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 Andy Ellis and Tim Brown 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 (00:00):

I'm Baratunde Thurston and you're watching Lenovo Late Night I.T., where we lock industry heavyweights in the garage and make them tell us everything they know. I'm here to rouse you from your newsfeed induced coma with some startling facts about cybersecurity. First fact, by the end of this show, there will have been 40 new cyber-attacks. Cybercrime is now the most profitable criminal enterprise in the world, more than drugs, more than loyalty card fraud. Yeah. Loyalty card fraud, that's right. So what conversations do we need to be having right now about security? How can businesses and consumers protect themselves? And what do we do after an attack? Curl up in a ball and cry probably.

Here to weigh in is Tim Brown, VP of security for SolarWinds, where he's responsible for internal IT security, product security, and security strategy. That's so much security. A former Dell fellow, CTO, chief product officer, chief architect, and director of security strategy. Tim's got more than 20 years of experience developing and implementing, you guessed it, security technology. Now here's a fun fact about Tim. He and his wife live on a 60-acre ranch, surrounded by horses and miniature donkeys. Aww. Sounds really secure.

I'll also be talking to CSO Hall of Famer, Andy Ellis, a 20-year veteran of Akamai technologies. Now Andy led the company's security program, growing it from a single individual to a 90 plus person team. He's now the advisory CSO at Orca Security, and the founder and CEO of the leadership development company Duha. Did I do that right?

Andy Ellis (01:46):

Yep.

Baratunde Thurston (01:47):

Yes. But its greatest accomplishment of all has to be taken first place at the Sherman Oaks Galleria spelling bee. That's literally around the corner from where we are right now. So Andy, if you want to go pop over and relive those glory years, we understand.

Andy Ellis (02:00):

I'm hopping over right after this.

Baratunde Thurston (02:02):

Thank you so much for joining Andy, Tim, how you feeling right now?

Tim Brown (02:05):

Great.

Baratunde Thurston (02:06):

Great?

Andy Ellis (02:07):

Fantastic.

Baratunde Thurston (02:08):

So a lot of security at the table right now, I feel safer already. And I want to know what keeps you up at night from a security perspective. I don't need to know your psychological issues.

Tim Brown (02:18):

So many things. So, large breaches, breaches that are affecting the world. Really one of the biggest threats that we have is a true cyber terrorism event. That is what is really truly scary.

Baratunde Thurston (02:32):

I'm duly terrified. Thank you. What keeps you up at night, Andy?

Andy Ellis (02:35):

I think what worries me the most is how people don't always understand the risks that they take. And it's important that we take risks. We're not going to get rid of risk. I'm not the person's going to sit here and say, "Don't take any risk." Like, literally we showed up here that was a risk. But the challenge sometimes is the systems we're using are so complex that they're risks that we just don't even understand, but we think that we're okay.

Baratunde Thurston (02:57):

I mean, when you talk about the level of complexity involved and we don't understand, it reminds me of the banking system that we had so much, no one understood. And when it collapsed, everybody did that. Is that what we're facing with our dependence on technology?

Andy Ellis (03:14):

Very similar. Although I might even argue the IT industry is even more complex than the banking industry, but that's a great model to start from. If we don't understand the banking industry and how everything is layered on top of something else, it could be some company you've never heard of, goes out of business tomorrow, gets compromised, when they go down it cascades, somebody else goes down, but that's the price we pay. If we want to have this rapid advancement, you get rapid advancement by building on top of complexity.

Tim Brown (03:43):

And none of the software we build is ourselves anymore.

Baratunde Thurston (03:47):

What do you mean by that?

Tim Brown (03:48):

That nobody builds a full suite of software. We all rely on an operating system. We all rely on subcomponents. We all rely on some open-source components. We all rely on other things, which are really termed the supply chain now. So we're all relying on other pieces. So if some of those critical supply chain components have an issue, that's another place you get that cascading effect of failure.

Baratunde Thurston (04:14):

So we have like a software supply chain.

Tim Brown (04:16):

Absolutely.

Baratunde Thurston (04:16):

A lot of people are familiar with our physical supply chain and how that can get pretty jacked up. I'm only imagining the complexity and the confusion around software supply chains getting...

Tim Brown (04:25):

Yeah, absolutely. And, no software today is built by an entity, a single entity. Everybody uses something else within their software.

Baratunde Thurston (04:34):

Okay. So we're getting really real with the talk, and I want to pull it back another layer. What are the things that CIOs aren't telling their boards or their CEOs in terms of the threats and the risk that they're facing?

