IT Matters Ep 13

Tue, Aug 22, 2023 12:55PM 41:56

SUMMARY KEYWORDS

ot, dragos, talk, security, people, plant, iot, controls, understand, conversation, technology, industry, detection, cybersecurity, jason, happened, podcast, keith, impacts, event

SPEAKERS

Narrator, Keith Hawkey, Jason Christopher, Aaron Bock

J **Jason Christopher** 00:07

Welcome to the IT Matters podcast, where we explore why it matters and matters pertaining to it.

A **Aaron Bock** 00:16

Welcome back to the IT Matters podcast. We are on lucky number 13. It is episode 13 today, thank you for listening. Remember to subscribe on your favorite podcast platform. Although, I did just find out Stitcher is no longer going to be a platform, so if you are listening on Stitcher, switch to Apple or Spotify or something else and subscribe to us. So, excited to have you on for an episode that we have not really done in the past before. We're excited to do this, it's going to be a little bit more of a focus on a specific technology. Today we're going to be talking with Jason Christopher from Dragos, which is a focused OT technology security company. And we're going to talk about all things OT security, what it means why people use it, etc. Keith Hawkey, my co host, welcome. Keith, how you doing today?

K **Keith Hawkey** 01:09

I'm doing fantastic Aaron, thanks for asking.

A **Aaron Bock** 01:11

What's new in the world of IT and what's new in the world of Keith?

K **Keith Hawkey** 01:15

What's new in the world of Keith is Keith is reading an article on a computer world. The title is "Makers of chat GPT have announced the company's dedicating 20% of its compute processing

power over the next four years to stop super intelligent AI from quote unquote, going rogue" and I'm wondering, is 20% Enough? I don't think so.

A Aaron Bock 01:39

20% is a lot to you know, I guess prevent your own technology if you had to spend that on employees from going rogue. So that seems like a lot, but I know it's a serious issue that we're hearing in the news. I mean, I saw I forget what it was, and I'm gonna get some of the details butchered, but I saw something recently, maybe Keith, you shared this a lawyer was too lazy to process his own case work. It was for a he was looking for case precedents for one ofhis cases that he had, so he used chat GPT or Bard, I don't know which one, gave him a bunch of case precedents and they all turned out to be completely made up. So not one was actually true. So our friend of AI in our chat GPT bot completely made up the case, the lawyer is going to lose his license, he's going to lose his practice and the AI went rogue. So be wary, be wary if you're using AI to do all of your work and not fact checking it somehow. But I do think it's an interesting debate that's happening, and we'll see where this goes. 20% is a lot though.

K Keith Hawkey 02:41

It's not enough, Aaron. It's not enough. It won't save us from the Terminator.

A Aaron Bock 02:45

All right, if you say so.

K Keith Hawkey 02:47

But yeah, so that brings us to Jason and Dragos. First of all, Jason, thanks for hopping on. Today we have a special guest. Jason, you have a background and IT and OT cybersecurity and you're currently the director of cyber risk at Dragos leading their OT cybersecurity organization. Besides the cool name of Dragos, which was founded in 2016, Dragos has taken it upon themselves to blend technology, intelligence and people to provide a layer of security to operational technology. So Jason, why don't you introduce yourself and welcome to the podcast.

J Jason Christopher 03:31

Thank you very much, happy to be here. Um, so yeah, I'm the director of cyber risk at Dragos. What we do is a conversation as you sort of already laid up for me on how can you start implementing and having a true detection program within your OT environment? When we talk about OT, and I should probably spend a little bit time on that, just because I know a lot of folks aren't familiar with the concepts. So IT, information technology. OT, operational technology. And when we think about operational technology, these are things that the zeros and ones aren't the data that we use to store sensitive information, right? If we're in the banking sector, we have zeros and ones that may be customer data, financial data. When we think of zeros and

ones in operational technology, those are actually opening a lever, turning a valve flow of molecules full of electrons. Those are the things that we're dealing with an OT. So those zeros and ones become a thing that interact with the physical world. It's just a little bit different. And because of that, the technologies are all over the place. Instead of maybe having a you know, laptop that we're going to refresh every three to four years like we would in IT, we've got equipment that's going to last for 30 to 40 years in OT. So talking about things like hey, how are we going to patch this device that's still running Windows XP is a totally different conversation in the OT space where we actually had to bring a plant down in some cases to be able to do that. So the security constraints are very different. The technologies that we use to be able to secure those systems are very different and the impacts are different. If I'm dealing with an incident in IT, I may be looking at system downtime, maybe things like ransomware, that can be able to lock my systems up. In OT, I mean, very, extremely have a hole in the ground, right? I may deal with loss of safety, loss of human life, impacts to community, environmental impacts, and things of that nature. So just everything about it, it like, it looks similar on the surface, right, I still have networks, I still have routers and switches. But everything sort of in the guts of the situation is going to be a little bit different.

