Rapid Response Transcript – Sudhakar Ramakrishna

“Urgent lessons from a cyberattack”

Click here to listen to the full Masters of Scale: Rapid Response episode with Sudhakar Ramakrishna.

> **SUDHAKAR RAMAKRISHNA:** We were the victims of one of the most sophisticated attacks, which has been attributed to a nation state.
>
> In every one of these attacks, you can always learn something that had you done those things, could have either dissuaded somebody or prevented it.
>
> Every enterprise must look out and protect its infrastructure, its data sources, and do the very best to train its users to protect its assets.
>
> At the same time, it is very difficult for any one company, no matter how many resources we have or how large we are, to be fully protected.
>
> Now that we have been thrust into this spotlight, we have to galvanize the industry and speak up and actually actively contribute to that.

BOB SAFIAN: That’s Sudhakar Ramakrishna, CEO of SolarWinds, the tech provider that became synonymous with cybersecurity risk late last year after a sophisticated attack compromised its software, potentially affecting thousands of organizations.

I’m Bob Safian, former editor of Fast Company, founder of The Flux Group, and host of Masters of Scale: Rapid Response.

I wanted to talk with Sudhakar because, in our increasingly digital world, cyber-risk has become an ever-present threat to scaling, whether you’re a startup, a brand-name platform, or even a government.

Sudhakar joined the company soon after the breach was discovered, thrust into a crisis that included leadership challenges, technology challenges, and business challenges.

His experiences illuminate what you can control and what you can’t, and how putting in place what he calls a framework can clarify your actions.

He also discusses the brand hurdle Solarwinds faces, and the ways in which he’s trying to turn the negatives of the crisis into an opportunity.

Cybersecurity needs to be anticipated, Sudhakar says, because no matter who you are, it's going to find you at some point, one way or another.

[THEME MUSIC]

SAFIAN: I'm Bob Safian, and I'm here with Sudhakar Ramakrishna, the CEO of SolarWinds. Sudhakar, thanks for joining us.

> **RAMAKRISHNA:** Thank you, Bob. Thanks for having me.

SAFIAN: So you've been CEO for less than a year, but it's been an eventful year. You were announced last December, and between the time you were announced and your taking the post in January, the company became aware that it had been a victim of a cyber attack. And not just any cyber attack, it was described as one of the most sophisticated and complex ever. SolarWinds provides IT software to thousands of places, and suddenly all of them were potentially exposed. So SolarWinds moved from relative obscurity to becoming this sort of household name, although not necessarily for what any business or CEO would hope for. So when you come into a situation like this, what do you do first? This wasn't what you expected to be handling when you agreed to do the job.

> **RAMAKRISHNA:** Absolutely, Bob. As you said, this was an eventful phase of my career and my life. You don't really prepare for these types of situations. But our collective experience over the years allows us to create a set of guiding principles. And if you had the humility to continue to learn and iterate on those, then you can start making progress. So that's the approach that I took.

SAFIAN: Well, you had some experience in the cybersecurity area before coming to SolarWinds. You had been most recently the CEO of Pulse Secure, which provides secure access. How do you know what to do and what order to do it in when something like this arrives?

> **RAMAKRISHNA:** So first and foremost, I did look at the security posture of SolarWinds. Like many CEOs who come into a new situation, you have already met the team, you've understood the situation, and you start building your 90, 100 day plans. In my case, I had to basically throw everything out the window and reset my plan. Because what needed to be done at that point in time, given the event, is taking care of your employees and taking care of your customers. That was the primary – and I would say – the only obligation. My previous experience dealing with cybersecurity issues definitely did help me address this. You look at what were the security investments, were they commensurate for a company of our size and scope, were there any obvious deficiencies, and so on.

And the way I would describe it is SolarWinds investments in security, as well as the tools we were using to establish our security posture were consistent with the industry average, and in some cases better than industry average. So it wasn't so much a negligence or a deficiency. We were the victims of one of the most sophisticated and I would say patient attacks, which has been attributed to a nation state.