Tim Brown (04:47):

They don't necessarily have full scope of everything that's involved in the organization. So just think about everything you need to know inside of a company to address risk.

Baratunde Thurston (04:47):

A lot.

Tim Brown (04:59):

A lot. You need to know physical, you need to know technological, you need to know everything that people are building, you need to know every application that's going on.

Baratunde Thurston (05:06):

You need to know the little device that employees are bringing in and adding to the network.

Tim Brown (05:10):

Right, so you need to know so many things in order to truly get to a risk assessment. I think they're not

telling the board and others, the unknown unknowns. We don't know. Well, what do you mean you don't know?

Baratunde Thurston (05:25):

Boards don't like to hear that?

Tim Brown (05:25):

No. No.

Andy Ellis (05:29):

Boards want to hear either we're safe, or there's a disaster and I'm on it. But anything in between those two things is a nuanced conversation that a lot of boards don't want to have.

Tim Brown (05:39):

I think they're getting better.

Andy Ellis (05:40):

They're getting better.

Tim Brown (05:41):

I think they're getting better and asking hard questions. Just really the unknown unknowns. It's like, "Yes, we have risk in the environment."

Andy Ellis (05:47):

I didn't say the known unknowns that just get filtered out. So the board asks the CEO, "Are we safe?" Let's just take Patrick, "Are we patching all of our systems? Keeping them up to date? Did you take today's 45-minute OS 10 update?" And the challenge is the CIO and CEO have to give a very short answer. It's either yes or no. But when they say yes, they're thinking, "Well, yeah, we're safe. But let me go just check with my director of IT." And at every level when somebody answers, yes, they're filtering. They're saying, "Yes, we're good in this one environment, which is 90% of our systems. It's what really matters." But the person they're drawing from was really only answering for 70%.

Tim Brown (06:26):

Exactly.

Andy Ellis (06:27):

[crosstalk 00:06:27] responsibility for. And so what happens is you don't have this complete coverage. So when you get an answer, you get an answer about the best part of your business. It would sort of be like saying, "Is everybody in America fed tonight?" And if you said, "Well, sure, everybody who lives in the high-net-worth locations are fed," the places we're making sure have food. Yeah. They're all fed, but you're not answering the question about the people who are living out on the streets, or who have food insecurity. We see that same thing within the CIO frame.

Baratunde Thurston (06:57):

Well it also seems like maybe we should stop asking binary questions.

Tim Brown (07:01):

Absolutely.

Baratunde Thurston (07:02):

This is an analog situation ironically.

Tim Brown (07:05):

And that's why we stopped talking about security and we talk about risk. Security's a terrible word because people do think it's [crosstalk 00:07:12].

Baratunde Thurston (07:12):

Well, security's a terrible word.

Tim Brown (07:13):

It is a terrible word.

Baratunde Thurston (07:15):

It was like five times in your bio.

Tim Brown (07:15):

I know, but it's still a terrible word.

Andy Ellis (07:17):

Because it means different things to different people.

Baratunde Thurston (07:21):

Give me some positive examples of effective cybersecurity inside of an organization.

Tim Brown (07:26):

So when we look at security, you know, good security means that you're talking about risk, not security, not in the binary, not saying we are secure, we're not secure. It's creating an education for the executive to say, "Here's what risk we face. Here's how we can mitigate risk. Here's how we can appropriately minimize the risk that we face by doing these things." So that's when you start seeing a cybersecurity program, you know, that is running well. Because everybody faces risk, everybody faces some level of risk, so it's more controlling it, managing it.

Baratunde Thurston (08:00):

There's been a breach. How do you communicate that there's been a breach? Do you put it on a cake, and have it delivered with dancing and all kinds of sparkles? Do you make a TikTok dance about it and hope they see it? And you say, "I tried to tell you." What's the best way to communicate when something has not been secured?

Andy Ellis (08:20):

So I think it's really important in that moment to not try to say, "I told you so."

Baratunde Thurston (08:26):

It's hard though, isn't it?

Andy Ellis (08:26):

It's really hard. In a great organization you don't have blame.

Baratunde Thurston (08:26):

What do you have instead?

Andy Ellis (08:31):

What you have instead is this acceptance that the organization failed, and you want the person or the people who are closest to the failure to be willing to stand up and say, "Here's what I did." And they don't know if they're going to be blamed or not. And so if they're afraid of being blamed, they're not going to tell you what really went wrong. So instead...

