uberknowledge

Jason Haward Grau, CISO, PAS

Operational Technology is Underrepresented in Cybersecurity

Jason talks about cybercrime in OT and the huge impact it has on human life, infrastructure, and energy resources. He discusses the importance of frameworks in encouraging good, ethical behavior and shares his thoughts on digital consumer rights being determined by geography.

02:41 OT is underrepresented and little understood, yet we use it ubiquitously every day.
05:00 60 percent more likely to see an engineering mishap than a cyberattack in OT, but they still happen.
06:07 Safety is becoming a more prevalent issue. Chernobyl, Bhopal, Piper Alpha all could and should have been prevented.
08:36 Frameworks provide a structure. They provide value for doing the right thing and discourage negative behaviour.
09:50 Exploits will happen. What is important is lessening the likelihood and the impact.
11:23 Every organization should deploy two-factor authorization. If you can prove your security capabilities, you will increase customer trust and revenue.
12:32 Don't just know your rights, exercise them.
13:51 What are your rights as a digital consumer and does geography determine how much control over your own data you are entitled to?
15:58 GDPR has had some unintended consequences for business.
17:30 If you do something wrong in OT, somebody gets hurt.
19:32 The challenge is in the proliferation of applications. Regulation is great, but remedy is more important.
22:54 We don't need more cybersecurity people in OT, we need more OT people in cybersecurity.
24:26 Diversity in cyber is a problem, but don't set a quota, set a goal.

Ashwin Krishnan: [00:00:38] Welcome to another edition of the UberKnowledge podcast. With me, I'm going to try and pronounce your first name and middle name, and I'm going to attempt to pronounce your last name.

Jason Haward Grau: [00:00:49] I'm looking forward to this.

Ashwin Krishnan: [00:00:50] Jason Haward Grau.

Jason Haward Grau: [00:00:53] Beautifully done.

Ashwin Krishnan: [00:00:53] All right, great. We got something right on the podcast. So welcome. I know we're reaching the "end" of RSA 2019. For the purpose of our listeners, why don't you introduce yourself and maybe start off with what are some of the aha moments for you — good, bad, and ugly — so far at RSA 2019?

Jason Haward Grau: [00:01:18] I'm Jason Haward Grau. Good afternoon or good morning depending on where you are listening. I am the Chief Information Security Officer for PAS Global, which is an integrated software company that provides ICS cybersecurity capabilities specifically to the operational technology area. We also provide high performance HMIs — human management interface capabilities — to a wealth of different operating industries throughout the world. We've been around for 25 years, so not exactly a fly-by-night, just turned up kind of thing. We are a U.S.-based company, so confusing that I'm British, but that's all good.

[00:01:58] Interesting insights. Let's start with the obvious ones. RSA seems to have got bigger and busier than ever. I think it's becoming an ever more challenging place to do business and have good conversations. I will confess upfront, I've barely managed to get to any sessions. And the reason for that is because, actually, it's the side conversations that I'm having with the CISOs, with other vendors, also with other customers that are becoming more interesting and actually take up more of my time. That's good because of two things. It means that we're engaging in dialogue. Part of the good thing about RSA is that you have the gift of, I believe, 45,000 people crammed into one place.

[00:02:42] So there is literally one of everything here. I think, once again, OT is relatively underrepresented. Operation technology is an area that we don't necessarily understand very well, most of us, and yet we use it ubiquitously every day. It's a fundamental, everything from turning a light switch on, to asking Alexa to do something for you — you require power to do that, through to the petrol or the gasoline that goes into your car, to the products that you buy. It all requires operational technology to make those happen and it's seamless for us. What I've seen is we do have the sand pit, which is great, but we haven't broken out into the mainstream. And I think that's something that I'm going to challenge RSA to do more of because actually it's incredibly topical. We have independent representatives in Congress suggesting that maybe we should uncouple the power grids. Literally a week or so ago, one of the representatives made that statement and from a practical perspective those conversations really should be had. It's a great place to have them.

