Arthur Jones (00:06):

According to checkpoint research and writers, cyber attacks on US utilities in 2024 increased nearly 70% compared to the year before, leading to an average of 69 attacks every week. In 2025, the trend has continued in the US and globally. So the question is, what can utilities do to protect themselves from these digital threats?

(00:27):

Unlike conventional information technology systems, OT systems, which are short for operational technology systems, directly control pumps, valves, and treatment processes. An attack on OT can have immediate real world consequences for water quality, safety, and public health. The OT environments at Hampton Roads Sanitation District is a success story. It protects one of the largest regional water and wastewater utilities in the US, servicing more than 20 counties and cities, and one and a half million people. Thanks to its signature program of embedded visibility, governance, and consequence-driven planning, it can serve as a blueprint for water utilities globally.

(01:06):

My name is Arthur Jones, and I'm talking about how to apply the cyber security blueprint with Ben Stirling, director of Cyber Security and OT at Jacobs, and Roger Caslow, chief information security officer at Hampton Roads Sanitation District.

(01:22):

What does it take to tackle the elevated risk we see from bad actors in the operational technology space? I'll start with you, Ben.

Ben Stirling (01:30):

One of the best things that Roger has done at HRSD is really elevate the visibility into the OT network and the challenges that they're facing. A- any time you are working on really setting cyber security, the first challenge really is getting leadership involvement and leadership buy-in. And, you know, once you set that risk profile and once you've said, hey, here's where we are, and you start moving that needle, great, but getting that first step is one of the most challenging things. And that's one things... Roger, I would love to know exactly how you did it so I (laughs) can get it to be replicated elsewhere. But the amount of buy-in and sync that Roger has at HRSD is I, very few clients I've ever seen it with.

Arthur Jones (02:19):

So, Roger, what's your secret? How do you get that kind of buy-in and how do you work with the, the kind of added visibility challenge as well?

Roger Caslow (02:26):

So, so my leadership, uh, number one, recognizes my expertise and they recognize that I still have visibility into some of my own, my old communities. And I still see and hear things that the average person may or may not see or hear. Not to mention, I have my local FBI field office backing me up 100%. My CISA, Homeland Security and, and, and, and CISA reps are backing me up 100%, uh, on things I'm saying. And they see the reports, they see the briefings I provide to them at the unclassified TLP amber level so that they're able to understand. And I have to digest that for some.

(03:06):

I have to articulate that in a meaningful manner, but frankly, the ability to articulate risk in a business tone, and it doesn't take much when I'm in a great organization such as HRSD. It really is an amazing organization. There is no other organization like it in the world. And I'll say it, I've seen a lot, none other like it, meaning that everyone here understands the mission and what we have to do. And it's all about protecting that mission, right? And our customers, and, uh, understanding that anything goes wrong in the cyberspace has a direct impact on the environmental and on our reputational risk, and our reputation is king. Uh, we don't wanna lose any of that public trust that we've, that we've, that we've worked so hard to build through the years. 85 years strong. So that's part of it.

(04:04):

And we've had cyber incidents. Yeah. And we've had published cyber incidents, um, and, uh, we've worked through those. We've never paid ransom. We will not pay ransom under any circumstance. We recover. We rebuild. And I have a amazing team around me that helps support that on the business IT side. And now with Jacob's OT, Jacob's cybersecurity on board, I think I have an amazing team to help support me on the OT cybersecurity space as well, because these are two separate houses, but they converge in the middle.

Arthur Jones (04:36):

And that, Roger, brings up a question from me in terms of, I mean, obviously there's more kind of digital transformation happening across all ward utilities, and I'm sure you know, obviously Hampton Roads and there's, there's no exception. So how does that change things?

Roger Caslow (04:50):

It's here. We have to get over it, number one, right? We have to continue to press forward. It's a fact of life. Uh, digitization is here, uh, in the OT space. It's been in the IT space for 25, 30 years. In the operational technology space, HRSD's move forward a little faster than a lot than many. And addressing that is having awareness, situational awareness, understand what you have, where it is, or assets, understanding the, again, the threat space and understand your risk overall. And it may seem a bit trite, but it's, it's true just to understand those basic things, be able to pull those together and then look at them in a meaningful way to be able to figure out the best way to defend.

(05:41):

We're not perfect. I, I know that. We have a long way to go, but at the end of the day, I've told my leadership this. I've told my board this. Uh, I've, I'm on the board of the water ISAC, and I've told them that, and I said, "Watch. I'm gonna be ahead of every single person here at the end of the day." And my, my goal is to make our HRSD the light at the top of the mountain for how every water wastewater utility should be. That's my goal. That's my stated goal. That is my vision. And that's where I know I can be.

Arthur Jones (06:12):

Ben, from your side, I mean, obviously this challenge is a, is a growing one as well as Roger so expertly outlined there. What is your take on, you know, digital transformation and the kind of ongoing risks around that?

