(0:00 - 2:50)
I want to put you in a, not in a box, I'm going to trap you here. I like boxes. Can my box be round and not square? No, because we're talking a lot about, we're talking about security investment, changing environments and constantly, you know, we, you and I both know what it takes to, you know, be on the defensive.

And it makes black and white sense sometimes that this costs this much and this costs that much. What do you do when the budget is not there? So, great, great question. And you're right.

That's not always as black and white as it might sound.

We are the Keyboard Samurai, a podcast about the business of cyber and tech, here to help you or your business improve. Here's your host, Will Kluge.

Let's hack into it now. Hey, everybody, welcome back. I'm excited today.

We're going to do a part two, something Craig and I had started earlier and keep digging into it. But before we get to the second part of our conversation, Craig, give us the 30 seconds of who you are and why we care. Yeah, no, thanks for having me, Will.

I appreciate it. So, Craig Duckworth, I'm one of the directors here at Barry Waymore Design Group. We do industrial cybersecurity.

We are a full systems integrator, a Rockwell Platinum partner, an inductive automation premier partner for ignition SCADA systems. We are a full AEC firm. For those that don't know, it's architect, engineer, construct.

We can build an entire building from start to stop and turn it over as a completed product. And I focus on industrial cybersecurity within the firm and risk mitigation and risk management.

So for clients that are starting the conversation, that are trying to go down the road of how do I begin securing and protecting my industrial assets? I know on the first episode, we talked a lot about visibility.

How do they begin that journey?

And our task of meeting them where they are in the journey, not assuming anything, but really understanding, doing a risk analysis or gap analysis and saying, okay, here's where you are. And then help guide them to where do they want to get to and what does the journey look like? That's a 30 second elevator pitch. No, I love it.

It's very consultative. It's the same world that I live from a cybersecurity standpoint. And I appreciate it because I don't like the people, firms, whatever that come in and be like, nope, you have to start from where we say, and we're going to take you on our journey.

(2:50 - 5:21)

I very much want to know where you're at and let's meet you and let's just make things better from where you're at. So kind of recap, we chatted a lot about, like you said, asset visibility, having conversations, bridging the gap between the technology team and the operational team and the executive specifically, whether that's a CISO or CIO, or even just the IT person, as well as talking to boards and the business units. And we got into needing to have context, needing to understand where your assets are, having some kind of framework and program built around that.

And then you mentioned, how do you figure out where to spend your money? How do you know that, okay, this is a critical asset or not? So tell us a little bit about that. So yeah, no, great starting point. And part of it goes back to, like a business impact analysis, for example.

What is the impact of an event to an organization? What is the risk appetite, the risk tolerance for that organization? And how do they view risk? Are they risk adverse? Or is their model risk transfers? We're buying cyber insurance for everything and we're doing nothing. It's not always the best answer, but that's some people's approach and that's okay, as long as they realize where they are. So again, you go in and you do an analysis and assessment of that environment and really trying to understand the critical paths from a process, technology and people of how that impacts the organization.

What do they need to focus on to begin hardening their environment? Can they put in mitigating controls or they have something already there? What is their internal controls look like to gauge and understand those processes as they're evaluating it? And really, like I said in the beginning, meet the client where they are, understanding where they are and where they need to get to is critical in that process. There is no such thing as one size fits all when you talk about control environments and manufacturing. And I think that you would agree with that.

(5:21 - 9:41)
Yeah. Where to get to where you want to be. And I think it's important for anybody listening, watching, it's like, that's not just you as a consultant, me as a consultant.

You're the IT cybersecurity people and you need to get the business that you work for. You need them to understand the position you're at and have a plan. How are you getting them to those next stages? Yeah.

We hear a lot. Look, the shop floor stays the same as much as it changes, right? I know. But I know there's been devices that are probably sitting there for, I won't say hundreds of years, but it seems like it, right? And then new stuff is getting chomped onto it at the same time.

How do you manage that ball of complexity?

