ICSI - Will and Craig P1

Will: [00:00:00] Hey, how do you make your money? Tell me about your business." And then eventually they're like, "Oh, yeah, these Rockwell devices, these Siemens devices, these PLCs, we have all this stuff down here. It cranks out widgets." And then I'd just say, "Okay. What are you doing to protect that?"

Will: I guarantee you, whoever that ops person is knows how many dollars and cents they lose every minute that machine's not running.

Intro/Outro: Welcome to the Industrial Cybersecurity Insider. In each episode, we dive into the world of industrial cybersecurity. Join us as we cover the latest trends, innovations, and practical insights as we talk with leaders and practitioners across the industry. Gear up and let's get into this week's episode.

Craig: Hi, I'm Craig Duckworth, and today with me I have Will Kl- Klusoffsky. There you go. Did I pronounce it correct? Nailed it. [00:01:00] Perfect. So Will, why don't you give us a quick overview of yourself, a little bit of background, and kind of what you do and why you decided to come on the show today?

Will: Yeah, sure.

Will: so 26 years in cybersecurity I've been doing this. Most of that time I've spent in consulting and managed security services, and .. spent most of my life sort of, in that advisory side of the world, helping CISOs and CEOs, build security programs, manage their cybersecurity, help them solve their challenges.

Will: and. for a stint I actually, launched and created an OT and IoT security practice, so I got very familiar with the manufacturing space. and the company I work for now, VLogix, we actually have a priority for manufacturers. and, for... I- I'm gonna get a- ahead of myself, but, asset visibility, and exposure management being so important to everybody, but also specifically for the manufacturing industry.

Will: So yeah, I was excited to come on and be able to talk a little bit about things from sort of the CISO point of view, as well as maybe some of the Shopfloor point of view. [00:02:00]

Craig: Yeah, no, I really appreciate that. as we're, we're trying to bring awareness. We're trying to help organizations that are beginning to understand

and beginning to go down this path of, you, you hit on one of the key tenets of visibility.

Craig: You... It's hard to protect and secure what you don't know if you have it or not, So why don't... let's just dive right in with visibility. let's talk a little bit about that and why that's so important on, especially for manufacturers that normally don't have the IT tools and IT technologies that can go out and just give you full visibility to everything.

Craig: It's the maybe some of the differences that we see.

Will: yeah, absolutely. And, God, the differences. That's... When I was first selling, solving the problem of OT security, I remember when we started doing OT security at the old firm The reason I built the practice was because people were like, "Hey, we're gonna deploy this technology on the shop floor, and it monitors the [00:03:00] network."

Will: And I'm like, "Man, I, I have manufacturing clients who don't do that on their enterprise side of the house, and you're telling me they're gonna buy stuff and put it on the shop floor where we're not allowed to do pen testing or patching updates? And you're gonna plug things into the network?" but it, it's interesting because it ca- it's all kind of spawned from the idea of asset visibility.

Will: most of the technology today the reason they're able to see everything is 'cause they grew up in that world. Because on that shop floor, if a machine's not working, you're losing money, right? And so it's just a matter of taking that and translating that risk now, or translating that now to, well, it's not just about why, that machine's not off and now we can see it.

Will: but now, well, something's happened. There's been a breach or there's been an incident or s- something has caused,something looks fishy and potentially could be a like, "Let's get in front of it." Which is something, the I- traditional IT cybersecurity side of the house has had for quite a long time, right?

Will: from back in the days where it was just antivirus and everybody kind of is well aware of I've got these [00:04:00] computers and these servers, and I need to protect them. I've got email coming in. But they don't think about the fact they're like, "Oh, my shop floor is air gapped," which you and I both know is never true, right?

Will: Because somebody installed a Windows NT server and plugged it directly to your Comcast line, 20 years ago, and it's still there.

Craig: and I would say part of the... And I don't know that it's necessarily a disconnect, but part of the, let's call it afterthought, probably a better terminology, is getting organizations, executive leadership, CISO, the risk team to understand that from a manufacturing perspective, it's almost a, it's almost a shift in terminology.

Craig: from an IT side, if you do a patch or you do something and you update a server or machine and things don't come back up in the amount of time that you think, okay, so somebody goes to the break room, they grab a cup of coffee, they have a conversation at the water cooler with their [00:05:00] colleague and come back in half an hour and everything's fine.

