Company Participants

- Nanda Santhana, Senior Vice President, Cybersecurity Solutions

Other Participants

- Anurag Rana, Analyst, Bloomberg Intelligence

Presentation

Anurag Rana {BIO 7440273 <GO>}

Hey. Good morning, everyone. Welcome to the Bloomberg Intelligence Webinar Series. Our topic for today is understanding risks due to COVID-19. So a couple of administrative notes for us. Today's presentation will be recorded and available for playback. You can access the replay via the link sent to you in an email from Bloomberg webinars. At the bottom of the slide window, you can adjust the volume and maximize your screen. To ask a question, there is one on the right-hand side. We will address questions at the conclusion of this presentation.

A quick word about Bloomberg Intelligence. We provide in-depth research and data on companies, industries, government, credit, ESG. We cover close to 2,000 companies right now and we have about 300 people who are part of our department that is established globally.

So the discussion today is on COVID-19 and the rising cybersecurity risks. Our guests for today is Nanda Santhana, and I will pass it on to him to introduce himself and talk a little bit about what we're seeing in market space.

Nanda Santhana

Anurag [ph]. Hope everybody can hear me, okay. And my name is Nanda Santhana, I run Global Head of Cybersecurity and Threat Solutions here for Securonix, and what I'm going to do is first walk you guys through a little bit about Securonix itself. We are a company founded in 2009. We have about 250 customers worldwide and couple of products that we produce today is the Next-Gen SIEM, which is built on Cloud. We also offer a Security Data Lake, essentially helps customers gather all the data in the cloud and we have a UEBA solution, which is a User and Entity Behavior Analytics solution. We also provide a SOAR solution, which is a security, orchestration and response. So we've been around from 2009, and these are our product suites that we produce.

In terms of the topic in hand today, like you brought up Anurag, hundreds of millions of people are now working from home as a result of ongoing COVID-19 outbreak. Now the challenges that we see is number one, the VPN, remote access, Cloud and

BYOD devices are opened up overnight for employees and contractors, right. Especially, VPN and collaboration tools are pushed to their maximum bandwidth. What that basically means is we have kids at home. There is a lot of virtual schooling that's happening. So both at home, the bandwidth is completely consumed.

And on the corporate network side, folks are using a lot of video conferencing. So the bandwidth is completely full. In some organizations, they have started to expedite cloud adoption, especially because of Coronavirus and the COVID-19 pandemic, and because of which, most of the folks have to work from home. They have overnight shifted towards using cloud emails, infrastructures and apps with very little security testing or even time taking to do an assessment in using some of these cloud solutions. While these are all the changes that's happening on the IT side. On the attacker side of the house, these hackers are absolutely merciless. They're now taking advantage of the fact that there is fear in across the globe and they are capitalizing on this fear, and will speak about a little bit more on how they're doing it so to speak.

Now while all of these things are happening, we see an enormous high number of spray and spear phishing campaigns, and these spray and spear phishing campaigns essentially targeting individuals with very specific class key messages out there, that talks about the cure words like, COVID-19 cure and these phishing events are absolutely successful. And the last thing that we notice, which often times in cybersecurity world not really talked about, is all the damages, the unintentional data loss done by employees and contractors. Remember in the beginning, I said the bandwidth is completely utilized, now because the bandwidth is completely utilized, we see employees and contractors essentially downloading a lot of sensitive data. Right now, it may look like it's -- this is as usual. Now what's going to happen to the -- some of those data documents is a big question mark post this pandemic. So net-net, users and their laptops, the way we see it are the new perimeter that needs to be monitored with respect to this COVID-19 challenges.

Now few things that I'll bring up here. Yeah, go ahead Anurag, sorry.

Anurag Rana {BIO 7440273 <GO>}

No, Nanda, go ahead, please. I was just trying to figure out who are these attackers and what are their -- what's their profile?

Nanda Santhana

Yeah, definitely. Yeah, I think some of these attackers that we see first of all, the traditional malware families and what we also see Anurag is that we see a lot of employees' contractors, we also put them in the attackers' bracket, because to us, a damage -- cybersecurity damage done to an organization whether it's by an adversary outside or by your own employees or contractors, in some scenarios, we even saw terminated employees. Essentially that's what constitutes towards this entire metrics that we are starting to gather across our engagements.

