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 differences in cybersecurity between IT systems and OT systems? And what can be learned from the IT world that could be shared with the OT world about securing these environments?

Eric Conway: Okay, thank [00:01:00] you, Paul. Well, one of the biggest difference we see with operational technology, or OT systems, and IT security is based on the fact that operational technology integrates the cyber, the human, and the physical elements of security, unlike IT security.

With traditional IT security, we are usually focused on protecting assets related to the operations of a business or an [00:01:30] organization. We're trying to protect customers' data, or business data, or privacy information, all of which are very important. And in traditional IT security, we usually follow what's sometimes called of the CIA triad, confidentiality, integrity, and availability of the system.

We kind of flip that with OT security. We move to a different prioritization, where availability of an OT system tends to take the priority, [00:02:00] followed by integrity and confidentiality.

And this is partly because availability of an operational technology-based system can really have an impact on human life, especially if there's a breach. You can imagine the availability of water, or the integrity of a safety system in a manufacturing plant or a military base.

Secondly, operational technology systems have not really enjoyed the same level [00:02:30] of technical evolution as the IT world has in the past couple of decades, especially with respect to cybersecurity. Lots of operational technologies are older. They were designed to be autonomous. They were designed to function in a peer-to-peer infrastructure.

They're not designed with typical networking stacks, typical operating system features, and all the interfaces that we have in the IT world. So [00:03:00] the way that you secure these networks can be fundamentally different.

That said, there are a lot of lessons we can apply from IT security. One being, approaching security from a risk-based assessment. Know what your assets are on the network, understand the impacts of a breach, and where your highest

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.

A CyberX study this year found in operational technology systems, [00:04:00] things like outdated operating systems, unencrypted passwords, lack of automated updates. And in a large case, direct connections to the internet were making operational technology very soft targets for cyber-adversarial attacks.

Paul: Hmm. Okay. And then, Dean, turning to you and thinking about distribution systems. As distribution systems like Amazon, [00:04:30] FedEx, and the Defense Logistics Agency become more mechanized and networked, what are the risks there? And how do you secure systems that inherently need to be connected? And what impacts do outages or attacks have on a distribution system?

Dean Hullings: Yeah, those examples, Paul, are really classic OT environments. And just to build on what Eric had mentioned. I like the way he [00:05:00] put that we've flipped the model of how we secure these devices from traditional IT environments.

You look at a production line of Amazon, they're filling orders. There's a lot of sensors that are connected into either a centralized server, or maybe multiple servers. Same thing with a FedEx package shipping plant, with all the sensors [00:05:30] that are looking at where the package is going, maybe taking weights of the package. Maybe some drug sniffing type sensors. Or, in this day and age, bomb material sniffing type sensors.

So all of these sensors now become critical to the operation of what we're talking about. Either Amazon, trying to fill customer orders, or FedEx, trying to move packages to where they need to [00:06:00] get to.

It only takes one of these sensors to get compromised, or to get corrupted, or really, operationally, to say "No," and now you've shut down the entire line, right? The dependency on these is critical to those operations. So anytime the line gets shut down, [00:06:30] now you're impacting the bottom line, and that's money to those organizations.

Defense Logistics Agency, the end state is a little bit different. Because now you could be processing materials, or personnel, or medical records even, that are affecting a unit's readiness. They could be getting ready to go down range to do important operations, and if that logistics process [00:07:00] gets shut down, now they can't get to where they need to be, or they don't have the supplies once they get there.

And then of course there's military operations and individual sailors, soldiers, airmen, Marines lives at risk. So outages are impactful in different ways, but equally important to those organizations.

Paul: As part of that, now how do you secure systems [00:07:30] that need to be connected? What would be some solutions in that way?

Dean Hullings: Yeah, Eric touched on it was, you can't think of them in the same ways that you think of IT devices. They're very often stripped down operating systems, with very minimal memory and compute resources.

You have to treat them differently than you would a desk or a laptop. [00:08:00] In that, trying to interrogate them or doing scans, or something that takes away resources from that device could cause the outage that you're trying to avoid.

So you have to treat them a little bit differently, and take on more passive methods of discovery and analysis of what they're doing. Analysis of how they're communicating with other [00:08:30] devices on the network. And making sure that there are no anomalies there, and if there are anomalies, figure out what's going on without impacting that production line that is involved.

Paul: Gotcha. I gotcha. Now let's turn the discussion a little bit to the US government, and securing industrial control systems there. I'll start with you, Eric. And then Susan, I'm going to bring you in on this, especially with your role at Jacobs [00:09:00] and working with the federal government.