A Aaron Bock 05:35

Yeah, Jason, it's, it's interesting. And I want to get into this a little bit more, you talk a lot about the importance of OT security. And I think what we need to do is go back and like you said, define OT, there's the OT and the IT. Where we're at today, I know it but I know some of our listeners may not know, I want to kind of go back into like, the largest OT breach to date and like how it happened, etc. But I also wanted to share previously on the IT Matters podcast, we actually had a guest, Scott Finkhouse, talking about, like an OT related issue. And it's really interesting from a security perspective, you mentioned, patching, like a really old Windows XP device, right? It's not so easy like in IT we just think, well, yeah, you're really behind on your patching, like, that's inexcusable. In OT, I think what people don't realize is, you spend $10, $15, $20, $30 million on a machine that runs a really core process in your plant, it's not so easy just to patch, that thing that's gonna break that whole machine. And now you got to spend that $30 million. So it's kind of got this very financially business driven use case over here, but a real live security issue over here. And I think there's a lot of people saying, well, like, geez, we've always kind of looked at these as two separate almost parts of the business, but you can't anymore. So I wanted to bring that up. But also, can you talk about like, I think we all know what it is, but share with you, in your opinion, what has been the largest OT breach to date, and what happened.

J Jason Christopher 07:03

So for me, the one that always stands up, and unfortunately, it's still an ever evolving issue is what took place in the Ukraine, from 2015 and 2016. Those ones in particular stood out to me because we were talking about it for a while like, hey, this could happen. The electric grid has some vulnerabilities, if there was a dedicated actor, we could have outages that could impact whole communities. And then the 2015 cyber attacks happened in Ukraine, which brought down about a quarter of a million folks without power for roughly anywhere between four to six hours depending on how well you're counting on the event timeline. And then it evolved into the following year in 2016. With a sort of Swiss Army knife of OT malware, a framework of OT malware that we hadn't seen before called Crash override. And seing an adversary start

investing more and more in automating their attack flows. There's something in IT, we see all the time. Seeing that evolution in OT became pretty concerning. The other one that I would say is extremely concerning would be the TRISIS attack. TRISIS if we think about the two different systems that are concerned about motion, I'll walk you through a plant. One is the control system that is what is allowing an operator to again, turn a valve, open a lever, and things of that nature. The other is a safety system, the safety system allows me as an engineer, to walk on site and understand that I will maintain my eyesight, my limbs and my life at the end of the day, because they're going to be these passive safety elements or controlled safety elements, that if something bad were to happen, at least you'd still be alive. And the attacker, instead of going out to the control system, which is what took place in the Ukraine events, went after the safety systems. So that tells you deliberately, they're trying to kill people. And those two things, if I were to look at those sort of evolution of events between Ukraine and the TRISIS event, those are the two that always stand out in my mind as really seen that the ante been upped by the attackers to really do damage.

A **Aaron Bock** 09:00

Got it, and Keith, I want to pass this over to you in just a second. But, you mentioned Ukraine and 2015/16, which is crazy. That's eight years ago, we're talking about breaches. I mean, TRISIS, you didn't even mention Colonial Pipeline, which is another big one. How has OT security, and how has OT security systems evolved over the last, say, five to 10 years in your mind?

J **Jason Christopher** 09:23

Yeah. And actually Colonial Pipeline's interesting because that was that was very much so an IT centric attack. It was a controlled shutdown and that's one thing where if you want to talk to the evolution, I think is interesting. We talk a lot about convergence. And convergence of technology is somewhat taking place, right? If I walk into a plant, I'll see computers, I'll see assets that look IT like, but they're OT because they they impact operations. For Colonial Pipeline, it was the system that allows you to understand what product is in the pipeline. So when that was part of the ransomware impacts, you had no idea if there was sorry, jet fuel in that pipeline or premium gasoline, and you don't want to mix the two up, right? You don't want to try to fly a plane on premium gasoline. Likewise, I don't want to fill my car up with with jet fuel. And because they could not understand that, because they couldn't have that visibility on the IT side, OT had to shut down in terms of being able to make sure that, hey, if we can't understand who's getting what, then we shouldn't be selling it. So that controlled shutdown, I think is an interesting piece and that evolution, I think, is where the boundary of IT and OT, that I think is the evolutionary state that we're currently in. Where does it reside? Who manages the firewall for an OT plant? Is it going to be enterprise IT who understands firewalls really, really well, but may not understand OT protocols, operations, safety? Or is it the folks in the plant who will understand those three things very, very well, but may not totally understand like why any any is a bad firewall rule to have in place. And so this convergence has happened somewhat with technology, but hasn't happened, really, with people. Understanding the sort of education that you need on the workforce, and both sides to come together to really be able to support that evolution that we're talking about?

