Paul: Joining me today is Susan Howard, the director of Federal ICS Cybersecurity at Jacobs, Eric Conway, the technical director of cybersecurity at Jacobs, and Dean Hullings, global defense solutions strategist at Forescout. Thank you all for joining me today. We've got [00:00:30] a great list of questions to go through.

We're going to start with Eric. And this first question is around the differences between informational technology systems and operational technology systems. And so, Eric, what I'd like to ask you is, can you describe some of the

priorities should fall. What are your most critical systems? And having good self-assessment [00:03:30] processes where you're continually assessing your risk.

Second thing we can always apply from IT side of things, is recognize that the human element is critical. It is the leading cause of cyber risk, whether you're talking IT security or OT security. You can't ignore things like basic cyber hygiene.

[00:13:30] But first and foremost, cybersecurity is an ever-evolving technology spectrum. And so I was talking to my mechanical and electrical discipline colleagues the other day, and they said their specs haven't changed in about 10 years.

In cybersecurity, 10 years is a lifetime. We need to find a more efficient way of upgrading these specs [00:14:00] to keep up with technology. That's one thing we've learned in the past couple years, as we've been going through these guide specs that the DOD has written.

Another thing we've learned is that there's no language or process defining

So you have to have a continual approach in assessing. And using tools like Forescout allow you to have that constant body of evidence that proves and demonstrates whether you're secure. And if you're not, where you may have those vulnerabilities.

And a third area that I'll mention that Jacobs is particularly well-suited in, is training workforce development. [00:27:00] All of these require people who have strong qualifications and understanding of network security, computer security, physical security, operational security. And Jacobs works very hard to train and develop the next generation cyber workforce to make sure we have the people that can do these jobs.

Paul:

are going to get impacted. Maybe some local government services that are going to get impacted.

Maybe some inconvenience because a commuter function, be it, those traffic lights or a train, Metro train here in the DC area. Maybe those [00:30:30] are impacted, and it impacts the community, the people themselves. But again, on a military installation, now you're talking about military operations. You're talking about the readiness of the forces being degraded.

Potentially being turned off and going to a red status, because of an impact to something as simple as, again back to Eric's point, someone penetrated a camera [00:31:00] on the corner of an intersection in the middle of the city. And used that access now to get to where they really wanted to get to, moving laterally across the network and causing a much bigger disruption than that specific camera.

So I think the way that we mitigate these impacts is going to rely on technology, right? Talking about the [00:31:30] technology of seeing everything and being able to segment those everythings into different bite-sized pieces that you can then wrap your security of policy around them.

But it's also going to take back to the human capital. It's going to take partnerships. Fighting the cyber fight is not a one group, or even one base type of an effort. It takes a community effort, both on the base [00:32:00] and off the base in the scenario that you brought up.

And collaboration to understand, How do we share information? How do we make sure that the response actions that we're taking in the military installation are not impacting adversely what's happening off-base in the community, and vice versa.

So I think there's a couple pieces here, and I'm really glad that Eric [00:32:30] brought up Jacobs' model of training the future workforce. Because that's going to be critical, having the right people with the right knowledge and the right expertise to be able to work through these diverse environments.

Paul: Interesting. Now you'd mentioned power and water and some of the utilities, of course that military installations increasingly are no longer islands, but they are part of a larger ecosystem. [00:33:00] And so what might new cyber requirements for, say, the commercial power grid, for instance, mean for US military energy systems?

Dean Hullings: Yeah. So it's interesting that Susan brought up earlier the 300-page document that becomes a checklist of, "As long as I do all these checks, I'm secure," right?

Paul: Right.

Dean Hullings: And what I'll bring up [00:33:30] is that there has been recent legislation and recent efforts, I think Eric alluded to them earlier. Specifically efforts coming out of the Department of Energy. Efforts coming out of the Federal Energy

There's lots of checklists. There's lots of security standards that, if they're followed properly, I think you'd find that our clients, our networks, and our critical [00:37:00] infrastructure would be fairly well protected.