Now, to your second question, if I break this thing down. I think the key things that we see here is, for some reason, I think the PDF when this entire excel spreadsheet got converted into a PDF, it lost the metrics, but I can speak through this. The biggest challenge that we see is, we see a ton of phishing campaigns, that's on the rise for sure. And these are, like I said, extremely crafty messages that hackers are using to attack an individual and that's definitely on the rise. The second big bracket that we see of issues that are happening outside, malwares essentially in the last three to four weeks, we see close to 72,000 domains that are created with either as word like Corona or COVID-19 and variations of it which starts with K and whatnot. Our research -- Securonix spread research shows that at least 8,000 of them are malicious, and what we also further see is that there are so many top domains meaning, the rest of those domains potentially could be used later on for any malicious activities. So unfortunately the metrics is not showing up clearly here, we'll get back to the listeners. But if I can dig in a little bit more deeper about these attack vectors to the previous point, what we see is the most notorious Coronavirus malware, right. So this is a malware domain that was registered earlier on in Jan and what we see is a lot of COVID and COVID-19 related domains, like I said. And out of which, this particular Coronavirus tracker website, in the front end, it looks like -- just like any other John Hopkins University's Tracker, but in the back end, what it's doing is it's essentially installing a malware on your laptop and the users don't even realize it.

So again, these domains are continuing to become a big challenge especially for employees, contractors who are currently working from home, and the reason why it's becoming a challenge is because the firewall rules when users work within an organization. There was a degree of preventive controls. Now when you're working from home, when you're using BYOD devices, it's just becoming much more easier for these attackers to essentially trick employees and contractors to click on some of these websites and that's continuing to become a challenge.

Moving on, couple of key things that I do want to bring up from our threat researchers. You guys probably must have heard this word called ransomware. It's really on the rise again, and what we have seen in one of our organization is, there is a COVID-19 document looks like a COVID-19 weaponized document. In one organization, unfortunately a human resource executive clicks on that, it locks the computer, it essentially asks for some sort of monetary transaction via Bitcoin, and these ransomwares are starting to become a big challenge in most organizations, especially right now, because you guys probably must have seen the news, there was a big issue in one of European hospital, where there was actually a ransomware on the most critical clinical systems and that started to create a big (inaudible) for these institutions to essentially fix it while they are already dealing with the most important things in hand, right.

The third thing that I'll talk about which probably applies to everybody here is the Zoom attacks. I think this is something that I definitely want to double-click on as we move along. Everybody is using Zoom today and I think, while Zoom starting to address some of the security concerns, what we have seen already is there is a lot of automated tools that can actually find your meeting IDs and a lot of academia, a lot of virtual schooling have been hacked via this method, folks have joined random

meetings, lot of privacy concerns have started to showing up, and most importantly, when we have been doing some research in dark web, we see close to 500,000 accounts that are on the dark web. So there are some recommendations that I'll follow through in the end and how to basically make sure that you don't become a victim, but Zoom attacks, the social media and collaboration tool attacks are definitely on the raise.

We talked about phishing campaigns. One of the key challenges that we see is with respect to phishing is, the messages are so tuned into what's going on in the market today, like one scenario, in one organization, they actually got it fixed CDC being [ph] phishing and if you look at this phishing email, we were able to bring this malware in our threat research labs and essentially detonated. What was interesting is, when you actually click on that link, it shows you the fake one drive log on and that one drive long on exactly looks like an authentic one drive log on, but essentially the hackers are collecting your credentials and they're sending it to -- they're using it for whatever malicious reason. But in this particular scenario, as soon as the hacker got access to the users account credentials, they started to forward significant gmail -- significant emails to an unknown gmail account.

Now I just have couple of more scenarios such as this, these are all real findings, real problems that Coronavirus and work from home has really brought in light. In one organization, we see, I can't compromise. Now what's interesting about this is, when you see an employee logging in from different parts of the world, especially right now there is a travel ban and you don't expect employees to be coming in from different parts of Europe and United States of America within 5 to 10 minutes. We call this as land speed violation. Previously, folks probably would take a plane to different parts of the world. Their home computer is still connected to the corporate network, so it used to throw people off and it never got a lot of attention. But now when you start looking at analyzing the data points, in one particular scenario, we saw an employee, he was logging in from so many different parts of the world simultaneously and it was actually very interesting and now the security operations team, the folks who actually investigate these violations, these incidents, they now have an extra edge to investigate them, especially now because of the travel ban, like I said, we start seeing several people logging in from different parts of the world and it continues to be a very, very big challenge.