Craig: But on the shop floor or on the industrial side, it equates to dollars and cents. When you're producing goods, that's a different risk to the organization, and I think that sometimes is lost in that translation.

Will: Yeah. Well, it's funny you mention that, lost in translation, 'cause when I first started doing this,

Will: Because sometimes, first off, they may not even have a CISO, right? You're talking to the COO or the shop floor ops, director, manager, whatever that is, and maybe there's an IT networking guy who doesn't know anything about what's going on over there, right? So, getting... First off, sometimes it's just getting all those people in the room to understand what's going on.

Will: But the easiest way to reframe it was basically saying, "Hey, how do you make your money? Tell me about your business." And then eventually they're like, "Oh, yeah, these Rockwell devices, these Siemens devices, these PLCs, we have all this stuff down here. It [00:06:00] cranks out widgets." And then I'd just say, "Okay. What are you doing to protect that?"

Will: I guarantee you, whoever that ops person is knows how many dollars and cents they lose every minute that machine's not running. So then it was just a matter of going, "Okay, you know when that thing goes down, you're losing money. Now equate that to a cyber risk that could cause that to go down, not an operational thing.

Will: Or even worse, somebody deciding to, turn off pressure sensors and start blowing things up. sending bolts flying, as I like to say. it's a safety issue, right? which at that point it's basically terrorism, but...

Craig: Yeah. and back to that, the dollars and cents,

Craig: It's, conceptually it seems easy, and I'm sure that mathematically it's a formula. But when you look at, the cost of what is that goods that you're producing, where are you in that, work and process flow and what is that cost of that particular product line [00:07:00] or the entire manufacturing site, forbid that goes down, and really truly say, "Okay, what is my mean time to recovery?

Craig: What is... How long is it gonna take me to do backups, restore, bring it back up safely and calculate a true risk number so that an organization understands the value?" And then you can say, "Okay, my downtime for a day," or let's say eight hours, it's probably more realistic. "My downtime for eight hours is a million dollars," pick a number.

Craig: "And it's gonna take, 200,000 to remediate, to clean up, to address that in a, on a yearly annual number," whatever. So again, it's an easy financial decision when you truly look at it from the big picture and the, and true total cost of ownership.

Will: A- and I... That's the right way to frame it, and I think that's the challenge a lot of people- both [00:08:00] those in the cybersecurity space and those in the manufacturing field, like we, we have, we miss, a lot of people miss that translation layer, which is a lot about me personally.

Will: What I try to help everybody learn is just what you said, like it's very easy to mathematically figure that out. It's much... And it makes much more sense instead of saying, "You need to be scared 'cause you can go out of business," right? But, and we can look at, JLR recently, and they'll probably never say it publicly, but they were probably very close to, a massive company who could not recover in a quick, in a short time, in a short amount of time.

Will: Had to take money from the government. I, from the outsider's perspective, it seems like there weren't backups in place. It seems like they didn't have a recovery plan for that kind of stuff. so thinking about operationalizing that and then quantifying, 'cause like you j- the example you just said, that's $1.2 million in losses that could happen potentially.

Will: Now, me as a risk professional, I can go in and say, "Well, okay." I can look at the [00:09:00] environment and figure out where all the, where all the threat paths are, what the potential exposure is to it, and say, "All right, these are the things that could potentially happen that could take that system down and make you lose that $1.2 million."

Will: Now, what do we do to reduce the likelihood of that? Okay, well, let's put in some asset management visibility, let's put in some exposure management, and it's gonna cost you half a million dollars a year. I'm picking a number, right? Well, okay. And then that's gonna bring that thing down to very minuscule.

Will: Now you can ba- balance out. Now the company has to decide, what's my risk appetite, right? Am I... Do I wanna spend that half a million or do I wanna risk that 1.2 may never happen, right? Based on what happens. that's where being able to frame that in the right context to the board, the business leaders, the, the executives running the company, and not just, the beep-beep-one-zeros kind of stuff.

Craig: Well, yeah. it's a back to a true risk practitioner and understanding the methodology, being able to [00:10:00] extrapolate the data and make a educated business case that's presented to the executive sponsors that are, that ultimately own that risk. as a consultant, we make recommendations all the time.

