Center for Strategic and International Studies

Online Event

"Lessons Learned from a Cyberattack: A Conversation with SolarWinds (Part 1 of 2)"

Part 1: Fireside Chat with the CEO of SolarWinds

RECORDING DATE:
Monday, February 22, 2021 at 2:15 p.m. EST

FEATURING:
Sudhakar Ramakrishna,
Chief Executive Officer,
SolarWinds

CSIS EXPERTS:
Suzanne Spaulding,
Senior Adviser, Homeland Security, International Security Program,
CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Suzanne Spaulding:

Welcome. I'm Suzanne Spaulding, senior advisor for homeland security at the Center for Strategic and International Studies, where I lead the Defending Democratic Institutions Project. Today I have the privilege of introducing and talking with Sudhakar Ramakrishna, the CEO of SolarWinds.

It was on December 9th, 2020 that SolarWinds announced that Sudhakar would be the new CEO of the company, in a transition that had been in the works actually for several months. And then it was two days later, according to published reports, that FireEye informed SolarWinds that during a FireEye breach investigation they discovered that updates to SolarWinds network management software, called Orion, had been corrupted and weaponized by hackers. As many as 18,000 customers had apparently downloaded those updates, although the number of entities actually compromised seems, so far, to be much smaller.

In a briefing last week, the Deputy National Security Advisor for Cybersecurity Anne Neuberger said that to date approximately 100 private-sector entities and nine federal agencies are known to have been compromised. Among those federal agencies are the Department of State, the Department of Homeland Security, the National Institutes of Health, parts of the Pentagon, the Department of Energy including the National Nuclear Security Administration responsible for managing our nuclear weapons stockpile, the Department of Treasury, Department of Commerce, and then lots of states and local governments.

As these government agencies and private businesses did the forensic work to see if they'd been compromised and the scale and scope of that, they found evidence of other vectors besides SolarWinds that may have been part of the same campaign. The Wall Street Journal reported last month that around 30 percent of victims have no ties to SolarWinds' products, widening the scope of the breach. A Reuters investigation revealed that suspected Chinese actors also leveraged a SolarWinds software flaw, alongside what has been presumed to be a Russian campaign. The Chinese actors targeting a federal payroll entity.

While at the moment it doesn't look like the hack went beyond IT networks into industrial control systems or other operational technology, we don't yet know what the adversary's objectives may have been. And as Neuberger noted in her briefing, there's concern about the ability of this to become disruptive. We will be months if not years figuring out the scale and scope of the malicious activity, and at least as long eliminating the threat from all of the affected computers, systems, and networks. This week Congress begins its investigations into this hacking campaign with a series of hearings.

But today we have the opportunity to hear about this hack from the perspective of the CEO of what seems to have been the first victim –

SolarWinds. Sudhakar Ramakrishna brought to SolarWinds nearly 25 years of experience in the IT business, most recently serving as the CEO of Pulse Secure, a company that provides secure and zero trust access solutions for hybrid IT environments. Prior to that he served as the senior vice president and general manager for the enterprise and service provider division at Citrix, where he had responsibility for their portfolio of virtualization, cloud networking, mobile platforms, and cloud services solutions. He's also held senior leadership roles at Polycom, Motorola, and 3Com. He's served on public and private company boards and is a partner at Benhamou Global Ventures, focused on investing in emerging startups in the fields of security analytics and applications.

Sudhakar earned a master's degree in computer science from Kansas State University and a master's of management degree from Northwestern University's Kellogg School of Management.

We are so pleased, Sudhakar, that you have agreed to join us today. Welcome. And for my first question, I guess, what I would ask is, why are you here? You know, most companies are reluctant, to put it mildly, to speak publicly about being victims of a hack. But you agreed to do this event, even before you'd been called to testify on the Hill. What made you decide to do this public event and why do you think that this public discussion is so important?

Sudhakar Ramakrishna: Suzanne, first of all, thank you for having me on your show today, and this is a true opportunity for us to have a(n) organizational commitment to the community is the way I think about this. And you made a comment about why would a victim of a hack be out there talking about it, and I, personally, think this is our obligation to do so, quite simply because of the context you gave right at the beginning was quite broad. This is not a one company issue, as you highlighted, and it's important for all of us that are going through this to be part of this community of learning and sharing our findings.

