Brian Contos: 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 Kevin Morrison. Welcome to the Podcast, Kevin.

Kevin Morrison: Hey, thanks Brian.

Brian Contos: Hey Kevin, before we get going can you give everybody a little bit of background about yourself?

Kevin Morrison: Sure, yeah, absolutely. I have been in IT information security for a little over 20 years now. I'm currently the Chief Information Security Officer for Pulte Group here at Atlanta, Georgia. I've been with the company for about four and a half months. I'm sorry, almost six months now. Time flies. I came from Jones Day where I was the head of information security for one of the largest law firms in the world. You know, I kind of came up through the IT ranks in different positions that I've held throughout my career.

Brian Contos: Very cool. Very cool. Kevin, we met a few years ago back when I was on the executive team for Solera Networks and you and I were at a customer advisory board event out in Utah and I remember at the hotel there just happened to be a Bentley test driving event, which was cool. Who's gonna pass that up? You and I hopped in a, it was a W12, not a V12, but a W12, which I guess is a little bit of a shorter, wider engine in this Bentley sedan. The gentleman hosting the event was in the passenger side, I was driving, you were in the backseat and I just remember getting onto the freeway. That car was so fast and so quiet and so smooth, we got on the freeway at like, 140.

Kevin Morrison: I remember him telling you, "Okay, the Bentley ride is free but the ticket is yours if you get one."

Brian Contos: That's right, that's right. Yeah.

Kevin Morrison: Yeah, you pressed that gas pedal and I was in the back seat. Felt like a G force hit my head against the backseat there.

Brian Contos: Hey, you know, one of the things I wanted to talk to you about, Kevin, you covered some of this in your background. You have a long and distinct background as a security leader. What do you see as some of the biggest cyber
security technology challenges occurring today and what's the effect of that gonna be on actually reducing business risk?

Kevin Morrison: You know, well, if we think about one of the prime objectives in security from an incident management perspective with regard to reducing dwell time to the absolute minimum, I think machine learning and process automation through orchestration will have a significant impact in accomplishing that due to the sheer volume of log data that information security teams have to sort through. I would say the volumes simply can't be, you know, effectively analyzed by humans as evidenced by the continuing breaching that have occurred over the past decade. Having anomalous activities identified by machine learning technologies will allow threats to be identified at near real time, 24/7 for continuous visibility, which is critical. That in turn will certainly reduce risks to the business. Especially in light of the talent shortage that exists.

Kevin Morrison: I think there [are] other technologies and changes I see as having a real impact on risk reduction to businesses as a move toward, you know, for instance, a continuous penetration testing through simulated attacks and a virtual environment where attacks and exploit paths can be rapidly identified and then mitigated based on the priorities that exist. Then I would say also probably a transition away from the traditional perimeter based and network central models to a cloud based and applications centric model that really provide a greater flexibility to the business and adherence to the kind of a data centric classification framework, if you will. There's no silver bullet but there are definitely some very innovative tools and capabilities available that are starting to help turn the tide.

Brian Contos: Yeah, you know, when we think about volume, just we'll pull that one topic that you mentioned out of the equation and just think about volume. You know, everything's connected now. Whether it's at home or whether it's in the organization, you know, people are bringing in where they used to maybe have one device, a laptop, maybe now they have five, six, ten devices that are connecting for business use and personal use and they're a hybrid of these things and there's just so much going on there. You know, if I just look at IP addresses like, you know, as IPV4 versus IPV6. In IPV6 we have 340 undecillion IP possibilities. That's 340 trillion groups of a trillion. Or another way of thinking about it is a heck of a lot more. The volume is just untenable approaching it from our traditional approaches and I really like what you said about more of a data centric perspective, especially as we embrace the cloud.

Brian Contos: Let's kind of pivot a little bit there and, you know, security. There's been a lot of talk about this being an IT issue or is it not an IT issue. What's your take on this? Is it becoming more of a business strategy? Is it a business imperative and less about the bits and bytes?
Kevin Morrison: I think it definitely is a business imperative. I think technology clearly plays a significant part of what information security needs, you know, in order to manage and implement a successful program. While that exists, I do agree that information security teams, at least that I've been a part of and the peers that I know and speak to are included in business risk discussions that are outside of traditional IT conversations, if you will. As information security continues to be increasingly seen more as a business issue to be addressed, the historical perception and the expectation of security teams engaging and adding value by simply managing firewalls and antivirus are long outdated, right?

