Tech show branding sequence begins with montage of colorful graphics interspersed with closeups of circuit boards and hardware tools. Cut to a digital clock on a desk as it strikes midnight.

Transition to a residential garage door with the words Lenovo Late Night I.T. prominently displayed.

The garage door opens to reveal an open workspace with a relaxed environment. Show host Baratunde Thurston and his guests Rahul Telang and Renee Guttmann sit at a large wooden bench in the middle of the garage. Cut to a closeup of host Baratunde Thurston speaking. The shot pans out as he turns towards his guests.

Baratunde Thurston (00:10):

Welcome to Lenovo Late Night I.T., where industry insiders tell us what they tell their therapists. We like to ask the questions' nobody's asking. Today's question, is ransomware a good thing? I'm here with Rahul Telang, one of the world's foremost experts in the economics of information security, privacy, and copyright infringement in digital media. Rahul is a professor of information systems and management at Carnegie Mellon University. He's also the author of Streaming, Sharing, Stealing: Big Data and the Future of Entertainment. A huge movie buff, he also wrote an academic paper on Bollywood films and piracy.

Joining us as well is Renee Guttman. Renee has more than 25 years of experience managing technology risk for multinational corporations. And she was one of the first women in the cybersecurity industry overall. She was the CISO at Coca-Cola, Royal Caribbean, and Campbell Soup Company. That's soda, ships, and soup, very alliterative, I like that. She created Time Warner's information security program and was AOL Time Warner's first chief privacy officer. She also nannied for a count and a countess when she was 21. I dare you to top that. Seriously, you can't top that. She's the dopest, she's the goat. Welcome Renee, Rahul, how y'all doing?

Renee Guttman (01:26):

I'm great. How are you?

Baratunde Thurston (01:27):

I'm doing well, thanks for asking. No one ever asks me how I'm doing. I'm already liking you.

Renee Guttman (01:31):

Well, you're looking marvelous.

Baratunde Thurston (01:31):

Oh yeah, flattery will get you everywhere. Rahul, you wrote this provocative article saying that ransomware was a good thing. So I have two questions for you. First, how much did the cyber criminals pay you to write that article? And second, what are you talking about?

Rahul Telang (01:46):

I think one has to be a little bit careful. What I mean is good, I said it's good for consumers. I didn't say it's good for the firm. For the last 20 years, we hear about cybercrime, data breaches, malware, virus, X Y Z. That has been going on for the last 20 years, and I think it will not end anytime soon. However, if you look carefully, almost all the losses there happen to the consumer. If the data was breached, if malware happened, it's me actually who lost, not the firm. Typically, the way our economy works is that if I lose something, the firm actually takes care of me, so they will respond. So if you think about it, if something bad happens to me, the firm will say, "Something is bad to my customer," and they'll say, "Okay, I'll make sure that doesn't happen."

Baratunde Thurston (02:42):

Yeah. They'll change their practices because if we get hurt, that's still bad for them.

Rahul Telang (02:47):

Exactly.

Baratunde Thurston (02:48):

But that's not been happening.

Rahul Telang (02:49):

So we have so much data, they take the data and monetize it. They make the money from that. In the process, some data gets breached, some data gets lost. Some sort of untoward accident happens. In that case, I am the one losing, not they. And they know they take care of me somewhat, but not completely. So they don't take care of my data with as much diligence that I will do that.

Baratunde Thurston (03:17):

Well, especially if we keep showing up as customers.

Rahul Telang (03:20):

Absolutely, we keep showing up.

Baratunde Thurston (03:23):

So it sounds like your argument is they're finally the primary target.

Rahul Telang (03:27):

And they're finally the primary target. Now their feet are held to the fire. So now you can imagine with that you will expect that they will actually be more cautious about the security.

Baratunde Thurston (03:41):

So then Renee, as someone who's been in a lot of these large firms and corporations, one, I'd love to know what's your take on Rahul's argument that companies have not taken cybersecurity as seriously because they haven't been the primary targets, but now with ransomware they might step up their game. Do you buy that argument? Do you argue with it?