Baratunde Thurston (08:53):

It's just like life.

Andy Ellis (08:54):

Just like life.

Baratunde Thurston (08:57):

If you're going to feel shame for something, you're not going to come forward with it. Okay.

Andy Ellis (09:00):

So you want them to know that there is safety. If they made an error, the problem was why didn't you have a process to keep a human error from causing this? Great. I want every human to tell me, like, they typoed something. Because the answer is, I should never have a high-quality system relying on human input, because we know humans make typos.

Baratunde Thurston (09:21):

Okay. Let's talk about trust. Zero trust.

Andy Ellis (09:24):

Yep.

Tim Brown (09:24):

Yep.

Baratunde Thurston (09:25):

What is it? You're explaining it to the CEO. Go.

Tim Brown (09:28):

Yeah, sure. Zero trust means that you're moving your authentication and authorization to those edge, moving them out to the applications, making the applications intelligent, making them make the decision, so that you can segment your market, your environment, into little spots. The way I like to explain zero trust is a pomegranate.

Baratunde Thurston (09:49):

Oh, okay. The annoying fruit that's delicious.

Tim Brown (09:51):

The annoying fruit. So think about the pomegranate. What does it have? It has the seed in the middle. It has a little gel coating. And then it has sections of gel coatings. And then it has a hard outer shell. So your enterprise is actually made up of many seeds. Your Office 365 is a seed. Your AWS environment is a seed. Your on-premise workstation is a seed. All of those seeds, and each one of them should have a gel coating around the outside, which is the security associated with it. And then a common policy around the outside, which is a hard shell. But if you think you can have this, what we had before, that one monolithic big avocado. It's not an avocado. It's a pomegranate. Avocado has a hard shell, and a big seed, and says, "Oh, I got firewalls around everything. And that's my environment." Nobody's environment looks like that anymore. Everybody's environment is a pomegranate.

Often you can't protect everything. You can't protect everything at the same level. And when you...

Baratunde Thurston (10:51):

That sounds so honest.

Tim Brown (10:53):

You have to give up land. You have to say, "I am going to protect this much better than I'm going to protect this."

Baratunde Thurston (10:59):

I feel like you're a general in a war I don't want to be in.

Tim Brown (11:02):

There you go.

Baratunde Thurston (11:04):

So, what are some misconceptions that people broadly have about cybersecurity? Whether it's the nature of the risk or how it even operates, or what it is? What do you think some of those are?

Andy Ellis (11:13):

I think the biggest misconception is that it's a hard field. It's actually a really easy field. It's really broad.

It's really complicated. But it's like cars a hundred years ago. A hundred years ago, nobody understood a car, you had to hire a car specialist, you had to do all these things. And today, mostly we all know how to drive cars. And I live in Boston, so I know a lot of people who don't.

Baratunde Thurston (11:37):

You definitely don't. But that's where I learned to drive, so same page.

Andy Ellis (11:39):

But we're in this world where security is still a maturing field. We're still trying to hire unicorns. People who can do everything. We don't need people who can do everything. We need people who can
understand how to get part of the job done. People who've done safety engineering in, you know, water supply systems. They understand risk trade-offs. You don't get to shut off the water unless it's really toxic, but there are things you're going to do, you're going to make risk trade-offs. We need people who have that kind of expertise to come into security and make risk decisions.

Tim Brown (12:11):

Keep going on this a little bit. The diversity of cybersecurity professionals, sometimes isn't as appreciated as what it could be. Because diversity gives you different thinking, and you absolutely need different, you know, models of thinking to be able to do things. So for example, we want to convince people that security's important and they should do the right things. So should you have a techy engineer do that? Or should you have a psychologist do that? Should you have somebody that can relate to people to be able to, you know, help modify behavior?

Baratunde Thurston (12:42):

You should have Beyonce do that.

Tim Brown (12:43):

There you go. Absolutely.

Andy Ellis (12:44):

If I could hire her for that in a moment.

Baratunde Thurston (12:48):

[crosstalk 00:12:48] things they weren't supposed to.

Tim Brown (12:48):

And they wouldn't complain.

Andy Ellis (12:48):

They wouldn't complain.

Tim Brown (12:50):

No. So, that's one of the misconceptions that you need techy cybersecurity people to fix everything.

Andy Ellis (12:57):

You need people to write reports for you, you should be hiring journalists, because they're really good at consuming data, and writing reports about them that other people want to read. I can teach anybody security. If they've got some skill that's relevant. I need people who can tell stories.