So Eric, just to start us down this path. Can you speak to the importance and strategy of securing industrial control systems in the US government?

Eric Conway: Sure. Thanks, Paul. You know, we have to recognize that our US critical infrastructure is completely owned, and operated, and run on industrial control system technologies. And that a lot of these, in fact the majority of these [00:09:30] systems are not owned by the government. They are owned by private enterprise as well.

So it is very important that the government and industry work together to secure this infrastructure. Our adversaries are very active right now. They're gathering intelligence, they're mapping our critical infrastructure.

They are already showing signs of being capable of disrupting our national critical functions. Everything from water, [00:10:00] power. Imagine the chaos they can cause by disrupting our healthcare system, something like what we're experiencing today with COVID-19.

And we have to recognize in our strategy, the additional risks that we're facing as we continue to connect operational technology to our enterprise IT systems,

and to the greater internet. This is expanding the cyber attack surface. It is increasing security [00:10:30] events that are happening within our critical infrastructure.

This increased access also gives our adversaries increased access to these critical systems. And it also has the effect of reducing the segmentation of our networks. We no longer have these standalone control networks that are physically air-gapped, or separated from the greater internet.

So now these systems [00:11:00] are much more susceptible to things like ransomware and malware attack, that traditionally have really only affected IT security. There's a number of published examples, for example, where water utilities had been taken offline because of ransomware attacks. So we're seeing this across the board.

Part of our strategy also has to focus on our supply chain. Supply chain risk management must be addressed, because the suppliers of all of these controllers [00:11:30] and devices need to make sure that they're developed in a way that is secure.

And finally, I'll mention that there are a lot of compliance standards that are being developed by the federal government, that are being put into place to try to address things like supply chain risk management, and industrial control system security. So that is a critical part of our strategy to secure our ICS-controlled systems.

Paul: Hmm. Yeah. Yeah, and listening to you, it [00:12:00] reminded me of a story I'd read, I think, last year. I think some bad actors had hacked, it was a small construction company in Oregon, and that was the door by which they were then able to, I think, end up compromising half of the US power grid. Which is just kind of amazing.

Susan, we had talked earlier this year on cybersecurity, and had touched [00:12:30] upon, I think, supply chain. And you had mentioned about working with partners, and making sure that you're mindful of the risks that you bring on when you're working with third parties. So I feel like that was very germane to this discussion on supply chains.

But turning to thinking about the Department of Defense in this context of ICS. Are there impediments in the Department [00:13:00] of Defense policy that should be reevaluated to help accelerate progress in cybersecurity defense?

Susan Howard: We were all really grateful in 2016 when the Department of Defense released their first set of criteria to protect industrial control systems. It was long overdue. It was about 10 years in the making. And it came out, and it was very well written. And there's guide specifications that go along with this criteria.

[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 validation and commissioning. So our contractors get out to the site, and they do what they're asked to do, but they don't know when they're done. The Navy has come out with a new commissioning [00:14:30] spec that'll help the cybersecurity practitioners understand this. And the Army and Air Force are soon to follow.

The other thing that is an impediment is what we call control lists. And these are based on NIST 800 series controls. In NIST 882, for industrial control system, there's about 17 control families. Well, Department of Defense has taken that [00:15:00] and turned it into about 300 pages of controls.

If you can imagine, I'm a contractor out on a job site, and I've got a checklist that's 300 pages long. I'm going to perform a box-checking exercise. And this is very not, I guess, conducive to creating a secure environment. We don't want box-checking exercises. We want secure environments when they leave the site.

So this has been realized, and there are [00:15:30] some efforts underway to improve the guide specs, and improve the criteria that was written. It was great when it came out four years ago, and it needs to be a continuous iterative process.

Paul: Okay. And then as a follow-up, a couple of terms that I was introduced to as we were preparing to have this discussion, is 802.1X, [00:16:00] and then Network Access Control. Can you explain what those are, and how are they different? And why is this significant in the industrial control systems environment?

Susan Howard: Yeah. So I'll start first with defining the problem a little bit. And I just talked about how the specs haven't kept up with technology in industrial control system. And so the basic problem here is that we're trying to fit the square peg that is industrial control system into the round hole [00:16:30] that is IT.

802.1X is an IEEE standard. It's been out for a long time, and it works great in the IT enterprise environment, especially for wireless. It's how your iPad, your laptop, your phone can authenticate to a wireless environment, right?