Kevin Morrison: That said, while there's certainly a critical need for security to be collaborating heavily with all IT functions, if the security team is seen primarily as an IT function then it will be limited in its ability to address those business risks and issues so, for those reasons, I'm a big advocate for seeing information security as a brand protection function, which I've seen, makes it easier to engage the business in discussions of risk.

Brian Contos: Yeah, I'm a big proponent of that. I would actually argue that I don't think a security team can be successful unless it's aligned with the business. Luckily, or fortunately, I think we're seeing that this is happening more often than not, especially in larger organizations. Mid-size, I think it's still a bit of a struggle to get that recognition but I think for large, you know, the Global 2000, Fortune 500, large government agencies, it's very clearly something that has to be aligned with the business mission.

Brian Contos: You know, with that said, across the board mid-size, large enterprise government agencies, there's a talent shortage. You've helped create and lead a large number of security teams. How are you dealing with this shortage and how are you ensuring that the teams that you do put together are successful?

Kevin Morrison: That's a great question. Yeah, the talent shortage is definitely real and there's the need to address the risks from the business while at the same time recognizing that, you know, the business has its priorities in what it wants to invest in. Me being in a Fortune 500 company and having the support of our board, clearly, it's something that we take seriously. By the way, for this podcast, I'm speaking on my own behalf. I'm not speaking on behalf of my company by any stretch. Our culture is good in that regard. You know, aside from what I'm doing, aside from formal, offsite training that teams need to continue to do, I've always been a big proponent in cross-site training or cross-training, rather, for those on the team to make sure that there's no single points of failure dependencies on any one particular person.

Kevin Morrison: That translates also to removing potential silos and then giving the broadest exposure to those on the team who need and want to continue growing. I certainly realize that there absolutely are organizations with very small security
teams who may not have that option and that's a decision that the business has to make and come to terms with in recognizing the risk that may exist should any of that talent leave and then finding that it takes six to eight months to fill, you know, that critical position. Along those lines, to be successful and to add the biggest value, I've been able to fill roles for internal IT talent who have shown the desire and the capability to take security on full time. I recall a number of years ago in one security analyst opening that I had for a company. I hired an IT site support person who had been with the company probably, I think, three, four years and had been actively engaged with my team and helping the security team deal with incidents at that site.

Kevin Morrison: He knew the systems, the people, the culture, the processes, etc., that allowed him to have an immediate impact in his new security role. He's gone on since them to become an information security manager at a different company so giving him that opportunity was a big win for the team at the time and for his career in general. So, you know, that's actually similar to my security manager now in him previously managing more IT specific systems and teams along with some security staff and being able to take that knowledge and apply it to helping me build a successful information security program, rather.

Kevin Morrison: When it's all said and done, I think it's also my job to be the type of servant leader that will support those on the team in succeeding and having the biggest value impact to the company so that leadership includes getting executive and board of director buy-in to the roadmap to ensure appropriate investments that will then allow the team to do what needs to be done in adding value to the business.

Brian Contos: That's awesome, and I love hearing cases about bringing people in from different areas within the company and bringing up their skillset and making it so that now this is a completely new career avenue for them. I think that's a testament to your leadership capabilities, as well. But Kevin, what do you look for now? So, we talked a little bit earlier how, you know, it's more of a business centric or something that's at least aligned with business today. Security's not just about the bits and bytes anymore but certainly you need people that understand bits and bytes, the folks and hands on keyboard. What are some of the things you look for in someone that either has a security background or doesn't have a security background where you're bringing them into your team? Are there a handful of like... is it a personality thing? Is it an eagerness to learn? What are the things that say, "Okay, this is somebody that's gonna be a good addition to our team"?

Kevin Morrison: Yeah, it's just a combination of those things that you spoke to. Early in my leadership positions I would, for the most part, hire the most technically capable person who interviewed. While technical knowledge and experience are still important, I've learned to look first and foremost at whether the person has the
social skills and emotional intelligence to fit well into the culture and whether they truly see security as a service, which I'm a big proponent of. If they have that and a decent technical background and the aptitude to learn, I'll take that person any day over the most technically savvy candidate.