Renee Guttman (03:59):

I think it's interesting. I think it's an interesting-

Baratunde Thurston (04:02):

Is that a euphemism for you're wrong?

Renee Guttman (04:06):

Because I do think companies have taken it seriously because there have been mitigating controls put in place. I worked at a company and a tape fell off a truck. Just imagine a tape falling off a truck today.

Baratunde Thurston (04:17):

A tape full of data?

Renee Guttman (04:18):

Full of data. That's what used to happen in the early days, tapes would fall off trucks. And that's sort of a fine line that creates that, "Well, do I report? Don't I report?" Because you have actually lost control. And so that's where a lot of the teeth gnashing, and companies now have to start making decisions about whether to report or not. So I do think a lot of companies, even today, I mean, people don't report. We know that. So I don't know that it's a big shift. And I think that companies have been responsible, it's just that now they are more the focus of attention.

Baratunde Thurston (04:53):

So when I think of ransomware, it feels like old school mafia protection racket. It's like, "Oh, that's a nice CRM you got there, be a shame if something happened to it. That's a nice water infrastructure operating plan you got there. You want it back, you pay me." And I see it from the outside through reporting, and it sounds terrifying every time. Like a huge deal and cities stop working, businesses shut down, and I guess they're paying in a lot of cases, but how big of a threat is ransomware? What do you both think about that? Because to me it's just an increasing and horrifying prospect.

Rahul Telang (05:27):

So yes, it's a big, big deal. My feeling is that over time, the firms will figure out how to cope with that. So it will kind of reduce. The second thing is that currently we actually don't have good numbers on how many firms are getting affected by ransomware. So a lot of time the firm get a ransomware attack, nothing gets disclosed. We don't have data, we don't have information, we don't have any idea. So right now it's all speculation. Depending on who you read, somebody will say, "Okay, 40% of the attacks are ransomware." Somebody will say, "It's a minor thing." So all we know is that we see that the things are getting worse, but we also know that they will get better.

Baratunde Thurston (06:17):

What are your thoughts, Renee, on how serious the threat of ransomware is?

Renee Guttman (06:20):

I think it's a big deal. And I think it's a big deal because it really does not only impact the victim, but it may impact the ecosystem. I don't believe that mankind can change their spots. So whatever we used to do and maybe run the risk of getting caught, now we have a better chance of doing it not being caught. But we can't fundamentally change our spots.

Baratunde Thurston (06:40):

Okay. What have we learned from some of the successful ransomware attacks in terms of how to better defend, how to better report, how to communicate, any lessons from this?

Rahul Telang (06:50):

It's a very tricky question because the moment the ransomware attack happens, you basically can't move an inch forward. That is you're frozen. You can't access your data, you can't access your computer. Now, what choice do you have? The choice is either you pay or you do something else. So the lesson actually is before something happens. But before that, you can plan. You can kind of imagine like you imagine that if I get hit by the ransomware, what will I do? What is my escape route? And I think that will play a role in how do we respond to that. Because once you get hit, then the question is, should I pay or should I go to FBI, or should I go to newspaper? Those are not good choices.

Renee Guttman (07:40):

I think that's actually a key thing. I mean, we have been talking things like business resiliency and business continuity and having a good backup, and, you know, what do you restore first? And all of those things and the business, I don't have time for that today. I don't-

Baratunde Thurston (07:58):

[inaudible 00:07:58] response. I don't have time to prepare.

Renee Guttman (07:59):

Well, look it, I don't... What to restore first, to make these decisions upfront, to say that team's going to be responsible for recovering X if something bad happens, your team is going to be responsible for Y, we're going to have project managers and treat it very seriously.