Ashwin Krishnan: [00:03:48 Actually you've touched upon a very important point and I completely agree. I think OT is underrepresented. I think the impact … and we keep having these scary-day scenarios of nuclear power shut down, our cars going awry. So, two questions: the first is as a CISO, and you mentioned conversations with other CISOs, is that how the evolution, maturity, learning from each other versus consultancies that come up with their surveys, versus vendor pitches — just from a CISO's education, evolution, where do you derive insights and how do you actually act upon it?

Jason Haward Grau: [00:04:36] So the cheating answer is all of the above but let me qualify that. The conversations that I have with other CISOs, whether they are customers or whether they are colleagues, ex-colleagues, the informal network serves so much more powerfully in terms of contextual understanding. What do I mean by that? Most CISOs will not commit or confirm that they have incidents, whether they are cyber, whether they're engineering. In OT the challenge is actually slightly different. There you are 60 percent more likely, or you have a 60 percent likelihood if you like, to have internal issue that relates to an engineering mishap, a mistake, a configuration analysis change or someone adding or removing something from the OT environment in an unplanned way, than you are to have a specific cyberattack.

[00:05:29] Now does that mean cyberattacks don't happen? Of course they do. Whether they are phishing-based attacks and someone jumps the air gap from IT into OT, whether it's malware introduced in, whether it's a firmware fail; those are all things that happen, but how many of them get reported? Think about it logically. Reporting is very, very insignificant in terms of the number of active issues that we talk about. One of the reasons that we do that is we say, the first rule of cybersecurity fight club is no one talks about cybersecurity fight club. Why? Because we don't want to admit the challenges that we have in a way that would make material sense.

[00:06:07] Engineering challenges are much easier. In OT one of the other things that we see a lot of — this is starting become much more prevalent from the consulting side — is the push towards safety. So the conversation is now becoming, if you apply risk and safety, and we've been doing this for 25-30 years going back to Bhopal, you go back to Piper Alpha …

Ashwin Krishnan: [00:06:26] Yes!

[00:06:27] The Texas City, they're all significant issues that were safety oriented. They could have been and should have been prevented. Chernobyl could and should have been prevented. The reality is that they weren't. So what do you do? You focus on safety. And safety is a component now; where you see a lot more emphasis coming in from the likes of the Big Four. They've started to talk much more eloquently about safety as a requirement. That's a really important message. If you think of cyber as just one more safety consideration in OT, you'll get a lot more currency and a lot more traction. Hopefully that helps.

Ashwin Krishnan: [00:07:01] No, it does. I think you've brought up ... I think that's the first time in my 11 or 12 podcasts that the word safety came in, and I think it's really relevant. The word Bhopal obviously rings a bell because I'm from India. I was in India and when that mishap happened of monstrous proportion.

Jason Haward Grau: [00:07:19] Absolutely.

Ashwin Krishnan: [00:07:20] So one of the things you've talked about is, and I quote you, "Well-constructed regulations provide a framework, and they're fundamental to getting things right. However, it shouldn't preclude us from going above and beyond to ensure our security." Now, I could not agree more about this, but again I'm trying to put myself in

a CISOs shoes. So, you're fighting for budget.

Jason Haward Grau: [00:07:42] Always.

Ashwin Krishnan: [00:07:42] You are in this constant world of negative press.

Jason Haward Grau: [00:07:47] Yes: fear, fear, fear.

Ashwin Krishnan: [00:07:48] And you are in this world of vendor overhype and noise.

Jason Haward Grau: [00:07:53] And underdelivering.

Ashwin Krishnan: [00:07:54] That's a dagger to my heart from my vendor days. But that's true.

Jason Haward Grau: [00:08:00] It is true.