Great, great question. It's not easy, but with the right approach. So in the manufacturing space, time, the life expectancy, if you want to call it, of assets is measured in decades, not years.

So on the OT side, you mentioned assets have been around a long time. It could be like a very large press or machine that's 30, 40, 50 years old. Some of the technology that's there, PLCs that were introduced in the 80s are still being in production today in large numbers around the globe.

So that technology was designed to last 20, 30 years back in the beginning. When it was developed, it was implemented and it's been in use. There was no security.

Nothing was connected. Nothing was exposed to the internet. So now as you try to manage that piece of it, you have those legacy assets.

So it's not about adding security to that asset. It's about how do you bring awareness to the environment that that asset is operating on? Has something new been interjected to that environment? Does something that's not supposed to be there is a new asset? How do you bring that and look at that from a holistic standpoint and begin putting, let's call them wrappers, around those assets to protect and shield them where you may not be able to, shy of completely replacing that asset, which may not be feasible in every situation. Yeah, most of the time it's not feasible.

And I think that ties in really well with what we talked about at the beginning, the business impact analysis, which is just like asset management. It's called asset management and asset visibility because it's continuous. And your impact analysis, which tells you, hey, these are the things that are important to the company.

These are the things that are kind of important. These are whatever. That changes too, right? So I think you could have a system that, let's say it really is air gapped, right? If we actually do miraculously find one that nobody plugged anything into and it's running, but then now is the time and that new thing comes on board and we've got it connected to the internet.

Well, now you've got to look at that asset inventory. You've got to look at that impact and go, well, okay, our most critical machine is now connected to the internet or has now got AI identities now have access to it because we have workflows and diagrams or whatever machining instructions that are all coming through. And we didn't want to pay an intern to do it anymore.

Now the AI is doing it. Well, okay, now we have to put in, we have to think about the controls in place of that. And now when before there was the risk of it going down, we know how much it costs if it goes down.

But before it was like, well, that chance of happening is really just relying on a technical malfunction. But now we have a cybersecurity risk that can potentially take it down. So now that million dollar an hour machine maybe needs a couple hundred thousand dollars of protection.

(9:42 - 11:25)
Yeah, for sure. And it's not an easy process to understand that. It's not just as black and white as it might seem.

It's all of those pieces that you just mentioned of, what's the attack vector look like? How do I identify what is my cost if this machine were to go down? What does that look like to the organization? And putting some guardrails around that tie back to the business risk. What is the appetite? Maybe they're okay. Maybe they can sustain an outage of let's say four days.

And in the history of the organization, they've never had anything more than eight hours. Maybe that's okay. Again, but all of those need to be considered as you're doing this business impact analysis and determining what is the right approach.

And then when you determine it from an executive leadership, how do you start structuring that from an implementation? Maybe it's a re-control, rewriting. Maybe it's a firewall down there. That OT needs some new skill sets to understand how to begin using that.

What does the process look like back to that third leg of that stool, the process? Now you pick the technology and how do we begin implementing that? I want to put you in a, not in a box, I'm going to trap you here. I like boxes. Can my box be round and not square? No, because we're talking a lot about, we're talking about security investment, changing environments and constantly, you and I both know what it takes to be on the defensive.

(11:27 - 12:58)
And it makes black and white sense sometimes that this costs this much and this costs that much. What do you do when the budget is not there? So great question. And you're right.

That's not always as black and white as it might sound. So as a risk practitioner, what I would say is identify all the risk, outline them in the risk register, make sure that the organization understands where they are. And the business, in my opinion, really has two paths.

One, put together a use case. You go back to the executive sponsorship and you say, look, here's the risk. This is what can happen.

Here's the impact. What's it going to do to the business? Here's the likelihood, probability that it's going to happen. And then here are some methods to, I guess, remediate it and build that business case if it's important to the business to get additional funding.

Again, the only way to remediate it is to present the business use case. That business case should drive the decision for funding. And if it's important to the business, they will fund the project, even outside of a normal CapEx or OpEx funding channel.