We talked about phishing campaigns, and I think we again see several of these phishing campaigns. So one thing I will tell you is that these attackers, they are not very keen in having a direct monetization with the victim, in some scenarios, they actually attack you for instance, and then use your credentials to start phishing other organizations, other users, other employees and contractors to get a much bigger plot, a plot that's much thicker that it directly attack you, pay me a ransom and I release your computer back to you, those days are behind us. And to that extent, in one particular scenario, there is a weaponized document again, it actually runs a lot of malicious process and these processes are connecting across different parts and it was kind of interesting to see how this phishing campaigns turned out.

The last thing that I'll -- couple of things that I want to touch on in cybersecurity space when we talk about bad things, when we talk about attackers or hackers, we often associate them to a malware group. We often associate them to an hacktivist, right. What we don't see is the possible damage that an insider and insider is somebody who is part of your organization, employee or contractor. The damage that they could do, nine out of 10 times, they could be unintentional, but the problem here is that it's still a significant damage to the organization odds, I'll tell you why? Most employees and contractors when they are associated to a critical project from an organization standpoint, the work that they do, the material that they create. They often have this false sense of belonging thinking those documents, those research work belongs to them, and most employees and contractors, they feel entitled to take this data with them when they go to the next job that they were to seek and they think it's okay for them to take that data out. So nine out of 10 times, what we deem as insiders in cybersecurity space are employees and contractors and typically their intentions are unintentional, very few times, we have seen some sort of a corporate espionage or an industry or a nation-state espionage that we see. But mostly, we brand them as unintentional.

Now the reason I bring this up is especially right now with work from home, the challenges that we see are huge. In one organization, the first week of March, the organization announced a mandatory work from home, and within 24 hours to 48 hours, the security teams in this organization, they have to relax all the cybersecurity controls. They had to release the cybersecurity controls because employees and contractors from their home couldn't keep up to the connection, the VPN or remote network connection, because the bandwidth is so full. So every five minutes, the connections kept dropping and it really started to hurt the business continuity (inaudible), it really started to hurt folks to do their regular day-to-day job. So the security teams decided that I'm going to now drop all the controls and folks can have a little bit of discretionary controls over their sensitive documents. What ended up happening was one employee, he starts to grant access to his own personal account and into a corporate share drive. On March 20th, this employee quits, and furthermore on 25th March, the organization did what they typically do. As soon as somebody quits, they disable all their access. But this employee because he is now put in a backdoor account which is his own personal account, he is starting to continue to login, he's actually working for a competitor organization and he continues to login. He starts to download all sensitive data. He's starting to download all his peers, his colleagues sensitive data that's how deep-rooted the backdoor entry is. So again, this goes back to all the challenges that Coronavirus, COVID-19, work from home phase that we are all going through, and these are some of the key findings that I want to bring up.

So that being said, I have couple of key takeaways that I want to definitely bring up on this call, right. So the first thing that I'll talk about is the traditional cybersecurity way of doing business is different right now. Users and their laptops, the new perimeter, because what used to be inside the organization, which is employees, which is contractors, now we are all outside, we're working from home. I think the boundaries that we know off is completely stretched out, so the new perimeter is users and their laptops, and because some folks are also using their BYOD which is

Bring Your Own Device, they're using their personal devices to connect the corporate network.

The first thing that I'll talk about is, I think the traditional way of monitoring needs to change, we need to monitor a user behavior monitoring because whether it's a phishing email, whether a hacker has a bad domain or there is a high number of sensitive data that's being downloaded. The common denominator is an employee or contractor, so the users are the common denominator amongst all these attacks. And so monitoring these users and their workstations is absolutely critical. The third thing that I'll tell and this goes to outside of the corporate organization, a big request to all the folks who are listening on this call, please update all your software applications, if there is a update that application owners or those vendors are providing you, there is a reason to it. Take a look at those notes if you can, if you see any security vulnerabilities that are being patched, I strongly recommend everyone to update your Zoom and all the other collaborative tools. And by the way Zoom has a -- now they produced a 101 best practices, don't use your personal IDs, use the lock room and whatnot. And so this is absolutely critical, also let your kids, teachers know at home schooling, this is definitely something that we are tracking very closely.