SAFIAN: But if I'm hearing you, sort of, the standard at SolarWinds was up to par for the industry, but still hadn't been good enough to protect from this attack.

RAMAKRISHNA: If I can be so bold as to say, if a determined nation state is after you, they can probably create an attack and breach through anything. So it is less to do with one specific company's resources or posture. But equally I'll be the first one to say that in every one of these attacks, you can always learn something, that had you done those things, could have either dissuaded somebody or prevented it, but this is the nature of our industry. This is the nature of the security industry, because if we had a blueprint for having no breaches at all, we would probably all be adopting it.

SAFIAN: Yeah. You mentioned nation state, the U.S. Government Cyber and Infrastructure Security Agencies, CISA, I think...

RAMAKRISHNA: Yes.

SAFIAN: ...is the acronym part of Homeland Security Apparatus. They've attributed the attack to state sponsored actors out of Russia.

RAMAKRISHNA: Yeah.

SAFIAN: You didn't know that right away, or did you know that right away?

RAMAKRISHNA: No, we did not know that right away. At the same time, while SolarWinds provides mission critical applications and capabilities to customers, I don't characterize us as a classical security company. Especially as a company that does security investigations for instance. That's not our strength or sweet spot. So we had to rely on outside experts to be able to do some of that work.

SAFIAN: There were initial reports that like thousands of companies, of your clients could be affected. And then it was revised to like fewer than a hundred.

RAMAKRISHNA: Let me actually set some context on that, Bob. The way we came up with the initial estimate of the 18,000, which is what we were reporting, was because of our data that said 18,000 customers approximately downloaded that piece of software.

SAFIAN: Right. This was a routine software update?

RAMAKRISHNA: Exactly. That they downloaded. So that is the largest possible set of customers that could be impacted. But as you know, in these cases what happens is customers sometimes download them, but don't deploy them. In which case, there is no harm done. In some cases, customers deploy them, but configure it in such a way that the software is not able to connect back into the internet. In which case, again, the malware cannot do anything. So if you start sifting through those, eventually it came out to be an estimate of less than 100, some said 60, but let's just say less than 100. Our focus was, let's assume all 18,000 were impacted, touch each one of them, make sure that they were updated and upgraded and worry about the rest after that fact.

SAFIAN: I think a lot of businesses sort of assume that the government or prior to this maybe, assume that the government was protecting them from state sponsored actors like this. And this sort of ripped the veil off of something that makes a lot of businesses, smaller and larger than yours, anxious about what's my responsibility to worry about and what's going to be policed by others. How do you think about that question about where the responsibility falls and what we've learned from this?

RAMAKRISHNA: My view on this, and this is a view that I've held well prior to joining SolarWinds, is that every enterprise must look out and protect its infrastructure, its data sources, and do the very best to train its users, meaning its employees, to protect its assets. At the same time, I also believe that it is important for us to be part of this community. You probably have heard me use the word community vigil as it comes to security, because a simple matter is that threat actors have to be right once to breach through. We have to be right every single time to protect ourselves. And especially when a threat actor is a nation state actor, it is very difficult for any one company, no matter how many resources we have or how large we are, to be fully protected.

So in that world, we have to have a very tight partnership of transparency and collaboration, both amongst the community, as well as with the authorities and the regulators. So you mentioned CISA earlier in the conversation, and that is a body which we are actively working with to support two-way collaboration and communication.

SAFIAN: There's been some news of late of regulators asking for more disclosure from companies about security – not necessarily from a cyber security point of view, more from a financial markets point of view. But it sounds like the more sharing of this information that there is, the easier chances we're going to be able to identify patterns.

RAMAKRISHNA: Most definitely. At the same time the point you made about the regulators is a key one. I think more disclosure is definitely important, but it should be done in an environment where victims don't feel ashamed about coming out, or the discoveries are not done with the intent of leading to punitive measures. That's not to take away accountability and responsibility from enterprises, such as us. We have an

obligation, responsibility, and have to take accountability. But if we are constantly worried about who is going to sue us or who is going to be punished for coming out and saying what we think will be better for the larger community, then we're going to be hesitant about doing it.