And so the reason why I'm here today is to work with you and talk to the audience about what have we learned here. How can we, potentially, help others who may be actively going through such a situation or better protect themselves for the future? Also, there is a very strong opportunity and linkage between private and public sectors here, and it's important for us to start that conversation and extend that conversation through all of our experiences and findings.

Suzanne Spaulding: Well, we, certainly, applaud your commitment to having this public conversation and are really pleased and looking forward to this conversation. I want to – you know, let's take you back then, because we're all anxious to hear how this all unfolded. You know, you're announced in a big, big public relations – you know, a new CEO for SolarWinds, and two

days later the word comes in that your company is implicated in this – in this what turns out to be very significant malicious cyberactivity.

I mean, I'm wondering, were you – were you tempted to pull up your contract and look for the escape clause or what was your reaction?

Sudhakar Ramakrishna: That's a very good question, and I'm smiling because it's barely two-plus months since that whole thing happened and it seems extremely surreal that it happened in the way and the sequence at which it happened.

And the way I would describe this, Suzanne, is that when I was announced and all the way through the day that I learned about this unfortunate incident, all I got were congratulations about how great a company this is, how good a move it will be, et cetera. And then later as this thing came out, I would say I got a lot of commiserations as well, saying, do you have something more to prove? You have proved enough. Why do you want to take on this?

I truly felt that that might not be the best way to look at this opportunity, and as difficult as it is, and, frankly, this wasn't the first thing I was expecting to deal with as my first priority in the job, but I believe I'm prepared to handle circumstances like this with my experience at previous companies. And through all of these events, there's always an opportunity to learn something new, to put that into action, and to serve customers in ways that they may not have been served in the past. And if we can actually combine those four positive endeavors, we can actually emerge a stronger company but, more importantly, a stronger software community, in my opinion.

So I really looked at it as an opportunity. Yes, there are going to be challenges, but an opportunity to work with the team and the community to make something positive out of an unfortunate set of circumstances.

Suzanne Spaulding: Great. So we will get to, you know, how you are working to make something positive out of this. But let's stay back in those early days initially, and so you've decided you're going to stick with this. You're not – you're not looking for that escape clause in the contract. And so what are some of the first things that you – that you did? And again, kind of walk us through how this unfolded in the, you know, corporate offices at SolarWinds.

Sudhakar Ramakrishna: So around the 14th – 13th, 14th of December, when I came to know about this, till January 4th, I was not yet officially an employee of the company. So in many ways I was like everybody on this call, learning about this in the press, reading about it, and extrapolating as much as I could. Obviously, my experience in this field helped me a little bit to visualize what may have happened, what could have happened, and how would I prepare myself for this.

About a week after the incident, I started getting engaged more directly on a company basis and learning every day about the infrastructure that was in place, what exactly happened with the attack, and so on, and started preparing my game plan, so to speak, of jumping into the company on January 4th and working with the teams on it. So in many ways I had the advantage of being an outsider for two to three weeks, learned as much as I could, and hit the road running on January 4th.

Suzanne Spaulding: And so then what were some of the first things that you put in place? I mean, obviously, at first you're just trying to get your arms around the scale and scope of this and what's happened, and be very interested in the ways in which you did that – you know, what you learned from your customers that you can share with us about the scale and the scope and the nature of this attack that might help inform our assessment of what the objectives of the adversary were, for example. But what were some of the things that you did initially just to sort of get your arms around what was happening?

Sudhakar Ramakrishna: The very first priority in all of these cases is customer safety and security. So the team had done a wonderful job of working incredibly hard to provide remediations and patches pretty much within hours and a few days after the incident was known to us. So that's step one.

So the vast majority of the effort of the team was engaging with customers, contacting customers, giving them technical support, human-resource support to get them upgraded to clean versions of the code. So that's job number one.

But as I entered the company, we also started looking at it in a few different ways. As I said earlier, what do we learn from this and how do we improve, that's number one because many – in many situations you can say I'm the victim and this is looking to be like a nation-state attack, and so maybe we can't do much about it. My urge to everybody is we can always learn something from any one of these instances and see what we can do to improve. So it was in that spirit that we implemented an initial – internal initiative called Secure by Design.

