Sean Gallagher:

Okay for our next panel, we're going to talk about a topic that sort of intersects with the last subject privacy information security. For many of us information security, the safety of the data on our phones and the networks of the companies we interact with and we work for is a thing that either gets in the way of us getting to what we want to do, or it's the thing that fails when we need it the most.

Sean Gallagher:

InfoSec is hard. I know all too well right now. It is harder than it should be. And we have by all accounts, a shortage of people to help us fix it. So in this next panel, we'll be discussing how we fix information security and reimagine it as both more personal and more ethical.

Sean Gallagher:

With that I'd like to introduce our panels for this next panel. Wendy Nather is the head of the advisory chief information security officer team at Cisco. She was previously the research director at the retail ISAC and 451 research leading IT security in the public and private sectors. She is also senior fellow of the Atlantic council and at the Robert Straus Center at the University of Texas, Wendy.

Sean Gallagher:

Vineetha Paruchuri is a security researcher, an esteemed one of that who solves real world problems by analyzing complexities between technology, public policy, law and economics. Paruchuri has worked at General Electric at the Indian Institute of Science and at Dartmouth College. And she's currently working on a computer science doctorate.

Sean Gallagher:

And last but not least of this [inaudible 00:01:59] is the VP of operations at Sychthe. Liz leverages almost two decades of legal, public policy, and business experience to build and scale cyber security and threat intelligence focused companies. Previously, she was a senior attorney responsible for technology projects and policy for Atlanta's ransomware incident response team. Liz, thanks for all being here.

Sean Gallagher:

So InfoSec, lots of fun. So wanted to start off by talking a little bit about why is information security so broken right now? We have, I don't know how many ransomware attacks in the past year. I spent a lot of time probing around into the wreckage of recent crypto ransomware attacks and other incidents. And it seems like people don't have the right things in place. They think they have the right things in place, but they don't.

Sean Gallagher:

They feel like they're overspending on security, but they're not actually because it's not the right kind. They can't find the right people to do it. But then they put out job requests that asks for 10 years of experience for entry level positions. How do we get this fixed? What's the status right now of InfoSec and how do we get past it? You want to take a crack of that, Wendy?

Wendy Nather:

Sure. I have a lot of thoughts on this. Contemplating how broken InfoSec is is something that I think is part of everybody's daily routine if you work in the field. There are several things. I find that first of all,

InfoSec started with a very authoritarian model back when the only time that you had access to technology was through your employer. They would issue it to you, they would manage it and they would decide how you were going to use it. And that is not the case anymore. Technology has become democratized for lack of a better word.

Wendy Nather:

But our security model has not been democratized. And we are still expecting people to receive wisdom in some technical fashion, from an employer as to how they're supposed to use things instead of making their own decisions in the context of their business work or their home life or whatever.

Wendy Nather:

And we were expecting them to understand security in the same way that this small group of very technical people did 20 or 30 years ago, that's unrealistic now. Security should be manageable and understandable by everybody in the context of what they're doing. They shouldn't have to learn the same thing that geeks do spending years studying this stuff.

Wendy Nather:

And then finally, every time we have an evolution in technology, there's a new demographic of people coming in to work with it. And it's not the same people over and over again. And that's why we see the same security mistakes being made with web, with mobile, with IOT, with biomechanics and everything else because they're different people. So we need to broaden where we teach security so that no matter who comes in, they have a basic understanding of what decisions they need to make and how to execute on them.

Vineetha Paruchuri:

So I have something to add. And I think that's what Wendy said is it goes in a lot of people who do security. So I think three things stand out for me. One, we are indeed placing too much onus on the end user, whether they're technical or not. For example, personal track models are like the closest we have for a regular person to assess what is safe and unsafe for them in terms of the decisions that they make. And this again goes back to the model Wendy was talking about where initially the people who did threat modeling or threat assessments were actual professionals. And now we are expecting a regular person to do this on consumer grade devices and internet connected devices, which when you think about it that way, it sounds ridiculous.

Vineetha Paruchuri:

Second, notice consent does not work. We wanted it to work. And the first time I said this in a bunch of peers, they were actually very resistant. They were like, "What do you mean notice consent does not work when we know what we are agreeing to. It's better than the case that we don't know." Sure. But how many security policies in terms of conditions are you going to read? There was a study where even when you take the shortest amount of time required to read a TC or like a security policy, it would still take you more than a year at least to know and understand and meaningfully, agree to read all the security policies for all the devices that you use in a single day. So is this really practical? Are you really consenting to what you know? Is that really consent? Is that really a choice?

Vineetha Paruchuri:

So notice choice is not really a choice. It's literally legal boiler plate where you're basically kind of covering.

Wendy Nather:

Covering buds.

Vineetha Paruchuri:

Yes.

Wendy Nather:

Yes.