From a business continuity perspective, I think having emergency contacts is very important, in one particular scenario, employees are distracted today. They have to take care of their kids, they have to take run a home and work and having a sort of a secondary person having your emergency contacts to support, especially the IT infrastructures and your mission-critical applications and whatnot, I think having a BCP plan in place is definitely a key takeaway.

In some scenarios, we also strongly recommend organizations to extend their endpoint. Endpoint is essentially a small application that runs on your laptop and it detects any suspicious activities, it detects any suspicious malwares or viruses on your computer, and it reports back. And I think a lot of vendors today are providing including us, we're providing some sort of a specialized package to help the communities, and our recommendation is to make sure that you have all the key monitoring in place, whether it's endpoint and whether it's the emails that you need to monitor or even cloud solution. I think those monitoring should be in place and collecting that logs are absolutely key.

Few more things that I'll quickly touch on, in one organization, an actual scammer, he impersonated himself to be one of the employees very close to getting a lot of sensitive data because now these scammers also know for a fact that most of workforce is working from home. And so train your IT service team members, train your customer service team members to have a multiple layers of challenge and response to absolutely make sure that the person who is calling on the other end is actually who that person is claiming to be who that person is. So some sort of multiple response framework is absolutely required, so that they don't fall for these scammers.

And but -- last but not the least, the confidential data is still confidential. Today folks are taking some of these documents out. The reasons are justified. Bandwidth

getting clogged up, data loss, whatnot. But once this whole pandemic is gone. How do we have an inventory of all these documents that have gone out, and I think this is going to be a very, very big challenge for organization post the pandemic times.

Questions And Answers

Q - Anurag Rana {BIO 7440273 <GO>}

All right, great. Nanda, thank you so much. This is fairly comprehensive overview of the stuff that you're seeing. And again a request to our listeners. If you have any questions please put them down and we'll start addressing them as they come through. So Nanda there are a bunch of things that are on our mind and some of the stuff that we are seeing in our research as well. And first and foremost, is the BYOD question. We have a question from the audience talking about, is the core risk of working from home, BYOD? Or if a company issued assets -- if a company decides to give you a laptop or a desktop, is there a reason that the threat level now should be different than pre-COVID, because if I give you the actual hardware asset, I would have all the built-in security, why doesn't that cover for a lot of the risks that we start just as people who are working from home on their own laptops?

A - Nanda Santhana

Yeah. I think it's a great question, right. So the key problem here is whether it's BYOD or its corporate asset that folks are sending out. The challenge that we actually see is when folks are working from home, there is a lot of different loopholes that you can have. I'll tell you, in few organizations, as soon as you step out, you bring your corporate asset to your home network, we've seen organizations where employees actually connect to what they call as a local cloud storage, because there is no firewall rules in most organization, that's not -- it's not enforce. It is so easy to copy tons and tons of data to your personal storage devices at home. So whether it's BYOD or corporate issued assets, these challenges existed even before COVID-19. Post COVID-19, I think all problems take us to one thing, which is bandwidth consumption which also includes a very high degree of victims with respect to phishing campaigns, right. And so for those reasons, I definitely see the challenge to be for both employees and contractors who are using BYOD devices, and in some scenarios, they -- corporate issued asset. I will tell you this, yesterday, we were doing an investigation in one of our organization. The folks are now working from home, obviously, the kids are home schooling. So what has happened is with this whole Zoom collaborative tools issues that we found, some organization started to react and they said, we are not going to allow Zoom anymore. So what these employees have started to do is because they still need to have their kids go through home schooling for which they still need to have multiple laptops. If you have two kids, they both have been home schooling, they need to have multiple laptops. So in some organizations, we also see these users disabling all the security controls on a corporate issued laptop which is actually adding on more pressure, more vulnerabilities in some of these scenarios.

Q - Anurag Rana {BIO 7440273 <GO>}

Now that makes a lot of sense. So now let's talk a little bit about the pre-COVID world and the post COVID world. Now when we looked at security, security products in a pre-COVID world, we -- one of the things we observed was why is it that the clients that you deal with or whether it's large banks or healthcare companies or retail companies, why is it that they have to buy so many security products in a sense that why haven't we seen these being embedded either in a public cloud offering or a -- or have a unified solution that takes care of a lot of these things? And just my ancillary to that question is one of the big themes that we have talked about as well over the last three, four years has been a hybrid infrastructure, and do you think that changes at all given what is happening?