Ben Stirling (06:25):

Anytime you connect a device, you increase risk. So when you're not going through a diode, which Roger hates, but when you're not going through a diode (laughs) and you're not just sending out historical data, you've got the ability to effectuate something. So whether it's a pump station for HRSD that's out in the water, that, you know, if this doesn't move the waste water, we've got backflow, we've got a problem. You, you need to recognize that connected device equals risk. What you do to protect that, how you effectuate that is what matters.

(07:02):

We're never going back in Congress. There's, there's been bills talking about going back to an analog, uh, electrical grid. Not gonna happen, right? We're worried about EMP. We're worried about all these different things. Digital is here to stay. It's not going anywhere. These battery facilities that we have, those are digital inverters, most of them manufactured in, you know, uh, adversarial nations. So we have to think about defense in depth, making sure that the architecture is correct, and really thinking that we're already compromised. Is my digital inverter already a compromised asset? How do I protect against that? Am I looking at supply chain risk? What are you gonna do? What level is the organization prepared to go?

Arthur Jones (07:49):

I'm gonna go back to, to Roger now, and I'd like to bring up, I mean, you've mentioned how you want to lead the industry in terms of, you know, place Hampton Roads Sanitation District as like the, the kinda the role model. So what were the biggest lessons from, from your work that other sectors like energy or transportation, what can they learn from you and your strategies now?

Roger Caslow (08:11):

Well, it's not about the regulation. It's about doing what's necessary and sufficient to protect your enterprise. Regulation is the floor. It's always the floor. The regulation, why? Because regulation is built by regulators. And regulators are not operators. Regulators are not, are not, uh, asset owners. Regulators, most, most, 99.9% of them have never been an asset owner, meaning they've never had to take responsibility or accountability for operations of a plant, a power generation facility, uh, any, any type of of refineries. They've never had to own those things. They look 'em aside. They've read a book. They, they figure, they understand it. They've actually gotten their hands dirty.

(08:57):

With the regulation being the floor, we have to strike a balance between what the floor is and where we should be, right? And, and here is where we should be. And if we drive toward a, a, a, a common operating picture, using of a tried and true tested models that are out there, start with the Purdue model, segmentation. I tell people in the IT space, operational technology was doing segmentation before it caught onto it. While, while OT was continuing to segment, IT started going flat. Uh, so you could go east-west lateral traffic inside an environment, which was a good thing for business, a bad thing when they get a cyber incident, right? Where there'd be a, a Trojan, any type of malware.

(09:42):

So driving toward that model and ignoring the regulation, I say that, you, you can't ignore regulators, but if you're going above and beyond what they're asking for, they tend to leave you alone 'cause they recognize that you're above the bare minimum, right? You're no longer, you no longer need remedial education or work there. And that's good for all, across all. And the power sector has been heads and tails, heads and shoulders above this because of NERC and FERC, the reg- the regulatory industry. But let's face it, the regulatory industry came in, came about because of nuc. Nuc is what caused most of this regulation to happen in the power space. It wasn't any other reason, right, Ben?

Ben Stirling (10:27):

One thing I would say is compliance is not security. Um, so you can be compliant and totally insecure.

Roger Caslow (10:34):

Compliance and complacence are two letters different. That's it.

Ben Stirling (10:37):

But what we need is people like Roger doing exactly what he's saying he's doing, and that's putting in practical security steps, making sure and assessing where am I at, and moving that needle and making sure that his security posture is changing in a way that says to the regulators, "Hey, I don't need you. I've got this. I'm doing the right things already." Makes a big difference.

Arthur Jones (11:03):

And actually it's a, it's a, it's a good, it's a good segue into the next question, which is gonna go to you, Ben. So we often hear about consequence-driven cyber strategies. So could you explain what that looks like in practice and why it's important to consider?

Ben Stirling (11:16):

Yeah, it, it's actually one of the things we're working on with Roger at HRSD. And consequence-driven cyber-informed engineering is out of INL. It's a very, it's a very boots-up approach. Consequence-driven, cyber-informed engineering is really about not if something is gonna happen, it's about when, and it's about reducing the amount of effort to recover from it. So you're assuming you're going to get breached, you're assuming your worst day is going to happen, and you're looking at things around it going, "Okay, how can we minimize this as much as possible?" It's a safety mindset. What I really like about this approach to cybersecurity is it's right there with your safety program. You try and engineer out anything you can, you ultimately end up with some PPE, right? As the last line of defense. But you, you go through the entire process of saying bad thing is gonna happen. What do we do to reduce it, reduce its impact and reduce our recovery time from it? And that, that's the key thing there.

Roger Caslow (12:23):

It's like the British band Chumbawamba, their song, I get knocked down, but I get up again. You're never going to keep me down. That's the truth. So, so it's about all those things. And if, and if you look at the... It, it, I tell that to people, it's, it's not about, it's not about getting knocked down. It's about how fast you recover. And, and, and, and that's why if you look at the other models out there, the CSF is fine for this. The last two are response and recovery.

