Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host, Brian Contos, and we've got a really special guest today. Joining me is John Pironti. Welcome to the Cybersecurity Effectiveness Podcast, John.

Thanks Brian. Happy to be here.

Hey John, before we get going, can you give everybody a little bit of background on you and what you do?

Sure Brian. Well, I run a small advisory consulting firm called IP Architects LLC. I've been involved in the IT world, doing IT architecture design, IT strategy, information risk management and security, ERP, CRM application, all this fun stuff, Info Sec and governance and risk management and enterprise IT for over 27 years now. Most of the clients I work with are mid to large enterprise clients across a whole bunch of industries and a whole bunch of spaces. I've written a lot of work and done a lot of work in the space on building out information risk and security programs. Threat magic models, metrics and modeling capabilities. And I spent a lot of time thinking about how to communicate effectiveness and how to align to information risk management, goals and objectives with organizations that I work with.

That's awesome, John, and, y'know, I've known John for I guess, I guess we're going on, what 15 years or something like that.

Brian, I think we're getting close to 20 believe it or not.

Geez yeah, back to the earliest days I think we first started connecting around Interop. Back then but, John, let's get right into this, you know, you get exposure to such a broad ecosystem of customers that both the very senior leadership level, and then of course the folks with the hands and the keyboard operational folks. What do you think are some of the biggest mistakes organizations are making when they're, you know, choosing their technology solutions?
John Pironti: Yeah that's a great question. I think that we, that many organizations I see both that I work with and that peers and I, what we talk about is that they assume that the controls they're buying and the technological controls, security controls they're implementing will even work, will work as designed, as expected for every threat that's out there. So, we have this ever-evolving changing threat landscape right, we always have things change.

John Pironti: The cool thing about what we do and has always been for me is that when I build something, somebody else is gonna build something to get around it. Build a better mousetrap kind of mentality. Constantly evolving. Well a lot of what I see is people working the threat of the moment, they look and they spend a lot of time with many security controls for that perceived threat and they're assuming that they're covered. They're not agile, they're not navigating and they're not validating, and verifying that the controls they're going with are actually working as they intended them to. They're also assuming they were implemented properly.

John Pironti: You know one of the things that I often joke about when I give speeches and I give a lot of them, as you know, Brian, all over the world lots of different arenas and things like that, is I always kinda talk about the fact that in my career I create these amazing visual diagrams, amazing architectural specifications, amazing things, and I bring them to operational staff and I say take this work of art I have and make it a reality. Take this concept and make it a reality.

John Pironti: And we assume that they're gonna implement it exactly the way that we designed it, and then 6 months later when you go to a shortens testing or you do monitoring or you're putting tools like the instrumentation models like Verodin provides you quickly realize what you thought was installed or designed didn't get installed that way. It wasn't actually there, it wasn't actually in place. And the last thing that I, that I'll say here, Brian, just to kind of top this off, is I really think about this is that you got to assume these things are effective, we assume their capabilities but we don't verify. And I always try to prepare a concept with my team, with my clients, with anybody who will listen to me, that if we're doing risk and security well, we have to follow a trusted verified approach.

Brian Contos: Yeah. You know, John, you mention the word assumptions in there, I'm seeing this big movement across really all verticals, from an assumption-based approach to security, to an evidence based approach in security, and we're starting to measure security like we do in other strategic business units, sales, operations, finance. And that really pulls into this statement you just made of trust but verify, and I've heard you talk about this in the past as it relates to information risk and security. So, what is it about this concept of trust but verify that you think is resonating today with these business leaders?
John Pironti: Yeah, I think exactly what you said, Brian, is that people want evidentiary based models. We've spent a lot of time in the last couple years applying lots of great tools and technologies, and spending a lot of great ideas doing a lot of things to deal with what our current and evolving threat models. But what we don't know is what is actually providing value to the business today, and when I see a lot of the business leaders I work with saying, "I've invested in some cases, millions upon millions of dollars in high risk and security programs, I've bought a lot of technology, a lot of tools, a lot of things. Is it really working? Is it really in place?"

John Pironti: You know, we have no assurance, and they want to know, “Why should I believe that I should continue to invest?” -- especially as we're coming up in refresh cycles now, we're coming into new budget seasons and new budget cycles, they want to know that this is being treated like a business, not as a defensive state as they might have been 5, 6, 7 years ago, where everybody is so freaked out and scared about the next hacker of the day.

John Pironti: Now they're saying, “Look it's a reality of the world we live in, I want to know the investments I'm making are useful and beneficial and I want some assurance and validation that they're actually working. I don't want to have this false sense of security, cause without that assurance they have a false sense of security.” They say, “Well, my firewall's in place, it must be working.”

