Intro/Outro (00:05):

It's time for supply chain. Now broadcasting live from the supply chain capital of the country. Atlanta, Georgia heard around the world. Supply chain. Now spotlights the best in all things, supply chain, the people, the technologies, the best practices and the critical issues of the day. And now here are your hosts.

Scott Luton (00:33):

Good afternoon. Scott Luton, Kevin L. Jackson, and Thomas Carter here with you on supply chain. Now. Welcome to today's live stream, Thomas, Kevin, how are we doing? Hey, how are you doing today? It's great. I can't wait for the weekend. I'm with you, maybe some, some drier and warmer weather. We'll see here in the Atlanta area. I got to say it's beautiful out here in sunny, San Diego. So, uh, Thomas you're on, uh, I understand you're at a beach house right now. Uh, yeah, and I like, it's a good little situation we're in right now, uh, enjoying every minute of it and glad to be on. Thanks everybody. You bet. Well, very jealous green with envy here, but we've got an outstanding conversation teed up of course today is our latest installment of our very popular digital transformer series powered by our friends here at total network service.

Scott Luton (01:27):

It's appreciate that Kevin and Thomas, we've got a wonderful show teed up around securing the ICT supply chain. That might be a new acronym for some of our community members. It was kind of new for me and I've been in the telecommunications industry information, information, communications, technology, ICT, and how can we secure that supply chain as well as get an update on some of the big challenges and topics impacting that really important industry, right? Kevin? Yeah, absolutely. I'll tell you the, we, we all depend upon the telecommunications industry to talk to exchange pictures or send out videos and listen to our music. It's really ingrained in our lives. So, um, I think this is very important for everything and every industry leverages this network agreed, agreed. It's very timely conversation we're having here today. We were talking pre-show as, as an our family and our household three small kids have been learning remotely for 12 months and, and that really brought it home in particular, if it wasn't already in terms of the value of that connectivity and how can we really protect it for all Thomas?

Scott Luton (02:38):

You know, when you think about what we're going to be talking about here today, what's one thing maybe that you're looking forward to before we bring our guests on, you know, I think it's, uh, again, everybody just getting a comfort to know that, uh, when they're, uh, when we need security, uh, and any communication device that, uh, you know, it's there. And I think blockchain is going to play a huge role, uh, that in right now and in the future, outstanding, good stuff there. We're looking forward to our conversation. Let's say a little bit to a few of our folks that have already logged in, uh, across the community here. Uh, deem is, is dialed in via LinkedIn. Great to have you with us here today, Peter, you can't do a live stream. Peter has been a little far a part of our live stream sharing his, his POV across the comments across social.

Scott Luton (03:20):

So great to have you back with us. Peter Madison is back from Indianapolis. Great to have you here. Madison Smoot via LinkedIn Daria, Daria Patel. Great to have you back as well, their own LinkedIn, and, um, hopefully you all have brought your voice with you. So we've got no shortage of big topics to weigh into here today. All right. Let's no further do Thomas and Kevin really excited right before we bring our

guests on quick programming note. If you enjoyed this live stream, not only check out digital transformers with Kevin L. Jackson, one of our hottest new series, but you can also find supply chain now, wherever you get your podcasts from be sure to subscribe for free. So you don't miss a single conversation much like this one. All right. So Kevin Thomas, y'all ready to bring in our featured guests. I'm excited. We are to let's bring in David Staley and CEO of the telecommunications industry association and Chris poli senior director product line management with Comscope. Hey, Hey, Dave and Chris. Good afternoon,

Dave Stehlin (04:20):

Everybody. Good to see ya. Hey

Scott Luton (04:23):

Greg. Hello, Chris and Dave, Dave, as we were talking pre-show I love your backdrop, your backdrop. They all know about y'all guys, but it just, it makes me feel more serene and peaceful.

Dave Stehlin (04:36):

Well, I'm in my unsecure location and say it's unsecure. Cause my daughter could walk in at any moment.

Scott Luton (04:45):

Hey, such as life in 2020, 20 and 2021. Right. Well, great to have you both re really, as we were talking before we brought you into the stream, really excited about this conversation, I'm ready with my 17 pages of notes to learn from your experiences and what you're seeing in industry and as is our community. So, so let's get started. Let's let's get know to kind of set the table a bit, Dave, um, tell us more about Tia and what the organization does.

Dave Stehlin (05:11):

Sure. Tia is a, an organization it's been around for more than 80 years in one form or another. And we kind of have four key pillars. One is we develop standards. So we're an accredited standard development organization have developed thousands of standards over that period of time. Two is we improve business performance. So we come up with a lot of different offers and solutions with our participants and members to improve business performance. And number three is we help enable new technology. So there's lots of new technology out there, but sometimes it needs a push and sometimes it, in order to reach its potential, you have to do certain things to bring that technology along. Even before you reach the standard

Dave Stehlin (05:58):

Level. And number four, we do government advocacy. So we will work with the U government, uh, the administration that, uh, Capitol Hill, the various agencies, friendly governments around the world to support what's important to our industry and our membership.

Kevin L. Jackson (06:14):

No, that that's amazing. You know, people really don't think about what's behind their smartphone. Right. Um, and you think about what you think about like in 2020, I thought a lot about toilet paper, right? How do it supply chain? You kind of broke and I couldn't do what I had to do, right?

Dave Stehlin (06:38):

Yeah.