Ashwin Krishnan: [00:08:01] So given all of this, while it seems like the right thing to do, let's not get caught up in GDPR. In fact, one of my prior conversations was about how do you shift the focus towards doing the right thing by the customer and then compliance will be a derivative of that. It seems to make so much sense, but again I'm looking at you as a CISO and saying does it make operational sense when you're fighting day-to-day battles? When you're looking at breaches that are likely to happen, looking at CVEs reported by existing vendors, how do you aspire to be ...

Jason Haward Grau: [00:08:34] Better than the foundation?

Ashwin Krishnan: [00:08:36] Yes, better than the foundation.

Jason Haward Grau: [00:08:36] So, I agree with what you said. Fundamentally, it is a requirement that we codify what we do. I want to use safety as a really good analogy. We are most familiar with OSHA from a safety perspective, something that's been around since the tragic disasters both Piper Alpha and Bhopal. Capability wise, that's a framework that also provides a structure. But what it also does is it actually provides value for doing the right thing and it discourages negative behavior which erodes the value you get from doing the right thing.

Ashwin Krishnan: [00:09:10] Right.

Jason Haward Grau: [00:09:11] The first thing is, you're right, we all fight for budget. Budget is always based on a negative premise, which is you want to tell me that you're going to protect me from a breach, but you won't protect me from a breach because a breach is going to happen because you're telling me they're always there; it's inevitable that I'm going to get breached. And then what you're telling me is that I need to be ready for it when the rain comes. So why are you selling me an umbrella when it's a sunny day? The reality is regulation gives you structure to do that. It also gives you the ability to manage risk. Risk has become a much more open mainstream discussion over the last five years, seven years, 10 years around the cyber risk measure. Risk and cyber risk has become

synonymous.

[00:09:50] People understand the fact that you have a risk of an exploit, and what you're trying to do is lessen the likelihood or lessen the impact. And organizations can place their money and take their bet. The good thing about that is that when you're fighting for budget you can actually quantify, "Look, I will reduce the amount of risk by deploying this framework." What I've seen over the last two years in every single conference that I've attended, pretty much every conversation I'm having with customers but also with suppliers and with vendors is, what's your framework? What are you using? So, it's not an unreasonable step to expect people to behave differently if there is a framework in place.

[00:10:29] The other thing is look at the implementation, and it's slightly different because it's a directive as opposed to a regulation of NIS in Europe. NIS is a recognition that we have to do something differently, and we have to force behavior out. Part of the understanding of that is that it's actually driven things like GDPR. And if you look at how much budget has been allocated to GDPR and how much of a consequence that has had already, that's an interesting argument. That being said, my very simple, simple view is if you cannot quantify your risk, you cannot ask for budget because budget comes after the explanation of why you might be exposed. It doesn't have to be rocket science or 100 percent accurate; it needs to be your best estimate. Then you have a debate about how and what you will do to mitigate it. It should also flow into positive territory because if you're mitigating risk, you're also improving the operational capabilities of the organization.

[00:11:23] Really interesting point, deploying two-factor authentication. OK. Two-factor authentication should be something that every organization should be doing. We know they are still those that don't. The argument is it's expensive to put the infrastructure in and do multifactor, but if I can boost the amount of sail that I have as an organization when I can demonstrate that I have good security capabilities in place — because customers will ask well how do you secure my data; how do you secure my personal information; how do I know that you are protecting me as effectively as possible — and those that do, tend to find a higher increase in their revenues. That's starting to come through. So, does that answer the question?

Ashwin Krishnan: [00:12:00] It does and it actually flows very well into the follow-on question I have which is customers starting to ask questions of their vendors.

Jason Haward Grau: [00:12:09] Yes.

Ashwin Krishnan: [00:12:10] And it's both B2B and B2C.

Jason Haward Grau: [00:12:13] Yes, and C2C.

Ashwin Krishnan: [00:12:15] So the awareness piece, and again I go back to GDPR. I'll give you this the simple example, which I found mind boggling. I was at a conference, I think about four weeks ago, it had IoT, blockchain, AI, and big data, all four.