So we called it Secure by Design because it has got three facets to it.

The first one is how do we improve the infrastructure security within the enterprise? So what do we do across the infrastructure?

Two is how do we, given that it is a supply chain attack – and I'll come to that in just one second – how do we improve the build infrastructure within the enterprise?

And three is, how do we improve our software development processes and lifecycles to the point where they essentially evolve to becoming secure development lifecycle processes? So in other words, you don't worry about

security after you deliver a product but you do it in the design construct itself.

So that's what we dubbed it as, Secure by Design. That implementation essentially started in the very first week that I was there. We got the terms going and we got the teams going.

Simultaneous to that is the investigation itself, which is what happened, how did it happen, and who may have done it. And here's where we involved a lot of third-party experts, be it CrowdStrike or KPMG, to work with us as an extension of our team and ensure that we are investigating them thoroughly.

And then, obviously, last but not least, going back to your very first question as to why I'm here, is, OK, how can we disseminate what we learned with the external world such that they become smarter and we become smarter in the process of learning through those experiences?

So those were the activities that we started organizing in the first few days and the first few weeks of my tenure there.

Suzanne Spaulding: Right. And as – and, you know, what we have heard and read in the press, and you alluded to this, obviously, is that this very likely came in through the process of building – developing the updates to that Orion software. And you know, I was struck, in trying to follow this story early on, by the SEC filing, which was made within a few days really, if I recall correctly, of this at least becoming public. And which the words that were used I thought were interesting.

"SolarWinds has been advised," said the SEC filing, "that this incident was likely the result of a highly sophisticated targeted and manual supply chain attack by an outside nation-state." And I particularly was stuck by the use of the word "manual." And I'm wondering if you have any insights into, you know, what that referred to, or at least what the state of knowledge was. Granted, this was within a few days of all of this breaking.

Sudhakar Ramakrishna: Suzanne, the investigation is continuing even as we speak today. However, we have been learning quite a bit about what happened as the investigation has progressed. I will go through the word "manual" as well, but the whole context here is the sophistication and the patience that it required for something like this to happen. So what we are learning, and still learning, is the breadth and depth of the sophistication of the attackers, number one. Number two, is the patience with which they carried out these attacks, and obviously the persistence.

So I'll give one example to just highlight and accentuate that point. Many of us from the software industry will understand build assistance and releases. Most of us focus on working on releases for the future. But when

the attackers did some of their test work and recon work, they did it on older releases of code that generally are not the area of focus as it relates to the development community. So that would be an example of not only patience and persistence, but some level of manual effort to understand what could have been in the past versus what is actively being done. Which when you're working on something that's actively being done, there are more eyes on it, versus something that may not be active and is somewhat dormant.

But so they used older releases as test beds, for lack of a better term, and then they carried that forward. So that could have been the connotation of the word "manual" there. The high point here is that there wasn't one single technique used, and it was a long, drawn-out process with a very deliberate focus on cleaning up after themselves at every step of the way. So that requires, again, more manual focus and more deliberation and understanding of the environments.

Suzanne Spaulding: Yeah. And there's been – there was at least initially, I think, some debate among the cybersecurity experts – at least those who natter on Twitter, et cetera – about whether this was, in fact, a really sophisticated attack, how sophisticated was it. I think – I thought it was really interesting that Brad Smith said in the last several days that when his team looked very closely at this and thought about what it would take to do the kind of things that were done in this particular attack, that they estimated it would take about 1,000 engineers. And that's a pretty significant number.

Sudhakar Ramakrishna: Absolutely.

Suzanne Spaulding: Yeah. And I think you're right, we're learning more every day about how long they were at it and all of the steps that were taken.

Sudhakar Ramakrishna: And that's exactly right, Suzanne. It required a tremendous amount of patience to do this because it wasn't like the run of the mill call it virus or a ransomware, whose goal is to spread like wildfire and grab a lot of attention and possibly do damage. Because when those types of incidents happen, most threat response teams – including ours – will be able to detect them and create inoculations to those. But when you are hiding, so to speak, in plain sight, where the traditional tools that you deploy in an environment cannot identify them easily and simply, or even with a lot of sophistication, then that becomes that much more difficult to identify.