We tried to do 802.1X wired in the IT enterprise for many years. Some have succeeded, but just as many have failed because [00:17:00] of a lot of things. But for industrial control systems, we cannot force 802.1X into that environment, which is how the specifications are written now on the DOD side, at least.

And there's a couple of good reasons for that. There's a few things that 802.1X needs in order to work. One of them is called a supplicant, right? A supplicant is something that the client has that they use to authenticate.

So imagine in the [00:17:30] internet of things, or IOT, a refrigerator. A refrigerator doesn't have a supplicant. So how is it going to authenticate? It can't, via 802.1X. It cannot. Same with a lighting sensor. Or I was just working on electric meters yesterday. They don't have supplicants either.

The other thing is a PKI environment. The industrial control system world doesn't typically connect to a PKI, a public key infrastructure, environment like IT [00:18:00] does. The certificates are not gained by a certificate authority, because a lot of the DOD systems are intentionally not connected to the internet. So this is not the default.

So the certificate, the supplicant, and then a management console is needed to make 802.1X work. Again, your refrigerator isn't connected to a management console. Your electric meter isn't connected to an authentication management console. [00:18:30] So this is why 802.1X just doesn't work in industrial control systems.

Network Access Control is related to 802.1X. But instead of trying to make it a one-size-fits-all, that something that works in IT has to work in ICS, Network Access Control, or ZTMA I guess it's called, zero trust network access.

It's not a one-size- [00:19:00] fits-all solution. You don't have to follow 802.1X. And vendors like Forescout have been very successful in developing solutions that work in water treatment plants, or wastewater, or electric.

We need to call it a day with 802.1X, and stop throwing good money after bad. It's not going to work in industrial control system. Major vendors already realize that. We need to take it out of the specs.

Paul: [00:19:30] Okay. And then, so Dean, Susan had mentioned Forescout, and Forescout's abilities in the industrial control system environment. Can you tell us a little bit about the product strategy of Forescout, and how it's positioned to help organizations with ICS cybersecurity?

Dean Hullings: Yeah, I sure can. And Susan shaped it very, very well. We've got a tremendous amount of [00:20:00] industrial control systems now, and all of the sensors we

talked about earlier, that are being connected now through what were and remain traditionally IT networks.

So, trying to apply the same security rules that we've all grown up with in the IT space to these OT environments, or the industrial control system environments, is just not going to work. And the one that was pointed [00:20:30] out is the .1X requirement. As Susan said, there are devices out there that are connected, that just cannot take a traditional .1X supplicant, an agent on the endpoint to report back to a server for authentication.

So Forescout's approach is to be able to passively and actively, in some cases, [00:21:00] discover and characterize every device that's connecting to the network. And what that does for us then is, we can then segment your networks to put the OT environment devices in an OT environment, and your IT environment devices in an IT environment.

Then you can wrap your security policies around them differently. Same network, same management console, same real [00:21:30] policy sets, but they're applied differently given the different environments that you're trying to protect, and you're trying to secure.

So we're reducing risk across the entire network, across the enterprise. We're reducing costs for administrators, that they're learning one tool that can control these different environments, the security of the different environments.

We're also taking into account the different [00:22:00] tools that are already out there for the management consoles in the different disparate environments. And connecting those together to pull all of that pertinent information into a centralized policy set so you can treat those endpoints differently and accordingly, according to your security policies.

Paul: Mm-hmm (affirmative). Okay. And then, Eric, I want to talk a little bit about smart city [00:22:30] environments, and the internet of things deployments therein.

I was looking, the International Data Corporation has some stats, and one of which that caught my eye said, "By 2023," so just about three years from now, "20% of cybersecurity incidents will stem from smart city IOT device deployments, forcing double-digit increases in cybersecurity software and staff training budgets."

So can you describe for our audience, [00:23:00] some of the more prevalent cyber threats we're seeing that face non-traditional IOT, such as building systems and smart cities. And then what are some of the steps that Jacobs is taking to help clients mitigate those risks?

Eric Conway: Sure, Paul, thank you. So I think the types of cyber threats that we're seeing with non-traditional IOT are largely a result of an increased amount of connectivity of devices on our [00:23:30] networks. An increased amount of data and data flow from those devices into our IT systems and our operational systems.

The kinds of threats we're seeing are similar to what we see in IT security. We're seeing multi-stage attacks from our adversaries. The tactics and techniques and procedures that our adversaries follow are very similar, in that they often start with a very simple [00:24:00] attack.