Baratunde Thurston (08:17):

When I think about fire drills, we practice for the disaster. The bell rings, you go to your meeting place in the garage, or you practice the escape routes, make sure the fire escapes actually work. Are companies practicing ransomware attacks? Are they simulating, "We've lost all of our systems, let's make sure those backups we said we've been making actually exist and see if we can get the business back online."

Rahul Telang (08:43):

How do you take care of the ransomware attack? After it happens, how do you recover? It's not so simple. Easy thing could be that "Okay, I will not pay the ransom."

Baratunde Thurston (08:53):

Right, yeah. Don't let the terrorists win. I like that, it's very tough.

Rahul Telang (08:57):

But that means that if you don't pay the ransom, you should be able to function with somewhat competence. And that requires that the data that they have encrypted, you are able to replace that. So you should have the backup as she mentioned that you should have the backup, that somehow, you're able to replace the data with the backup and get to the function. Now to do the fire drill is not so easy. So you can do short scale, but not at the large scale. The simple fact is that there's so much data that the firms have...

Baratunde Thurston (09:34):

A practice to restore [crosstalk 00:09:37]

Renee Guttman (09:37):

There's no way to simulate your entire company going down. So 50,000 workstations, well, let's do a fire drill around that. So let's just kill all 50,000 workstations and see if it takes us more than nine days to recover.

Baratunde Thurston (09:52):

What if you did it randomly to the employees you didn't like?

Rahul Telang (09:58):

I don't know if that's a ransomware response.

Baratunde Thurston (10:01):

That's why I'm not a CISO. Okay.

Renee Guttman (10:03):

You know what, but you do bring up a good point, because philosophically I do believe that you do better training your employees because now it's a different topic, and you use carrots and not sticks.

Rahul Telang (10:16):

So the major reason or one of the most prominent way somebody gets a ransomware attack is somebody clicks on the phishing email. So employee clicks on email, download something, you want to stop them from doing that. So you can simulate that. So the question is that if somebody clicks on that, that will give you a signal that this guy is not paying attention.

Renee Guttman (10:43):

There are things called lures, and there are things... Fishing lures...

Baratunde Thurston (10:45):

It's called fishing. Oh my goodness. I'm an idiot. I just got it.

Renee Guttman (10:50):

So if I send you an email that says we're moving offices. You're coming back after COVID, your offices are changing locations. And click here for your new office assignment. I bet you people will click. So at that point, you look, and you see, "Okay, well, who commonly clicks?" And maybe you want to do some more advanced training, to your point, delete their computer, but you don't do that. You don't do that.

Baratunde Thurston (11:21):

No, that's a very aggressive response.

Renee Guttman (11:22):

That's very aggressive.

Baratunde Thurston (11:23):

Well, you said carrots not sticks. So what's the carrot?

Renee Guttman (11:25):

And I do believe that I do believe that. Because I have found if you say, "Look, when in doubt, report." All right. So I won't penalize you for reporting.

Baratunde Thurston (11:36):

So insulting people, not a great strategy.

Renee Guttman (11:39):

I'm not so sure.

Rahul Telang (11:40):

I mean, if you think about it, this whole phishing thing has been going on for last 20 years. So we know that the phishing email should not be clicked, but now the consequence of that is enormous.

Renee Guttman (11:53):

So you can actually make it a bit competitive and say, "Okay, well, that unit consistently does better than that unit." So you can actually create a little bit more of a gamification or a different approach to it to the point where people are like, "I got it. You know, I used to get attacks all the time, you couldn't fool me, you couldn't fool me."

Baratunde Thurston (12:13):

People are proud of themselves. Yeah, yeah.

Rahul Telang (12:16):

With this kind of simulation, you can actually test what strategy or what carrots actually work. So you might try thing A and you see how people respond. Then you might try thing B and then see how people respond. That way you get an idea that what is clicking? What do I say that is actually internalized by my employee? So that is a good tool that way.

