[music]

Paul Thies: If a hacker gets a hold of your credit card information, that's pretty bad. You want to talk about bad, however, try considering if a hacker compromises the operating system of a water treatment facility or an airport or a nuclear power plant. No cyber attacks are good, of course, but some are much worse than others. In the age of the fourth industrial revolution, with increased connectivity and emerging technology, even disconnected network systems can still be confronted with potential cyber risks. When it comes to critical infrastructure like the examples previously mentioned, cyber defenders absolutely have to get it right.

Hello, I'm your host Paul Thies. On this episode of *If/When* I discuss the topic of Operational Technology, or OT, cybersecurity with Adi Karisik, Global Technology Principal OT Cyber at Jacobs. Adi shared his insights on the types of threats that OT cyber defends against., the principles for operating an OT network, the challenges of staying ahead of the bad actors out there and some examples of successful OT cyber projects. Adi, thank you for joining me. Today we're going to talk about operational technology, cyber security and what Jacobs is doing in this regard, what it means and some of the exciting things going on. The first question for you is what are some of the kinds of cybersecurity threats or dangers that OT cyber detects and defends against, and how does OT cybersecurity differentiate from IT?

Adi Karisik: It's a very complex question, all the threats and everything else, but if we look at the changes where they are happening in the world, I would say the IT cybersecurity or the data cybersecurity as we know it went through a renaissance phase in second part of the first decade in 2000s. All of a sudden something that nobody cared about became a big issue and everybody started ramping up and providing IT cybersecurity services, protect my data, I want confidentiality, I want this, I want that, and so forth.

That is happening now with OT, because for years and years and years, for decades, we're building the critical infrastructure pieces without any consideration for potential vulnerabilities on a digital side that can cause all of that to stop working or affect people's lives. In terms of the threats, threats are radical, because we are dealing with critical infrastructure. On an IT cybersecurity side, the threat is somebody's going to read your email or access some sensitive information. On our side, the threat is there won't be power, there won't be potable water in a state.

That creates life-changing environment for people. The nuclear power plant will explode. We've seen all of these escalate over the last 10, 20 years, from the first aggression of Russia on Ukraine in 2014 with the famous attack by NotPetya, OT attack that they did to Ukraine energy system that nobody was prepared to deal with. We saw several attacks towards the Middle East countries that people were targeting their ability to produce oil. This is real, and there are so many bad actors that are trying to hurt both US and individual nation economies by attacking the OT infrastructure.

Now, in terms of the differentiation probably the best way to approach this is on the IT side of cybersecurity we are concerned with privacy, how to protect that integrity of data, that somebody doesn't see what you're writing, your personnel records, your salary information, your medical history, these are all important things. Your

passwords that you use for work. At the same time on the OT side, data is not really relevant. What's relevant are processes and systems that are working. There is no much need for secrecy, because if you drive by a nuclear power plant you can tell if it's working or not working.

You see a smoke coming out of a smoke stack, guess what? It's working. There is no need for somebody to tell you it's being generating power, so we can't protect that. There is no need to hide that. What we protect is who can log in from outside and change parameters on the generator, because explosion of that facility would have horrible consequences for the area that we are in. That is the difference. We are working on protecting equipment, assets and processes, integrity of those versus confidentiality of data that's being collected.

Paul Thies: Okay. You mentioned, the differences between OT cybersecurity and IT cybersecurity. Let's talk about OT and IT networks. How is an OT network different from an IT network in respect of cybersecurity and network performance?

Adi Karisik: The best way to approach there's a beautiful data published by actually United States Department of Defense, and this is not classified. If you look at the data they provided, and DOD is a great point, because they typically don't have as much of a challenge as a local utility to get budget for funding their own security. The difference between the IT and OT that our Department of Defense controls is from 2 million devices that they have in IT on their networks to 1.3 billion devices that they have on their OT networks, to typical corporate procedure in any developed organization is that we change our computers every two or three years.

DOD does the same thing, but on OT side, on average, every 30 years. You would in many cases dealing with an obsolete technology that you have to protect against the contemporary threats of today. Lastly, the networks on IT side are following the same principles no matter what the network is, so if one is to design a network for their home, that network will have all the elements as the professional network. You're going to have connection to your printer, to maybe other computer, maybe some smart devices in your home, and it's going to be following the same as you are in the office.