There are also organizations, Dean mentioned DHS, Department of Homeland Security. The Cybersecurity Infrastructure and Security Agency, or CISA, puts out a lot of guidance these days that is very useful for organizations looking to secure their networks. Department of Energy's done the same.

It all kind of feels a bit fractured still. [00:37:30] And so there's another element to that. There's other key players. I think that the manufacturers of equipment, in particular operational technology, the Siemens, the Honeywells, those kinds of manufacturers have a role to play in producing controllers and PLCs and SCADA equipment that is more resilient to attack.

The IOT devices that are coming out in large [00:38:00] numbers should be developed in a way that they are secure. So they have a key role to play there. And then, as Dean mentioned, partnerships between companies that specialize in cybersecurity.

Companies like Jacobs, that have a broad reach across the federal government, across the Department of Defense, throughout the intelligence community, as well as the commercial sector. Partnering with companies like [00:38:30] Forescouts and the cloud service providers and network service providers, so that we can implement those security controls in a way that's something beyond just simple checkbox compliance.

I think checkbox compliance, it's recognized now that it's not enough. That we really have to have active security. These policies are different now. We recognize that IOT, IT, [00:39:00] and operational technology, this convergence, it's ubiquitous.

Air-gap solutions are really not viable anymore. We know with the remote workforce that there's an increased need for connectivity. So the policies that are being defined have to recognize that this connectivity is here to stay, and that it does pose an increased risk. And that it has to be addressed in any policy.

We have to recognize that our critical [00:39:30] infrastructure is largely owned and operated by the private sector. So managing this risk, it really becomes a

was CMMC, which I believe stands for cybersecurity maturity model certification.

It made me recall a podcast we had done a while back, where you spoke about [00:40:30] organizational maturity related to cybersecurity. Can you describe what CMMC is, and why it's important for organizations to achieve that certification?

Susan Howard: Yeah, it's great that Eric is emphasizing supply chain, because that's what CMMC is about, supply chain, supply chain, supply chain. And how to ensure that your defense contractors who are the supply chain for DOD are protecting controlled unclassified information.

[00:41:00] Technically speaking, CMMC incorporates DFARS 252.204-7012 and another NIST specification 800-171 for unclassified controlled information. The real goal is to prevent data breaches where the defense contractor is the weakest link in the chain.

And it's really a natural [00:41:30] evolution of digital transformation, where we now realize that all of our sensitive information exists in the digital realm and not on hard copy, where we can just head to a shredder and shred it. So it is part of the digital transformation, the CMMC.

But it's also part of the supply chain, acknowledgement that supply chain is high risk. I think the most recent example in [00:42:00] the past several decades is the Edward Snowden example, where a defense contractor was able to do so much damage. And we want to prevent things like that from happening to the furthest extent possible.

So right now everybody is rushing to the finish line to be ready for CMMC. And right now there is no official accreditation body for CMMC, but there is tons of self-assessment software out there, ranging from a couple hundred [00:42:30] bucks to a couple thousand bucks, that anyone can purchase and do a self-assessment.

A lot of these are happening at the small to medium business range for defense contractors. And then large contractors, like ourselves, and the Northrop Grummans, and the AECOMs, and all the A&E environment, we are preparing daily for CMMC accreditation. And we've done a lot of self-assessments.

The way it's going [00:43:00] to roll out is that there's going to be a five-level certification process. So most people will probably land somewhere in the middle, like a level three, where we can say we have good cyber hygiene.

And towards the end of fiscal year '21, we're told by DOD, all of our contracts, our federal contracts, are going to require CMMC certification. And you're going

to have to say, "Okay, we meet level three or level four or whatever." If you

So it can be done in the enterprise IT, and it will be done more and more. We're pretty excited in the cyber world about that. And I just always tell people to go look at, Have I Been Pwned site. Because a lot of cyber people have meetup groups that do pwning hacks. And so pwning came out of the gaming world, but there's this site called, Have I Been Pwned?

So all [00:47:00] these huge data breaches, if you want to know if you were affected, you can go to this site, it's a well respected site, and you can type in your email address. And it'll tell you if somebody has your credentials because of all these breaches that have occurred. And so those are a thing of the past though, if we roll FIDO and FIDO2 out in a bigger way.