K Keith Hawkey 11:09

Yeah, that's fascinating. I'm curious as to what industries or business segments is Dragos seeing the most growth in and what has been the catalyst for the adoption for another layer of OT security? Understand, understandably, human life is a catalys, but you know, what areas are kind of more the hyper growth mode.

J Jason Christopher 11:33

So I feel like it's the same thing in IT, where we talk about unfortunately, once an event happens, that's when people pay attention. Same thing in OT. So I would say there are two drivers, mainly that have been happening, and one is regulation, and the other are events. So we see the most growth and probably also the most maturity in the electric sector and the energy sector. Electric has had mandatory cybersecurity standards in place that impact OT since 2010. So there's a bit of maturity there that you don't see in other sectors as a result. Same thing in the energy sector, especially things like Colonial Pipeline, that force new regulations coming out of TSA, and that again, forced a little bit more growth there. What I think is, one of the impactful ideas that people need to understand is that again, I can't put traditional IT controls in those OT environments. Where we talk about the idea of prevention is ideal, detection is a must, really, really strong in OT. When I talk about OT, we talk about the M&M model, and I mean, the the candy, not the rapper from Detroit. In the M&M model, it's hard shell,

A Aaron Bock 12:35

Both good, though, both good though.

J Jason Christopher 12:39

So the hard shell, gooey center means I need to invest my perimeters, I need to invest in firewalls, I need to invest in physical security perimeters, but they're going to fail. How many firewalls have you ever worked on that was like totally pristine, didn't have a temporary firewall rule that has now been in place for 10 years, very, very rare. And so that's where we really lean into detection. That's what Drago specializes in. Looking at detection inside those OT environments, knowing that the perimeters will fail and knowing that we can't put in things like antivirus. You're going to walk into a control control center or control room and you go to a device, it's not gonna have any idea how to authenticate, maybe if you're lucky, you can enter a four digit PIN. So in those cases the traditional IT controls won't be in place. So prevention is ideal, detection is a must. I'd further qualify detection without response is probably of little value, right? Like if I see something on fire, but I don't know how to put out a fire, it's not going to help me out too much. And so that evolution is where I see OT really strengthening, less so in the prevention discussions, because we can only do so much, more so in detection and being able to respond to an incident quickly.

A Aaron Bock 13:45

So you bring up a really interesting, I think, question, if I'm a CEO, CFO, CIO, I'm a leader in an organization that would have some amount of OT that they need to be concerned about right?

organization that would have some amount of OT that they need to be concerned about right? In IT, CIS framework, NIST framework, they're very popular, it's easy. Insurance companies come in, whoever comes in and assesses and says, Yeah, meet these controls, right? If you do this, you're 90% of the way to security. What would you advise a new CEO of a manufacturer and they're concerned about do I have OT security in place? Like, are we doing everything we can? How do they assess that? What's the best way to do it? What are some successful stories? What are some, some maybe not so successful stories you've seen? And like, what is Dragos? Like how do you guys approach it?

J Jason Christopher 14:32

So we actually approach it using a framework called the five critical controls for ICS. Five critical controls for ICS are just very simple, very easy ways to be able to bucket things, sort of starting with the idea of incident response and understanding what that means to you. Really, for example, understanding the scenarios that mean the most, not sort of boiling the ocean, but those scenarios that mean the most to you. Do you have the playbooks in place? Do you have the processes in place to respond? And from there then pivoting to the idea of what is defensible architecture? A defensible architecture for us being based off those scenarios you care about. Because again, we can't put in traditional IT controls. So let's say I'm worried about ransomware in my environment. There may be a set of 50 controls or so to help me prevent ransomware in our OT environment. But let's say you're really concerned about TRISIS, right? The TRISIS event that I talked about earlier, targeting safety events, that may be like 120 different controls. And so understanding your environment, understanding what you care about most is what will then sort of flush out this conversation around our defensible architecture. And so the controls then sort of build themselves upon from there talking about things like what do we do for secure remote access? What do you do for key vulnerability management? All of them at the end of the day, really trying to supplement and have a big bucket idea of if I don't know where to start, let me only start with these five critical controls and move from there. There are larger frameworks. So similar to like what we have in IT if you're familiar with the NIST sort of SP 853, we have SP 882. 82 is just an overlay on top of the 53 that says, hey, you know what you're not gonna be able to do in OT, multi factor authentication and the control center. So we allow you to do things like have badge card reader access count as multifactor. And so there's a different set of audit techniques that you can do there. I mentioned electric sector, again, we have mandatory regulations there. Same with energy with TSA. So we do have frameworks in place, we do have standards that are in place, I would say, just like every other IT program that you run into the risk becomes is it compliance based? In which case is it just check the box? Or are you really looking at it from a security perspective? And that's where I challenge CEOs to look at it from from that perspective of saying, hey, what do we care about? Are we doing this safely? Can we maintain reliability even during a cyber event? And those are all conversations that would have to have as opposed to I do 882 and just call it a day.