Jason Haward Grau: [00:12:29] That's a lot of buzzwords.

Ashwin Krishnan: [00:12:32] Yeah. There were 12,000-13,000 people. I was in a speaking session with about 300 people in the audience, and I asked them a simple question. "How many of you have heard of GDPR?" All hands went up. "How many of you are LinkedIn users?" All hands went up. "How many of you have actually exercised your GDPR rights with LinkedIn" No hand went up. And it's the simplest thing to do because I did it. And it was shocking for me to see the amount of digital trail I'd left behind, right.

Jason Haward Grau: [00:12:54] Did you ask for an SAR, which is your right to do right as a citizen?

Ashwin Krishnan: [00:12:59] Right.

Jason Haward Grau: [00:13:01] Within the European Union I can ask for it. Interestingly enough, when I do the same thing here in the U.S., I was told since the data is residing here, even though I am an European, I am residing temporarily at least in the U.S. or I'm in the U.S., and therefore they are not obliged to share. Isn't that interesting?

Ashwin Krishnan: [00:13:18] Yes!

Jason Haward Grau: [00:13:18] I can use the spirit to defeat the law.

Ashwin Krishnan: [00:13:21] Correct. And that's a great point. Where does somebody go to find the right information? I mean yours is a perfect example right here. Presumably an EU citizen, temporarily residing in the U.S., working for a U.S. company with a global footprint. So, it's one thing to expect consumers and C2C, B2C, and B2B to be activist, to at least start exercising their rights, but another thing is what is my right?

Jason Haward Grau: [00:13:51] And that's the other part of the equation that is incredibly interesting. So historically, I want to go back to another law, it's a consumer protection law in the U.K. that was established in the late 70s, and the reasons it's analogous is because it's exactly the same thing. What are my rights as a citizen for consumer protection? So, what are my rights as a digital consumer? What are my rights in terms of understanding the right to be forgotten, the right to know what you hold upon me, the right to know when you're going to hold it and when you're going to remove it, and what legal frameworks are in place to ensure that I can ask those questions?

[00:14:25] The challenge is actually that it took about 10 years to go through a significant amount of case law to establish what it really means to me as a consumer. So, I can do an SAR request right now. I should be able to do so as a European citizen. I have a British passport. I'm entitled to that as part of the U.K. But if I'm asking an American entity, where the data resides in America, they are required to share — but they're not really because there are certain arguments that can be made that I am a different person or I'm in a different place. Now if I'm in the U.K. and I'm doing it, I'm fully entitled. The challenge is also the fact that if you look at it simplistically, you'll lose.

[00:15:09] This stuff is highly complicated and there are an awful lot of moving parts that

we need to consider. It's a challenge, especially for things like GDPR, I know because I'm going through it. Look at Google. I can request meta tags for images that relate to me to be removed. I have a right to be forgotten. They can turn around and say, well actually, we have a right in the public interest to suggest. Hang on, you're Google.

Ashwin Krishnan: [00:15:32] Yeah.

Jason Haward Grau: [00:15:34] Since when have you been a newspaper or a publisher or a journalist or anything similar? What is a public interest? We are a provider and purveyor of information. So, I think the challenge is actually going to be for the next three to five years, we're going to feel our way around it. And I think there's going to be a couple of significant cases coming to ultimately the European Court of Human Rights, the European Court of Justice, to force the outcome and that will be the codification.

[00:15:58] We've done something which is very sensible to protect consumer data, but actually there are some unintended consequences. I was talking to some of my colleagues in Europe, and they've had to purge huge databases because they didn't get a response from a consumer. And I asked the question, "Well interesting. So, when you wrote to your consumer, how did you phrase your opt-out or your opt-in?" And depending on who you spoke to, you had a different reference. So, we've a long way to go.

Ashwin Krishnan: [00:16:27] Talking about that opt-out, opt-in. There's a lot of talk about trust at this conference which I found to be uplifting yet concerning at the same time.

