Beyond the Network: A Matter of Security

People are facing the ever-growing risk of having their personal information exposed in a data breach. According to the Identify Theft Resource Center, more than 446 million records were exposed in 2018 – up from about 198 million the year before. The nonprofit organization identified more than 1,200 publicly recorded breaches across multiple industries, including banking, business, education, government and healthcare. The numbers are disquieting, and no one knows how many more breaches are happening that go unreported.

How, then, are businesses tackling the challenge of protecting company and customer data? Cisco recently released its fifth annual Chief Information Security Officer (CISO) benchmark study. Its findings are based on a double-blind survey of more than 3,200 security leaders from 18 countries. The survey explores

- *How companies are training employees, managing security budgets and implementing best practices*
- *Their approaches to vendor and solution selection and alert management*
- *And finally, how they manage breaches in terms of what systems are affected, how much is lost, and how long it takes to recover.*

Arthur Woo sat down with Marisa Chancellor, senior director of Cisco's Security & Trust Organization, to discuss the CISO report as well as how Cisco approaches cyber risks internally. Listen, as they go Beyond the Network.

ARTHUR WOO: "Marisa, thanks very much for your time and for joining our show today."

MARISA CHANCELLOR: "Sure. I'm happy to be here."

ARTHUR: "So, before we jump in can you perhaps provide an introduction about maybe your team and their responsibilities in terms of information security?"

MARISA: "Well, to put it simply, our Information Security team is responsible for protecting Cisco while helping accelerate Cisco's business. So it's all about balancing risk and productivity."

ARTHUR: "So, recently I know that there was a report done – and we do this every year. We collect data from various CISOs – again, chief information security officers."

MARISA: "Say that fast."

ARTHUR: "It's a bit of a mouthful, right? And we talk to different customers from different sectors, different countries, and we gather this data and then we pull this together into kind of a report, which we then annually share with internally and with customers. Could you perhaps talk about some of the findings or some of the information that came from that data? Any surprises or new trends or issues that you may want to elaborate on?"

MARISA: "I think that it wasn't surprising, and not because that there isn't anything new, but in the security world we live in the day to day all the time so as new threats emerge we start to see that even before the report comes out. So, nothing surprising in that respect. I think, though, that what we are seeing is that organizations are having to respond to their businesses moving in – using a different business model. I'll use Cisco as an example. Our move to reoccuring revenue and sort of the business cycle around that, our move to cloud, introduces different security considerations whether it be in the business security side or in the information security side, but I think probably the biggest thing that we see is that the risk appetite from companies are changing. And that has a lot to

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

do with the level of publicity that these breaches, these very high profile breaches, are getting in the mainstream media. And so we're seeing at the very top – from the board of directors, from the executive leadership team – that the risk appetite is decreasing considerably when it comes to information security."

ARTHUR: "And so especially in this mobile world, this social world, things are moving so fast, communications happen so quickly, a lot of times you don't even know something's happen until you read about it and you don't even know if you can respond or not."

MARISA: "Yeah, you know, you're absolutely right. And we are so lucky here at Cisco to have the world's premier threat intelligence research organization by the name of Talos, and so they see things on a daily basis in terms of what's out there on the regular web and then they have their contacts into the dark web and the other underbelly components of the network and the Internet."

ARTHUR: "Interesting."

MARISA: "And they feed a lot of that information into our product in terms of signatures and other things to be aware of. But they also feed that information to our security incident response team, so we are always up to speed as to what to look out for."

ARTHUR: "So it sounds like a combination of being reactive but also very proactive."

MARISA: "Correct."

ARTHUR: "Because you can't just react you have to look ahead or try to be as proactive as possible and not just respond then."

MARISA: "Absolutely. Yes, I would agree."

ARTHUR: "So, let's talk about customers. There's probably a lot of things that are just on their mind and causing them to just really not sleep very well. Could you perhaps share some of the things that are happening or things that you've heard from them?"

MARISA: "Yeah, I would say that in most cases, whether I'm talking to a customer or to a partner, we all are in the same position when it comes to security. We all face the same challenges from the outside and from the inside as well. What allows me to sleep well at night is obviously that we have a great team here in terms of the security professionals and so it is a little bit of a luxury and we've just recently done some outside benchmarks against other peer industries and other peer companies and we're rated not just best in class but the best of the best when it comes – "

ARTHUR: "Congratulations."