SAFIAN: This fear of liability will have people resist being as transparent as they might be?

RAMAKRISHNA: I believe so. I believe so. I believe there are some progressive senators like Senator Warner, who are talking about how do I indemnify you for coming out early and speaking about these types of issues?

SAFIAN: In February you testified in Congress alongside Microsoft President Brad Smith and FireEye CEO Kevin Mandia. When you're asked to testify in Congress, you could feel like everyone's looking at you, that idea of blame or shame. Was that part of that experience?

RAMAKRISHNA: Yes, at some level, Bob. But my focus going to the Senate was to directly and transparently communicate what SolarWinds had done and was committed to doing. This was a great opportunity for three great companies to come out and talk about what we can do for the future.

SAFIAN: As you were preparing for that testimony, at the same time you were preparing for your first earnings call, working with a team that was new to you, and you were new to the team. How did you approach that leadership challenge?

RAMAKRISHNA: The approach that we took was first and foremost, when you deal with an issue like this you got to have a framework of how you have to solve this problem. The framework also has to be fungible because you learn new things every day, and you have to adapt to it, but there has to be a framework.

The second part of it is the transparency associated with it, with employees, customers, your partners, on what's happening, what do you know, what is next. You have a framework, you have transparency, you have to work with a great sense of urgency because you gotta act and start making progress. But equally you have to demonstrate a sense of humility as you go through this urgency because nobody knows how to solve these problems. It's framework transparency, communications, humility, and doing it with a sense of calm across the board. And so I would say we were leveraging all of those principles across the team. We call ourselves Solarians, by the way. Having them on my side helps me a lot in doing my job.

SAFIAN: This concept of a framework, can you explain a little bit more what the framework is, and why it's so important?

RAMAKRISHNA: Definitely. The framework I used here is called secure by design, and I take you back to the comments about, was there anything deficient, was the investment enough and so on? There's always things that you can do to improve. I'm an engineer. I've built software. Just like you build quality software, you build secure software. The framework had three key pillars. One was: how do we improve the infrastructure security and infrastructure posture of SolarWinds better than what it ever was before? How do we make it best in class?

Two is: given the unique nature of the supply chain attack, how do we protect and secure our build system, software build systems to the next level? The third is: can we innovate in the build systems themselves such that it makes it difficult if not impossible, for a threat actor to break into your supply chain? Those were the three pillars.

The reason for that framework then is, if I look at any particular employee in the organization they should be able to relate to, “I'm contributing to that pillar, and these are my actions.” Independence is very, very important because without independence you cannot act with a sense of urgency. But then interdependence is also extremely important because, without that, you cannot support a broader mission or a broader framework. Independence and interdependence became part of the fabric and the value system of the business.

SAFIAN: Can you give us an example of a track you were going down and then you learned something and you adjusted?

RAMAKRISHNA: More than I can count. When you have an issue like this, Bob, the first thing that you have to be open to is establishing hypotheses. Could this have happened? Did that happen? One of the very early hypotheses: when you are in a global company with presence all over the world, could this be an insider job? If it is, then you act on it. In that vein, for instance, we came up with multiple hypotheses.

I had the unique vantage point of being an outsider coming in so I was not biased, so to speak, by anything that was happening inside. I came up with my set of hypotheses, the team had some, we pooled together, and we said we'll go after every one of these and figure out, where does it lead us? Many led us to nowhere so we had to keep reinventing or recreating hypotheses.

[AD BREAK]

SAFIAN: Before the break, we heard Solarwinds CEO Sudhakar Ramakrishna recount how he responded to a high-profile cyberattack. Now he talks about how the episode impacted Solarwinds’ brand and business. He offers practical advice to other leaders about how to best protect yourself from cyber risk and how to respond when you do find yourself in the crosshairs.