(12:59 - 15:40)
Because if you've got an exposure, for example, you mentioned putting something, an asset online, and now you've got your critical asset for your production exposed to the internet. But now you see the vulnerabilities, your continuous monitoring, you see all the vulnerabilities that are associated with this, and then you've got

problems. So now you're in the middle of June and budget doesn't come till January.

So how do you address that? Again, I would say that's a one-off. Here's the concern of the business. Go back, build that use case and present it to the leadership of this is why this is important.

This is an exception to the rule. There's change management within organizations that are there for a reason. This would fall under that change management exception.

And I think it would warrant the budget allocation if it's important to the business. And that's how I would address it. Yeah.

And I'm thinking now as they're presenting that, we talked before a lot about translating the technology to the business side, making sure the board understands. And we were reminded, and you even mentioned it, maybe they're just going to have cybersecurity insurance. I think it's important.

You and I know this, but there's probably some people listening who don't. Having insurance doesn't necessarily mean anything. And there's a lot of small print on that stuff.

And I've definitely encountered several people who have said, so if you're taking that to the board and be like, well, we have cybersecurity insurance. You probably want to know that before you present it. And at that point, you can say, well, yes, we do, but it requires us to have done A, B, and C. We have to have a... It may say we need to be using a framework.

It may say we need to have penetration testing, or we have to have done an actual risk assessment. And again, in that risk assessment standpoint, when an insurance company, you know, organizations who are built on auditing and assessing risk, they know a risk assessment is not a vulnerability scan. And they know a risk assessment is not a compliance assessment.

It means the stuff we've talked about, quantifying, calculating, manipulating all that stuff out, right? Insurance is not necessarily just going to be the saver for you. Well, and their practices and policies are built on paying. So their goal at the end of the day is, how do I find a loophole that says I don't have to pay? That's maybe not the exact method, but again, at the end, it seems that way sometimes.

(15:40 - 18:19)
So, and you're right, the fine print, the coverage seems to be dropping in value. The exceptions to the rules seem to be going up, and the loopholes to qualify for it are a lot. So you're 100% correct.

The legal teams need to make sure that they are addressing and reviewing on an annual basis your cyber insurance coverage to make sure that in the event something does happen, you actually get what you believe you're paying for, not what you're being asked to pay for. Yep. You mentioned

legal, and I love that because I like to, again, different audiences here.

We've got the security leadership, the technology leadership. We've got the business leadership and the board. I think it's important for both to have talked to legal, right? I think in most cases, a lot of the board is going to be listening to legal.

A lot of times they're the ones telling them what to do, but as a security leader, they can be your best friend in helping get that budget and helping do that other things because they can come to you and say, well, this is what we're potentially, this is what we're on the hook for, and this is what that says, and this is what we need to be doing because if we don't, we can be, this is the litigation and potentially things. And a lot of times, it's not enough to just be like, oh, we're monitoring the network, right? No. Well, again, that goes back to someone is checking a box.

There's a difference in due diligence and doing the right thing and checking a box. I can go down and check a box. That doesn't mean I've done anything.

I can pretend. But if something were to happen, there's going to be reasons that you're not going to be paid, and they're going to say, look, in this policy, we stated you needed these five things, and you clearly didn't do four of them. Yes, you have monitoring.

It's not continuous. It's on demand, and you're scheduling it once every month. That doesn't work.

And you've done no mitigating response other than we are evaluating. Okay, that's a start, but are you going to evaluate for the next five years? Are you going to do something with it? What's the plan? So it just doesn't work. It doesn't mean that that's the fix.

So you're 100% correct. It needs to be evaluated a little harder and more of a due diligence process. I like to say compliance is the floor.

(18:20 - 23:08)
We talk about programmatic security, and in most cases, because we're on the conversation here with insurance and just in general, cybersecurity management requires that program. And if you come at things programmatically, you're generally going to be in good shape. But that means, okay, cool, I'm going to be compliant with the things I have to be.