Ben Stirling (12:49):

Mm-hmm.

Roger Caslow (12:49):

Right? Identifications, all these things have happened, the first three have happened. It's the recovery that's so important. How fast can you recover? What's your recovery time? It's you're gonna get hit. There will be, whether it be some, some simple kid in his mom's basement sucking down Mountain Dew and eating Hot Pockets, or whether it be a brigade attacking you, you will get hit. You'll get hit. How fast do you recover? That's where the INL approach works best.

Arthur Jones (13:21):

What is the biggest lesson that other operators or utilities need to consider when they, when they think about securing their systems and building a culture of resilience, which you explained earlier?

Roger Caslow (13:31):

Well, re- a culture of resilience usually is already been inculcated amongst the operational technology world. So that should already be there. So the culture of resilience should already be present within, uh, most industrial control systems. Resiliency is king, right? It really is. All of the utilities or, or operators within the space, how to secure them is going to be, my approach has been to adopt the SANS ICS top five. Honestly, take the SANS five ICS controls. And it's not... There are other security controls within that. Trust me, this special pop 853 has over 500 approach to 800 security controls at very low granular levels, but I don't look at it from a control standpoint, that level. I look at it from a capability standpoint. And that's why the SANS ICS five are the most important because they're building on capabilities. Do you have the capability or have you done these things? It's not about this, it's about this larger thing and what fits under the umbrella.

Arthur Jones (14:43):

Is the SANS an acronym or is it a just the actual name of it?

Roger Caslow (14:47):

It's, it's an acronym, but it's, it's an organization. Yeah.

Ben Stirling (14:51):

So the SANS stop five is SCADA or OT-specific incident response plan. And these are in order, by the way. They're in order of importance of implementation because if you don't have an incident response plan while you're building your defensible architecture and you get hit, what do you do? So, you know, SCADA-specific incident response plan, defensible architecture, uh, network monitoring and visibility, making sure that you have visibility into the network, secure remote access, and then risk-based vulnerability management.

(15:25):

So, you know, in, in, in industrial spaces, you will have an HMI that has a vulnerability on it, but if I have access to that HMI in order to exploit the vulnerability, well, guess what? I already have access to the HMI, so what difference does it make? And this is where Dragos has really adapted the now, next, never approach to patching. And I, and I really agree with this. I think this is a great strategy.

(15:55):

Now, safety's implicated. We, we have to do something because human life safety, operational, you know, the mission is at risk. Next is, hey, this can wait till the next time you're going through an outage or, uh, you know, the, the system's gonna be shut down, whether it's a manufacturing line, generation plant or a water treatment facility. Never is, yeah, it's technically a vulnerability, but dude, if I'm sitting on your HMI, I can change the position of that valve anyway. So what difference does it make? That is a good basis. When you're looking at risk-based, um, uh, to use a Gartner term, exposure management is a key thing here.

Arthur Jones (16:41):

Well, I think you've both given a very strong answer there, but, uh, the last one was going to be actually, um, before wrapping up, asking for one piece of cyber security advice that you'd like to share with infrastructure leaders.

Roger Caslow (16:53):

Yeah, it's simple. It's simple. Pick a plan and stick with the plan, right? Pick a model, whether you do ISO or S- or, or, or NIST or SANS or, there's at least, there's at least, yeah, that's, that's, yeah, there's at least a, a, a half dozen or more models or programs you could align with. Pick one and stick with it. Pick the one that's mo- most... Do some research, understand what these look like, and then understand what your investment will be to align with that model. But pick the model and stick with the model, right?

(17:33):

It's no different than when you're doing risk assessment. You can either do the fair model, which is having the financial space. You can follow the NIST RMF, risk management framework. You could do all these different models. There's a coup- there's at least that many more risk models out there to follow, uh, but again, it's all risk-based. Cyber security by itself is worthless without understanding risk and understanding how to measure the risk, assess the risk, and work through the risk. And be able to articulate that up and out, has to be a communications point with that. So those two things, pick a model, be able to communicate it up and out.

Arthur Jones (18:15):

Ben, from your side?

Ben Stirling (18:18):

Any of them can work. Just depends on how hard you want to beat the square peg into the round hole. That all said, um, start, start now. Like, the biggest problem we have in OT cybersecurity is everybody trying to figure out what model or what thing to do instead of just starting to move that and starting, you know, like Roger said, communicate the risks. Figure out, uh, next steps as far as, okay, um, I, I, I have a bunch of people already peeing into my manufacturing network. We should probably stop that. Ha- ha- you know, figure that out. The SANS top five is a great place to start.

Arthur Jones (19:05):

I'll just say firstly, thank you both, uh, Roger and Ben, what an amazing conversation. I know that I've learned a lot about visibility, digital transformation, you know, risk assessment. Um, and I understand just seeing the relationship between the two of you, I can see why you work so well together. So thank you both. I really appreciate it.