Kevin L. Jackson (06:38):

But what, what are the key supply chain challenges with my smartphone? You know, I'm worried

Scott Luton (06:47):

Well, so right before, uh, right before we talk about those key supply chain challenges, I want to give Chris an opportunity to weigh in really quick about Tia. And, but before Chris, we get you weigh in. I understand in our appreciate, appreciate conversation that Dave, you and Kevin both are a Nat Annapolis. I graduates. And I think we all in the same class together,

Dave Stehlin (07:08):

We all are younger than I am.

Kevin L. Jackson (07:13):

Well, it seems like, you know yeah. A while ago, but, um, yeah,

Scott Luton (07:18):

Well, you know, bless be the ties that bind and I'm sure there's plenty of stories or we'll have to have the address tatted on, on an upcoming episode. So really neat there. So Chris, before we, before Kevin kind of takes us down and we talk supply chain challenges, Chris Comscope from my understanding is a long time, big supporter, a member of the Tia community, you know, where do you all see a lot of value in, in your participation?

Dave Stehlin (07:41):

Sure. So, um, before I get to that, I just want to tip my hat to both Kevin and Dave. I wanted to go to Annapolis. I got, as far as the nomination, I didn't get an affordable. So, uh, it's, it's good to, good to hear that both of you have that connection. So, um, I know, I know it's a, it's a, it's a very, um, challenging path to take and, and, uh, certainly come out with a lot of, a lot of, uh, experience and knowledge and so forth from, from that type of experience at any rate, CommScope is just one member of Tia. I think that they have hundreds of members, probably four or 500, 400 members. Anyway, companies were just one of them. We do get some benefits out of that participation with Tia. But I think that, you know, one of the things that Tia brings that particularly with respect to the standards works, but also the other elements that David mentioned was that they absolutely work on neutral grounds. And I think that that becomes valuable for industry acceptance.

Scott Luton (08:45):

I agreed that agnostic voice, such a great point there, Chris. All right. So now Kevin, we're going to talk about one of our favorite subjects here, which is what supply chain.

Kevin L. Jackson (09:02):

So I'm dying to hear what spot, what, you know, how do I make sure my pictures in, um, videos on my cell phones are still there. What are the supply chain challenges in T in telecommunication?

Dave Stehlin (09:17):

Oh man, let me, let me start off. Number one, it's ever changing. Number two, it's pervasive. You know, when you think about the supply chain in any industry, uh, as you alluded to earlier, Kevin, there are many, many aspects. And one of the biggest challenges we have right now is that technology is outpacing security. And I heard that from a very high level, uh, government, uh, secretary level this week. And because Tia, as I mentioned does a lot of advocacy work with the government and they clearly recognize that technology is advancing at such a rapid rate. That security is struggling to keep up. So from one perspective, when we take and the, the view of, of our using our cell phones or using our computer, and we're how we're connected, it not only is that wireless connection back to the closest cell tower, which may be currently a mile away from your house soon, it will be maybe a thousand feet away from your house as 5g and 6g kick in, but then it's wired from that point back into the network.

Dave Stehlin (10:30):

So then you connect to fiber optics and you, uh, connect to switches and routers and you connect to systems like Comscope makes it Comscope is a company that's been around for years and years. And maybe Chris can give us a little bit of an overview in a minute, but then it goes to your home, or it goes to your building, the data center that you're speaking to, where a server is located, that you place your Amazon order through. And you just think about all those different components, hardware, software, all the labor that goes to make it happen. All the labor that goes to keep it working. It is massive when I got in this industry in the 1980s, that's when we had these regional bell operating companies are, you know, at the time it was bell, Atlantic and Ameritech and Southwestern bell and PacTel, and it's, it had been broken apart in 1984 by the government, uh, when at and T got too big. So that's helping to these baby bells at that time, a company such as a bell Atlantic might have had 20,000 suppliers, 20,000 suppliers. Now they're down, I don't know the exact number, but you're down to maybe a thousand, but then when you look at each of those suppliers and all the aspects that make up that system, you have not only software, although you just, we kind of lump it together and call it software. But how does a software

Dave Stehlin (11:54):

Service get built? It gets built on various stacks that then get added to and built on. And it is, it is something that makes up hundreds or thousands of companies behind the thousand that a service provider might use. So it is a very, very deep and challenging way that we need to look at this industry and understand how deep and wide it is, how important it is to our life. It's just like the air we breathe these days. Conductivity is yes, technology is outpacing security.

Kevin L. Jackson (12:29):

Chris, what are those components? I know, um, that Comscope really provides a lot of real value to

Chris Poli (12:39):

Good network, so to speak. So we play a lot in, in all parts of, of, uh, I shouldn't say all parts of the network, but very many parts of the network, right? We, we do everything from access points to cable, modem, termination systems for the cable companies to optical line terminators and, and, and so forth. So we play heavily in the back haul. We pay at play heavily, you know, across fiber optics and so forth all types of access network components, as well as the, you know, the head end and consumer premise equipment participates in all of this. So routers and cable modems and so forth in terms of, of the overall challenges from a supply chain standpoint, just to, re-emphasize what Dave already said. If you

just look at, at the rollout of 5g, or if you, if you start to roll into, um, an overran type of environment, you now have multiple, multiple players that are building up a functional component of that 5g radio access network and back hauling and, and those different components comprise of, and it doesn't matter if it's all one supplier or many, you know, open source content that gets drawn from the network.

Chris Poli (13:55):

And how do you vet that to make sure that there's nothing malicious buried in it. Yeah.