A - Nanda Santhana

Yeah, so great question. And by the way cracking up just a little bit, I don't know if it's just on my side, Anurag. But I mean, companies have to -- if I essentially get why do companies by so many different cybersecurity solutions, right post -- pre-COVID. If I break this thing down, from a cybersecurity perspective, a lot has changed in the last 15 years. What used to be a very focused compliance function has now become a much bigger program in most organizations and why? First and foremost the threat landscape has changed, right. And if you think about before, there was not much of phishing campaigns. There were not many different attacks -- sophisticated attacks. And the reasons why these attacks have evolved is because our adversaries today, they are using some of the most sophisticated cloud infrastructure, artificial intelligence, AI enabled BOTs. And so they are super advance. So one side, the threat actors and the threat landscape is super advanced. On the other side, it's not like the simpler times that organizations are working in, where you just had something called a firewall or a perimeter and you just punched a small hole in it to send out emails out, to send out -- to browse internet from your corporate network. Things have so much changed -- the IT landscape has changed the lot. Today you've opened up cloud in most organizations and you have third-party vendors connecting to your network. So given an advancement of IT and the usage of cloud applications, and on the other side, you have so sophisticated threat actors and threat techniques that are constantly attacking you, and on top of that, some organizations are opened to BYOD, I mean we starting to see in the last two years smishing, phishing is now gone to smishing, which is sending you malicious emails through SMS. So that's the state that we are living in. So what we see as a result of that is that old schools technologies, which were very focused on compliance related scenarios, they are starting to get displaced with the NextGen solutions and hence you see -- it may look like you're seeing multiple different vendors in cybersecurity space, but essentially, they're all targeting a specific function, detecting a specific technique. And I think -- and that's probably why you see Anurag, a lot of different cybersecurity solutions in the market today.

Q - Anurag Rana {BIO 7440273 <GO>}

So perhaps explain to me that, I mean I understand that larger companies that that are very difficult to move some of the critical applications. But if I'm a small to mid-sized company, why don't I just go to AWS and Microsoft and just move everything to them and let them worry about so many of these things and get out of this heterogeneous IT infrastructure that I have and let them worry about spending on

security and not me. How do you -- will that help or even with those companies that are risks involved?

A - Nanda Santhana

That's a great question, right. So I think, first of all, companies are not going to stick to one cloud solution provider. And so let's start with that, right. So for two reasons: a, they don't want to have some sort of an advantage. They don't want to have the vendors have an advantage towards price, and so the cost is the main driver for most companies to, first of all, consider a heterogeneous environment, right. So big organizations will probably use the top 3 cloud solution providers. And needless to say, for the next five to six years, we're starting to see a new trend of private cloud, right, and we have a lot of companies really helping these organizations build private cloud. And then come what may, the way we see it the next four to five years, the data center is not going to completely go away. I mean if that was the case we would probably see all the legacy old school mainframes completely be gone, but that's not the case. Most of the top-notch critical financial transactions still happen on mainframes. So you have a heterogeneous cloud solution, you still have an on-prem data center and no matter how you call it, the private cloud is still a fancy word for expanding your data center, right.

So this is what we think organizations are going to face. It's going to be a heterogeneous environment with multiple different cloud solutions provider with a little bit of a data center presence, but doing the most mission critical ones. So when these cloud solution providers provide their own security as a built or an add-on, it's just going to be only focused on their service that they're going to be providing. So you still need this bigger mothership which is going to get all this information in, and hence -- and then we strongly feel that just sticking on to one cloud solution providers and end this security solutions that they provide is not going to be the answer, Anurag, in the long term.

Q - Anurag Rana {BIO 7440273 <GO>}

Well that's a fair point. The one area that we haven't touched on today and it's -- I know we got a lot of questions about it is privacy. Europe is all over it, and this is only going to make things worse in terms of access to different applications or moving to third-party applications without any sort of security, you could say scrutiny. What do you think needs to be done when it comes to improving the privacy across an organization or in between one vendor and another when they share data?