Tim Brown (13:12):

We need people that talk and can tell stories and be entertaining.

Baratunde Thurston (13:15):

Hot dang.

Andy Ellis (13:17):

There you go.

Baratunde Thurston (13:17):

Thank you for the new job. I appreciate you both. We are going to take a break from the interview mode that we've been in, and we're going to play a fun and weird, slightly awkward, little game. Are you game?

Andy Ellis (13:27):

I'm game for it.

Tim Brown (13:27):

Absolutely.

Baratunde Thurston (13:28):

All right. Now, IT experts aren't always the best at explaining their work in layperson's terms. So we created a segment that challenges our guests to describe what they do for a living in language that anyone can understand. You are going to explain your jobs to each other as if you're on a first date. And you'll each have about 20 seconds to win over your partner. And with any luck you'll graduate to date number two. That's right. It's time to play Date Night IT.

Tim Brown (13:59):

So did you ever hear of SolarWinds?

Andy Ellis (14:01):

I have.

Tim Brown (14:01):

Oh, well I ran security for SolarWinds.

Andy Ellis (14:03):

I'm sorry.

Tim Brown (14:06):

And you know that breach that occurred, that thing that affected the world that was on 60 Minutes.

Andy Ellis (14:10):

Even my mother heard of SolarWinds.

Tim Brown (14:12):

Yeah. So I ran security, or I run security for the company. I manage everything associated with that. And yep, it's an extremely interesting job.

Andy Ellis (14:22):

That sounds like a really hard job.

Baratunde Thurston (14:25):

I'm going to pause this right here. So Tim?

Tim Brown (14:28):

Yes.

Baratunde Thurston (14:28):

Just look, I haven't been on a first date in a really long time.

Tim Brown (14:31):

That was a bad first date.

Baratunde Thurston (14:32):

But I will say starting off with your most infamous failure per chance.

Tim Brown (14:38):

Ah, not a good idea. Just didn't feel right. Okay, let me try again

Andy Ellis (14:42):

[crosstalk 00:14:42] people who get past that, will stick around.

Baratunde Thurston (14:44):

Oh, is that how you received it? Was it like, "This is a vulnerable moment."

Andy Ellis (14:47):

At least he faced up to it, but I still don't know what he does.

Tim Brown (14:51):

Ah.

Baratunde Thurston (14:51):

Okay.

Tim Brown (14:53):

So I should try something different.

Andy Ellis (14:54):

[crosstalk 00:14:54] like, "Should I run away at this point?"

Baratunde Thurston (14:57):

So why don't you give it a shot, and let's see how...

Andy Ellis (14:59):

Am I giving a shot on his or on mine?

Baratunde Thurston (15:00):

On yours, it's your turn.

Andy Ellis (15:01):

Okay. Yeah. So, I am like a landscaping architect for computers. My job is to help tell other people who are building big computer networks, what's the right way to do it, so that they can deal with weeds in a more sustainable fashion, weeds being the bad things that would happen to computers.

Tim Brown (15:21):

Sounds pretty boring.

Baratunde Thurston (15:26):

Oh! I did not see that coming. I was like, "You had me on landscaper."

Tim Brown (15:27):

Landscaping. How is he going to make any money landscaping?

Baratunde Thurston (15:31):

Harsh, harsh crowd, man. Well, at least, you know what he does.

Tim Brown (15:38):

Landscaper.

Baratunde Thurston (15:38):

All he knows about you is that you missed. Second date or no, it's up to you. What do you think?

Tim Brown (15:45):

Let's do it again.

Andy Ellis (15:46):

Okay. We'll give this a try because I don't know if anybody else is going to take me.

Baratunde Thurston (15:49):

There you go. Thank you both for playing our weird, awkward, and sometimes fun game Date Night IT.

Here's an incident that a lot of us are experiencing directly, or seeing in the news, or both. Ransomware.

Tim Brown (16:05):

Yeah.

Andy Ellis (16:05):

Yep.

Baratunde Thurston (16:05):

And I've heard you describe it as a self-inflicted wound. I'd love for you to expand on and explain what you mean by that.

Andy Ellis (16:12):

So many of our enterprises have this sort of flat monolithic administration model. So you have IT admins who have root access to every machine. So all it takes is for the adversary to compromise that root access once. So that's what happened in NotPetya. A number of places get compromised because there's this accounting software, that they'd outsource it to somebody, downloads an update, it's infected, an admin happens to be logged into that machine doing something, their credentials are stolen, and your entire enterprise just shut down. Like, that's a failure on our part as IT professionals, we should not be designing systems that everybody trusts the administrators. When I talked about users having their laptop as part of their ecosystem, I literally mean we shouldn't have control of that from a central IT shop. We should have it isolated, so if IT goes down, at least our users are still up.