Scott Luton (14:01):

Great point. Yeah. I can real quick, Kelly Barner shared something and we were talking about this a little pre-show and Kevin she's really latched on to your point, but you know, if you think about a traditional dial tone, not cellular, but dial tone that that's still, of course, hugely prevalent. Every time you pick up, it's like breathing air, right? And it's, we were talking about Dave, every time you pick up the phone, you're going to hit, you expect to hear that dial tone. And it's just that expectation that we have as humans these days. But think about if Kelly has a great point, we all think is consumers know far less about what makes smartphone work than where TP comes from. But think about, look at an automotive industry, right? The semiconductors, right. W we're we're having a hard time meeting demand. And so they're making less automobiles. Right? Got some plants have shut down. Well, we can't afford for connectivity to shut down if we can't, you know, if we can't make sure we meet that demand and, and Dave, your point about 20,000 suppliers now, there's just around a thousand man that is eye opening, you know? All right. So Kevin, we're going to be talking about what Tia is doing, right?

Kevin L. Jackson (15:07):

Yeah. One thing, I mean, it seems like the challenges could be overwhelming. And while the challenges of growing and changing the, the resources seem to be going down. If you're gone from 20,000 to a thousand, you know, how, how is this done and how do you Tia, help members like Comscope, you know, deal and address these challenges.

Dave Stehlin (15:36):

Yeah. It's, uh, we have to pick and choose those things that are really important to the industry. As Chris mentioned, we're neutral, we're technology neutral, but we're very, very big advocate for the industry and our membership. So, number one, we need to have a private public relationship, meaning we have to have a relationship with the government. The number two, the private industry has to lead the change. We can't be forced to make changes by the government that never works. The government typically is further behind. It gets too overbearing. It becomes unworkable. So we want to have a great relationship with all the various government agencies, Capitol Hill, who makes the laws, the FCC, or the NTIA who implements the laws, the various administrations department of defense department of Homeland security, for example. But we want to make sure that we're staying ahead of them and solving problems before they become massive.

Dave Stehlin (16:34):

That's first of all, second of all, to, to build on something. Chris said the world, as we go more and more software oriented also creates great opportunity. Think about all the apps you have available on your phone right now, 15 years ago. You never would've thought of that, but now there's almost an unending number of applications. That's all software driven of the hardware makes it possible, but the creativity

comes from the software. Now the challenge with that is you got all these people making software applications and other things. So how do you, how do you know, they're honest, how do you know they're trustworthy? So that's a big focus of what we do is with a, a new identity, to an long existing standard we have in place that is focused on supply chain security. So we believe that security is a subset of quality.

Dave Stehlin (17:25):

You can't have a quality product, a quality service, a quality network, unless you build in rather than bolt on security. So in order to build in that security, you have to go back to the supply chain. We both talked earlier about where does that software come from? If a company is making a, uh, an application or a service that's software based, they will buy stacks or multiple stacks and add their, uh, proprietary value on top of that, where do those stacks come from? How can you ensure that, that whoever made those stacks is a good actor, is a trustworthy actor. How can you ensure that what they developed a year ago is still good and secure today? So these are all issues that we're dealing with with, uh, a new supply chain security addendum to our existing what's called TL 9,000, which is the industry's total quality management standard that we've been running for over 20 years, working with service providers, governments, individual companies, members, participants, and we've, we're in the process of adding this addendum, the supply chain security addendum that'll be released this year.

Dave Stehlin (18:39):

You know, you just kind of answered the question a bit, but maybe you could touch on it a little bit more. Why is Tia the right organization to address these issues? Sure. Well, we are neutral where we are advocates for the industry. Uh, we talked earlier about how a conductivity is like the air that we breathe. And we, our intent is to be the trusted industry association for the connected world for us. So we need to, we need to build trust in the industry and around the world with subscribers, with members, with participants, with anyone that uses conductivity we're industry association, which means we're, we're neutral from a technology perspective. And we recognize that the world, not just the U S for example, but the world is connected. So this is a worldwide issue that needs to be solved. So having an organization that can come together and bring together, participants knows how to create standards is neutral and advocates for this industry. We think we're in a pretty good spot.

Chris Poli (19:42):

Yeah. I'd like to, I'd like to just add to that. Right. And it, and it builds on not just what you just said, but also what you had said before about, um, governments, right? The government, um, I'm from the government and I'm here to help.

Dave Stehlin (19:55):

Hello, Brian runaway.

Chris Poli (19:58):

It's actually quite a bit worse than that. It's I'm from the governments plural, and I'm here to help, right. And that's really where Tia with that, with that international footprint, international customers or international membership, and so forth comes into play and is able to build across, I'll just say, governments that have a very personal invested interest and keep that neutrality. And also to Dave's prior point about building security in from the outset, right? You can't, it doesn't really help to build a fence after the horse is out of the barn. So it really, it it's really something that is, uh, that has to be

addressed upfront because there are going to be some times when you're not going to be able to get horse back in the box.

Dave Stehlin (20:48):

I love

Scott Luton (20:48):

That Chris, Hey, Tom, let me interject really quick. I want to share a couple of comments from the community here. Uh, first off, uh, David is with us and David says, I must being able to slam that phone down and anger pushing on the glass. Doesn't have quite the same effect. It's one excellent point there, David. Great to have you, Peter makes a great, I mean, I think this is one of the key themes and recent, you know, since the pandemic started in particular, you know, trusted, vetted relationships that deliver that, that solves problems together. Excellent point. You know, we're talking about us, I mentioned a second ago about this among the semiconductor shortages, right? The chips he remembers, I think this might be [inaudible] and clean. Amanda, let, let me know who this is. I remember four years ago feeling the pains of the bottlenecks and the global capacitor supply point there. Pretyt great to have you join us. And David says supply chain. Now OtterBox is your friend and go droid

Dave Stehlin (21:44):

Cheaper,

Scott Luton (21:46):

Uh, great editorials there by David. All right. So Thomas, where are we going next?