The usage of that network varies, because today you might be working from home and the office IT network will look different, and tomorrow you are in the office, so that footprint of where the signals go and how the traffic flows will change. On OT side, it is a little bit different. Network is custom designed to follow a particular process. You can have two water treatment plants, but they have different networks because the equipment that they use is different, or the process that they follow to produce water is different, so network has to be built around it.

Then finally, they're always the same, because of the air gap. These networks are traditionally never ever connected to internet. You always going to see the same picture on the network. Always the same devices. There is no, "Oh, I'm going to work from home, so I'm going to log in into the water treatment plants from home and change configuration something," that doesn't work. We are dealing with new versus old. The other good example is, in the same DOD study, the Department of Defense has five operating systems that they have to protect within the network of Department of the Defense.

On OT side, they have to protect 93,000 operating systems, because all of these devices that exist on OT network speak different languages. The programming logic controllers, the human machine interfaces that are there, the very specific design in a particular generation, particular age to operate a particular process. Hopefully that makes sense.

Paul Thies: Let's talk about the principles that go into operating an OT network. Prior to our chat you'd shared with me some of the stories that have made the news involve the Colonial Pipeline, Oldsmar Water Utility in the US and Maroochy Shire in Australia. In those examples, what went wrong there and how were their networks accessed?

Adi Karisik: The principle problem is the human participation, as always. There are two things traditionally in infrastructure world, in a role of operational technology. We segregate the information from operation technology networks. The reason they're segregated is not necessarily just to follow the official guidance, like National Institute of Standards and Technology prescribes that you have to separate these. The point is to minimize risk, because if somebody gets infected by a virus because they opened a bad email, you don't want that to affect your manufacturing process or your weapon control system.

You want to segregate the potential contamination only to one bucket. You don't want IT issues to spread over OT and other way around. If you look at the Colonial pipeline, what happened was basically somebody opened a bad email. Because they were sharing the same network for IT and OT, instead of just users getting infected they infected the control system that was operating the fuel flow for the eastern part of United States. In a case of the Oldsmar facility, which is a water manufacturing plant in Florida, there was actually an attack of the same nature on west coast of the United States just five days before.

The hackers were using the operating procedures of some of these smaller facilities who don't have enough people, and they enabled their people to operate some of these automated processes from home. All they were doing is jumping on that channel that they were using to communicate with the equipment, operating the plant, and they changed the chemical compound mix that was going into the water. If that was not caught they could have created water that would be poisonous for all the people that are drinking it.

The good thing about industrial control systems, though, is typically no matter how good your automation is there is always a set of manual controls that you can revert to in case that the digital side gets compromised. Maroochy Shire is a very interesting one, because I think we're going to see more and more of these as the time progresses. I don't know if you know the whole story, but Maroochy Shire is a giant wastewater treatment plant in Australia. They had the case where they had a temporary employee because somebody was on a very long sick leave. This gentleman in particular was serving in that capacity of operator for some of their OT systems for about nine years. The person who was on medical leave passed away and they opened the job requisition for a permanent placement of this gentleman that was there, and he did not get a job.

They picked somebody else, which can happen in any free economy and market, but when they walked him off the site, they forgot to take cyber security into consideration. They let him keep all the access controls, the logins, the keys for the systems. This turned into a perfect insider threat because it's not a cyber attack if the person is using valid logins and passwords to access the systems where he has been given rights to operate. What he did was criminal. He released 750,000 gallons of untreated sewage into a clean environment. At the same time, this is the type of human behavior that we have to expect in the future because human connection is probably the biggest point of vulnerability.

Paule Thies: When you think about critical infrastructure and you think about large-scale events and public events, there's a lot of collaboration that goes on across various players and vendors and whatnot. Can you speak to those collaborations, and what are some of the positives and maybe some of the negatives there? Are there some case studies? For instance, Jacobs has been involved in that-- You can demonstrate how we successfully navigate that complexity?

Adi Karisik: Absolutely. Let me maybe say this. For Jacobs in particular there are two angles of looking at this. One is within Jacobs. I made graphics that were circulated in a couple of briefs in which I presented what we do as a layered cake. The point of the layered cake was to showcase that each layer of a sponge represents a conventional engineering offering Jacobs has. Then all the frostings that connect those layers are digital services such as OT cybersecurity, that connect this into more valuable, more rich, and more interesting cake to taste. Then you have the fondant that brings the cake together, which is our overall corporate structure and guidance and whatnot. Then the sprinkles that are all over the plate, which are our connection with a variety of necessary technologies from our trusted partners.