MARISA: "– to our cybersecurity. Which is great, it's not to say that we don't still have work that we have to do. But when I think about what other customers are facing, one is the level of investment that they're getting from their companies when it comes to security, although as I mentioned their risk appetite is lowering so they're starting to invest more in that side of it. And sometimes I think it is, we have a lot of strong operational procedures here in Cisco, and in particular in Cisco IT, that help us tremendously. So just the fact that for example our desktop team looks at every security patch that comes from Apple or Microsoft and has a standardized procedure about how they're going to evaluate and what is their SLA before they send it out to all the desktops and laptops across the company, that is not a typical operational procedure that we see maybe in a small-medium business. It's all a little bit ad hoc. So I think coupling our knowledge and our operational excellence strength is what helps us sleep better, together."

ARTHUR: “It’s not necessarily based on size or number of resources it has to be relative to your company. So, whether you’re a big company or a small company it’s not about having lots of people, it’s about having the right processes and the right people and the right focus relative to their industry or their size that would be best.”

MARISA: “I would agree with that. And we have the luxury to also focus on automation. We can’t hire 600 people just to do security, so we have to look at ways at how we automate. How do we automate how we discover things? How do we automate how we get visibility into what’s happening? How do we automate control of our components in our network, etc.? And that allows us to operate at scale. Because we’re looking at tremendous amounts of data.”

ARTHUR: “Right.”

MARISA: “We look at 47 terabytes of network traffic on a daily basis when it comes to security data. And that’s huge. And so all that requires some type of, whether it’s scripting or AI type of capability to then go through this and determine what are those insights, what do we need to block, etc. And that’s the only way we can scale.”

ARTHUR: “And to build on your feedback on customers, do you have any perhaps guidance or advice for those who are maybe just starting to build a security practice or security discipline or those who already have a security practice or discipline but perhaps need to refocus or repivot because there’s always something new so I may have to change the way we do things a little bit.”

MARISA: “I would say at least what works here at Cisco and what resonates with the customers I talk to is that you move what you measure. And so if you measure where you are when it comes to security posture it moves the needle collectively because you either say I accept where I am or I believe this is a risk and I need to do something different.

And my advice to companies who are just getting started that it really comes down to doing the basic stuff. And what I mean by the basic stuff is having a secure set of operating models, meaning I’m patching my operating system to the latest security patches. I’m patching my applications to the latest security patches. I’m doing things up front before I deploy into my production environment by making sure that there’s scanning for vulnerabilities before they go live. Those types of things. Those are processes, those aren’t necessarily technologies, and that is the basic stuff that probably 93% of the companies out there fall into the trap of ‘Oh, I wouldn’t have gotten attacked had I just basically deployed that patch when I should have deployed it.’ “

ARTHUR: “Like table stakes.”

MARISA: “Yeah.”

ARTHUR: “Like this is a bare minimum. If you don’t even do this, you’re never going to be able to tackle the even complicated ones if you don’t even do this kind of base level is kind of what I’m hearing.”

MARISA: “Yeah, and you can be doing the more complicated things but if you don’t take care of your hygiene – ”

ARTHUR: “Right. That’s a good way to put it. Absolutely. So, let’s talk about the people side of security, because you’ve mentioned about patches and the technical aspects of it, but there’s obviously a people component. When you guys are looking at the threat landscape, not the technology side, but ok what do we need to make sure out people know about or do or not do in order to keep themselves safe but also Cisco safe as well?”

MARISA: “Well I can tell you sort of the joke in my family is I’m always, my kids or my husband they’re always sending me ‘Oh, the bank sent us this text or the cable provider sent us this thing,’ and my number one thing I keep going ‘Don’t click! Don’t click!’ And so it’s easy to say but you have to be scrupulous when you receive e-mails, when you receive – just don’t stick USB drives that you randomly get or you find someplace because you never know what’s on there. And so that’s kind of the simple things that you can do. But I think it’s also being aware. It’s no different when you're walking down a dark street. You want to be aware of your surroundings and aware of what could happen and that just makes you a little bit more vigilant about not clicking and downloading things where it's an unknown sender. Or it just looks a little suspicious. It's, you know, OPS instead of UPS. Like 'huh, I didn't know what that new shipping company was.' Those types of things."

ARTHUR: "And I know that within Cisco at least we're very fortunate that we're pretty much very open. Like, we let people surf wherever we want. We let them load and install things on our laptops and USB keys and things. It's very easy to do that, so –"

Marisa: "Yes."

ARTHUR: "I can imagine that just exponentially increases the things that we have to worry about, or what your team also has to be vigilant about."

MARISA: "Yeah."

ARTHUR: "Because there's just so many different potential opportunities. With openness comes… there's risk to that."

MARISA: "Absolutely. One of my colleagues used to joke that our biggest threat is the human being, the carbon life form out there. And when we talk to other companies about our practices in many cases, and we are a secure company, but when we say 'Oh, every employee has local admin rights to their laptops,' their jaws just drop. And they're going how can you be secure? It's oh, ok, but we have mitigating controls. And how we have mitigating controls is that, ah, to get connected to our network you have to be a trusted device. It's kind of like a carnival ride – it's like you must do these 10 things."