But those things, almost all compliance frameworks, and not cybersecurity frameworks, but stuff that's actually giving you a stamp and saying, I'm doing this. They're driven towards a specific area. It's not applicable to the entire business.

So leaders need to understand that, especially on the business side, that well, just because you have gotten this compliance thing, doesn't mean that it applies to everything. And it doesn't mean you're secure. And the

goal, I always say, to build a program, you take the stuff you talked about the beginning, your business impact analysis, your risk appetite, how decisions are made.

Then you take your compliance requirements, pick a framework, put it all together, jumble it up, and now you have how we're going to run the business. You can't just, if you're going to do something, you have to know why you're doing it. If you're going on a road trip, you want to know where you're going, right? And you need a map for that.

And that's what that gives you. And if you're not making progress on that map, because you could say, well, I'm here and I want to get to here, to your point earlier, well, how long are you going to evaluate the fact that you're at a one out of five and you need to get to a three? Well, again, that goes back to that gap analysis. You go in and you do that analysis on the organization, whether that's internal or somebody comes in and you assess and you say, okay, here's where we are.

And the organization needs to be here. And you set achievable timelines. You work with the organization, you understand, okay, this is going to take $5 million.

Okay. Is that a three-year process? Is it a two-year process? Can we stomach all of that right now? And we just take the hit now, get secure right now and not worry about the risk down the road. Or do we want to take it in small bite-sized chunks? And we say, okay, this month we can do, or this quarter of this year, we can do this amount.

And next year we evaluate and you really set achievable goals and begin working through the process. But you're a hundred percent correct. I can be busy all day long, but if I'm not doing anything, I don't need just to be busy.

I could sit in the park and watch the birds fly by and do something fun versus, you know, being busy is not productive. Yeah. I just posted something about that.

Like, I don't remember if it was me or my company page about the whole idea of like, busy looks productive, but it doesn't really mean it's anything or doing anything. Yeah, sure. Yeah.

Yeah. So I do want, but to your point, to the stuff that you mentioned there, like that brings us all the way back to the beginning, which comes into the impact analysis and the criticality, right? That whole idea of, all right, where do we need to invest our money? And a lot of times we do see, and I've seen it, you've probably seen it. I've gone to companies where the IT side of the house, what we call the enterprise side, they have IDS and firewall and DLP and all this stuff in place.

And then the OT environment, if they even call it an OT environment, right. It's just down there, like doing its thing and funding the entire company, right. At the end of the time.

But there's no connection. There's no visibility. So even if there is a security team in there, they're not allowed to look at the OT things.

So for those organizations that haven't solved that gap, how have you been able to kind of make that happen? So I see it from both sides, to be fair with you. There's the example that you said where the OT teams or the shop floor or whatever we want to call it, is funding the entire organization. Because again, without the production, there's nothing to sell.

There is no organization. And I've had a conversation with a client that we are facilitating, helping to build a facility for. And I'm like, look, we need to have some conversations around security.

We need to be thinking about visibility, monitoring, what's the DMZ look like. And the response was, hey, Craig, if I don't get the building built, there's nothing to secure. I'm like, OK, but surely security is important to someone.

(23:08 - 23:59)
So if you're in the weeds like that, it doesn't work. And then I've also seen it on the opposite side where you're right. IT is a rich, deep, mature piece of the organization because it's been around 35 years.

It's got a huge head start on the OT side. And how you can't just literally take the tools from one and apply to the other. It doesn't work quite like that.

So how do you get to that balance? And it's difficult sometimes. It's difficult. Having that blend of making sure that they can come in and do the right thing and support each other is important.

(24:00 - 27:56)
Yeah, I know, I will never name names, but I know massive, what I would consider massive organizations from an employee account standpoint and multiple locations all over the globe that have, like we mentioned before, an IT manager and two or three help desk people. They don't have a solution for, they may not even be able to have some of these conversations because they're so busy dealing with help desk tickets and stuff. And that's where somebody needs to have the conversation with leadership while you're talking about, hey, these are the risks that exist.