Craig: We don't own that risk. We can guide, we can support, we can make recommendations, we can provide the continuous monitoring to show is there something in my environment? We can provide the remediation path to harden that environment, to mitigate some of that response. But again, at the end of the day, the business executives own the risk and are ultimately responsible for the decision of do we run the risk and put that 1.2 million out there and hope nothing happens, or do we play it a little safer and say, "Okay, we're gonna spend $500,000 and we're gonna mitigate that, and we're not gonna have a one-time episode."

Craig: Because [00:11:00] now our percent likelihood, as you mentioned, is 5% and not 75%. It's a big difference.

Will: the risk decision is on the business, like you said. And I think that's so important for business owners, business leadership board, and the CISO, CIOs, the technology people, because so often that gets confused.

Will: As somebody who's done a lot of work around asset management and visibility, it's well, okay, do you have all your assets mapped out? Do you have

owners assigned? "Well, yeah, IT owns everything." No. They do not. No. The people who do the... HR owns HRIS. the person who owns the shop floor owns that equipment because as a sec- and the board needs to understand as much as the CISO does because, like you said, it's our job as risk professionals to come in and say, "This is what could happen.

Will: This is the potential impact. Here are three options that you can do. do nothing, transfer, spend this and reduce it a little bit or reduce it a lot." [00:12:00] "Hey, Mr. and Mrs. Businessperson, what do you want to do?" Because that's not the CISO's job, that's not the CIO's job to make that decision. Our job is to l- present you with the options, basically.

Craig: Yeah, and I... you touched on it just a minute ago. fear, uncertainty and doubt is definitely, I would say, a very poor selling decision on any vendor's part. Everybody turns on the news and there's 15 things that are happening. we talked about JLR. It- it's all over the place, and we see it, but I think that we as a society are becoming numb to that, and I don't believe it's effective and I think it degrades versus going in, presenting the facts, looking at it and saying, "Here are the options.

Craig: Here are some scenarios," and really helping educate and bring the value to them to really take a look and make that decision. part of it is that [00:13:00] res- roles and responsibilities. So you look at uptime or the inverse of unscheduled, unplanned downtime, and from an operations standpoint, the goal is maximize uptime, OEE.

Craig: How do I get the most efficient time from the machinery that I have and the technology I have to produce my widgets? And h- and hedging that bet to kind of figure that out.

Will: Yeah, I... Yeah. The idea... It- that's the idea now. it's, is... I was talking to somebody else about this, about, I like to say cybersecurity risk is not, it's business risk, right?

Will: there's probably very few companies today who are doing business without technology, right? And the fact that everything operates on that technology, it holds your business up, means that anything that could impact that technology can impact your business, your ability to make revenue, just like you said.

Will: So it [00:14:00] doesn't matter what you're doing. that's a conversation that needs to be had around, how do we mitigate that? How do we manage that?

How do we... And to your point on uptime, that's the framing for the technical leaders or the technical contributors who are trying to do their job better and get funding from the boards and the business owners who are trying to maximize profits, right?

Will: You have to bring in and like you said, hedge those bets. Figure out where the ri- And that's where, this is a little off-topic, but not necessarily. like I talk about programmatic cybersecurity all the time. You can't just- You can't just be like, "Well, okay, we're gonna, we're gonna monitor our shop floor.

Will: Cool, we're done," right? There's so much more that has to be done because you've got vulnerability management, business continuity, disaster recovery, identity and governance, and now you've got AI and all of this stuff that exists, has to be managed continually, right? It's not a one and done thing, and you have to build a program behind it.

Will: And a program [00:15:00] requires people and processes as much as techno- more than technology, I would say.

Craig: Yeah. and you look at a couple factors within that, that really kinda stand out to me is, and we've talked about this on other shows, is, vendors, OEMs bringing remote access tools.

Craig: We go and we'll see a Cradlepoint cellular modem. that's one concern is, how do you limit or, I guess more appropriately, regulate the remote access into the environment to ensure that it is a secure method? The other thing that I would mention is back to the first thing I said was the ownership, and you touched on it earlier.

Craig: If I own the assets, the PLCs, the control network, and you as a CISO are coming to me and saying, "Hey, Craig, I need you to take down your Windows servers to patch this [00:16:00] and bring this back up. And because we are tracking some security stuff or whatever." But I don't report to you. My metrics aren't tied to you.