Suzanne Spaulding: So clearly the three areas of focus that you've outlined were developed in large part by looking back at what happened and figuring out – sort of one way to think about it might be kind of looking at the kill chain, looking back and thinking about how could we have prevented at various stages, right, what happened. And I assume built into all of those is some way – some tripwires to – not just to prevent bad actor from getting in, but increasingly

we understand that we have to assume that they're going to get in, and how do we detect them more rapidly, and then how do we mitigate the consequences that can be caused by a successful breach. And that applies, as you said, both to SolarWinds itself, but also to your clients.

So maybe if you could walk us through a little bit on each of those – the enterprise security, the build infrastructure – improving the build infrastructure, and then then software development – in a little more detail, I think that would be helpful.

Sudhakar Ramakrishna: Definitely. I'll go through each one of those, and you had previously asked me a question about how our customers are understanding and appreciating the situation. I'd like to cover that as well because many of our customers are also developers of software. So as much as they are buying and consuming products from us, they are also trying to learn what happened to us, how are we fixing those, such that they can apply those concepts and principles in their companies and enterprises as well. So it's a – it's a real supply chain in a different context, and we can – we can talk about that as well, Suzanne.

But coming to your question first, let me start with the product development process and the integrity of the code that we deliver itself because, ultimately, the attack happened because while it was code that we delivered and was signed by us, a malicious actor was able to inject something into our code unbeknownst to us. So the traditional way of highlighting and demonstrating that a piece of code was actually delivered by us as a vendor is to sign it with our certificate. And in this case we actually did it, customers trusted it, and delivered or used it. But because of the narrow window in which the malware was injected into the code, the ability for our bill systems to identify that did not exist. So that is one of the key areas of focus that we are working towards, and there may be an opportunity here to share that more broadly with the industry because this problem exists in every company. So what happened to us can happen to any software developer in the world.

So to that end, what we are doing is we are building parallel build systems within the company, number one. What that'll do is having different environments, different people accessing them, and different techniques to build our software, and then cross-correlating the output of those three will essentially reduce the opportunity for a threat actor to do damage to our build systems. So that's going to be a(n) involved process, but we believe that is really what is required in light of these findings to be more safe and secure going forward.

So that's a commitment that we have made. We are documenting the findings. I'm even working with the likes of CISA and others to help potentially improve standards such as NIST and CMMC such that these are not simply compliance-related guidelines, but how do we truly increase the

excellence in software development and development practices. So that's a key area that has a connotation on both our build environments as well as the build processes themselves.

Earlier I mentioned: How do we evolve software design lifecycles to secure design lifecycles? And traditionally, a lot of security practices are things like pen testing and others on delivered code, not necessarily in the design and development phase. And so we are evolving our own internal processes to inject security in the design phase and in every phase of the product development lifecycle, and then supplement it with pen testing, ethical hacking, and other communities at the – at the back end of it. So that's the balance that we are trying to strike before and after the fact. So those are the two items.

And then the very first thing that I mentioned, which is about the structure or the infrastructure itself, is: How do we create a world – you've heard the term zero trust? How do we create the world of least-privileged access in these environments? The reason why – one of the reasons why I believe the Orion platform, in my opinion, was targeted is when you gain access to the Orion platform, you gain administrative privileges to the Windows server that the Orion platform is running on. And so if you were to run that with lower privileges, even if an attacker were to gain control you won't be able to do as much damage because you are a regular user and you're not an administrator of that network. So we are taking those into account, both from our infrastructure standpoint as well as from our product standpoint.

So that's the full spectrum and scope of what we are engaged in doing as this point.

Suzanne Spaulding: Yeah. That's great. You know, there's a lot of talk these days about zero-trust environments and far fewer examples of how it's actually being implemented, so I think that's really helpful.

And you talked about the fact that you're working with CISA and the folks over at NIST in terms of trying to see if there's some generalized best practices that you could bring to bear beyond your customer base, which I know you're reaching out to with some of these – this mitigation suggestions as well. But I'm sure that all of your interactions with the government have not necessarily been either voluntary, necessarily, or just looking at possible mitigation. The federal government has a way of becoming involved very quickly, not surprisingly, in something of this scale. And so I'd be really interested – and I'm no longer in government, so you won't hurt my feelings – in what your relationships – what your dealings with the government throughout this process have been like and particularly, you know, if you're got some suggestions for how the government might better assist a company like yours or your customers as they try to respond and mitigate something like this.