ARTHUR: "Yep."

MARISA: "You must be this tall to ride the ride. And we have great technology, once again, that helps us. Our Identity Services Engine looks at the posture that our trusted device offers. If it meets it, it says 'Ok, you can go onto the network.' If not, we may quarantine you or we may say 'No we're not going to let you on into the network.' And so even though we may do things that other companies may view as slightly insecure or even massively insecure we never do that without balancing with mitigating controls."

ARTHUR: "And I know that also inside the technology side it's definitely reinforced with the business side of where every Cisco employee has to sign the code of business conduct every year and say, 'Hey, you know, I'm responsible for my stuff and the resources that Cisco gives me or if something happens then I can get into big trouble as well, and I'm bound by that employee rule.' And every one of us has to do that every single year to kind of reinforce and remind us that hey, you know what this is not your personal stuff. We have to take responsibility so it's not just a technology side it's also the business side as well. "

MARISA: "You bring up a really good point. I think that accountability has definitely been permeated not just to the individual but as we share what our security posture is to our board of directors and to the ELT (executive leadership team) it's broken out by function and so they know that they are accountable. It's not just InfoSec but it's also the head of Customer Experience – Maria, she's accountable for the security posture of her organization and what she does. Same thing for Supply Chain, etc. We see that accountability being permeated not just at the individual level but at the organizational level and it's our executives and our board of directors who are holding, ensuring that those postures increase and commitments are made around increasing their security posture or health."

ARTHUR: "It's everybody's business. It's everybody's priority. And it has to be part of everybody's daily lives in one fashion or another. Maybe some more than less, but at the end of the day it's not like 'Oh, well we'll do

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

security later' or 'Oh, wait, I forgot I have to do security. Let me go back and do that.' It has to be a part of our lives is what I'm hearing."

MARISA: "It has to, and I would say it's not all roses today and there are people who still view security as a bolt-on to what they're doing, but if you think about any program or project that you're working on, you're accountable for understanding what the costs, the quality, the user experience of it, the delivery date of it. Security is another thing that you're accountable for. It isn't somebody else's responsibility. That is part of the entire product or package of that project you're delivering."

ARTHUR: "And then speaking of security being part of everybody's priority, there's one thing I actually wanted to talk to you about. It was fascinating as I was doing the research and I had actually never heard of this. I've heard of car insurance. I've heard of health insurance. I live in California so there's earthquake insurance but I've actually never heard of cyber insurance."

MARISA: "Cyber insurance started out I would say probably – I'm guessing – probably a decade ago and it was I think a little bit slow to sort become mainstream. But certainly in the last five years it is quite mainstream. Cisco buys cyber insurance policies and what it does is it's similar like with your health care provider is that it's encouraging you to do the things that would lead to sort of ongoing good health. For example your health care provider may say 'Ah, if you wear this health care device on your wrist and you walk 30 minutes a day I'm going to lower your insurance rates, because we know that walking will lead to better health outcomes.' And it's the same thing with cyber insurance and it encourages people to say if you do these things then we can lower your rates and it will lead you to better cyber security outcomes. Cisco has a partnership with Apple, with Allianz and Aon – Allianz and Aon are two large insurance providers – and the premise behind that partnership is that if you do these things and use these Cisco technologies that means that you are going to be in better shape from an operational excellence perspective when it comes to security and therefore we can lower your rates. And they will insure you for damages whether it's related to a breach. Now what it can't necessarily insure you against is around brand damage or loss of stock value related to an incident, those types of things. You can say it's up to this amount but there are – "

ARTHUR: "Stipulations or requirements or things like that. Fine details."

MARISA. "Yeah. Yeah".

ARTHUR: "Well, that's interesting. So, before we sign off, I would like to ask do you have any kind of takeaway or call to action?"

MARISA: "Security is part of everyone's role. Regardless of what function you're in or what type of work that you do and so embrace that. And I'll leave you with a last bit, which is once again what I tell my family, which is just don't click on anything."

ARTHUR: "Think before you click."

MARISA: "Think before you click, yes."

ARTHUR: "Absolutely. Yeah, always either do a search on it or hover over it first. Don't click! My goodness."

You've gone Beyond the Network, with Cisco IT. This episode was written and produced by Douglas Alger, and its interview conducted by Arthur Woo. Follow and like our podcast on SoundCloud or iTunes. Visit cisco.com/go/ciscoit for episode transcripts and related content. For more information and access to Cisco's complete Cybersecurity Report series, visit cisco.com/go/securityreports.

For More Information

To hear additional Beyond the Network podcasts, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)