Hopefully they've got a partner like you or me in there, right? At least shameless plug saying, hey, this is what you need to be doing. And then that's also, I think how they fix that solution. I am very happy to say, or very happy is not the word, but I will not shy away from saying if you're not a massive company with tons and tons of money to spend, you shouldn't build your own security operations center, right? It's much easier to use a service provider, right? And most of those service providers will also help you do this work, right? They will also have other services that you get.

And then you get a partner who basically becomes part of your team and you don't have to hire, you know, 50 people and three, you're already dealing with three shifts on the shop floor. Now you want your IT people to have to do the three shifts on the shop. Again, there's no reason this organization is designed to support people.

We are here to help guide. There is between the partner ecosystem, the channel, the systems integrators, the organizations that do this every single day for organizations to try and go this alone makes no sense. Look at the model that IT has adopted over the last 20 years of outsourcing those services because they realize it's cheaper, more efficient, and sometimes better quality to have an organization that specializes on just instant response or just third party access or whatever it is.

And because to build all those teams internally, super expensive and just doesn't make sense. Yeah. It's not something I, you know, you don't have to go at it alone.

And I can tell you, like for me personally, and the firm I work for, like, I will tell you everything you need to know. There's no gatekeeping. There's no, like, if you want to know the secrets and you want to go build it yourself, I'll give you the handbook and you can go do it.

If you need help, then we're here for you. Like, that's kind of how I look at it. Like it's not, it's not rocket science, but it is difficult.

It does cost a lot of money. But that is kind of how, you know, how you have to go about it sometimes. And the other part, something you mentioned about the talent.

In cybersecurity, there's no shortage of talent, right? The challenge is the companies that are providing these kinds of services are way more appealing to the professionals because, you know, somebody who comes and works for me, they're going to get to look at an OT environment, a manufacturing environment, a healthcare environment, and medical IOT. And then they're going to have, you know, some retail clients, like their life is going to be different every day. And they're going to learn a lot and have a lot of cool things to look at versus coming to work every day and looking at just your stuff over and over.

And then, and not only from the talent acquisition standpoint, but also from the, like keeping them fresh, right? It's difficult to look at your stuff and be objective. Exactly. You have a very biased opinion or a very biased view sometimes of your own environment.

(27:57 - 28:12)
You know, I go into my house at home. My house is always clean, in my opinion. Some of my neighbors or friends who come in, they're like, Craig, this is a mess.

I'm like, well, that's perspective. But again, that's reality. So it's how it's addressed.

(28:14 - 29:22)
Yep. You get, what was it you said? You get, not numb, but like how you see things is not how everybody else sees them, I think, right? That's the bombshell I think we end on. Because to me, that's just the way it is.

Like that's, you get too comfortable in what's going on. Your perception is reality. Your perception is your reality of me.

And if I'm looking at it from an organizational inside only, again, I believe my team can do this. I believe my team is capable to perform this when the reality may be, maybe they can't. Maybe they need some guidance.

Maybe they need some support. Maybe they need a partner. Maybe they can do part of it.

Maybe they aspire to want to do it one day. They're just not there yet. And take advantage of those situations.

Leverage that partner community, like your organization, our organization. Get guidance from professionals. Don't do this by yourself.

There's no reason to. On that note, I will tell my DIY story. Okay.

(29:24 - 29:59)
I'm a handy person. I needed a microwave replaced a couple of years ago. So I went out and bought the microwave.

Got home, took the old one off. The panel was different. Had to go back out, get that panel, put that in up.

The wire was different. Had to wire on another thing. I got it done, right? A few ibuprofen later and half a day wasted.

I'm good to go. The next time I called, I just, the company I ordered it from, the big box store I ordered it from, I paid them a hundred dollars. The guy was in the house for fifteen minutes. No ibuprofen no pain.

If you need help get help, don’t take things on your own if you don’t have to.