It may be something that takes advantage of poor user cyber hygiene. An employee in the city who clicks on a link in their email. That link downloads some software to their computer that is able to gain access to that system that can then be used to elevate privilege to gain access into that network. And from there, the adversaries can pivot to other are parts of the network.

Once you're in the network, you tend to be in a trusted zone, [00:24:30] and you can take advantage of that trust. And you can continue to percolate your way through the network. Mapping the network, gaining access to additional resources, and closer and closer and closer to your critical resources. So we're seeing these kinds of attacks already underway, and they all take advantage of the user error, the increase of connectivity, outdated infrastructure.

What kinds of things [00:25:00] are we doing? Well, what Jacobs is doing is we are partnering with companies like Forescout that bring products to the market that can do intelligent asset management. Anomaly detection.

We can use these tools to build managed security services that integrate security functions. They allow us to analyze network traffic. They allow us implement things like user and endpoint level protection and [00:25:30] anomaly detection.

Another area that Jacobs is working is helping customers and clients implement zero trust solutions. When I mentioned that kind of common tactic of getting into a network, excuse me, and then pivoting into other sections of the network, taking advantage of the trust models. The zero trust solution, or the zero trust architecture, disables that by essentially wrapping all [00:26:00] of your critical assets in a zero trust paradigm, where you have to constantly authentic with your system before you can gain access to any critical piece of data or system or software.

We're also finding constant assessment is a very, very strong way of mitigating risk. It's not enough to just institute a bunch of security controls, but you have to continually assess [00:26:30] your security posture. Things change. Adversaries' techniques change. Systems become outdated.

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: Excellent. Excellent. Yeah, I think human talent is going to be key, both in how we address it, but then also [00:27:30] raising awareness. Social engineering and just greater cyber hygiene, as you've been saying, among an organization.

Dean, kind of pivoting a little bit on this. We're talking about smart cities, we're talking about an environment that's rich with devices that are trading all kinds of information, sensors and whatnot. We're talking about attacks, and [00:28:00] the attacks in the city environment, but what about military installations? Particularly that might be embedded or networked into these communities. How is the impact different there for military installations compared to, say, a civilian community?

Dean Hullings: Yeah. Absolutely. Thanks, Paul. I mean, smart cities are the way the future, right? Just think about that for a second. Can you picture in a city, [00:28:30] every single traffic light turning red at the same time, or every single traffic light turning green at the same time? I mean, it's astounding to me.

So, what Eric had talked about, with getting people trained and understanding the impacts and the details of all of this, is going to be critical. And I start out that way, because our bases are not standalone bases anymore.

[00:29:00] Maybe back when I started in the Air Force in the... Well, a while ago. Maybe we had a whole lot more standalone capabilities on our bases. But today the DOD installations are becoming more and more integrated into the communities around them. They get power generation, power distribution, water. The fuel tank farms [00:29:30] that house the fuel for the vehicles or the aircraft on a flight line. These are traditionally off-base.

So getting the pipelines to feed the fuel, and the sensors that monitor the fuel pressure on those lines. Or that power that we were talking about, the distribution to get power onto the base. All of that's dependent on what is happening in the environment around them, in the community around them.

And so, [00:30:00] again, back to what we talked about earlier, the difference is, when you're talking about the community, yes, there's a lot of businesses that

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 Regulation Commission.

And what we're seeing is a lack of trust that the guidelines that are coming out are really being [00:34:00] followed to what they need to be, to raise the tide, so to speak, of all cybersecurity across this tremendous connected environment that we all find ourselves in today.

So whether it's the Department of Homeland Security, or the Department of Energy putting out guidelines that say, "You shall follow NIST principles, 800 series principles." [00:34:30] 82, that Susan brought up, or basic IT principles, 800-171, to secure your networks. But then that follow-on activity to ensure that those are being followed on a continuous process, to Eric's point.

And then the curiosity, from my standpoint is, it hasn't been really clearly defined how these new regulations and these new guidelines and these [00:35:00] new directives that are coming out for the energy world, how are they going to get applied to yet another thing on that 300-page checklist that our DOD designers and operators are going to have to pay attention to?

And that's not really clear to us yet. And certainly something that we're going to be watching very closely. Really, probably with partners [00:35:30] like Jacobs, to see how we can help make a positive impact on those DOD users.

Paul: Well, and on that point about how the requirements are changing and evolving, Eric, I've got to assume that the government cybersecurity policy is continuously evolving, or trying to anyway, to stay current with changes in cyber threats. The bad guys aren't resting, and so the good guys can't rest either.

Who are the key players [00:36:00] in this evolution? And what are the key attributes that make the new cybersecurity policies different than from the past?