It's already being used at Bank of America and a bunch of other big players. Target adopted it on their website [00:47:30] presence. But it has promising applications for the enterprise as well.

Paul: Interesting. Well, I will have to check to see if I've been pwned. So that is a [crosstalk 00:47:41]

Susan Howard: Yeah, please do.

Paul: Thank you. So Dean, getting out your crystal ball here, looking at the next five to 10 years, where do you see the future of security operation centers and tools like security incident and event manager, intrusion prevention and detection,

But what I think is going to change is the comfort level of automated action. We tend to want to share information between sectors, between verticals, between organizations, between companies. But we don't want each other to affect each other.

We want to have [00:50:00] that human in the loop that says, "I've got to be able to get this information, to analyze this information, to take appropriate actions, to make decisions, informed decisions, and then task my operators to do something about it."

That just took me a couple minutes, and guess what? We got hacked a whole bunch of times just in that conversation right there. So I think the evolution [00:50:30] of SOCs over the next five to 10 years, is going to be really taking the technologies that are either already available, or will continue to evolve and get better and better and better.

But putting trust in those to be able to, based on policies, take automated action so that we can react. We can quarantine. [00:51:00] We can control. We can bring a wrapper around a problem before it spreads all across, for instance, the medical community, like Mirai did, or something along those lines.

And so the SOCs already have in place the command and control for their individual organizations. The SOCs already have in place connectivity [00:51:30] to other SOCs to share information. I think we'll have to evolve into automated action between those SOCs, and amongst those SOCs, to really be able to keep ahead of these cyber risks that we've been talking about today.

Paul: Interesting. And it will be interesting to see how things like artificial intelligence and machine learning are going to be deployed in this automation effort. I imagine that more and more organizations [00:52:00] are going to find, they're going to want to share data sets to help inform the training sets for their AIs.

So there's a certain level of trust that has to go there. And, like you said, you have to mitigate the risks of that interconnectivity that could be an in for bad actors. And so, how are you going to mitigate those risks in between organizations?

Eric, [00:52:30] to wrap us up for today, I've got my last question is really about best practices. And what do you see are some of the best cybersecurity practices organizations, both commercial and governmental, would do well to adapt?

Eric Conway: That's a very good question. And there's lots of guidance out there, and some of it's conflicting guidance. But I think probably the most important [00:53:00] thing is to establish a culture of security in your organization.

Whether you're government, whether you're commercial, you really have to integrate both cyber and physical security into your operational policies, your operational processes. Including your leadership, your daily operations. This is critical to addressing that human element we've talked about in cybersecurity.

And it also has to be integrated into all [00:53:30] of your regular business processes. We've talked about supply chain. You need to know your vendors can be trusted. Not only that, but you need to know that your contracts are with trusted companies. And if you have subcontractors, you have to know that they're also going to come and work with you in this kind of culture of security.

So that's a very human-based best practice that we need to follow. The simple idea that I've mentioned several times, [00:54:00] and I've heard both Dean and everybody talk about, knowing our architecture. Knowing what you have, understanding what your assets are. Having baselines of what assets are in your organization.

And again, periodically assessing and auditing what your organization has, and understanding the impact of change in that organization. If you're going to swap out a system and bring in a new system, [00:54:30] you have to be aware of the security implications of that. So you plan that security into your budgeting. You plan it into your next five years, your future plans.

And it helps to have an established security manager or leader who can help you sustain that direction and that momentum. Making sure you're testing your security often. Making sure that you're keeping up with all [00:55:00] of these procedures and policies that are being put into place.

And one other area that I'd like to mention is making wise investments in your security technology. Last discussion about artificial intelligence is a really good example. There's a lot of tools out there now that claim to have artificial intellige 298.35 Tm0 g0 G[(exam)4(pl)ow(w)10(t)-6(ha)4(t)-5(c)-9(la)4(im)6(t)9u 460b] TJETQ0av

It sounds [00:56:30] like Jacobs and Forescout are doing a lot of great things to help their clients mitigate the risks, and also look around the corner with what might be coming next and anticipate that. So thank you all for joining me, and I really appreciate your insights.