John Pironti: Well as soon as you explain to somebody that that as soon as you start using encryption and going it breaks through most firewalls. And they will say, “I got SSL” encryption on my firewalls, they say well you see how many attacks don't use SSL anymore, they use PGP or other encrypted modules, and their firewalls can't do anything about those. And the leadership says, “Well wow, 'cause that landscape has changed, the atmosphere has adapted. How have we adapted to them?” So we need that assurance, we need to kinda go in that Trust but Verify model because they want to know that all that investment, all that work is gonna be positive and then be fruitful, and be able to demonstrate full to their stakeholders as well as their customers that they're doing the right things.

Brian Contos: Well John let's take this notion of the changing threat landscape that you just mentioned and let's dive into that a little bit deeper. What are your thoughts on how to implement a pragmatic approach to constant or consistent monitoring of your security posture? You know, how do we get to the point where rubber meets the road, and we've actually got an approach that's effective in this changing landscape?

John Pironti: Yeah, I'm glad you asked that, Brian. I'm a huge advocate of the concept of first applying the concept of threat involved analysis, to what we're going after. So, we can look at threat scenarios and use scenario-based modeling so we can highlight the high impact and high likelihood scenarios that can affect us. And
understand how the adversary is actually gonna navigate through our systems, navigate through the world, and cause negative impacts to us or cause problems to our world, things of that nature. And once we have those scenarios built then I can bring in instrumentation models, then I can bring in monitoring concepts. It’s not good enough to just do a one and done pen test on an annual basis. I'm not saying they're bad. My team does them. I rely on them. I think they're important and they're very important to have some human conditions sometimes to do cause and effect analysis, and cause and effect modeling.

John Pironti: But we're not going to be able to keep up in an agile development model in a rapid deployment model with those testing concepts. So, I need something that can be automated but tuned to my risk profile and tuned to the scenario basis that I'm concerned about, as well as understanding new scenarios that I may not have been able to factor in because that analysis takes time.

John Pironti: So, I need to incorporate the concept at a high level to say, let me apply these principles of application security or network considerations. Or modeling of attacks for denial service attacks or ransomware attacks or things like this, and say we’re all the permutations that might come there and let me use monitoring in instrumentation models like those provided by Verodin, to say, how can I start monitoring for that on a regular basis, not a point in time basis.

Brian Contos: Yeah, you know, I always hear these phrases, you know. Pen testings are great but, our red teaming exercises provide value but, the immeasurement of vulnerabilities juxtapose to, our patching exercises are good but, so there's always this notion that we know, we know these things add value yes, clearly they add value, we’re not saying they should go away, but were saying there's a huge gap especially with the way organizations are depending on cyber security to be a critical piece of, when they're making business decisions. So, with that in mind, what are some of the considerations that organizations need to incorporate when they're developing metrics and measures associated with their security effectiveness?

John Pironti: So, I know some of the things I'm going to say are cliché, and a lot of our audience is gonna shake their heads and say yeah everybody says that. But we gotta stop thinking of security as a bolt-on. When I do risk and security modeling I like to work with it from the day we think of the new business idea and it has to be aligned with the information [risk] of an organization.

John Pironti: The pain chart, for an organization. When does it hurt, when is it material, when is that negative outcome or negative behavior going to deteriorate the organization versus just being a nuisance? When does it get to a point where we’re gonna do action against it, do something with it? And if we have to build in these points of instrumentation, these points of monitoring, these points of capability have to be built in along the way as we’re doing that build, as we’re
building up a business processes then the supporting technological infrastructure and capabilities in user activities that go along with that. So, that we understand tolerances, we understand thresholds, we understand what are key indicators of concern and interest. What are we gonna navigate through, not after the fact where security comes in and says, okay yeah, we’re here to design and review, it looks pretty good.

John Pironti: Being embedded in the conversation saying, “Hey you know, we know we’re gonna have this many user transactions, let’s look at what a volume metrics analysis should be on an hourly basis in our assumption models.” So, we can start buildings baselines of behavior even before we get this technology in place. And these are the types of things I like to think about, a security built in, not bolted on.

Brian Contos: Yeah, you know, I think expanding on this idea of it being built in means, in a lot of cases the understanding from executive business decision makers that might not be security savvy or even in the technical field at all, might be a CFO, a CEO, a board member somebody that’s on the audit committee of a publicly traded company's board. There’s this need now, to be able to communicate the state of security effectiveness up to these non-technical, non-security executives. How can organizations approach that today?