A - Nanda Santhana

Yeah, I think the most cloud solution providers are today are very, very keen on sharing this data, right. I think privacy is going to be a big challenge. Organizations, one of the main drivers for them to also build their own private cloud is because they are worried about the data leaving the organization is exactly for the reasons you brought up, Anurag, which is privacy is a main driver. And so for which what they're trying to do is they're trying to see if they can do some sort of an analytical work on the cloud or any point computation work on the cloud which is what some of these vendors really specialize in. And they want to see if they can have the data in-house within their data center, because privacy is still a big question mark. All of

these evolution in cloud just happened in the last five to six years. Only now things are surfacing up. There is a lot of regulatory requirements that are catching up on the privacy angle, right. So I feel companies are going to be, in the next few years. the data may probably end up staying on trend within their data center till we have a very strong regulatory requirements where the cloud solutions providers are able to -- some sort of go through a certification process that they are extremely cognizant towards the privacy concerns that they'd probably need to meet. So up until then, I think you're going to have sort of, again like I said, a hybrid solution so to speak.

Q - Anurag Rana {BIO 7440273 <GO>}

Great. Another area that we have written about a lot and talked about is managed security services. Company like IBM and Accenture have very large practices that are dedicated to areas such as this. And what's your take on it, can you see uptake in managed cloud -- managed security services over the next few years or do you still see a much more aggressive embracement of product companies out there?

A - Nanda Santhana

Yeah, I think from a trend perspective, these managed security solutions providers are definitely helping especially the life sciences space, the manufacturing space, and the reason is very simple, right. I mean if you are a pharmaceutical company, you probably want to focus, especially times like this, you want the entire workforce to work towards one goal. And what you don't want is the security team focusing on, there is 101 triaging of cybersecurity incidents.

On the other side, the managed security service providers they have done a fantastic job in terms of providing repeatable process building up a team, they're specialized in automation, they work very closely with vendors in cybersecurity space. And so for those reasons, we definitely see the life sciences, the manufacturing and even in telecom in few places, they're all pivoting towards having the 101 operations, cybersecurity operations, go towards the managed security services or MDR which stands for Manage to Direct Response type of companies. They've outsourced their task. What they have in house is essentially security folks are working with business. The new term that we hear often is a frictionless security. And so they're repurposing their existing security professionals within the organization to focus on enabling that frictionless security and less worry about security engineering, worry about building that sort of center of excellence, if you will, and also develop a relationship with multiple vendors et cetera, so they don't want to manage that. So we for sure see a big rise in managed security service providers, definitely times like this right now.

Q - Anurag Rana {BIO 7440273 <GO>}

That's good. You did bring up a couple of verticals in between, is there any of the sense you're seeing over the last few months or even over the past few weeks, industries or verticals that are spending more on security products now that they did, let's say, a couple of years ago? Are there any industries that came back to you?

A - Nanda Santhana

Yeah, for sure. Prior to the COVID-19, the financial institutions were always the first adopters, if you will. Now post the COVID-19 what we see is in the space, the life sciences, especially the healthcare teams, they are forced to invest the lot. And I'll tell you a quick interesting story here, in one organization, the COO gets an email which looks like another peer hospital COO sending an email, but it's actually a fake email that went to the COO of the first organization, which basically requested for some sort of patient data or some sort of a cure or whatever that is going on. And because the name looked so much similar to an actual COO of the second organization, the first COO emails out the most sensitive data out, right. Especially right now, we -- these are the challenges that healthcare are definitely seeing. So the point that I'm trying to make here is the spend from a cybersecurity standpoint is actually getting better. They have to and it's getting better in life sciences overall, and we are also starting to see manufacturing companies' folks who have a lot of intellectual property and folks who are really worried about their business continuity and they are also spending a lot of money in and security products. So these are the two verticals that we see on the rise outside of the traditional financial institutions.

Q - Anurag Rana {BIO 7440273 <GO>}

One of the things we've talked about a lot over the years and it's the importance of machine learning and security. Oracle talks a lot about their autonomous database and how it can do self-patching, because one of the things you brought up as part of your suggestions and recommendations is for people to patch their software with the latest upgrade of whatever new patch they put in, but Oracle talks about it a lot for the databases. Do you think at the end of the day, we need security -- we need software products that can pretty much either patch themselves or do provisioning so that humans are basically taken out of the equation?