Sudhakar Ramakrishna: Suzanne, I would say that our engagements with the government have been broadly constructed if not always completely informational – and I'll go through that in just one second – because I recognize the government has its own restrictions on what it can share, when it can share, et cetera. We took the commitment to share with the governments, and generally speaking the national defenders, very proactively, and we continue to do so.

As it relates to the government, I alluded to the public-private partnership earlier because what is clear with these attacks is that no single enterprise – how large or how many resources you may have – or a single government can completely identify, protect, and kill these attacks that continue to emanate. So there is a need for a tighter public-private partnership.

One of the areas that we suggested or we suggest is having a single entity within the government to whom we can report these incidents, and that authority has then the ability to disseminate it to whomever is interested in it and it's pertinent to communicate. Today, as a mid-sized company, I find myself having to deal with multiple government agencies, and there is information asymmetry, and when that happens we are losing time in fighting these attacks. And so having a simpler structure of communication and exchange of information with a singular entity would be hugely beneficial, in my opinion.

The second piece of it is collaboration between public and private as it relates to standards such as NIST and CMMC. And we at SolarWinds are providing resources to actually help with some of these engagements because we truly believe by committing dedicated resources we not only contribute, but we extend our opportunity to learn on the reverse direction as well.

Three is regulation itself. A lot of victims, as you mentioned very early on in this conversation, are hesitant to come out about exfiltration of data or attacks on information, and that is – that could be because of liability concerns and other potential punitive concerns. So providing regulation, and helping them, and giving them comfort to step forward and step quickly and step in a timely fashion with information will, I believe, help us all be more safe and secure.

Suzanne Spaulding: Yeah. Great. Great insights and important points. And as a member of the Cyberspace Solarium Commission, you know, wholeheartedly endorse your, you know, concern about needing to have a single place for folks to go with incidents, and a better coordinating mechanism to make sure that there isn't an information disparity, at least across government, and to try to reduce the information disparity between government and the private sector. So all of those are really important questions and insights.

And we're going to turn to our audience questions in just a minute. And I want to make sure that folks understand that you can submit questions.

You need to go to the events page – the CSIS events page and there should be a green button for, you know, submitting questions. And please do go and submit your questions there.

But, Sudhakar, you mentioned – at the very end there you talked a little bit about regulation. And one of the questions I guess that has come up in this context is whether, you know, a company like SolarWinds, that is so successful and therefore so ubiquitous, you know, the customers of SolarWinds – not necessarily just Orion, but of SolarWinds generally, include 425 of the U.S. Fortune 500, the top 10 U.S. telecommunications companies, the five top U.S. accounting firms, all branches of the U.S. military, the Pentagon, the State Department, hundreds of colleges and universities, et cetera.

You know, do you – what's your sense about whether a company that is so – upon which so much depends has a greater responsibility with respect to cybersecurity? And you've spoken a bit about the degree to which you've kind of taken that onboard voluntarily. But what would you think about, you know, looking at a – is there – and should there be a requirement?

Sudhakar Ramakrishna: So, Suzanne, on that front we are a provider of tools and capabilities to IT professionals to solve problems and manage their IT environments. We are not a security company per se. However, I believe it's our obligation to take security seriously across the board – not just within our products but across the environments of our customers themselves. And so it is with that intention that I'm actually coming out and openly stating what we are doing with the secure by design, highlighting what we learned from this situation. Because a lot of these apply to us directly, but a lot more of these apply broadly speaking to our customers.

So I'll give one example of what we are doing, because one of the learnings that I have had through this process is it is not sufficient to establish the security of my product alone. It's important for us to look at customers as environments and do the best we can to protect their entire environment. And to that end, if we have to provide them, let's say, hardening guides, configuration guides, of other security components in their environments then it is our obligation to work with the ecosystem where the customers do not have to face the burden of having to do all of those, and we as vendors are collaborating alongside the government to provide more protected and protective environments for our customers.