Craig: My bonus is based on uptime, and you're saying, "Take down the plant." So I'm really in a conflicting state. So those are things that really play into that. how do you think that overall those two pieces of... and they're kind of different, but they're tied together because remote access into the environment poses a very large risk, and so does ownership of the assets being directly impacted by someone that doesn't have a vested interest in that.

Craig: Talk about that a little bit.

Will: I, I, so I love the,So o- on the remote access one, 'cause I think there's... Going back to programmatic security, because- Like manufacturing has a lot of ISO compliance around how things operate, but they're not necessarily doing the [00:17:00] cybersecurity compliance like the ISO 27001 or the NIST framework.

Will: They're not doing PCI on the shop floor. any cybersecurity framework will have requirements for how that secure access is controlled and how multi-factor has to be done for au- authentication. And going back to identities and AI having access as w- as much as humans and non-human, like non-human identity is a thing now.

Will: So that includes all your IoT. They have some type of identity. So there are controls and methods that, that should be, adhered to there. The CISO topic though I like a lot better, or even more is because I... And I wish I remember, I was consulting a long time ago and I met a CISO and he said, "Do you know what CISO stands for?"

Will: And I was like, "Yeah, of course I do, but go ahead, tell me. What's the joke?" And he said, "It's chief inside selling officer." he says, "I spend my days going around to the other business units and telling them what we're doing and why it's helpful for them, why it's valuable, because you have to get them on board."

Will: And it's something I talk about in, in [00:18:00] a- in all my talks where I've done about how to build a program in podcast, like constantly. You, the, you have to get buy-in before you get a budget and a roadmap. And so going back and ta- the, yeah, it's absolutely competing returns and that's where it comes down to, okay, you, we need to patch this Windows server that's on the shop floor.

Will: It's your decision, shop floor boss, not mine, but here's the risks and know what you're accepting. And I think that's the mistake a lot of, technical professionals make is they say, "Well, we need to do this because it's the right thing to do." It, when the right thing to do is to say, "Okay, here's the risk.

Will: This is what could happen if everything goes wrong, and you're making the decision. You're signing the dotted line because if that blows up and it does go down, I don't want the board pointing at me." They're gonna point at you.

Craig: I would say it, it really should be looked at a little differently, and I'm not disagreeing [00:19:00] what you're saying, but I think it should be framed differently.

Craig: Because ultimately the executive team, they own the risk. they own... The shop- manager. He doesn't own the risk. he has say in what happens on the shop floor, but so really the exec team- It's a matter of

Will: that decision.

Craig: Like you said, that's where the ownership comes in ... the executive team should say, "Hey, we feel it's important.

Craig: We are going to communicate that decision down to the plant floor, and we are not going to hold against you production requirements or metrics while this machine is down so that I don't, and my entire team don't feel that they're being penalized to do something that is counterproductive of what they're doing."

Craig: And that's why I use the get out of jail free card. I'll take this down when my boss says, "Hey, Craig, here's a get out of jail free card. You still get your full bonus for not making your production because I'm asking you to take this offline and [00:20:00] perform this security function." So I think it, that's more the approach.

Craig: I think it's better received. It, at the end of the day, it gets the same result, but it's gotta come from a different n-

Will: I love that angle because what it harps on something else that I constantly harp on, which is understanding the mission of the business and making sure that all flows down.

Will: And I've seen that situation play out in k- differently, like in the consulting world where you get asked to go and work on this other project, and you're like, "Well, my bonus is tied to me doing these things, not that thing." So, or, or my boss, our company mission is X amount of profitability, utilization, whatever that may be, and I'm gonna go over here and work on non-utilized stuff that's not impact- Like, how...

Will: and I think to your point, it's about, well, how are we gonna rationalize that, and is everybody on board with it? And that is definitely the, yeah, I was

probably coming at it from a little [00:21:00] more lower level than that. But I believe that everybody should go to work knowing what they're supposed to do.

Craig: For... Yeah, for sure. And at the end of the day, the right thing is as a business to make that decision, accept that risk. But again, if the CISO says, "I need you to do this," he's that ain't gonna work for me," versus a different approach. But yeah, I like that methodology.

Will: And that's probably happening today, for the firms that have CISOs and for the ones that don't.