Kevin Morrison: I've hired some absolutely brilliant people who, you know, look like they came out of their mothers' womb coding from the get go, you know? Could run circles around me but they really should have been in a different type of role to really leverage their capabilities. With how often information security teams must be engaged with business projects and initiatives, you simply can't afford to have candidates come on board who are going to, you know, potentially alienate others across the business or even their own team with an approach that's aggressive or, you know, candidates who just may not play well with others. So you know, looking for those well balanced folks certainly makes filling the roles that much harder but I've definitely seen that doing so is worth the wait.

Brian Contos: What would you suggest for somebody that's in college and maybe they're on a track that's a technical track or maybe it's a cyber security program or somebody that's already in the field and they're working in a non-cybersecurity role but they're thinking about getting into cybersecurity. What areas would you say, "Hey, these are some of the things you should focus on. These are some of the core skills or techniques or ideas that you should subscribe to." Where should they start? How should they approach this cyber security career?

Kevin Morrison: You know, there [are] so many different areas within the information security profession. Incidence response, forensics, on and on. I would suggest really there are two that are on the forefront right now that I don't see going away any time soon and I would say application to cloud security should be a really serious consideration for study. There's a healthy need for those who can collaborate with developers in their own language and for developers who in turn can understand and incorporate security not just in a coding practices but architectural considerations, as well. Again, as organizations move to a more application centric model, those with that type of skillset I think will be well positioned to assist in translating business requirements into secure applications.

Kevin Morrison: Then with the rapid transition to cloud-based services, obviously, it's clear that a firm understanding of security issues and considerations for all things cloud based need to be in a security practitioners tool set. You know, and I'll throw in a third option for those who may be less technically focused and that's to consider the area of privacy. Though many attorneys currently fill, like, chief privacy roles, chief privacy officer roles, there is, and I think will continue to be an increasing demand for security professionals to understand how security decisions effect privacy requirements and vice versa. You know, if we take a look at what's been thrust on organizations this year with GDPR and what's now
on the horizon in the US with state based regulations like the California Consumer Privacy Act and, dare I say, eventually with Congress passing some decent federal regulations, if they could ever get their act together, there's certainly an opportunity for those who choose to pursue a more privacy based path instead of a technical path. There are certainly a lot of different opportunities to consider there.

Brian Contos: Yeah, you know it’s interesting, I started seeing this and I don't know if this is going to be the trend going forward or if these individuals are going to be bifurcated but folks that have the title of CSO and chief privacy officer, to me it seems like honestly too big of a role for a single individual unless they have some really good directors under them who are following up. At the same time, to your point, there's a lot of connective tissue between those two things so maybe it's a more elegant and efficient and effective approach to this strategy. I guess only time will tell and it's probably dependent largely on the organization itself.

Kevin Morrison: Yeah, you're absolutely right. I do have some peers who are in both roles and they have my sympathy. I wouldn't want to do both. I think you're right, it does largely depend on the organization, depends on the industry they're in, how large of a privacy footprint they may have. There are a number of variables that would determine whether or not it makes sense to have that into a single role but more and more, I mean, I see that as it's gonna take up so much time in one or the other position that I don't know if you could do both well.

Brian Contos: Yeah, it's great if you can do it but it's probably pretty, pretty challenging, like you said. I don't know if I would want that role, especially for a large organization.

Brian Contos: Kevin, as we wrap up here I have a question that I like to ask of all of our interviewees, which is who's your favorite superhero or super villain and why?

Kevin Morrison: Wow, you know, it’s a question my 10 year old son asks me lately just about every other day. He's a huge fan of all those types of movies. I would have to say Iron Man. I think it's because, you know, he wasn't gifted by, at least those creating the character, with actual superhuman abilities like a Superman. He used his ingenuity to create something that could actually take on those otherworldly characters, if you will, and kind of move beyond his mere mortal capabilities. That said, I also like his dry sense of humor. Yeah, Iron Man's pretty cool in my book.

Brian Contos: I love the character and I don't know if anybody could play Iron Man again now. It's just such a... it's one of those characters where once you see it and you know, you're like, "Oh, Robert Downey is Iron Man." I don't know if I could ever
see anybody else play Tony Stark. I think he pulls off the idea of being a billionaire and a genius and hey, why not a superhero, too, pretty well.

Kevin Morrison: Yeah, somebody else would have some pretty big shoes to fill there.

Brian Contos: For sure. Well, thanks so much, Kevin and thanks to all our listeners for joining. Be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.