Jason Haward Grau: [00:16:37] I understand. It's a duality of significant proportions.

Ashwin Krishnan: [00:16:39] It is. It's one thing to talk about trust, but the other thing is, just like the example you mentioned, how does it translate into transparency? How does it translate into words that I can actually understand? And I'm not saying this because I love Apple, which I do, but I love the fact that I can actually go to their website, look at their privacy page and it's in one screen and I can actually understand what's being said. When you're talking about the spirit of an organization of that size taking privacy to heart and being able to educate their consumers, presumably most of them are not even tech, how does that translate into your world of OT, where you're actually talking about an even more complex situation? Apple is taking the most complex devices and making it simple to consume, not just in marketing but now also in our privacy.

Jason Haward Grau: [00:17:30] Wow, that's a huge question and probably a long answer. So, let me try and think my way through it. It's a great on-the-fly question. If I look at OT as a challenge, how do you develop and build trust? How do you then assure that the suppliers are doing the right things the right way? Two things that I would say stand out right now. The first one is that there is the concept of trust but verify, which is pretty much synonymous with security, but it's becoming synonymous with OT in general because we tie back to if you do something wrong, somebody will get hurt; there will be an environmental explosion; there is a risk to life which results in significant penalties. So, there is that kind of carrot and stick, certainly a big stick, not much in the way of carrot, to be fair.

[00:18:17] I think when you look at how do we qualify trust within OT, it's growing awareness that I can ask. So, I will go to Dell Secureworks, they provide me with security capabilities inside my organization, and I will ask them to show me their equivalent of SAS70 as it were. Show me how you are qualifying, controlling, and managing the information that I provide for you on our infrastructure, on our people on our infrastructure. The wonderful thing about the Apple statement which I absolutely love, you're absolutely right, Apple have done this beautifully, but they've deflected accountability to the application providers. So, "Hey, it's not me; we're very transparent. But listen, if you're using this mapping technology that gets you from A-to-B, and they happen to keep all the information about where you stop, how often you stop, where you go, who you stopped to talk to, what interactions you've had, well hey, that's not me, that's them." Which is a little bit obfuscating. I love Apple, I'm a big fan of Apple. I love the closed network system that they were on, I love the architecture that they built, and I love the products. One day they will have a touchscreen iMac. I know, one day, one day, I'll believe it when I see it.

[00:19:32] But in all seriousness, the challenge is actually the proliferation of applications. That is presenting the challenge, and privacy policies are not designed by most organizations to be simple, easy to read, clear, unambiguous, and most importantly give you the redress. So, what's my remedy if I want to complain about Google Maps? "Hey listen, you guys, I did a download of you, what's my remedy?" I can complain to the information commissioner maybe, but is that appropriate or right? There should be a better, clearer and more effective mechanism in place to do that. Most of us don't have that.

[00:20:10] If you look at privacy policies in general, most of us will deploy what our marketing or sales organizations have said we have to have in there and then what legal have interpreted as the best guess evidence. So regulation is great, but remedy is more important in my experience. You should have the remedy to be able to go back and say, "Hey listen, I want you to forget me. I want to be able to confirm what data you're holding on my organization. I want to understand what the implications are. Are you processing data in the cloud? How do I know that data is safe and secure?" So, there are certain things I can do, but there is a lack of remedy. Does that make sense?

Ashwin Krishnan: [00:20:43] It does. We have a few minutes left, so I want to touch upon the human element of this thread. It's a two-part question. The first one is we have a cybersecurity skills gap and that's only growing. OT is not the most preferred destination for cybersecurity professionals.

Jason Haward Grau: [00:21:03] It should be.