K Keith Hawkey 16:51

Yeah, that reminds me that how important the human element is to securing IT and sounds like OT as well. You mentioned a reinvention of how to think about security, you're badging in and out, the controls are able to implement on the IT side are numerous, but it sounds like as far as authenticating and training employees to view their jobs in a different way that bring about security to the organization is a task in and of itself. How does Dragos us help the human element side of things if you're leading a team, and you're having a conversation with Dragos?

J Jason Christopher 17:33

Yeah, so we actually have some complimentary services that sort of surround the platform. So the platform being the detection platform, looks for abnormalities understands OT specific protocols and sort of how operations should work. So if something, for example, if you're speaking in a certain protocol, let's say if you're in the electric sector, DNP3 is a very popular protocol to be able to operate. All of a sudden you see a device using like an IEC104 protocol that you don't use at all, that's likely an attacker like, like, there's very few reasons that a device that is deterministic, would all of a sudden start using a different protocol that it should not understand or know. So we're able to provide that additional conversation about here's the detection piece. Within the platform also, we have playbooks. So hey, you just saw this sort of indicator trigger, what should you do? Here's sort of the top things you should run through. And then we can augment that further. We have training, for example, at Dragos Academy that allows people to sort of understand OT a little bit better, understand what you should do during incidents. We also have professional services that sort of, again, help augment your team. So if you don't know how to do an architecture review, you're not certain where you should start, the services come into play. And then we also have intelligence. So being able to provide OT specific intelligence, which is very different than IT, right? In IT there are hundreds, if not 1000s, of activity groups and things you need to keep on top of, OT is actually, it's a little bit smaller, right, we're talking about dozens of activity groups that understand operations, understand how to attack OT, and providing that very specific information, again, allows you to what I like to call a patch the human, right. If the human understands the things that are going wrong, then they should be able to build better processes and leverage technology a little bit better as well.

A Aaron Bock 19:11

You mentioned earlier, well, you kind of have been talking about it throughout, with, I appreciate you sharing that because that's really helpful for I think the listener to understand like, kind of framing OT technologies and security. You mentioned highly regulated industries, being the first adopters. And I think it makes total sense why right, like electric. If the electric grid goes down, we're all screwed, ie, Ukraine excetera. Which industry you think will be the next one to really adopt this technology? That's kind of the first question. And feel free to kind of get granular because I think like manufacturing has OT everywhere. But I think there's probably certain manufacturing, that's probably more likely to adopt. So that's kind of the first question so feel free to answer that one. I'm curious what you think on the next industry.

J Jason Christopher 19:57

Yeah, the next industry I would support this idea of manufacturing. You're right, though manufacturing is so broad, right. There are, you know, these fortune 50 manufacturers also like, believe it or not like Mom and Pop manufacturers right where they're local community driven. And maybe they don't understand sort of what those impacts could possibly look like. So I see it probably going more towards the more mature manufacturers and I'd also include sectors like chemical sector into that too. Chemical sector has hit the accelerator, same with pharmaceuticals on more digital transformation. And that means that we're seeing cloud connectivity to OT systems, persistent cloud connectivity, which should frighten a lot of people.