John Pironti: You know, Brian, there’s a common theme that I like to give when I talk to organizations and vendors and such, is a thing I learned early on in my career. Geeks don’t write checks. So, we have to appreciate and represent. While the usage audience may be technical staff, and they may be amazingly brilliant individuals. They don’t necessarily have the pulse of the organization when it comes to actually understanding what makes the company money, or what is the goals of the company, what is the key business process, what touches the hearts of the executives that they’re trying to deal with. ‘Cause their total customers are those executives.

John Pironti: In many cases, securities represented as a cost center. And when something is represented as a cost center you want to minimize cost. You want to contain expense, you want to make it something that you really carefully model and monitor very closely and only spend what you have to. If we can make security more an advisory concept, a supporting concept, and phrase it in ways that support revenues, support business activity, support businesses achievement, things of that nature. That’s one angle that I often use that really supports doing more with business security. Some of the other things is actually as you’ve heard me say many times in this call already, risk and security.

John Pironti: I don't believe you can do security until you understand risk. And when I go speak to an executive I never talk to them about security first. I talk to them about risk management first. As in let’s talk about what risk appetite we have,
what's our profile, what's acceptable, what are you comfortable with, what's okay for you and then I'll build you instrumentation models and security controls and things like that, that will ensure that we're monitoring to that level of comfort, to that level of capability. We're supporting you in that way and we're demonstrating you with data in a way that you can correlate and say, yes I see how these controls are actually helping me. They don't need to understand how our firewall works, they don't understand how encryption works in detail, how then correlation works, how threat modeling works. They just need to understand principally at a high level.

John Pironti: So, you're using scenarios to help them understand where we could be heard, you're gonna put things in place to monitor for key points of indicators, you're gonna leverage that and reporting models that also back in the saying why you have many certain things you might reduce my availability or put onerous natures on my processing capacity so I have to make balancing acts against that. You're giving me the ability to be empowered by giving me risk-based decisions and the goal really is to give information to decision makers to make informed decisions, not good or bad decisions in the eyes of the security professional. Because myself as a security professional I don't see myself as owning much of these business processes in many organizations. I'm supporting them. So, I have to let them make decisions and act against them but I want to give them information – then they can make informed decisions as well.

Brian Contos: Now are you actually seeing executives asking for this? Are they, is a CEO, CFO, some other leadership role are saying, “Hey security team, hey CISO, I need some metrics that I can use as 1 of a 1000 other variables to put into my risk calculations or our business decision making processes”? Are they asking for this or is the security team just trying to supply it to them saying, “Please make use of this”? Where do we stand now, have we matured to the point where the leaders are actually saying security team give me this data?

John Pironti: The better leaders are. The better leaders are looking for metrics to treat this like any other business model. So much money's been invested and it's really come to be understood now that this isn't a one and done model of investment. This is gonna be a constant level of investment going forward, there's gonna be a constant level on resources required, funding required, impacts to performance that are gonna occur so they need to calculate that into their whole enterprise risk model. If you look at what most business leaders are, they're people who are comfortable with risk, they're risk managers, not just from a technical security risk but business risk, is what most CEOs are known for, invest CEOs are known for is how to identify, analyze, assess, manage risk.

John Pironti: So, when you look at what we're seeing more and more of the evolution of security metrics coming in, you're seeing more people saying, you know what, this falls into my enterprise risk program. Information risk is just a component of
enterprise risk, and as such I'm gonna hold it to the same standards I hold other areas of risk, like operational risk, finance risk, market risk, other areas that have to report metrics, have to demonstrate value, have to give me trade off decisions, that's what they're coming in saying, let me factor this into my overall enterprise risk portfolio, not keep it as something that's on the corner, as it was probably between 2000, 2010-2011. It was this specialized subject that we were just getting comfortable with. Now it's turning into business as usual conversations, in my work.

Brian Contos: Yeah, very insightful and of course with the amount of organizations that you work with, I think that's a very good representation of sort of the ebb and flow of the community now and how it's maturing. So, thank you for that, John. Hey, John, final question here, and I like to ask this of all of our guests and it's a little bit on the fun side but. Who's your favorite superhero, or super villain, and why?

John Pironti: Well I can't give away all my secrets so I'll have to keep the villain to myself. I would probably say the cliché. I probably have to say Superman, because he has the most dynamic set of talents and super capabilities. He's not a one trick pony. He's a many trick pony. And that means he can be dynamic and adjust to these situations and adjust to the environment and navigate and succeed.

Brian Contos: I love it, I love it. And honestly, if it wasn't for Superman, we wouldn't have probably any of the superheroes that we all know and love today anyways and the movie theaters gonna be filled with all these blockbuster superhero movies, but absolutely. Hey, John, thanks so much and thanks to our listeners for joining, and be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored my Verodin.