Ashwin Krishnan: [00:21:04] It should be because, like you said, it's safety and human life, and the impact is much greater. Number one, how do you make it sexy enough that people want to be part of that. The second question is, and I've had this conversation with many of my prior guests and I want to get your take on this, there's clearly a diversity issue or lack of it in the cybersecurity industry. So how do we get not just more women in the organization but also young adults who are otherwise attracted towards other professions, not cybersecurity? Is there a remedy to making OT more attractive? Is there a way to attract the next generation, I don't know Gen Y, Gen Z, whatever?

Jason Haward Grau: [00:22:04] Ok. Let me start with the easiest bit, which is how do we make OT attractive. I think — this is going to be fun and I'm going to be a little bit contentious — what I think we need is not necessarily cybersecurity professionals in OT. What we need is OT professionals in cybersecurity.

Ashwin Krishnan: [00:22:12] OK.

Jason Haward Grau: [00:22:12] I know it's kind of backing into it, but let me give you the expression as to why. If you look at the legacy and the history of operational plants in general terms, they are heavy engineering organizations backend in. Actually, what we need to do is build more engineering-capable people in cybersecurity as opposed to having more cybersecurity people in OT. You do need a mix and match, but if you look at the cultural difference between the two, it's actually really important to bridge that gap first.

Ashwin Krishnan: [00:22:41] Got it.

Jason Haward Grau: [00:22:41] I'd rather have 10 engineers that I can train into cyber than one cyber guy that I can train into OT, as I'll probably have roughly that kind of order of magnitude. At the same time, how do I encourage diversity? That's a really, really hard thing because the perception is it's a white, male, degree-orientated organizational structure that is very dry and terrifying, and you have a two-year lifespan as a CISO — you're going to be working terrible hours, lots of coffee, and not much life.

[00:23:15] The reality is different. What I've done personally is I've encouraged good females, not just females but a good broad range of people into my organization through internships, leveraging that as a way of bringing young grads in, so Generation X plus one. Also, I'm an old-fashioned guy, I'll go and talk at university campuses. One of the reasons that I do that is because I believe I'm an atypical CISO in many ways. I am relatively articulate, I'm happy to have conversations outside in the daylight.

Ashwin Krishnan: [00:23:52] [Laughs]

Jason Haward Grau: [00:23:52] I'm not frightened of doing it. And I actually can have a really engaging debate about why it's important. I actually did one of those at the University of Houston last year to their postgrad program and it was a really good — supposedly half an hour lasted an hour — argumentative discussion about why we need more people from the diverse backgrounds.

Ashwin Krishnan: [00:24:09] Right.

Jason Haward Grau: [00:24:10] And this included ethnic backgrounds, religious backgrounds, rockstars. I kid you not! I had a guy who worked for me who was a bass guitarist. He was the most effective SOC analyst I ever had because he could pick stuff up that nobody else would see because he saw musical patterns.

Ashwin Krishnan: [00:24:25] Right, right!

Jason Haward Grau: [00:24:26] But at the same time, you have to recognize it has to come down to each and every one of us. Don't set a quota, set a goal. I want to bring somebody into my organization who is … I want to be able to find a diversity. But the other thing I remind my boss of every single day is in my organization I don't have a team of X, I actually have the entire company as my cybersecurity team because every one of them has a responsibility and accountability. I brought people into security by virtue of leveraging things like awareness and assurance activities, building projects where you bring business and security together. People suddenly realize actually this is quite interesting. It's a bit different. Ok, it's kind of like an IT project but it isn't. Oh, I see how the bottom line makes a difference. Right. Those are things that you can do and every organization needs to. Equally, very simple, attrition is a killer. But the reason that 99 percent of people leave organizations is that they join companies and leave managers. They leave the managers because they don't develop the people. My career is my responsibility, but my boss needs to support it.

Ashwin Krishnan: [00:25:32] Right. Never was a truer word said. I completely agree with you. On that note, Jason thanks for your time. This has been a really interesting conversation.

Jason Haward Grau: [00:25:39] It's been a pleasure. Thank you.

Ashwin Krishnan: [00:25:41] Thanks Jason.