Vineetha Paruchuri:

Didn't know whether I could say, but yes, that's exactly [inaudible 00:07:32] technical.

Elizabeth Wharton:

We can say something like that. Sorry.

Vineetha Paruchuri:

And the third thing is the whole data broker stuff in terms of data and what giving... Virus privacy matter because we are consenting to giving our data or foregoing some of our privacy toward something in a certain sense. And this creates a variance of perverse incentives. For example, it's like variances if you cap snakes will give you money and then people bread snakes so that they would get money for snakes.

Vineetha Paruchuri:

So when you think about data brokers and why they want your data, and even if you are finding them or enforcing policies, their literal revenue stream is through this data. So if you find 20% of their revenue for poor practices, it's still 80% more than what they would make, which is like zero. Because their literal business model is by harvesting your data. So then the whole premise is about kind of you foregoing your privacy and agreeing to things. How do you even counter this unless you change that premise. So I think these are the three things that stand out to me in terms of why everything's burning

Sean Gallagher:

Nice.

Elizabeth Wharton:

Well, there's that big data disconnect. You don't understand and really conceptualize what we're talking about and you can't without education of one, it's not just information. Think of the data as your healthcare information. So data care, but then you have that shift of now you know what we're talking about so now you're empowered to make better decisions. So you know what you're agreeing to. And one of the biggest steps in kind of building on what Vineetha was saying with you've got the data brokers de-identification by default. You should have to opt in rather than having to opt out. That it should be privacy by design. And once you're empowered and you're educated, then you can make the better decisions of how to protect it, what you're protecting and what you're agreeing to.

Sean Gallagher:

So let's get a little bit towards the nitty gritty here of why we have the problem in the first place. And that is that what we've built information systems on is fundamentally broken. The foundation of what we build on is got lots of holes in it. That's why there's a patch Tuesday every month. And that's why there's always an exploit Wednesday. What do we have to change about the way basic IT products are made and maintained to make it easier for people to secure them?

Wendy Nather:

Well, I hate to say it, but today we don't have a manufacturing model of software development. We have a literary model where everybody is doing their own artistic thing. It's their Magnum Opus. People are writing things that they don't need to write. And I think in the future, we're going to have to take away choice in a lot of our critical components and say, there is only one way that you can put safety controls into a car or into software. And I'm sorry, but you cannot get creative with this. You can't pivot and do something completely different for the sake of the common welfare, for common security. We're going to have to cut back on how many different ways you can do something. And we have to use tried and tested components. We're starting to get there today with things like the software bill of materials, where you at least can look at and know what's in the software.

Wendy Nather:

But the very big question comes after that. What do you say about it? What are informed consumers looking at an SBO and saying, this is too high risk. We're not going to accept this. Are there enough economic incentives in the marketplace to drive us in the right direction? Or are we going to have to just put something down and say, "Look for critical infrastructure, you cannot get creative. We have to simplify continually. We have to make this accessible and understandable, and that's going to have to be in the service of general security."

Vineetha Paruchuri:

So there are other things we could do for spaces other than critical security. There was a study where even if you educate people about security, even within one system, and these are professional software developers. Although you know about security, your brain can only hold so many decisions at one point. So that is like your heuristics of decision making in any human brain, irrespective of whether you know security or not.

Vineetha Paruchuri:

So what they tried was to give prompts to software developers through the tools so that even though they know the concepts of security, they would functionally code more securely. So for example, yeah, if you get a prompt, then maybe your education would kick in and you would know why you're being prompted, but these are not just warnings. Again, that goes back to decision fatigue and notice choice where you just like, ignore, ignore, ignore. It's like clicking. I agree. I agree. I agree.

Vineetha Paruchuri:

So what I mean is functionally helpful prompts that would work with the human decision making capabilities that work with the heuristics of the human brain, how people make choices, thinking fast and slow is one popular example. Daniel Conman did this, but they're being explored in economics as cost of like picking one stock or the other. But the same could be applied in security. And people haven't

really tried that yet. And from my understanding, it shows potential. The map seems to work out. That is probably another direction we could take in terms of making it simpler for people to make more secure decisions. And when I say people, not just regular people, but also professionals. Because even as professionals, we cannot foresee literally every possibility that would occur in a really large system that's basically glued together with tape. So

Elizabeth Wharton:

Let's say tape bubble gum, duck tape. But that's why it's important to also kind of when you're designing and when you're building flip the switch. So that it's not, again, going back to that, you're not opting like, oh cookie tracking via good. But when you look at consumers, like, do I really know what I'm agreeing to or in the de-identification do I have to opt in to the retailers, the marketers, being able to track my information, putting the burden, not on the everyday consumer who isn't in the best position, perhaps to make the decision, but putting the burden back on the business team, the design team, the software team that says, "Hey, yeah, this is a business decision to design and go with this piece rather than that piece, because who in the world would ever take advantage of a wireless mouse to then gain access to the entire laptop?"