Tim Brown (17:09):

So when I look at ransomware, I look at it as a much more efficient business model.

Baratunde Thurston (17:17):

The shakedown has evolved.

Tim Brown (17:20):

Seriously. So when you think about it, what did you have to do before ransomware?

Baratunde Thurston (17:25):

You had to get in a car, get a gun, go stick a place up.

Tim Brown (17:28):

You had to get into systems, steal data, sell data to somebody that was going to pay for it. So you had many chains and your process.

Baratunde Thurston (17:38):

Your target and your customers were different people.

Tim Brown (17:40):

So now...

Andy Ellis (17:40):

Not the same person.

Tim Brown (17:41):

Now you just go in, you compromise the system, you encrypt it, and you get paid.

Baratunde Thurston (17:46):

So you steal from a company and then force them to buy it back. Which is how hip-hop works [crosstalk 00:17:52] black community. It was exactly... Good job music industry, you're ransomware.

Tim Brown (17:57):

So with that, right, now that model works. That model works because of Bitcoin. That model works because you can essentially usually get paid, they're doing a little bit better at getting money back.

Baratunde Thurston (18:08):

People are happier to pay than deal with trying to...

Tim Brown (18:10):

Absolutely. So you get a good payment. Now the thing we're seeing though is ransomware is getting more sophisticated. It's getting to the level often of sophisticated attacks. It's not simple attacks anymore, because I get a $5 million paycheck, I can afford to spend a few hundred thousand to execute that. And so that's our worry for the future is that you know, the attacks become more sophisticated, bigger pay days and more time spent.

Baratunde Thurston (18:40):

Because these hackers have a growth mindset.

Tim Brown (18:42):

Absolutely. So they're all about business, all about growth, all about meeting their fiscal plans.

Baratunde Thurston (18:48):

Now, what do their boards have to say?

Tim Brown (18:50):

Absolutely, what do their boards say? Their boards say they expect to see 40% growth.

Baratunde Thurston (18:54):

Yes.

Tim Brown (18:56):

And I'm not kidding.

Baratunde Thurston (18:57):

How does the changing nature of these threats affect how we keep up, Andy? And how we shift?

Andy Ellis (19:04):

So I think we keep up by hiring people who have different experiences, because they'll understand that model. Like your reference about hip hop, to you that was instant, to me I get it once you said it. But I never would've come up with that and said, "Oh, Hey, that's a similar business model." But maybe that's an insight that's helpful in the boardroom.

Tim Brown (19:22):

Yeah. One of the things that we also just need to consider, is our new model... work real hard, real fast, all the time. All the time. One story, some lawyer told me as they went into IBM, took over IBM. And there was a guy that was there, and he just had his feet up on his desk. And the CEO walked through, again, he had his feet up on his desk. And it's like, "What's up with that guy?" He said, "Well, last time he won the Nobel Prize he had his feet up on the desk for six months." So he said, "don't interrupt him." But the bottom line is thinking right now is underrated. The time to think, the time to discover. You know, John Adams also, if you look at, he kept a diary of every day of his life. And, in probably 40% of the entries, one word, thinking. So when we think we often come up with new ideas. We think with groups of people, we talk about things.

One of the things people ask me also very often is, how do you describe the adversary? And the word I come up with is thoughtful. Very, very, very, very thoughtful. Not one thing was done that didn't need to get done. Not one piece of noise was made that didn't need to be made. The code that they dropped waited 14 days before it ran. Would not run inside of our environment. Again, thoughtful. They attacked a virtual machine that goes away. It's not there all the time. Thoughtful. They didn't attack the source code control system because they knew we would see it. So they thought and thought and thought and thought and thought, and we have to outthink them.

Baratunde Thurston (21:10):

You need time to do that.

Tim Brown (21:12):

Thinking needs to be part of your program. It needs to be part of the stuff that you are dedicating time to. It's not just about doing it; it's about thinking too.

Baratunde Thurston (21:24):

Can't think of a better way to end. Thanks for joining us in our garage for another episode of Lenovo Late Night I.T., where you'll always get a fresh unfiltered look at what's going on in the tech industry. And thanks to our guests, Andy Ellis and Tim Brown. I'm Baratunde Thurston, and I'll see you next time.