A - Nanda Santhana

I think the bigger concern here, Anurag, is actually patching is one piece of it. What to be patched, meaning, unless you have a first victim, it's really hard for organizations, the developers who are developing some of the softwares. There is a shift in this entire organization in the industry which is called making security to the left, right, meaning, pushing security to the left. What that essentially means is every developer who develops an application is cognizant about obviously the 101 vulnerabilities that exploits can -- the hackers can exploit those vulnerabilities and they're working towards making sure that they address those loopholes.

But oftentimes what we see is, whether it's the latest Magecart or Carbanak or whatever those attack of families are out there, the problem that we see is most of these developers cannot have that much of foresight in figuring out whatever they have developed actually potentially could be used as a back door or an entry for the attackers to come in. So the point that I'm trying to make here is, while the automation that most organizations, most cloud service providers, most vendor solutions are focused in patching the vulnerabilities. The key challenge is not in actually patching goes vulnerability, in identifying them and that's why it's called a Zero-day vulnerability, meaning, nobody else has discovered that. That's the challenge. And as long as that challenge exists, taking humans out and taking cybersecurity professionals out is going to be a challenge, I don't know, for sure.

Q - Anurag Rana {BIO 7440273 <GO>}

No, it's good. And my last question on this particular aspect of area. In terms of spending patterns, do you see that companies across all -- whoever your client base is in terms of different verticals, are they allocating money from like legacy security products into new security products or are you seeing a broad-based increase in all security products? What's your like current sense of the IT budgets that when you talk to CIOs and CISOs?

A - Nanda Santhana

Yeah, I think the pre- COVID-19, I could definitely see that the CISOs, which is the Chief Information Security Officers. They are now able to have a very good play or a very strong role in the Board meetings and they are able to brief the Board that one cybersecurity incident can exactly bring the company down both from a reputation perspective and in terms of profit that the organizations are going to get. So from that perspective, the overall spend on cybersecurity solutions have gone up significantly in the last three to four years. That's definitely a trend.

Now post COVID-19. I think some organizations are focused towards being a little bit careful in what they spend. And so what they're really analyzing right now is, do they really need the 101 compliance -- very strictly compliance focused solutions or do they need a Next-Gen solution. I mean from Securonix standpoint, what we have done is post this whole COVID-19 scenario, some of our threat models and, what we call a threat models is essentially how we detect some of these sophisticated threats, those things have completely changed because everybody is working from home. So the point that I'm trying to make here is, right now the setup is completely different. And so with that being said, I think some of our cybersecurity teams are really focused on probably decommissioning their legacy solutions, they are more focused on having the Next-Gen solution solving the actual problem in hand. And from what I hear from the news media, this whole COVID work from home could possibly be in waves and it is not a short-term, it's not a one-time thing. So if it's going to be in waves, we're going to expect to see users, employees, contractors, third-party vendors continuing to work from home. I really do think that the cybersecurity professionals are going to make a change in what they really going to spend, what tools are really going to stay or stick within an organization. I think they're making some of those tough decisions. Too early Anurag, we -- for us to be definitive on that, but we definitely think they're going to analyze it differently and really be careful on what they spend on.

Q - Anurag Rana {BIO 7440273 <GO>}

Nanda, any final words from you. Then I will wrap it up.

A - Nanda Santhana

No. I think, first of all, thank you for having me in this webinar. I definitely do want to thank all the front-line heroes. I hope everybody is safe at home. First outside of the digital world there -- washing their hands and making sure that they're continuing to do whatever the CDC is advising them to do. And big thanks to, like I said, the front-line heroes. I also want to thank Bloomberg for this opportunity for inviting me here.

Some of the threats that we are seeing is absolutely real, and from Securonix standpoint, we now have ready to go packages that we are ready to offer to a lot of our customers and prospects, and we would love for them to take advantage of it. Again, thank you Anurag for inviting me for the session.

Q - Anurag Rana {BIO 7440273 <GO>}

Great, thanks. So just to wrap it up. The replay of this session can be heard from the link that was sent on your webinar. We will have a transcript of this live on the terminal. And in any case, if you have any questions, you can reach out to me or Nanda. And a big thanks to Nanda here. He's one of the best storytellers I know. So great having you on.

So that concludes our session. Thanks, everybody.

A - Nanda Santhana

Thank you.