Suzanne Spaulding: Yeah. I think it's a great point, and not enough to just push out a more secure product and then, you know, leave people to fend for themselves. And not only, you know, is that important for our nation's overall cybersecurity, but obviously it's not – it does not serve SolarWinds well if its products are not used in an intelligent way, and then breaches happen through your products. So that makes perfect sense.

We do have some questions coming in from our audience, folks who are still curious to, you know, learn more about exactly how this happened. We know that the malware was initially introduced to the victim companies when they downloaded that Orion software. And one of the questions is whether those updates were pushed automatically or were they downloaded manually? And my sense is, you know, I remember hearing early on the statistics about the number of potential folks who received the updates, and then the number of people who actually downloaded the updates. And it was a good news/bad news, right? Good news was not everybody downloaded the updates and therefore not everybody was infected. The bad news was the number of people who didn't download the updates, which is also not good.

Sudhakar Ramakrishna: Yes. So the code or the Orion platform, as you are referring to, runs on the premises of customers. So these updates are not automatically pushed. A customer will have to download the piece of software and then install it in their environment for it to be running with the malware. So that's step one.

So the reason why we came out with a number of 18,000 when we filed our 8-K is because that was our best estimate at that point of how many customers downloaded the software. That doesn't mean that all 18,000 of them actually install it because it's quite common for customers to download it, not install it, and sometimes wait for the next release to show up as well. That happens quite often in the software industry.

Now, the secondary step that has to happen is that once a customer downloads that software, it is not the case that in every case that malware was trying to cause damage. The malware was written in such a way that it would do some checks and in – only in some environments would try to contact its backdoor server. OK. And for the backdoor server to be contactable, so to speak, the other security elements in the environment like a firewall will have to provide access to the Orion platform to connect to the internet.

And by the way, the Orion software platform does not require connectivity to the internet. Therefore, in those environments, there was no scope for the malware to do any damage.

So I have spoken to a number of customers, as you can imagine, over the last seven weeks that I've been with the company, and in many instances, as we go through this process and even before that through our support engagements and support calls, we discover that when the firewall is not configured to let the Orion server go out into the internet, their potential for damage through Orion is nonexistent and all they had to do is apply the remediation code.

Unfortunately, there have been a few instances where that code did contact the backdoor server, as has been reported in various forums, whether it is

the hundred customers, in some cases, or whether it's a few dozen, as has been highlighted, et cetera. What we have been focused on is touching every single customer of ours as best as we can to see if, individually, we can help them both upgrade to the remediated code as well as to see any help we can provide them in the assessment.

So I would say, thankfully, out of the 18,000 that downloaded, through various reports that we are reading ourselves and what we are hearing it's a very small number of customers that may actually have been impacted or compromised at this point in time, and the details of that we are still working through.

But I do not want to at the same time minimize the potential risks that will continue to be there in the supply chain vectors, which is another reason why we are coming out and talking about this openly.

Suzanne Spaulding: So I think it's fascinating. It's really interesting that, obviously, there were some configuration decisions and ways in which the application was been used that protected some companies from becoming more significant victims. But were there companies where there could well have been, that the opportunity existed, for exploiting that access that that initial, you know, hack had gained the adversary – who has been publicly, you know, presumed to be Russia and presumed to be the SVR, the external intelligence service – but was not actually exploited?

I mean, you know, one of the things that we have learned and, again, I think Brad Smith alluded to this, is – and you certainly did, that getting in is, obviously, always just the first step and tremendous amount of effort to hide their tracks and close doors that they had opened and replaced their, you know, code with the preexisting code when they were done and all those things that happen. So very labor intensive.

So is there something we can learn about the objectives, potentially, of the adversary based on where they expended that effort and where, perhaps, they did not, even though they may have had an opportunity to do so.

Sudhakar Ramakrishna: Definitely. Suzanne, the first observation, I would like to reemphasize it, which is: Even if the backdoor was open, so to speak, and the adversary is within your house, for them to do any damage required a lot more sophistication and a lot of other breaches within the environments – like, you know, misconfigurations or other breaches within the environment. Which I don't believe will be the case in every environment. That made the potential for exfiltration that much more difficult.