Will: I know some large manufacturing clients, prospects I've talked to that, still just have, an IT manager, right? and then a small team who's struggling to, to get that thing done, right? To get that stuff done. So them kinda going back to the business and being able to frame that so that they can say, "Hey, this is the situation we're in.

Will: Here's the problems that we have, and here's what it means to the business." Not, "We have X amount of critical CVEs, and we have,all of this stuff that needs to be pa-", but "Hey, this is [00:22:00] potential impact to the business. Here's the outcomes that we need to have mitigated. what do you wanna do about it?"

Will: Right?

Craig: Well, it's a collaborative conversation. both sides should sit down and rationally say, "Okay, here are the points that are important to me. here's where I'm really struggling with your ask," or, "Here's what, I'm needing help with." And it comes from both sides.

Craig: you look at, we see more downtime from internal mistakes and errors that are not malicious and not intended to do harm than we do from true adversaries. And that, I think that the industry as a whole would agree with that. But how do you, I guess, better support that and remediate that piece as well?

Craig: 'Cause it should be taken into the account as you look at that.

Will: Yeah. Two things on that. One, and this is, documented, like IBM [00:23:00] data breach co- cost of data breach analysis report, whatever. I think it's somewhere in the 50% range of all breaches, are basically a result of misconfigurations or human error, right?

Will: So it is not just, just not just the one industry. Most of the time somebody just made a mistake, right? and I think to your point, like that's, like getting on that same page and having everybody understand what is it we're trying to achieve here? How do we come together and talk, be adults in the room and figure this out?

Will: The other thing is,and manufacturing has figured this out actually a long time before us, because very much so don't wanna patch the systems, don't wanna take them down. Okay. Well- What can we do then? Or how critical is this vulnerability? I have a story I like to tell. I have a CISO friend of mine I talked to who told me he had, 600 critical and high vulnerabilities in his environment, had a team test them all, found out none of them were actually exploitable because of the way they're...

Will: So it's all about context, it's all about visibility, and in today's [00:24:00] world where AI and the criminals are gonna use it as soon as it comes out, in fa- we can't adopt it as fast as they can. So we as defenders are always on the back, on the, on our heels. So the only way to prioritize what you fix is to actually understand what would really be exploitable, which means attack path mapping, exposure management, being able to see, okay, sure, this is a critical vulnerability, but it only exists in this one version of the OS, and it has to be on a data file of this type and a person with this kind of access.

Will: That's, .001 likely. We can put that off. Or we can put in, a, some... This piece of technology or this rule's gonna mitigate that down, right? Compensating controls. context. Use context to make decisions.

Craig: And I would take it one step further and I would say, okay, now add in where does that vulnerability sit within your process, and what does it affect?

Craig: If it's over in the corner running some internal thing that means nothing to your [00:25:00] production and has no harm to stop production, I'd say if it's got a vulnerability of a 10, who cares? If I've got a vulnerability of a four or five on a critical key asset that's managing production, that's where I want to spend my money.

Craig: That's where I want to focus first about how to do it, And again, what matters the most to the organization? Helping them understand that, helping them determine that, sitting down, having that collaborative conversation about breaking down silos and what's best for the business, and how do we collectively move forward to protect the business, not the shop floor, not the whatever.

Craig: So, I think that's a great start. I know that we're probably gonna need to continue this conversation as... 'cause I'll be honest with you, Will, this could be a six-hour conversation. [00:26:00] So I think that we should do a part two. I think we should have the same thing and continue the conversation to get more in depth so that we can really expand and explore some of the topics and go deeper in it.

Craig: What do you think?

Will: I love it because you just hit on business impact analysis, which is my other bugaboo.

Craig: Beautiful. I love it. . Thank you so much for coming on. I appreciate it. And then we'll schedule let's call it part two, and then we'll go into business impact analysis and determine what kind of the next path is.

Will: Appreciate it. Great time, Craig. Thank you.

Intro/Outro: Yep. Have a

Will: great day.

Intro/Outro: Thanks for tuning in to the Industrial Cybersecurity Insider. To stay up to date with our latest episodes, be sure to click the follow or subscribe button now. And if you found this podcast helpful or have a topic you'd like us to discuss, please leave us a review or let us know.

Intro/Outro: Thanks again for listening. See you next [00:27:00] time.