Thomas Carter (21:52):

Tell us about what sort of progress has Tia made so far and you know, where are you guys at with a lot of these issues? Sure, sure. So we are building on that infrastructure I spoke of before. So we've been running this telecom total quality management process system for 20 years. So we have a, a long embedded experience level and membership base that we can build upon. We did a very deep and continue to do a very wide analysis of the landscape of all the other standards that are out there. There's a ton of standards, but none are specifically addressing the ICT industry, the telecom space. When it comes to security three, we spent a lot of time with the us government talking about what they're doing now. Security is a buzz word that everyone talks about. Now, one of the challenges that the government has is you might have 10 or 15 different organizations that are all working on something.

Dave Stehlin (22:50):

They all have a working group, but what's the output. How do you measure it? Are you really going to improve security? So part of what we do is educate on why, what we're doing is different and, and really the big difference is we know how to build a standard and we know how to build a standard that can be certified against. So it's one thing to say, here's the bar. It's another thing to say, let me see if you can get over the bar, right? And then let me do some benchmarking to see how many companies can get over the bar and what the, what the best in class is, what the average is, what the worst in class is. So, you know, the security is something that you always have to improve. You always have to raise the bar. So we brought together well over 35 companies, well, over a hundred individuals that are working on developing this standard.

Dave Stehlin (23:37):

We have multiple working groups and Chris's involved in, in this standard specifically, we have multiple working groups that are looking at this problem, hardware, software. How do you evaluate trust? How do you measure trust all these types of working groups that are creating the standard by, uh, by the middle of the year, we'll have kind of our first pilot release. And by the end of the year version 1.0 will be completely released and we'll have all the measurements in place at that time. And one of the challenges you have is to continue to build commitment, to take on this standard. As I mentioned before, nobody likes the standard because it forces you to do things that you haven't been doing already. And maybe kind of puts you a little bit into a box, but we've seen clearly we've seen in recent past how important having a standard and how important it is to be able to measure trust, right.

Scott Luton (24:34):

And you know, really quick when it comes to standards and in many ways it can be seen as building blocks. Right? One of your points you made a moment ago is you can never, you can never, you know, uh, from a cyber security standpoint, you know, put in place a protection and then it's done, you know, I mean, it's an ongoing, evolving, and, and, and the way I've always seen standards industry, it provides us, uh, a best practice foundation. And then as the industry evolves, you know, the standards of all the, you know, living and breathing, uh, and, and, and everyone wins, uh, there's that great, a community of proven best practices. I'm a big fan. And, and, and Dave, I believe, uh, speaking of standards, you recently joined the ANSI board, which sets a ton of standards from a safety standpoint. So standards may be maybe part of your DNA.

Dave Stehlin (25:21):

Yeah, yeah, yeah. I just joined the antsy board and, uh, is the U S the American national standards Institute, which looks at all standards and bringing them into the global community and the importance there is, you know, it's, it's a known fact that over the past 10 or 15 years, the Chinese companies have been really trying to drive the leadership of various standards, institutes and associations. And the us has not been pushing as much as we should. And I saw that the telecommunications space was kind of underrepresented at ancy and, uh, in specific. And then in general, the U S is underrepresented in international standards, bodies out.

Scott Luton (26:04):

That's wonderful wanting to make their art. So quick question, before we keep driving, you're Kevin to our community, uh, y'all weigh in, what are your cure? You know, this is a wonderful opportunity to weigh in with what you're seeing, uh, standards wise, cyber wise, uh, when we're talking about the solar winds, huge news development here in a moment. So y'all weigh in and let us know what you're thinking. What, what keeps you up at night? All right. So Kevin, where are we going next?

Kevin L. Jackson (26:29):

Well, I mean, this is in a way it's scary that the mandate is so wide for Tia. So many things that are critical to our entire society, our global society, but you talk about solar winds, um, from a software point of view, you highlighted the fact that it's not just one thing, there's a lot of components in that software. And as we transitioned the five G the services, the web-based services that are going to be consumed the API APIs or application programming interfaces that a need to build services, and that these services are going to be constructed in real time. You know, they won't, they may not exist when you start your call, but the infrastructure will figure out what you need and pull in the right API APIs and

the right software just in time to, uh, deliver it to you. So how did these recent cyber attacks affect your current activities, especially around the security of software and web services and API?

Dave Stehlin (27:46):

Yeah, let me just start that off. I think, I think it pounded home the reality of the magnitude of the problem, as I mentioned before, technology is outpacing security. And this is just an example. And while I'm not an expert on this specific issue, at least 18,000 enterprises and government agencies were affected, it went on for over a year before they even got wind of it. So to speak, they use some very interesting way of going through third-party distributors to modify the software before it went to the end user. So if you're buying, you know, uh, an operating system, rather than buying it directly from the company, uh, distributors make money selling, operating, uh, passing on, passing through and distributing software packages while they opened up the, that software. They put a little now, well, where in there, uh, they repackaged it and send it on and hoping, and clearly it happened that people wouldn't realize that this is a problem.