We're seeing, you know, I've walked into some facilities where they're, they're managing some of the things on iPads, which looks really cool, but again, from an attack surface, it's probably adding a lot more that you want to be able to detect. So seeing manufacturing, chemical, move in that direction will be next. The one underlie the one that I'm uncertain about, just because I think budgeting is hard for them is water sector. And we've seen events, right, that have sort of grabbed national attention. Water is as vital as power. I want, I want to be able to have safe drinking water. But there are 50,000, water utilities ish around about the United States alone. And they're very small in some cases. You know, the profit margins on those, they don't drive by profit, they drive by serving the community. And so it's relatively cheap commodity, which means that there may not be a budget at all, for somebody who's doing OT. As a matter of fact, that OT person could just be the operator. You know, it could be the IT person who doesn't understand OT and so there's a lot of constraints there. I would love to see water mature, I just don't know where that sort of incentive or funding would come from for a lot of the smaller utilities.

A Aaron Bock 21:43

So let's go back to the question. Earlier you answered, you know, where is OT security and kind of high level what is it. Now for, I guess, from Dragos' perspective, and what you talk to customers every day, Dragos is obviously an advanced OT security and helps companies mature their OT security practice. Like if I'm a CEO, and I'm walking in, I'm taking a new role in a manufacturer in a utility company and I'm kind of questioning like, do we have any security? Like, what are you typically seeing? What are you replacing? Like where are people in the like the you know, the spectrum of OT security? And how bad can it be?

J Jason Christopher 22:21

So what is typically interesting for either new CEOs, or even new board members, right, because now boards, especially for the good things here in the states, like the new SEC guidance is coming out saying, hey, you have to have a board member who understands cyber risk. They'll look at their budgets and say, well, we're spending in cybersecurity. And so they'll talk to the CISO and the CISO will talk about, you know, the scorecards they have and all the things that they're doing for you know, phishing, and being able to look from the outside in inside out all those good things. But, the CISO rarely has any visibility into OT security. That may be managed by the plant manager. That could be managed by the VP of engineering. And if you ask that person, what's been their budget for cybersecurity, it's very small, if anything. And the first time CEO or first time board members, the thing about them is that they typically understand operations, right, the CEO probably came from the plant floor came from the utility and worked their way up. When they say, wait, you mean, the thing that that we produce, the thing that like, provides power to a community or that we are actually producing as a manufacturer has no security on it, but our IT enterprise stuff is really secure. That becomes a culture shock, because they look at the money they've been spending, and not understanding that it doesn't cover OT maybe at all. And so for some people, it's the first time ever for them to invest in OT, and they put everything into IT, not realizing there's supposed to be a mix, not realizing that there's differences in technology or protections. And that is where unfortunately, I see a lot of folks if they're just starting on this journey, they get sticker shock from the perspective of I've already spent money, what do you mean, I need to, I didn't, I didn't do anything? That's that's a scary prospect for some people.

A Aaron Bock 23:58

Jason, can you give an example of like, just it can be a basic one, like where has OT, where's Dragos thwarted an attack? Like, what was the attack that came in? Like, how did it stop it? Like, what's a common one that you see every day?

J Jason Christopher 24:13

Right? So you know, there are the cool sexy things that I could talk about. But I can also talk about the really mundane.

A Aaron Bock 24:19

Well let's start with the mundane, then you can get really sexy if you want.

J Jason Christopher 24:22

Because the mundane stuff like frankly, when an IT person comes into a plant, and we can talk about some things that could get detected, we can find things like common IT commodity malware from like the 2000s, right? I'm talking like Conficker, code red, slammer, and it can be propagating throughout the network of a generation plant or facility. And the traditional IT response will be knee jerk, I need to be able to quarantine that, I need to be able to wipe that machine. But that machine may be doing operations. And so we'd actually talk to them about is actually you should just leave that running. If it's not impacting operations leave it running. I understand Conficker it's a nuisance, it's not really, you know, that great, but it doesn't know OT, it doesn't know how to bring down the plant. The probability of doing so is so minimal. It's clogging up some traffic, clogging up some resources, but if everything's fine, let's worry about in the next maintenence cycle, which may be three months from now. And so again, from a detection platform perspective, finding the mundane is just as important as sort of the cool intricate things. And those mundane things are happening more often than not. It doesn't mean it's not a good day, like you still talk to an operator be like, so did you plug in a USB that you shouldn't have? Like, there's still like an investigation. It's like, I want to like undercover this not a, you know, no worries situation. Somebody did something they shouldn't have, but it's not bring down the plant, which could be $50,000 per day of, you know, product that could be leveraged in your organization. So the mundane is, you know, pretty mundane. I would say that the more escalated things are when you're able to sort of see and what we do are called threat hunts. We actually build out hypotheses for what would you do if you were an adversary, and being able to understand and see that and in particular, those boundaries between IT and OT, similar to what I talked about with Colonial Pipeline, right. It wasn't really an OT attack, it was an IT attack, but crossing those boundaries is really important. And being able to detect, you know, any sort of activity there, I would say is where things get escalated and get a little bit more interesting.

