acceptable levels.

Ajit Sancheti: [00:13:42] Yes. Well, it's just a week away from RSA. Two years ago, there was a session, a one-day session in conjunction with RSA, where there were board members being educated for an entire day on how to challenge and how to question and how to get information from a CISO. And I spent the entire day there which was very interesting because there is so much they have to learn. Now, boards are getting much smarter. They are finding one lead security expert as much as they can, an IT expert, and they're getting better. It will take time. Yes, to your point, you cannot as a CISO impact the transaction, but you will have to deal with the impact of the security post-transaction.

[00:14:24] So the best thing you can do for your board is to tell them how you're going to go about solving the problem. How you're going to think about the integrations. How you're going to think about bringing the two teams together and not just from a networking standpoint but also from a security posture, from security behaviors. What is allowed and what is not allowed. Some of these things are cultural and they're going to take time.

Ashwin Krishnan: [00:14:48] So let's go back to identity. I know this is a central theme and I'm sure that's going to be a big theme at RSA. You mentioned earlier the complexity when it comes to diverse environments going to cloud, hybrid, etc. Has the definition of identity evolved? I mean the conversation we just had about different groups being in charge. From a security standpoint an IoT device or a sensor could be a device with an identity. It might not be on the AD Auth domain from an IT perspective. So how has the definition of what identity means to security evolved, given your vantage point of talking to multiple stakeholders within an organization?

Ajit Sancheti: [00:15:34] Identity in most general cases is tied to some kind of human or a service account or a programmatic account or pick one of those versions of it. It's primarily tied to that but devices are becoming just as

important. Let's hold that thought for a second. Just from an identity standpoint, why is it becoming a big deal for security? Look at all the transformations. We've gone from very static enterprises to remote workers. We've gone from contractors, from people engaging, the nature of work is changing so the role of employees is changing. That has become dynamic. Now, even banks are allowing people to bring in some of their devices. You won't get access to everything that you want to get to, but you can bring your own devices in. So, people are doing a lot more and that's changed. The second thing is we've moved away from applications being on-prem or in private data centers into the public cloud. So it's changed from that perspective. Everything has become dynamic.

[00:16:32] There's only two ways you can think of where security can be really effective. One is around the assets and applications. The other is around your identity. Because everything else is amorphous. So that's why identities become very important. Now identity by itself is not sufficient, if the device underlying it is not that secure. So the identity of the device — we're using identity a little bit more loosely here — it's more about the posture of the device itself. Because one of the things you want to know is when you do have an issue is, what is the blast radius? If someone used this device, who else used it? What did they use it for? What were the other activities that happened on this device? That becomes just as important. So, in an IoT world there will be a lot of importance given to the device, but it will be in the context of who and what happened on that device. And that's usually tied to a human or a service account or ... think about it in a hospital, more than people there are machines, and they are all to some degree an identity.

[00:17:34] And so the concept of identity has changed. It's become more about humans and devices. But there will be a very tight linkage between the two, especially if you want to understand sophisticated threats more than just things like run-of-the-mill vulnerabilities that you see on IoT devices, which is going to be around for a long time.

Ashwin Krishnan: [00:17:54] Yes. I think that battle is just starting. One of the other things you mentioned, talking about false positives or just the cyber-skills shortage and the number of alerts that the security admins are faced with, one of the so-called panaceas that is being offered is everybody is a platform. Come integrate with me and I can be this single pane of glass. Probably one of the most overused phrases. Given your conversations ... I mean we've seen best of breed. We've seen let's integrate all these point solutions and let's have this this really robust environment and have humans be the point of distillation. Now saying that's too much, let's put all our eggs in the platform approach, is there truly a one size fits all? Is it going to be still in this kind of a heterogeneous world where there's going to be one solution, there's going to be platforms, some integration? What's it what's your thought?

Ajit Sancheti: [00:19:03] Good question. Have you seen an army go into battle with only tanks or only people or only airplanes? It's very difficult to fight a really multifaceted battle with one solution. On the other hand, if you look at it from a security standpoint there's probably 3,000 or 4,000 different vendors offering different angles of different security challenges. If I was a CISO, I wouldn't know where to start because everybody sounds the same. It's crazy.

Ashwin Krishnan: [00:19:33] [Laughs] It's refreshing to hear that from a vendor.

Ajit Sancheti: [00:19:35] Everybody sounds the same. The noise floor has gone up, but the noise is still the noise. What I do think is it cannot just be a full platform play or it cannot just be point solutions. What you're going to find is, as technologies mature they will start to show up more and more in the platform environment. And the technologies that are emerging will be point solutions. And it's nothing, that's not radical. It's just a chance for enterprises to say the innovation in this kind of technology has come to a plateau. Let's build it into a platform. Let's buy it from a good platform vendor, especially a platform vendor that can play well with emerging technologies. And so, I don't think that you're going to end up with only point solutions or only one monolithic platform. You're going end up with both, but you're going to make that decision based on the

maturity of the technology and to some extent also the industry that you're in: finance is different than healthcare is different than industrial, law firms, things like that.

[00:20:34] And that's really how I think people will think about platforms versus point solutions. It's not one or the other but you're going to figure out where it makes sense to be platform, especially mature technologies, otherwise you go for the bleeding edge. With bleeding edge, you do have the challenge that it could be incomplete. It could fail. The technology might fail. But you're really doing it because you understand the risk reward from that bleeding-edge technology.

Ashwin Krishnan: [00:21:02] That's probably the most comprehensive answer I've ever got from a platform versus point product question.

[00:21:09] Any parting thoughts? We mentioned RSA a few times and it's less than a week away. What would success mean for you at RSA 2019 as the CEO of a hot startup?

Ajit Sancheti: [00:21:24] Surviving. [Laughing] Likely everybody says the same thing. On a more serious level, I think what I want to leave RSA with is a better understanding of where enterprise CISOs are finding their challenges. If we as vendors are not solving those in a scalable way, we're not solving them without having them go find resources that don't exist, I think we will fail. But to the credit of most vendors they understand that. So more and more and you are starting to see that when vendors talk about product, they talk about how open they are. They talk about what kind of problems they solve, how they play well with other products. And you will see more of that. If you see less of that kind of openness between different technologies, I think that RSA would have would have been a waste of time. But I do think CISOs are going to leave saying these products are starting to work together better and more naturally through APIs, through integrations, things like that. And that would be a win. If that happens I think we've made progress.

Ashwin Krishnan: [00:22:30] Collectively we're resolving the bigger problem rather than trying to fight it. Great parting thoughts. Again, thanks so much. Looking forward to future engagements as well.

Ajit Sancheti: [00:22:38] Thanks, Ashwin.

Ashwin Krishnan: [00:22:40] Thank you.