Dave Stehlin (28:47):

So you've got software issues, you've got hardware issues, you've got piracy issues, you've got counterfeit issues. You have a lot of things to look at here, and it's a massive issue. And we're only at the beginning of what it could be. Now, somebody earlier in the conversation talked about 5g. One of the, and, and we also separately talked about how we're used to and rely on our cell phones. Well, fi one of the benefits of 5g is it enables very low latency services and real-time services. So connected cars, for example. So now you're going to be relying on a service through the network, and you're not, you know, you're playing a game on your phone rather than paying attention to where the, where the cars going, because the cars driving, what if somebody screwed up your software and your system there? So the importance of a secure network only goes up, probably an order of magnitude, at least, uh, when we start thinking about what 5g can enable in six G after that and how important these networks are to us, it is the air we breathe. We want clean air. We don't want dirty air.

Kevin L. Jackson (30:02):

Wow. That's really amazing. And, and, you know, the, the importance of this, not only as in software, but as you mentioned in hardware as well. So does the, and it was a supply chain attack, right? They attack the software supply chain. So they may also attack the hardware supply chain. So it makes me think, does the solar winds hack on software have anything to do with the recent law that was passed about replacing the wild way and ZTE equipment across the entire telecommunications infrastructure, they made that a law. And it was, you know, I guess the FCC is really involved in that. How, how was Tia what's going on with that?

Dave Stehlin (30:56):

Yeah. So, uh, of course laws get written by Capitol Hill. Um, and then the FCC implements the laws if you will, um, in, in this case. So Tia was very, very involved in helping to write that law and give, advise Capitol Hill and the congressmen and senators on what ought to be written. We spent months and months and months helping them understand the issue. Now, what is loosely called the rip and replace bill that was signed and funded by Capitol Hill. And now that funding is, uh, administered by the FCC. Uh, that's goes back to something called the universal service fund. So a hundred years ago, when, when phones were just coming out, it worked well in urban areas, but couldn't reach the, the S the suburban or the rural areas. So part of a tax that was put on every user, still in place, in many cases, every user of

a phone service goes to provide a connectivity to the rural parts in the smaller towns around the country. So anybody that's getting that universal service fund money is now required to pull out any untrusted vendor's gear. You mentioned a couple of those companies and replace it with trusted vendors gear. So the government says, Hey, we're giving you a subsidy, but we're not going to give you that subsidy, unless you pull out this gear. These companies bought this gear years ago, in some cases it's seems like it's good, good gear. There are issues around it, but there, lot of the issues come from are these companies controlled a state

Dave Stehlin (32:40):

Owned entity. So that's part of the route. It is, um, uh, it is related in, uh, into the solar winds issue, not directly, but indirectly because it's connected to on trusted suppliers, right? Solar wind seems to be traced back to Russians. The issue when it comes to rip and replace was initially driven forward with an issue concern related to Chinese companies, but related because it's untrusted suppliers.

Scott Luton (33:10):

So if I could interject for a second, Chris, I'm gonna come to you next. I'm gonna read a couple of comments from our community. And Chris I'd love for you to weigh in on what Dave has just been sharing, but really quick, uh, from our community AA. You know, I was asking what what's keeping folks up at night, really from a ICT standpoint, we've got a wide variety of question of comments that cabin fever, allowing Netflix keeps AA. They're in the air capital of the world in Wichita, Kansas up. And we wake him up in the morning. I love that AA. And he's a catch on a bit. Gary says spoken like a true academic Gary. Good afternoon, Peter. I don't think I've gotten a tan. I certainly hadn't gone anywhere. I'm not, not in San Diego, sunny San Diego, like our friend Thomas here.

Scott Luton (33:52):

Y'all let me know who, who made this comment here, but, uh, you know, do we have a steady stream of experienced security experts in supply? Do we make too many assumptions with regards to security? Those are some great questions there. So may hi. Hey, good morning. Great to have you here with us. She says her infant is pretty skilled at keeping her up at night. A lot of challenges. One more comment here. Madison says about technology. I get worried about what's being shadow banned and not shown to us. That's an interesting comment there, as well as how much access others have to your personal information info. Excellent point. All right. So Chris, no shortage of big meaty topics that are facing both the ICT industry and for that matter global industry global business, what are some of the things that you like to weigh in on based on what day was just sharing about?

Chris Poli (34:41):

Yeah, so, so I think that the, uh, the comments that they made about the last couple of questions are actually spot on, right? When you talk about the overall, uh, supply chain process and, and, and that dominant suppliers like a Walway could have a potential security impact as reflected by the legislation that ended up being passed in the United States, right? It, it didn't get passed, uh, worldwide, but, but it speaks more to what's possible and what you need to be diligent vigilant about, right? Nobody, everybody wants security. I'll go ahead and preface it by saying, nobody really wants to pay for it, but nobody really knows how much is enough. Right? And that's what the standard process is intended to try to capture. At the end of the day, when you talk about supply chain, you're going to need to capture everything from hardware to software, to every type of asset tool and operation operational.

Chris Poli (35:38):

When you look at a supplier, it may not just be that the supplier that you're looking at is OEMs and OEMs that make equipment for them. And so there's a spider web of supply that comes from any given entity, right? If I, if I buy a server that has a battery in it, there might be six different suppliers of, of that battery. You don't know which battery you're going to get into that particular piece of hardware or whatever it might end up being. So I think that looking at the supply chain with zero trust and providing, say a defense in depth type of approach for every aspect of that supply chain is, is just related by the solar winds. It's time. The ransomware that has hit some OEM folks, the in the solar winds attack was, was kind of interested where I'll, I'll kind of make a correlation to coronavirus.

Chris Poli (36:37):

Cause I think everybody can relate to that. Given this past year, you, you isolate what you can, right? So you basically try to separate bodies from each other so that there's less interaction between opiod take precautions and put up firewalls and different types of, of barriers, right? You wear a mask, you try to avoid being exposed to the infection. And if, if you do get the infection, you know, you look for ways to, to treat that infection. And so when you approach supply chain security, you kind of have to look at it holistically and in a similar type of way.