Now, as to their intent, given what we have learned it doesn't seem like – as I alluded to earlier with a virus or a typical malware – spread as fast as I can, create as much damage as I can. That wasn't the intent in this particular case. Given the tools, techniques, and processes that they have

been using, and the attribution to a nation-state, I feel that they were after a few prized assets, so to speak, in terms of maybe in some cases simply learning about those environments and in some cases trying to get something out of those environments from an intelligence standpoint. We do not have enough knowledge or expertise as SolarWinds to independently affirm that.

Suzanne Spaulding: Yeah. And I have been concerned from the beginning that part of – there are probably multiple objectives, would be my assessment, and that part of it may well be reconnaissance for future disruptive kind of attacks. And so I think – you know, I think Anne Neuberger said this and we've been saying this for quite some time, that we should not view this as simply espionage.

So, Sudhakar, you're going to be in front of Congress at least a couple times this week. They'll be asking you lots of questions and about – you know, talking to you about what you should be doing. One of the – one of our audience members has asked – giving you an opportunity to make a suggestion about what Congress should do. If you've got any thoughts on what Congress can do to ensure that something like this – or, to mitigate the likelihood that something like this would happen again.

Sudhakar Ramakrishna: Definitely. I'll go back to the three things that I was referring to, broadly speaking in the context of government, but Congress helps government form rules, regulations, and processes. So the first thing is to encourage more private-public partnership, and have – call it incentives or protections for people who are coming out and openly admitting to attacks and use them as information sources, because in the Solarium Commission report, Suzanne, I seem to remember the number of times that you highlighted speed and agility as the way to circumvent and thwart these types of attacks. So that's, I would say, number one.

Number two is that leverage the work that we are doing and others are doing to essentially enhances standards such as NIST and CMMC, such that – I like to call them as excellence focused versus compliance focused, which is at this point, because a lot of us can pass through the checkboxes of did you do this, did you do that? But obviously the results prove that we need to do more. So how can we achieve excellence versus simply being compliant? That's the second thing that I would highlight.

And three is make it easy for us to communicate with the government by having a single forum or a single clearinghouse to whom we can report, and have the responsibility to be from there to disseminate it across the government entities and private sphere entities, as opposed to us having to run from pillar to post, so to speak.

Suzanne Spaulding: Yeah. That's been a significant compliant of – a long-standing complaint from the private sector that we've got to address. And you talked about the, you know, maybe need to look at liability protection for those who come

forward. We have a question from the audience about liability protections for sharing information. And I think many of those exist. Congress enacted the first CISA, Cyber Information Sharing Act, that provided some liability protections. But what the Solarium determined is that we need to go beyond simply sharing threat indicators, for example, and pushing information back and forth with each other to get to a place where we share understanding, where we share insights, where we are collaborating to understand what's happening and how to respond and recover from that. And so there is a recommendation to establish a kind of joint body, private sector and government. Do you think – were you concerned about potential liability as you enter into these discussions you're having with the government? How serious is a – is liability as an issue for you?

Sudhakar Ramakrishna: I would say from a SolarWinds standpoint it is a topic that we think about, Suzanne, but that is not a top-of-mind topic for us at this point in time. The reason I bring that up is, being a student of this industry, I know that there is a lot of hesitation to openly share information, and – to your point – insights, and to your earlier point about victims not wanting to be identified as victims for a variety of reasons. And what we need to provide is the liberty and the liberation needed to come out and speak about it, because the more offers in the community that can create essentially the notion of a community vigil, so to speak, the more protected we are going to feel. And that is the point I was making about liability.

Suzanne Spaulding: Yeah. Great.

Well, Sudhakar, they say, you know, never let a good crisis be wasted. I think you are taking good – making good use of this crisis that confronted you on day one of your term here at SolarWinds, and we are very grateful that you thought it was important, think it is important to be part of the public discussion on this and to be, you know, really a leader in helping to address these issues going forward. So thank you so much for the insights you shared with us today.

Good luck this week in front of Congress, and I hope they do give you an opportunity to share with them what they can do. But I want to thank you for joining us today. And thanks to all of you who tuned in.

Sudhakar Ramakrishna: Thank you, Suzanne. Thank you to our employees and our customers and partners all over the world, as well.

Suzanne Spaulding: Great.

(END)