K Keith Hawkey 26:23

Yeah, speaking about crossing the boundaries between OT and IT. I'm curious, how does cloud

Yeah, speaking about crossing the boundaries between OT and IT, I'm curious, how does cloud enter the conversation here? How many processes have the OT side of the business offloaded to a public or private cloud and what are the implications when it comes to security? And how does Dragos tackle that conversation?

J Jason Christopher 26:46

Yeah, so the cloud, thankfully, in a lot of areas, like for example, the highly regulated areas, off limits, right. If your electric utility, you're not putting any operations in the cloud in North America. But like I said, before, I've gone to chemical facilities where, and they're real conversations, because you can talk about real cost savings, if you, you know, were to implement this cloud solution, not only we're monitoring your fleet, but the worldwide fleet of all the things that we as a vendor can see, we can save you maybe millions of dollars in efficiency, if you just installed this one cloud solution. What we recommend there is having a dedicated DMZ, dedicated demilitarized zone just for the cloud, and have monitoring on that, right. Being able to say it's not persistent, we're going to make sure that we're detecting the things that we need to detect. But don't muddy it up with like the way I connect to the enterprise IT like have something dedicated just for that solution. Because we're in the wild, wild west, when it comes to the cloud and OT, we need to be able to monitor a lot more than we currently are.

K Keith Hawkey 27:40

What are some ways for, let's say we have a CEO listening to our podcast. What are some questions that he should ask his organization to assess the use case for introducing a conversation with Dragos? Who should he consult and speak with? What questions should he ask? How does he start? Yeah, or she? Excuse me, he or she begin?

J Jason Christopher 28:06

So I could start it off as a very simple one of sitting down with the folks in your plant and asking them what does a bad day really look like? They already know, from an operational perspective. They're like, oh, that turbine over there starts making this humming noise like run for the hills. But they've probably never looked at it from a cybersecurity perspective before. And so having a security person with them to understand, could we do that from cyber means that starts a conversation. The next piece that I would then ask is how would we know? When we talk about a, you know, event in OT it's not going to be the classic 1995 film The Hackers. I'm not going to have a virus singing Row, Row Row Your Boat, whilst capsizing ships. I've never seen an adversary put that much dedication into writing malware. What you will see and what it will feel like is a maintenance event, right? The controller over there no longer operates. It's not communicating to the main HMI, human machine interface, where the operator is actually working with a thing. And so if it looks and feels like a maintenance event, when would you ever know it's a cyber event? And what CEOs find jaw dropping for those aspects is we would never know. And so that's where the idea of Dragos as a detection platform come in, because we will be able to tell you, yeah, that's actually a maintenance event. No, this one actually looks like activity, you need to be able to do an incident response and recovery plan ASAP to be able to bring you back to a safe state. And so those two questions what my bad day looks like, and how would I know would be the two that I would give any CEO to start off with?

A Aaron Bock 29:30

Switching gears a little bit so we talked we've talked a lot about here IT vs. OT, I want to really muddy the waters, IoT. So an IoT is popping up, let's go 5g, you know. And I can't listen to a podcast now on any podcast like some form of 5g IoT is now coming in. Like last night I was listening to a podcast and it was like "You tired of your podcast dropping? Get T Mobile because our 5g network blah blah blah." Like it's ridiculous the marketing that's out there, but it's coming. So you've got the mobile networks improving. You've got 5g been rumored for a while. It's coming, but it's not quite there yet. Define like IOT security and OT security. Like, where's the convergence? Are they totally separate? Because I think sometimes they do get interchanged. And it's not clear like, what's the difference?

J Jason Christopher 30:22

So for me, the difference is that the industrial scale, right, because we do have IIoT as one of the other tag lines, which is industrial internet of things, or industry 4.0, or digital transformation discussions. And it's the same concept, but it's elevated. So instead of talking about, you know, my HVAC in my home, which would be IoT, I'm talking about a multimillion dollar refrigeration unit in a plant. They may still have the 5g conversation, they may still have this idea of being able to program everything from an iPad, which scares the bejesus out of me. So the concepts are the same, but the scale is very different. And so when you start talking about things in an industrial scale, that's where the IIoT piece comes in and that's where you'd find, you know, the Dragos' of the world sort of working through what can we do to prevent a really bad day from happening? IoT side, I would probably put that into a blended area more so where we probably sit with IT, but you need to understand the impacts. So for example, what do we consider our data center processes, our data center HVAC, that may be industrial. You know, some of these data centers have their own power facilities have their own sort of industrial refrigeration capabilities, in which case, I would put that under OT, but if it's something like our office building, or you know, whether it be elevators, HVAC, anything that could be a 01, that moves something in a building that could be in this weird area where sure it can sit within building management, but it probably needs to have some overlay then with IT as well.