Eric Conway: Yeah, I think Dean really did hit on a lot of the key players, and Susan mentioned some of the NIST standards as well. So from the government point of view, some of the key players would be the National Institute of Standard and Technology, which [inaudible 00:36:27] NIST, and a series of controls [00:36:30] called the NIST 800 series.

These are security controls that are defined for federal systems, for organizations, as well as for contractors and supply chain contractors that provide services to the federal government. There's a wealth of material out there.

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 shared responsibility between the industry and the government.

And we have to recognize that our supply chain is a critical component to any way of securing our systems. We have to implement supply chain risk management policies into our security planning for our national infrastructure.

Paul: [00:40:00] Okay. And, Susan, turning back to you. We've talked about supply chain and about partners. And a term that had been introduced to me recently

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 can't do that, your [00:43:30] days as a defense contractor are numbered.

So of course there's a lot of money on the line here. Which is a good thing, because this forces accountability on the supply chain. And so it's a very good and natural evolution of the cybersecurity digital and digital transformation.

Paul: Hmm, excellent. Excellent. And then, yeah, I had come across something from the FIDO, or FIDO [00:44:00] Alliance. It said that passwords are the root of over 80% of data breaches.

Now I understand there's some work being done to transform the processing and handling of passwords and authentication. Can you tell us what is the horizon in terms of password authentication that may impact risk mitigation, user experience, and how organizations handle passwords?

Susan Howard: Yeah, so right now the FIDO and FIDO2 standards, they [00:44:30] apply to primarily internet web access. But there's some promising use cases to bring these into the enterprise IT world, and maybe even the industrial control system world, for some HMIs and historians and things like that.

But once again, this is a natural evolutionary step in digital transformation, because passwords are definitely a thing of the past. They're so '90s now.

[00:45:00] They're clumsy. They're hard to remember. People put them on yellow stickies and put them on their screens. There are lots of password vaults that can be downloaded, but the human error, the human factor, is the problem with passwords.

So the FIDO Alliance got together, probably about eight years ago or so, to come up with a solution so that they could use something called public key cryptography, what's been around since the '70s [00:45:30] really, but use it in a different way. So that now when Experian or Adobe or EVI, when they get breached, they don't have my credentials anymore.

When I managed a campus university once, somebody stole the password file out of the /etc/ directory in our Linux... This was a long time ago. But we don't want that to happen anymore. We don't want your stuff, your credentials, to be onsite at Experian [00:46:00] or Yahoo. We want you to hold your authentication, right?

And that's what FIDO allows us to do. The private key you own, and it stays on your device. It stays with your device. The biggest use case, I think, that everybody knows about is, when Google started using these things called YubiKeys, which is a FIDO technology. And around 2009, all of the Google employees were using these keys to help [00:46:30] mitigate the risk for passwords.

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, [00:48:00] where do you see all that going?

Dean Hullings: Yeah. Wow, five to 10 years is an awful long time in cyber. Somebody mentioned it earlier, 10 years is a lifetime. Five years is at least a couple generations, right?

I had the opportunity to be on some NSTAC subcommittees. NSTAC is the National Security Telecommunications Advisory Committee to the administration. And [00:48:30] we were tasked to look at a couple different areas of cyber and cybersecurity in the public sector, for the public good.

And one of the key things, the key ingredients for improvement that always came up, was the sharing of information between organizations. [00:49:00] Sharing not only the threats, but sharing potential solutions before a problem even happens. So really raising the level of security across the overall environment.

And I think that our SOCs today are really the key areas that are making that happen, right? Sharing the information, sharing intelligence, sharing solutions. What I think is going to change... [00:49:30] And five years, if we don't have this right in five years, it could be a very significant impact to us.

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 intelligence in [inaudible 00:55:23], and they often do. However, we've seen also in DARPA, for example, that artificial [00:55:30] intelligence can be spoofed. It can be tricked. Adversarial artificial intelligence is a real tactic.

We need to make sure that we're investing in technologies, and we're also doing the research to make sure that these products that are based on advanced technology, whether it's artificial intelligence or automation, they have to be resilient. They can't be easily spoofed or easily attacked, because then that just makes us more [00:56:00] insecure or more vulnerable to attacks. So those are some of the best practices that I think we can follow.

Paul: Excellent. Excellent advice. Well, Susan, Dean, and Eric, I appreciate all of you for joining me today to talk about cybersecurity. It's a lot to consider, both in the information technology sector as well as operational technology sector. So both software and physical.

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.