Baratunde Thurston (12:39):

When it comes to cybersecurity, there's a pretty big knowledge gap between people in the tech world and the general public. To get a better sense of how wide that gap really is, we sent a team out to the streets of New York City and asked random strangers what they know about cybersecurity. Here's what we found out.

The screen cuts to a wide aerial view of New York City. A montage showing the streets of New York and people laughing flashes across the screen. A pedestrian stop light changes from stop to go as the words Tech Walks appear next to it. A man holding a microphone interviews various people outdoors in New York City.

Tech Walks host (13:03):

All right. So we just want to get a little bit of background demographic, just basic information. Where are you from? What town are you from? What was your first car? What was the name of your best friend? What's your mother's maiden name?

Interviewee 1 (13:14):

I feel like this is getting-

Tech Walks host (13:14):

It doesn't matter, I've already stolen your entire identity. Check your bank account. Our topic today is in fact cybersecurity. What do you do?

Interviewee 2 (13:21):

I work as a cybersecurity consultant.

Tech Walks host (13:24):

That's bullshit.

Interviewee 2 (13:25):

No, I'm deadass. Am I allowed to cuss?

Tech Walks host (13:30):

I don't fucking know. So first off, what is cybersecurity?

Interviewee 3 (13:34):

Oh, we're starting with me, okay.

Tech Walks host (13:36):

Yeah, because she'll give it away.

Interviewee 4 (13:37):

Making sure that we're safe. We're so exposed now by giving passwords and this online, and it's very easy for people to access your information. So we want to make sure that it's safe.

Tech Walks host (13:46):

Do you know what ransomware is?

Interviewee 5 (13:46):

Oh yes.

Tech Walks host (13:47):

What's ransomware?

Interviewee 5 (13:48):

Ransomware is when they steal your data and make you pay to get it back.

Tech Walks host (13:52):

So you write them on your computer? That is literally the worst place to write your password. I'm going to list some devices and you tell me if you think they can be hacked, okay? Phone?

Interviewee 4 (14:02):

Yes.

Tech Walks host (14:02):

Coffee maker?

Interviewee 6 (14:03):

Yes.

Tech Walks host (14:04):

Pacemaker?

Interviewee 7 (14:04):

Yes.

Tech Walks host (14:05):

House plant?

Interviewee 4 (14:06):

Hundred percent.

Tech Walks host (14:08):

Garage door opener?

Interviewee 6 (14:09):

Yes, I think so.

Tech Walks host (14:10):

That's amazing. You got hundred percent right. How did you know?

Interviewee 6 (14:14):

That's what it all sounds like, things you can break into.

Tech Walks host (14:16):

As a cybersecurity expert, what worries you the most?

Interviewee 2 (14:18):

Since COVID has hit, everyone has actually moved to a more obviously virtual environment. Ransomware hits have been increasing, and everyone's also moving to cloud. I feel like in general there can be better awareness about like phishing and stuff like that. And people definitely don't know enough. Also, all the old people just always click on that type of stuff.

Tech Walks host (14:38):

Are you saying I'm old?

Interviewee 2 (14:40):

No, I did not. I did not say that.

Tech Walks host (14:41):

Hypothetically, if I stole all the information on your computer, everything, all the files, everything, $500.

Interviewee 6 (14:48):

I don't own a computer. I'm sorry.

Tech Walks host (14:50):

Oh man, this is tough. Do you own a phone?

Interviewee 6 (14:53):

Yeah.

Tech Walks host (14:53):

What is this thing? Is this a... Do I...

Interviewee 6 (14:57):

Flip it.

Tech Walks host (14:57):

Flip it?

Baratunde Thurston (15:02):

All right. What did y'all think of our tech walk video?

Rahul Telang (15:06):

I was surprised that people knew quite a bit. I thought they would be kind of, "What is this? What is this?" Ransomware, people knew.

Baratunde Thurston (15:14):

It was a great definition of ransomware. And I loved the guy who was like, "Can this be hacked? Yes. Can this be hacked? Yes, because they all sound like things you could break into."