A Aaron Bock 31:51

Got it. It's interesting. What about like, let's take it to a an industry that everyone kind of knows, like the food service industry. We all, we all go to, like fast casual, or, you know, there's a lot of technology coming out there with like, the like food safety, and you know, we're talking about kind of critical infrastructure when we talk about OT versus IoT, but like, for a retail food chain critical processes are like, how safe is the food and how likely is the food to go bad? Like, do you consider that IoT? Versus like, how do you where do you draw the line? Or does it? Yeah, so I would say, so we've actually done a lot of work in food and beverage industries. And it's, it's again, at the plant level. So you know, where's the food being processed, and doing sort of like the crown jewels analysis of what would a really bad day look like in a food processing plant? Absolutely, is safety systems, and not just sort of safety of the food, but also safety, of the people working at the plant, because those environments are rough. Like if you've ever

been to a chicken processing plant, it is a is a rough and dirty place to be. And so making sure that again, we're talking about safety, both from the end use product, as well as safety of the people there is where again, the Dragos conversation would happen. That is more like on the, you know, wholesale manufacturing side of the food and beverage industry. As we get more into, like what's happened at the restaurant floor, that's probably where we see more IoT and that again, will probably fit more inside the IT framework of things. Got it. Really confusing. OT, IOT IIoT, IT? We should have more I's and O's in there, honestly. I mean, let's keep adding. So no, thanks for sharing. This is it's a really fascinating topic. Keith, I'll let you kind of chime in here.

K Keith Hawkey 33:31

Yeah, sure. I'm curious. Where's the IIOT IAB, where's the industry going? What do you see coming down the pipe for Dragoa in the next year? What is the new technology? What can people get excited about that you're developing and the industry as a whole, the OT cybersecurity industry?

J Jason Christopher 33:54

Yeah. So I would say with Dragos in particular, just everyone's seeing that, I would say, convergence of what we do internally. So again, if you want to be able to have a platform, it's meeting you where you are maybe in that journey to the platform, you need services to be able to start you out, right. Not everybody can, you know, immediately get a technology in some cases, and they want to be able to understand their environment a little more, in which case, we leverage our services department. Maybe you just really want to be able to have an instant response retainer. That's one of the great services that we provide is, I don't know what a bad day looks like and I don't have the security expertise in house to be able to respond, being able to bring somebody on site from our team to help out is again, where I see the future of the state going is a combination of all these things, intelligence, response, platform, and being able to have professional services. That's where, you know, Dragos we've been focusing on and we're going to continue to focus going into the next year. For the industry, I think we actually already tackled the big one, which is this idea of digital transformation and cloud. There's no avoiding it. Now 20 years ago, we were having the conversation about TCP IP. And so what does it mean to start connecting substations to each other that were never connected before? And professional security professionals say "No, no way, no how, you'll never have TCP IP in my substation." And they obviously won the debate, which is why we have no TCP IP. And that's not true, we lost the debate really badly. Because we said from a security perspective no, not understanding there's a business need for efficiencies that was going to win the debate. Same thing's happening right now with cloud. If any security practitioner out there saying no to cloud, you're going to lose the debate, because we're talking about so much more efficiency. Instead, you have to say yes, and. Yes, and here's how we secure it. And I think that's where we're going to really see the next drivers of things happening. I'm talking about regulation, electric sector, they're already looking at virtualization and cloud technologies and what that could mean. And I think that's where we're going to see probably the next decade or so really pour out in terms of what we're going to do in the OT space.

A Aaron Bock 35:55

It's kind of a very obvious topic, like we should secure the most critical pieces of our plants, our production lines, etc. But it's kind of complex. I mean, it's like, you really are getting into the weeds of IT, the weeds of the business processes technology. One, is it the government's responsibility to continue to pass legislation to like regulate the OT and have requirements run OT security? Like, how do you see that whole piece playing out? And like, do you think we're doing a good job as a, you know, as a nation or as a world like regulating?