Scott Luton (37:16):

So if I can weigh in really quick, because Chris, you were speaking to trust Thomas, as we came on on the front end here, you've talking about blockchain and we got to talk about blockchain when in time trust comes up. So Thomas based on what Chris and Dave has been sharing, what are a thought or two as it relates to blockchain and how that might can be utilized in, in, in some of these challenges?

Dave Stehlin (37:38):

Well, you know, uh, with the blockchain, you're going to get an immutable record of, you know, authentication. And I think having that authentication, uh, is going to establish trust through the entire supply chain. Um, you know, I think it's going to improve security around these issues and, um, it's definitely gonna help, I think, solve a lot of problems here, uh, in the, in the near, currently and in, in the near future.

Scott Luton (38:05):

Yep. All right. So where are we going next, Thomas with Dave and Chris,

Dave Stehlin (38:10):

I think, uh, you know, that day, what are some of the, um, technologies that can solve some of these challenges?

Scott Luton (38:18):

Yup. So I think first of all, you have a process in place. You build a standard that's holistic to help address this. Number two, you have to start from zero trust. As Chris mentioned and go from there, uh, number three, you have to continuously improve. But your point earlier, Thomas,

Dave Stehlin (38:36):

The objective is to create a supply chain where you can trace everything back to its root, not only the software stack, but what makes up the software stack the hardware, the software, and then you add that immutability capability and blockchain is a fantastic way to make that happen. So it locks it down. It's not perfect. Nothing's perfect. You have to continually improve, but by locking things down with a blockchain, by chaining those blocks together, you then have a record of everything that's in there and it will help you lock it down, make it more mutable, but help you trace it back to the root, if there's an issue, uh, and you know how to change things, I'll give you an example. So in the telecom space, when a net, when a service provider is upgrading their network, they're upgrading their software. Typically they do it in the middle of the night.

Dave Stehlin (39:30):

So a wireless service provider name, anyone around the globe will do it in the middle of the night. And they do that because very few people are on the network and it sometimes takes, uh, hours to upgrade that network. Well, they put an upgrade in place, then they try to switch over. And if there's no problem, they let it run for a little bit. And everything's fine. 6:00 AM 7:00 AM along, comes rush hour, and they've got their new, uh, maintenance upgrade in place. If it doesn't work fine, they try to switch back quickly to the old load. But sometimes that doesn't work either. And so they need to find a way just like any of us in any supply chain have to find a way to understand where did things go wrong? How do we lock it down? How can I find the root problem? And if you have something that's all mutable and locked down in advance, your transition to that new upgrade will be much easier and probably be more successful. So, you know, Tia is working on that standard with, uh, with a wide range of, uh, industry representatives. And then we are working with individual companies, such as TNS to help build a blockchain and add that security in place. So, you know, we think blockchain is a wonderful way to help add that immutability, something that has not yet been used widely in the telecom space.

Scott Luton (40:53):

Hey Nate, how you've got a great question. I'm gonna come to you in just a second and Peter, your comment, but Chris to Thomas' question and th th th what Dave's already shared, what other technologies are you seeing that can help us here?

Chris Poli (41:05):

Yeah, so, so I mean, I'll, I'll go back to the, to the solar winds example and it should illustrate and bring in the use of blockchain and also, uh, the comments that they didn't mention. But, um, if you look at, at that set of breaches, it was done, and I'm going to use some, some names that are, you can go and Google them if you want to. But, you know, the one that was most highlighted is something called sunburst and a sunburst was, was something that was buried in a DOL. Uh, there was also a supernova, which was also buried in a DLL, sorry, buried in a, what a DLL, it's a dynamic link library. It's basically an executable, uh, within the, within software, but, you know, the way that they got, uh, the supernova, um, element was never signed to sunburst, peace was signed.

Chris Poli (41:54):

And the way that they got the sunburst in was through something called sun spot, which was mail malware on the build server. So, so something like code signing can be useful, but understand, it's not a magic bullet, right? Your school need to authenticate the sources of the inputs to that code. And you need to, again, go back to every piece of asset, the operational tools that are used as well as the, uh, the code itself, where you can scan binaries, you can scan source code. All those types of activities need to

happen in order to establish that trust for whatever it is that you're putting out there. The code signing helps from the standpoint of, you know, that what you're putting out there is what's going to actually go on to the, the elements in the network. You know, you take for granted on your cell phone, when you look for an application at the app store or wherever you go for your applications, or even as you add to an add on, on your browser, you'll you inherently, if you're going to load the application or the add-on, you trust that source. Right? But as a consumer, I'd be willing to bet that over 99% of the time, it's not fitted, it's not checked in any way. Right? What do you know what we're loading onto your system? Right.

Scott Luton (43:10):

That's an excellent point. Everyone can relate to. All right, we've got a great question. We're talking blockchain and there's a ton of, of interest in blockchain. And, and of course there's a ton of already current solutions, current applications that are leveraging blockchain us. Now [inaudible] has a great question here, and whomever wants to address it. I'll throw this up to our panel. That is all for your, uh, much, uh, uh, above my technological pay grade, by the way. All right. So she says, how effective do you suggest blockchain will be if it's not mirrored by the upstream supplier base as well? Great question. Anyone want to want to jump in on that?

Kevin L. Jackson (43:46):

Well, one thing I'd like to say is that she's absolutely right. That's why no single organizations or single vendors blockchain could help here. And you need a industry wide organization like Tia, that's non vendor specific, and really non technology specific to look at really what's required to deliver the service and to, to build trust all the way up the, uh, the supply chain. Yeah.