Rahul Telang (15:14):

I think they understood the word ransom.

Renee Guttman (15:22):

But the house plant.

Baratunde Thurston (15:22):

The house plant, yeah, he was just saying yes. It was like the multiple-choice answer, you just go down the same column.

Renee Guttman (15:29):

I think a house plant could hack you, but... Well, I'm kidding.

Baratunde Thurston (15:34):

I was like, "What do you know?" See, when you make a joke about security, I take it seriously.

Renee Guttman (15:39):

I know, I know. People put my phone number, you know, when I'd call into their like, "Okay, it's Renee calling." And they were like literally, "Do I pick it up? Do I Do I? Why was she calling me? What could this be?"

Baratunde Thurston (15:53):

Oh, because they assume something bad happened. [crosstalk 00:15:55] You got to get a burner phone just to call people, so they don't freak out and they actually answer. What did you notice about the video? Anything stand out to you?

Renee Guttman (16:05):

I'm not surprised. That's why, I mean, our date was going to happen, right, because you read newspapers. I knew right away I liked you. Or maybe you don't read newspaper, but you go online. I'm not surprised. I'm not surprised.

Baratunde Thurston (16:18):

I was surprised to just stumble across a cybersecurity person.

Renee Guttman (16:21):

I was too, but she swore, and I was like, "Okay, she's a cybersecurity person."

Baratunde Thurston (16:26):

She kept it very real. That was New York and cybersecurity...

Renee Guttman (16:31):

At its finest.

Baratunde Thurston (16:32):

[inaudible 00:16:32] together. Do you pay the ransom?

Renee Guttman (16:38):

That's above my pay grade.

Baratunde Thurston (16:40):

Really? Who answers that question? Is that the CEO answers that question?

Renee Guttman (16:45):

I think the company does. I think the company decides that up front, and they take a position.

Baratunde Thurston (16:48):

Are you in the meeting where that decision gets made?

Renee Guttman (16:49):

Generally, but I haven't been there. We've had this conversation, and, you know, I talk to... Well, and even the research says a lot of companies do pay.

Rahul Telang (16:59):

Absolutely.

Baratunde Thurston (17:01):

Would you pay, Rahul?

Rahul Telang (17:03):

That's a really difficult question. Okay, I'll give you a simple analogy. When there's hijacking of an airplane, okay? The US government policy was we will not pay ransom to anybody.

Baratunde Thurston (17:16):

Yeah. I saw it in all the movies, and those are factual.

Rahul Telang (17:20):

But I also know that the other governments, other countries, even though they have the resolve, when the actual thing happens, they may not do it. So I feel ransomware has the same flavor. That you kind of believe that you should not do it, but then you say, "If I don't do it, I lose this, this, this, this. Am I willing to bear that brunt or, you know, I can get away by paying five million, 10 million." What is the ethical part? What is the unethical part? What are the economic part? That's a really difficult question. I mean, if I look at the ransomware, our thought or focus is how much ransom are you paying? But the moment you go down for three days, four days, the losses percolate all the way, your customers, your suppliers, everybody's suffering. And we don't measure that. So again, the way I think about-

Baratunde Thurston (18:20):

Well, it must not be a problem if we're not measuring it.

Rahul Telang (18:22):

That is one issue that people talk, hide it under the carpet. But, you know, that is what I'm saying that as we become more and more IT, our network, the more and more we are going to be affected by any disruption.

Renee Guttman (18:40):

I was talking to somebody who was telling me that in healthcare, they might do something in the hospital. Well, now you're not conducting surgeries. So I think there's a life and limb component to this thing now. And where I get most afraid is the crossover into safety and people's perception of safety.

Baratunde Thurston (19:03):

Do you think, putting your business hats on, is ransomware a good business model?

Rahul Telang (19:07):

Suppose I breach you and steal your data.

Baratunde Thurston (19:10):

I don't like it, I don't like you, but keep going with the analogy.