J Jason Christopher 36:27

I think some sectors have done better than others. I also think some regions have done better than others. We actually, 2022, I just did a Sans ICS summit talk on this, but 2022 was the most active year ever for ICS OT security standards and regulations. It seems like everyone just got hip to it all of a sudden. And so we started seeing activity out of Europe, activity out of Australia, activity across the globe, focusing on this problem. I do think that there's some value to a public private partnership that talks about what should we do? What should be the bare minimum requirements that we should all agree like we can do? But there also needs to be conversation about okay, well, how do we actually incentivize that? How do we put that in place? There have been also some really good marks there too, here in the United States, the Federal Energy Regulatory Commission, just released an order talking about incentives. So how do we incentivize you being more mature than just the very baseline minimum requirement standards that we have? And I'd be curious to see how that goes. So I think we're still discovering the relationship, even though we've been doing it for so long, in terms of what our strengths and weaknesses for government and private sector, but I do believe that both parties have a sort of spot at the table as it were.

K Keith Hawkey 37:35

That's awesome. Jason, we're running up toward the end of the podcast and typically, toward the end, we like to spend a little time talking about if, if you had a message that you could broadcast to everyone in the industry, any decision maker or organization, what would that message be? Let's say you had a billboard that everyone could see, what would you say?

J Jason Christopher 38:02

So if I were to broadcast a message, it would absolutely be that conversation about how would you know, if you are secure and safe in OT. One of the things that we talk about a lot is that if you're not cybersecure in OT, then can you really be cybersafe. And that's this big conversations about again, if I don't know an attacker is there, I send an engineer on site, they're going after the safety systems. As an engineer, I always want to make sure that I'm going to be safe. And so that's absolutely, I'd probably even just shrink it down to are you cyber safe? And make sure that safety and security are talked about in the same breath when I'm an industrial plant. If we can do that, then I think that the cultural issues, the funding issues, the Hey, is this really important all sort of go away. Because we understand that safety and security are going to be the same thing when I'm in an industrial environment.

A Aaron Bock 38:54

Hey, Jason, we really appreciate having you on. I guess, as we kind of close out, and I think that's great advice for everyone. I guess a follow up question is what would you recommend? And how do people get in touch with you? Because I think people are gonna find a lot of interest in this and question, if they've really done enough for this space. What would you what would Dragos like tell our listeners the best way to kind of start this conversation? Yeah, and kind of frame it pre meeting with you or someone? And like what you recommend?

J Jason Christopher 39:23

Yeah, so obviously www.dragos.com. Not only from the perspective of what we have on our website, but we have a lot of free material that we give to the community. The ICS community is very small compared to IP security. So we view it as a community effort to be able to provide education where we can, and part of that is actually every year on November 5, no matter what day of the year that fifth lands on, it could be a Sunday or Saturday, we host the Dragos Industrial Security Conference, DISC. And it's free for asset owners in the industrial space. So if you don't know where to start, start with dragos.com. If you want to get deeper into it, we've got a free conference that we leverage for everybody to be able to attend and just be able to learn a little bit more, you'll be able to hear from us on the research that we do, understanding how it is that we can leverage things like detection, or like the professional services or incidents that we've dealt with. And another thing that's really valuable on our website is the year in review. We've been doing a year in review every single year since Dragos has been a company, and that year in review provides you sort of this look back as to the top vulnerabilities, the top threat actors, the top incidents that we've seen, and that should really, hopefully get people the right questions that they may need to be able to ask their organization. So the hub is Dragos.com, but there's so many avenues that you could pick from from there. I just recommend maybe starting with looking at DISC, looking at our free webinars, and looking at what we do in year in review.

A Aaron Bock 40:41

Yeah. And we'll, we'll link these in the show notes so that if you're listening to this while you're driving, and you want these later, look in the show notes, you can also reach out to us at Opkalla. We partner with Dragos and we're big fans of what they're doing in the space. Jason, this has been great. I think it's a really interesting, fascinating topic that's going to become more important. I think it's going to continue to evolve with like you said, the cloud adoption, etc. I know Keith and I are excited to talk to our customers and understand a little bit more about what they're doing. And I think you share a lot of knowledge today that people will find valuable. So thank you for joining thank you for being our 13th episode, which could be unlucky, but I think it's lucky. Keith has Santa Claus on his roof so that's it's a lucky day for him. Once again, thank you to all the listeners. Oh, yeah. Yeah. Thank you to all the listeners out there. Continue to subscribe to the podcast and we look forward to the next episode. So have a great day.

J Jason Christopher 41:34

Thank you for having me. Take care.

A Aaron Bock 41:35

Bye, guys.

N Narrator 41:38

Thanks for listening. The IT Matters podcast is produced by Opkalla an IT advisory firm that helps businesses navigate the vast and complex IT marketplace. Learn more about Opkalla at opkalla.com.