Scott Luton (44:21):

Excellent point. And sets us around those protocols. Yeah. Great points. Cause what's the standard, if it's not embraced, endorsed by, by the, the complete industry. Right.

Dave Stehlin (44:35):

Right. And you want to link together various, uh, blockchains. So you might have a blockchain that makes up a specific product, but there are multiple products that are needed to create a service. So how do you link together? Those various blockchains that might be on different clouds made by different suppliers in different organizations. So there seems to be a need for an interface that connects various blockchains together in the ICT space. And that's something that Tia is, frankly, in the middle of researching right now,

Kevin L. Jackson (45:09):

I think to bring up an important point, people hear the word standard, and it sounds like we're going to tell you what you have to do, and everybody has to do it. But, you know, I think what Tia is working on is more like a specification sort of, how do you interface? How do you communicate across all these blockchains? This is interoperability. Is that, is that correct? Is it more interoperability or specification than a standard?

Dave Stehlin (45:39):

Yeah. So, um, you know, there are very technical standards and that's kind of one perspective on the standard. Another is management systems, uh, such as we do with TL 9,000 on the business

performance improvement side. We're not in that scenario. We're not telling people specifically how they're going to do something, but what needs to get done. If you need to build something that's immutable, it's up to you to figure out how to make it immutable, as long as you can show us that. Yeah. It's meeting that requirement, how you do it is up to you. So you still have that individual company, uh, creativity, but we're just trying to say the intent is to solve a security problem. Allie do is up to you, but you know, the, the, what is a checklist of things that you have to prove that you've accomplished, uh, in the same would apply here in blockchain.

Scott Luton (46:34):

Excellent point. And something also points out as, as we've seen in the event that the, the defense industry here in the U S as it, as it implements more rigorous cybersecurity measures, some of the mom and pop companies are unable to meet and, and implement it due to budgetary constraints and other constraints, a great point here. So Neha, uh, AA also says I'm waiting for blockchain to mature so that we can apply it in aircraft industry. A trusted third party would definitely contribute greatly well. There's good news, AA. Peter who spent several decades with air Canada says that the airline industry has been tracking cradle to grave for decades. And he's got former colleagues and friends working on blockchain solutions to manage this currently good stuff there, Peter and AA. All right.

Kevin L. Jackson (47:17):

Um, just I'm off sort of playing off of that. I mean, the airline industry uses the telecommunications industry to track all of their components. So

Scott Luton (47:30):

There must be something there. Yeah,

Dave Stehlin (47:33):

Yeah, absolutely. And like we said, conductivity is pervasive and becoming even more so, so it, it crosses all types of verticals, uh, whether it's inside a building in, in, uh, you know, w w it's another standard that we've been, uh, working on. And at our first release about a quarter ago is a smart buildings, assessment criteria, the health and wellbeing, the safety, the security, the power and energy systems. We all know that we can get more efficient with the power and energy systems, perhaps using something like IOT and machine learning, but you have to solve that security problem. You know, you don't want someone backdooring into that building and tunneling into your network through some unsecure IOT device. So like we said, it's very pervasive.

Scott Luton (48:19):

Yeah. There was a great, uh, w we've had, um, some folks from a certain, a very large global electrical manufacturing organization. They had a great commercial on that. It was based on true story to your point, Dave, about smart buildings and through employees participation in a bowling league. And, and by having their information in a very low level database for tracking scoring Packers were able to, once they made that connection via social media, that they were in his bowling league, they followed them to the bowling center, penetrated that low level of security, and then was able to track back in through a, through a smart thermometer on the manufacturing site, via the IOT. So all of these jobs, it always brings back and I got to, we'll have to find the commercial, drop it in, but it always brings me back to that long, um, uh, proven saying you're only as strong as your weakest link, and that is so applicable in these conversations like we're having here today, Chris, before we, um, you know, start to wind down. I

know we've, we've covered a lot of, uh, brought a lot of topics here in the last few minutes. Any additional thoughts on your end as, as we talk our T talk white chain, talk about some of these other things.

Chris Poli (49:30):

Sure. I mean, all of those, all of those approaches are applicable, right? And so, and so are also the idea of, of bringing, um, the security from the operational networks that are in place today and applying them to the supply chain activities explicitly, right. Um, to, to secure end to end networks is, as David alluded to telecommunications is part of, of everything. And those networks are part of that factory function as well, code signing, scanning to component elements and so forth, right. And, and really vetting every aspect of what's there is, is, and using every tool in the toolbox, right? Uh, uh, that, that you're able to afford to use and apply effectively to improve the resilience of what you have. But you also need to be able to plan for what you do when something is compromised, going back again to the solar winds, right? What do you do in order to restore the confidence in exactly what you're doing and ensure that you don't have other infections that have happened as a result of that one breach

Scott Luton (50:39):

Excellent point, but the horse in the barn example of that, or another example is when you you've got a house leak in the first thing you do, you don't start getting the water out, you find the leak and repair it, and then you get into mitigation so much good stuff here, Chris and Dave, and I hate to start to wind the conversation down, but I didn't want to correct myself. I think I said, IOT thermometer. I meant thermostat. So I want to clarify that really quick. Uh, we all love our smart houses and smart factories these days. All right. So Scott, I will inject for a second. You, uh, you talked about having small kids and when I had small kids, my wife would always say, be a thermostat, not a thermometer.