I know there are different labels that have been used to describe this particular attack. The government said that it shouldn't be labeled SolarWinds, but of course that was the dominant association in the media and the marketplace. From a business and a brand point of view, what can you do about that? Did you think about changing names?

> **RAMAKRISHNA:** That has been suggested to me, Bob, and I had the freedom to do that, even from my board. When I think about brand, brand is a function of my people, my products or offerings, and my customers, meaning what value I deliver to them. Yes, name is significant, but those are the three things that we should really be focused on. There are a few reasons why I chose not to think about changing the brand or the name of the company immediately. One is: the most critical thing here was addressing the issue at hand, which is the security breach and the safety of the customer segments. By changing the name and spending time and money doing that, we're distracting from the job at hand and potentially coming across as swiping an issue under the rug. So that is fundamentally opposed to the approach of saying, we are going to be transparent, collaborative, and communicative. Two is, focus all your energies on the problem at hand and not try to deviate from it. It was painful, I will tell you, because it should not have been called the SolarWinds breach. As you said, even the government agrees with that.
>
> Would I wish that there was a more generic name attributed to it? Yes. But I would say that by serving the primary obligation we have, in the long run, I'm confident we'll come out better.

SAFIAN: And just a quick side question, just to clarify for some of our listeners. This term, supply chain attack that we have used, can you explain what that term means? Because it's not specifically about a traditional view of a supply chain, but more of a technology supply chain.

> **RAMAKRISHNA:** Yes. More specifically in this case, software supply chain. In a traditional supply chain, let's say physical parts. Let's say you're assembling a television set. You are taking electronics from different sources, putting it in a supply chain, and then assembling it towards the end, and shipping off a finished good. The process in software supply chain is very similar in the sense that you take various pieces of software or code, as it's called, and you compile them. So compilation is similar to assembly, and after you compile it, you ship it. So what a supply chain attack is, is from the time you collect all these pieces of code to the time you compile them, if a threat actor were to inject, let's call it another piece of code into that, and you inadvertently compile it and ship it, then in a sense, the malware becomes part of what you actually shipped to customers. And so that's what a supply chain attack is.

SAFIAN: And because your own distribution is so broad, that malware is getting into lots of places.

RAMAKRISHNA: Absolutely. And I've been asked, why did you think you were picked? Why were you the victim? And I have been describing it to some degree as this is a price you pay for ubiquity. Meaning, we are deployed in over 300,000 customers. And so we can be a very large target. So for instance, if you look at breaches that are reported, or I should say security vulnerabilities that are reported in the industry, Microsoft ranks very high in the list. I attribute that to their ubiquitous nature, not because of necessarily deficiencies in what they do. So, that's kind of the connotation here.

SAFIAN: Yeah. If you want to have impact, you go to the places that have the broadest reach and the biggest impact. I was asking you about the brand name and the noise around that. Are there any positives to the notoriety that has come to SolarWinds? I mean, the company's certainly more widely known, if not for the ideal thing. Are there any business opportunities that can be unlocked from a crisis like this?

RAMAKRISHNA: Yes. As long as we stay true to what we are trying to work towards, which is first and foremost, learn from this and improve. Many customers since the time of the breach have expanded with SolarWinds because of how we are approaching secure by design tenets.

The fact is, many of my customers are also producers of software. So they appreciate that if it can happen to us, it can happen to them as well. They want to protect themselves ahead of time, so to speak, but it also allows us to serve them on a broader scale. And as a result, enjoy better business success as well.

SAFIAN: Through the pandemic certainly, through this era we're in, all companies are more and more dependent on technology. In some ways every company has to be a technology company today. A lot of the folks listening today are business leaders, some at smaller startups, may be dependent on technology, remote access in ways they never have before. How can we learn from this?

RAMAKRISHNA: The first thing I would focus on is awareness inside the company: security awareness, security training, and behavioral training of the employees. More than any technology that we can deploy, that has to be a priority. Phishing attacks and spear phishing attacks are one of the most common ways in which threat actors gain access to your environment. The percentage of users that are clicking on synthetic attacks is still very, very high. As high as 40% in an enterprise.