We are a large integrator, and as such we cannot come to the market and say, "Hey, we're going to offer you one technology and you don't like it, we can do the work." What we do instead is we team up with the leaders of digital world in the industrial sector. We approach this idea of remaining in a leading position in the world, in terms of the digital development, by integrating the newest technologies and the best technologies out there in a set of comprehensive solutions that each one of our clients can choose and pick which ones to include and how deep to get involved with a variety of technologies.

I'll give you a couple of examples. For example, a very good client of ours is the city of Wilmington. This is also another interesting story because Jacobs doesn't just advise their clients on what to do. We also operate and service operators a variety of infrastructure facilities. In Wilmington, we won a contract to rebuild, refresh technically, and whatnot, the Wilmington wastewater plant, which is one of the largest in the United States. Then we teamed up with some of our partners like Cisco and Microsoft and many others, and we asked them to provide us with the best possible technology so we can integrate that and provide the sample of what the utility of this type for the future should look like.

We did similar project in United Kingdom testing the environment for the European-style utility of the future with many other partners. We're doing some integrations in the Middle East where we have our partners team up. Some of these technologies are just absolutely amazing. The new gateways that enable us to extend the reach of

the conventional networks wirelessly, the new network behavior anomaly detection systems that are our eyes and ears if there is any type of cyber attack on the facility as long as we're controlling it. The analytical pieces, the integration with some of our partners on a data analytic side to tell us the trends and frequencies and predict possible maintenance issues, whether we're utilizing some of our in-house developed tools or some of our partner tools. The objective is to give the best axis of technology to our clients.

Paul Thies: My last question for you is what kinds of technologies are necessary for a successful OT cyber project, and how does an organization stay a step ahead of the bad actors out there?

Adi Karisik: I can answer in reverse format. It's hard to stay step away from the hackers and from the bad actors out there. It's hard for so many things. One of the things that we do is while we talk about a lot of technologies that we do, we never advertise which technology have we used on which site or which combination of technologies. That would potentially give information to the bad actors that they could exploit against us. The second thing is we got to keep researching. We got to keep our relationship with our partners. We got to look at the cross-technology solutions that will enable the clients and operators to get maximum effectiveness in terms of protection.

There is no ultimate protection, per se, that anybody can provide to any client and say, "You buy this box and you are safe." It doesn't work that way. It's a constant relationship. It's the constant upgrading, it's the constant improvement that keeps them safe. Lastly, because we're talking OT, most of these solutions if not all of them have to be completely passive. That's one of the differentiation approach between the IT and OT, because of OTs process network that operates things. I'll give you an engineering example. We were asked, I'm not disclosing the name of the client, but we were doing some checking on a fire suppression system in a tunnel.

If you think of a tunnel and a fire suppression system, what happens typically is if it's an IT network, you ping all the devices they report back and you know what systems are there. On OT network, we can't do that, because one thing that you can do by pinging these devices is cause them to inertly activate. Imagine if we get one of the key tunnels through the United States where hundreds of millions of dollars of daily economy goes through. By pinging these devices we cause them to release the foam and fire suppression systems and stop the traffic in a city like Atlanta or New York or many other places in the United States. That can have horrible consequences.

We have to be what I call a submarine mode, more like a sonar type of thing, eavesdrop to the network traffic. Based on that we have to determine what is really going on and if there is a reason to intervene. That's why we need to keep investing. OT market is very, very large marketwise, very small personnel and talent-wise. We need to invest in building more professionals, more technicians re-skilling and upskilling some of the existing Jacobs employees. We might have one of the biggest OT groups, market-wise, but it's nearly not enough to cover all the global needs that we're currently seeing.

Paul Thies: Wow. That's amazing. Well Adi, thank you so much for sitting down with me and talking about OT cybersecurity today and some of the ramifications and some of the various factors at play and keeping society safe and keeping critical infrastructure functioning. Thanks so much.

Adi Karisik: Thank you.

[music]

[00:20:56] [END OF AUDIO]