Scott Luton (51:23):

Let's steal that from you, Dave. Completely a lot of good stuff there. All right. So let's make sure I know that we can barely do any, any of these really deep issues, justice in an hour conversation. However, I really appreciate what both of y'all have shared. Dave, how can folks plug in and know, connect with you and plugin with Tia, or, uh, just go to Tia online.org, and you can learn more about some of the things we're working on, uh, feel free. You can connect to us that way to perhaps be a participant in some of these standards that we're creating, or at the very least understand some of the things that we're working on for this very, very important industry. Outstanding really appreciate your time here today. And I really appreciate the, you know, serving as that agnostic voice, really helping, you know, protect us all as we all consume connectivity and technology, you name it so appreciate what you and your team are doing. And Chris, uh, what about yourself? How can folks connect with you and learn more about Comscope?

Chris Poli (52:17):

So commscope.com, we're all about, uh, connectivity solutions and, um, certainly reach out with any questions and so forth

Scott Luton (52:26):

Standing. Well, really appreciate both of your gentleman's time here today. We've been talking with David stale and CEO of telecommunications industry association and Chris poli senior director product line management. Comscope thanks to you both. Alrighty. All right. Thomas and Kevin, man, I couldn't

get to all the comments. There's so many different wrinkles of that conversation. That's tough to get into in an hour. You know, I want to give y'all. I want to, before we sign off here today, I'd love to get, you know, y'all almost key, really key takeaway. So if our, if our community doesn't, they forget everything else. What's one thing that they should really latch on to, and, and, and key in on. And, and Kevin let's start with you.

Kevin L. Jackson (53:09):

So how important it is, how critical it is. I mean, it's not just telecommunications, right? We, the airline industry uses telecommunications. Every building you're in uses telecommunications smart home uses telecommunications software is this is part of all of this. So if we don't get the software and our telecommunications secure, nothing secure, I can't trust my toaster. Right. Or your cars. So this supply chain for telecommunications, it's just so important and people are under appreciated. I believe,

Scott Luton (53:54):

Uh, Kevin PR folks probably under appreciated their ability to drive into any grocery store at any point in time, any day of the week, any hour of the day and pick up TP.

Kevin L. Jackson (54:05):

Right. Right

Scott Luton (54:07):

Now it's right. Everybody just took it for granted. And that as we talk about quite a bit here at supply chain, now, if there's any, you know, there's so much heartburn and loss and, and a lot of challenges to the pandemic, but there are great silver linings. And one of them is consumers are much more aware of how global supply chains work. And it probably going to be a much more aware about how the ITC ICT and why you're able to have connectivity, you know, if at any point in time, and then awareness is really important. And that's where I really appreciate some of the great things that Tia is doing to drive that awareness really important. All right. So Thomas there's so much, you probably have 17 pages of notes. Like what's the one big key thing,

Speaker 6 (54:48):

You know, uh, it, I think it gets back down to trust. You know, there needs to be, uh, more trust and more, uh, you know, authentication end to end from inception to exit and, uh, having, you know, blockchain technology implemented through the different layers I think is going to, uh, help support that trust. And with that trust, we're going to get more efficiency and, uh, we're going to be able to build better technology solutions and layers on top of these.

Scott Luton (55:14):

Yeah. Excellent point. And of course we appreciate total network service for helping us get these conversations out there. You've gotten a lot of comments already in the community, uh, appreciative of the information. So really appreciate that Thomas Carter. All right. So Kevin, you're going to get the last question here today. Digital transformers, you know, we went from zero to a hundred really quick. Um, you know, I'm selfishly I'm learning a ton because I'm unlike our great panel here today. You know, I'm not a technologist and, uh, it doesn't come natural to me. So I've enjoyed the learning opportunity, but what can folks expect as we, as we, uh, at a minimum, have a monthly show, uh, Kevin, what can folks expect from the series?

Kevin L. Jackson (55:56):

We're just like this one, every industry is transforming and I'll networks, I'll software, uh, business processes trust. I mean, we can no longer build trust through physical connection. I was talking to the other day is that the, the old way of building trust was through shared experiences. You would, you know, take your, your colleague or customer to a Braves game, right. And you can't do that,

Scott Luton (56:28):

Not a Yankees game. Right.

Kevin L. Jackson (56:32):

And putting time in with people is how you build trust. Well, in this virtual world, no, the time has to be over what done network. So how do you vet the information that you're getting over to network? You got yet another area where maybe maybe blockchain can help. So digital transformation, the show is about addressing all of these challenges around, you know, business model transformation, social transformation, business transformation, supply chain transformation. So that's what we're going to address every week. And I am ecstatic about all of the, um, organizations and companies that have been reaching out to, uh, to us. And we're a young show. So thank you very much, uh, Scott for giving us the opportunity.

Scott Luton (57:31):

Well, Hey, again, I've really enjoyed it. Our team's enjoyed it. Our community has really consumed that the content thus far, and it's a great professional development and a market and industry Intel opportunity. And that's really what the last hour was. So we all check out by the way, click the transform, which also walk you through digital transformation and very meaningful. Been there, done that way, but check out, I think in the show notes, Amanda and clay, we've got Chris and Dave's LinkedIn profiles. We've got their organizational URLs or websites. Check it out again on behalf of Thomas Carter and Kevin L. Jackson, and a whole team here at supply chain. Now, hopefully you've enjoyed this conversation with challenge. I would challenge ourselves every day. Hey, do good gift forward. Be the change that's needed. And on that note, we'll see, next time here right now. Thanks for buddy, buddy. Look for the digital transformer figurines. Okay.

Intro/Outro (58:30):

[inaudible].