Elizabeth Wharton:

Because it's just this little dongle you're just going to put, but, and Logitech had it in their decision making tree of like, this was a business decision. We went for this piece over that piece, fast forward, what, 10 years later. And it's a threat point.

Vineetha Paruchuri:

Yeah. That USB attack is exactly how that works. Yeah.

Wendy Nather:

And in an enterprise a lot of developers will simply collect everything in case the business decides it needs it later. So that's that's the default with everything. And so changing those models as well and making this sort of software designed to last a long time, rather than, oh, we're just going to patch it the next time we see a problem. Longer term thinking in the design is also going to be very important.

Vineetha Paruchuri:

Yeah. Very simply. But you cannot lose the data that you do not have.

Sean Gallagher:

Yeah. And it seems to be like, so there's a lot of this where, especially with small organizations, they outsource a lot of the handling of these tasks where they have a service provider that helps them.

Sean Gallagher:

One of the things I saw recently, service provider providing a specific type of service to a government organization required inbound remote desktop protocol access to a server on the network in order for them to be able to support it. And that it required the firewall be open for them to come in.

Sean Gallagher:

So this comes down to software design and service design. As we become more dependent upon other people to do things for us, which is really honestly essential for InfoSec for smaller organizations, because they can't staff up.

Sean Gallagher:

Aside from a software bill of lading and things like that, how do we get companies to act ethically and how they deploy product to make sure that we can secure the product, and the flip side of that is information security providers. How do information security providers do a good ethical job of handling the cases for these smaller customers and keep keeping them from getting into trouble?

Vineetha Paruchuri:

May I take that? So in terms of ethics, I don't think initially at least companies are trying to be overtly unethical. I think the simple question here is people are doing to do what is easy and what is, if not cheap, at least not costly.

Vineetha Paruchuri:

So these are, I think the two driving forces behind any of these decisions. And ethics comes in as long as it's convenient because when money is involved and when you do the trade off, if you're going to earn this much or lose this much as opposed to ethics, which again is relative in terms of what people consider ethical or not. So I feel like if we make these decisions easier and cheaper, that would automatically shift these kinds of decisions that may make the system insecure.

Vineetha Paruchuri:

There are multiple ways which we could make it easier. For example, one of the approaches that I said in terms of working with human decisions, heuristic decisions, and other approaches, maybe seeing what we can do on scale or adopting that as a standard, which then makes it an equal playground for everyone else.

Vineetha Paruchuri:

So it's not like you are making more money or less money as opposed to somebody else who has to follow the same standard. So I feel like if these two primary driving factors are taken care of, the ethics part would automatically fall in line. Because no one at least... Okay, call me cynical. But I don't think people are sitting here and thinking about businesses or sitting here thinking about, "Okay, I will do this if it's ethical, although I would lose 20% off my revenue." I have not seen a business person think that way.

Wendy Nather:

Oh hi. No, but actually I was going to say, I don't think it's so much that businesses are unethical that there are constraints and trade offs that they have to make. If you think about business wise, if you don't implement a certain type of security that's going to cost until just before you need it. And then you've implemented it and you've avoided a certain risk event. Then you are a wise business person you did it right. That was good stewardship of funds. And so this is always going to be a driver. And the key is the timing. If you're a startup, you're not going to hire a chief information security officer and put in all sorts of expensive things until your risk model is at the point where you're going to start needing to protect against certain types of attacks.

Wendy Nather:

But again, it's all in the timing. Sometimes businesses are lucky and they get it right. And sometimes they're not lucky. And they say, "Oh, we were just about to deploy MFA, but this happened instead." So that's another thing that we have to take into account.

Sean Gallagher:

Sure.

Elizabeth Wharton:

Well, and it's like back putting on my former city attorney hat and looking at the conversations we were having. It's that education of reminding kind of the, do we really need this data? That it's not just information, it's not just, again, that esoteric system. It's like, no, this is city data and it doesn't have to be personal data, but it's information. It's data that we have. And this vendor wants to set up this or do X. Well, it's taxpayer data, it's taxpayer information, do we know what that means? Do they really need this? Are they going to use it for this or are they going to use it too? And so educating even the consumer, but not the individual consumer, but the businesses to say, "Hey, this is a decision that's being made. You can push back, you can say, no, we prefer not to do that. Or no, let's keep this setting on."

Sean Gallagher:

So we've got a few minutes left. I want to get to the personnel side of things. I want to get to the human side of this thing. By all accounts, we don't have enough people who understand information security at a level required to implement it. Organizations don't have enough people. At the same time I hear people, there was a survey recently that said people felt they were overspending on security.