We did a recent IT trends report where we interviewed various professionals in the IT sector. What are the trends? What are the concerns? Lack of trained personnel always seems to be at the top of the list. And so we just need to keep training our people better and better and better.

SAFIAN: As you described this need for better security hygiene, say, that existed before this attack though, right? So is it that there's not that much different that people should be doing today than they would've been doing a year ago, even though all this new activity has come to light?

> **RAMAKRISHNA:** I unfortunately think the basics still remain the same Bob. And this is more of a human and a behavioral aspect, which is, as long as it doesn't hit me, I continue to believe it won't hit me. And this is true in jobs and in economies, and unfortunately true in security as well.

SAFIAN: What's next for SolarWinds? Do you know the point where you say, okay, crisis over, we can go back to our regular planning? Or does the impact of this change your business forever, like indelibly?

> **RAMAKRISHNA:** I would say it did change it indelibly, but I hope for the better. In 2021 we basically established one primary goal, which was to support our customers come back online, and customer retention is our number one priority. And so, eight months, or two quarters plus, into this journey, I am pleased to say that that has panned out.
>
> Equally, we have ambitious plans of continuing to build on our capabilities. Customer environments are becoming more and more complex as we all know. Cloud and deployment of cloud, both pre-COVID and post-COVID are accelerating. That creates many more areas where there could be security issues, management issues, monitoring issues for customers.
>
> And in this world, customer budgets are not increasing commensurate to their needs and their complexity. So what can we do at Solar Winds to support them in those needs? And so that requires us to continue to deliver powerful solutions to address those multitude of needs, but do so in a simple fashion that increases the productivity of our customers.

SAFIAN: So I'm not hearing in your voice like, oh, if I'd known this was happening, I would never have taken this job in the first place.

> **RAMAKRISHNA:** No.

SAFIAN: This is not what I signed up for.

> **RAMAKRISHNA:** No, it was definitely not what I signed up for, but I look at it as an opportunity, as I like to say, an opportunity to learn, an opportunity to serve, and an opportunity to grow.

SAFIAN: So what do you feel like is at stake for SolarWinds now?

RAMAKRISHNA: What's at stake for SolarWinds now is taking the obligation of being thrust into the limelight. I would say SolarWinds was perfectly happy not being in that limelight and simply focusing on customers forever and ever. But now that we have been thrust into this spotlight, we have to be more transparent, be more collaborative, galvanize the industry around these topics, and make it okay to speak up about those, and actually actively contribute to that. So speaking of contributions, the innovations that we are doing in building better and more robust supply chains, we could use that as proprietary information, but we have decided that we are going to publish that broadly for the benefit of the broader community. So that is an obligation that has got a certain cost involved in it. And so, my commitment is that we will continue to support that going forward.

SAFIAN: And if I'm a business leader or a CEO who's listening to this, and I have just learned, or I'm hearing about a potential breach at my organization, what's my roadmap? Like what are the things that I should be doing when I'm faced with that?

RAMAKRISHNA: I'll go back to the basics on that, Bob. And the unfortunate fact is if you are a business leader, it's probably more likely that you have to deal with this issue than less likely, no matter what your level of preparation is. So you might as well start thinking about a framework, similar to what we did with Secure By Design.

Two is, I would be relentless in my communication with my customers and my partners and my employees in terms of what happened, what do you know, what are you doing, and what's next? There's no reason to hide from those facts and getting out there is more important than anything. Three is, leverage others. And they could be competitors. They could be unrelated, but it didn't matter. So making this a community vigil, a community event, and learning from others, and applying it to your context.

And then be humble. There is no such thing as "I won't be breached because I'm too secure or too smart." You could be breached. And when it happens, be humble. Learn from it, adapt, and act with a sense of urgency.

SAFIAN: Well, Sudhakar, this has been really fascinating and instructive. Thank you so much for spending time with us.

RAMAKRISHNA: Thank you, Bob. It was my pleasure.