Rahul Telang (19:13):

I understand. But how do I make money from that? I sell your credit card for $1, $2, whatever. So my ability to make money from all this activity is kind of stretched over a period of time, and I don't even know. On the other hand, if I have a ransomware and I say, "If you don't pay me $5 million, I will not decrypt. So you can imagine, what do I do? I can make the money right now, right then.

Baratunde Thurston (19:40):

I go back to old school burglary. If you stole a bunch of art and goods from someone's house, then you got to fence it somewhere. You got to find a secondary person, you got this chop shop over here. And that could take, like you said, time. And it's complex and probably exposes you to more risk the more other people you communicate with trying to fence these stolen goods. Or you can just sell it back to the homeowner. You're just stealing, and then selling back to the people you stole from, which is a simpler business model for sure. How do you, Renee, tell "good guys" from "bad guys" in this world we're talking about, where the boundaries seem to be shifting. You have vulnerabilities and markets around those. You've got tools and markets around that. You've got employees who are making innocent mistakes. You've got companies who are trying to weigh ethically and financially to pay or not to pay. Just as a person, how do you navigate that? It seems really hard.

Renee Guttman (20:39):

For me, the biggest concern that I have is still safety. I think when that line, when those lines are crossed, that's what really worries me the most. The money part I get, but the safety part really does worry me. And it's hard because even the good guys that will call you and say, "Listen, we found X, and, you know, we're letting you know. But it's a product vendor. And then you struggle with even, do I believe you or are you making it up to sell me something? My children think that I'm a wildly paranoid person, and I try not to be all the time. But it's a little... I don't know that I have a better answer than that. It's just difficult.

Baratunde Thurston (21:22):

Because technology is everywhere now, all kinds of places are getting hit with ransomware attacks that don't have the resources. I think of my in-laws, you know, who get sucked into scams and malware things, and they would not know what to do if they lost all their... They would call me actually. I'm the CISO in the family. And I think of small governments, I think of nonprofit organizations, how do we prepare folks who don't have the budget financially or technologically to withstand or recover from something like this? What might work there?

Renee Guttman (21:57):

The government has put out the cisa.gov I think is the name of the site. And I read some of it last night, and I thought, "Man, this is a good list."

Baratunde Thurston (22:08):

What is on this government website?

Renee Guttman (22:10):

It's a lot about ransomware. It's about how to protect against ransomware. And I mean, there's more advice out there than you can shake a stick at.

Baratunde Thurston (22:18):

Rahul, what are you seeing or hoping for in terms of distributing some of this preparation and protection to the smaller end of the spectrum? Whether we're talking small businesses, non-profits, folks who don't have the financial resources to handle a big ransomware attack.

Rahul Telang (22:32):

I think the easiest solution is don't fall for the phishing email. Really, you don't even have to do very elaborate thing. And [unintelligible 00:22:42] protection, but don't fall for the phishing email.

Baratunde Thurston (22:47):

It's like a mantra, don't fall for the phishing email. Is that the primary way in for a ransomware attack?

Rahul Telang (22:52):

Yes, yes. That is the dominant way.

Baratunde Thurston (22:56):

Yeah. Are there any others of note that people should be aware of?

Renee Guttman (23:00):

People are funny, right. So there's this thing called romance schemes, where I get into a relationship, an online relationship with somebody and never meet him. But I get to know him, he gets to know me, and suddenly he's got a legal issue. And so maybe he's the love of my life supposedly, and I send him money. So I think it's really hard. I mean, how do you not be human? I can be a paranoid human, but it's hard not to be human at all.

Baratunde Thurston (23:33):

Absolutely. I appreciate that caution in that note and that empathy. Thanks for joining us in our garage for another episode of Lenovo Late Night I.T. That's all the time we have for tonight, though Rahul is clearly happy to keep talking regardless of the limits. Thank you to our guests, Rahul Telang and Renee Guttman. I'm Baratunde Thurston, and I'll see you next time.