Sean Gallagher:

How do we get the people into the pipeline that represent the people that need to be protected? How do we get a more democratized workforce in information security and get past this? So that sort of must have CISSP 10 years experience with this product as like four years old.

Wendy Nather:

I think it is not as big of a problem as people seem to think it is. You have to broaden your vision as to who can make security decisions. If you're writing on the Metro and you start talking to the person next to you, chances are no matter what walk of life they come from they are capable of making good risk and security decisions. You simply have to give them the chance. And you need to start early.

Wendy Nather:

For example, I don't use parental controls on my kids' devices. And one day my 17 year old came to me and said, "Can you help me turn on the parental controls?" And I'm like, "Why?" And she wanted to use them for her purposes to enforce her own study time. And I said, "Great. You set it up the way you want it. I will put on a password and whenever you want to change it, you bring it back to me."

Wendy Nather:

But the thing is she was making the decisions in the context that made sense for her. And I firmly believe that we can teach everyone to do that. Once you do that, you do not have to hire geeks. And although

they are great to have, but there are lots of people from diverse backgrounds at any age who we can bring in to the pipeline and we should start doing that right away.

Sean Gallagher:

Well, the readers of ours, technically, if they look back at my articles will find how I taught my kids information security. It wasn't that way. But Liz. So I'm sorry. [inaudible 00:23:43].

Elizabeth Wharton:

Oh, no, I will take being mistaken for Wendy Nather any day.

Sean Gallagher:

Okay. Sorry. Ain't no problem. So, Liz.

Elizabeth Wharton:

And twice on a day is till okay.

Sean Gallagher:

So how do you feel we deal with the manpower, woman power issue here, the personnel problem and [inaudible 00:23:59].

Elizabeth Wharton:

Well, when you look at this panel and perhaps even like, I did not come to my career path as I went to a technical school, but I was a communications major. But because concepts were broken down and then explained through other work I was doing. Yeah. Again, it's kind of that educating about breaking it down into those little bits and understanding you don't need 10 years experience to do this. Can you identify a problem? Do you have the ability to come up with solutions, be willing to be wrong, be willing to be right and defend yourself?

Vineetha Paruchuri:

Yeah, that really is what it boils down to. I think barriers of entry. So for example, I have a master's in computer science, I'm doing a PhD in computer science now. But it's actually a lot of things I do in security don't really deal with a lot of computer assigned stuff. Yes, I do algorithms. And I know how to script things and I can understand what the systems mean. But at the end of the day, it boils down to how do you assess the risk or the threat in terms of these decisions that you make in these kinds of systems?

Vineetha Paruchuri:

So there's like a policy component added to a lot of security stuff. And there's also like the human aspect as to understanding how people make decisions. So these need to come together. But the downside of it is like a lot of times when computer scientists think this way, they are perceived as not very technical or soft skills. And the credibility is taken away a little bit.

Vineetha Paruchuri:

And that's why I had to state what my degrees were in. Like, I don't really care. I could have measured in bungee jumping for all I know. And it would still be the same, security problems would still be the same. It all depends to whether or not you're able to understand the system and understand the risks in the system. And understand how people make decisions, and understand where the law stands and how the policies work.

Vineetha Paruchuri:

And so in terms of all of this, I think the barriers of entry is not that we don't know that this is what it takes to work, but in terms of accepting the credibility of somebody, for example, somebody who's not doing computer science would probably make decisions the way I make decisions in terms of assisting-

Wendy Nather:

I'm an arts major.

Sean Gallagher:

Yes.

Elizabeth Wharton:

Yes.

Vineetha Paruchuri:

Right.

Sean Gallagher:

Same here.

Vineetha Paruchuri:

And I don't see them being brought on as much. And I would like for it to change. Where more people from humanities and sociological and legal backgrounds would do security.

Sean Gallagher:

Well here lost to talk about critical thinking skills and that it's not necessarily something that's a comp sci thing.

Vineetha Paruchuri:

Yes. But a lot of times when you go for interview, they want to see how you do algorithms and how you do me math side. You can do big off something or the other.

Sean Gallagher:

Yeah. We can do a whole rundown of bad interview questions [inaudible 00:27:16] that job.

Elizabeth Wharton:

Well, to say, how many CVs do you have to your name? Yeah. How many repo pools do you have? Like, oh.

Vineetha Paruchuri:

How active are you on GitHub? Yeah.

Sean Gallagher:

Well, we could go on forever on this. I wish we could, but we can't. We're running out of time. So I'd like to thank you, Wendy, Vineetha, Liz for joining me for this. It's has been great. Hope we can carry on the conversation outside. Thank you all for joining us for this. And I will catch you out in [inaudible 00:27:50].

Vineetha Paruchuri:

It was nice talking to you.

Sean Gallagher:

It was great to see you, great to have you all in person.