uberknowledge

Tom McAndrew, Coalfire

Thought Leadership and Leading the Field by Sharing

Ashwin Krishnan: [00:00:03] So, we have execs from Coalfire, Tom and Patrick. And the idea here is, what we talked about briefly before kicking off the podcast, is given your fairly vantage position of what you see in terms of trying to build a framework around critical items, especially in terms of security and compliance, what in your opinion are vendors doing and not doing? And more importantly, as you built frameworks, how to essentially baseline or put a template in place that both the provider and the consumer can align to. Given that, what do you have to say to our listeners who are both practitioners as well as vendors?

Tom McAndrew, Coalfire: [00:00:57] Yeah, I'd say that there's a couple things in the way that we look at the world. We see two different worlds. There's a world of service providers. A world becoming cloud and people buying services. And they are migrating from on-prem to cloud service providers. Those needs of service providers and what their customers want is very different than retailers on premise so I'm trying to separate those two. So, as people are looking at moving to the cloud, I think we all agree that the trend is more and more are going to move to the cloud. What do those customers want? They want higher levels of assurance around three areas. There are security concerns; how secure is what I'm buying, how do I know? Privacy concerns, which are relatively recent over the last one or two years; how do I ensure that I'm meeting privacy and secrecy. And then the third part is really around what level of assurance do I have? Is a third-party report, a self-assessment questionnaire? We're seeing that world of service providers, whether you're selling a product or purchasing those, people have to be prepared to answer all three of those.

The unique part about that is those are three different worlds, the security world is driven by IT, administrators and the safety technology functions, security, password management. The compliance function or the assurance functions, are largely managed by auditors, software, and something done annually. Then the privacy world, which has historically been in the legal area. So, in legal, CISO compliance team haven't historically worked together but that is happening now. Vendors and people need to realize that's the trend that's happening now. If you're only coming with one leg of the three-legged stool, you've got to be prepared to answer the other two legs or realize you're not going to get a whole lot of traction.

Ashwin Krishnan: [00:02:37] Why don't we double click into that, as a vendor coming in, let's assume you even have a framework of understanding that you're talking to security and that stakeholders of privacy and compliance also exist in that mix. Should vendors come in and say, "Okay, if I come to you as security, how do you take my product and answer questions that compliance has or answer questions that privacy has," and historically have vendors done that? And number two, if not, what does it take for them to truly understand what's happening to the customers? Because most of the time you are so fixated on the competitive environment and making sure that you get leads from Black Hat. I haven't seen too many vendors who've gone that extra step or mile of truly understanding that there are different constituencies in the customer's organization, and how do I make life easier for my immediate counterparts?

Tom McAndrew, Coalfire: [00:03:39] So, maybe I can answer both of those in one question which is whether security, and obviously security for all of those areas, whether your security approach is a reactive one or a proactive one. So, immature organizations are in a reactive approach because, "Hey we've got a great product, tell me what you need and I'll tell you how we meet it." If you start with that you're already in the backseat. If instead you start with, let's say I'm approaching hospitals, you need to say, "I've worked with 100 other hospitals.

I know these are the top security concerns. I know these are the different ways to approach it. Let me tell you how we do it differently, and whether you're using our product or somebody else's, I'll show you these are the things you should be looking at." Now it becomes an educational thing, where they say, "Oh, I didn't realize there's ten things and I'm missing seven things." So, it's pretty obvious if you look at security, privacy, compliance, are they enablers to your product or are they prohibitors? If prohibitors, it better be a mandatory buy. You've got to be the cheapest.

I think that the second part people realize is security. We've struggled with ROI reducing risk. Companies are interested in three things. They are interested in driving increased revenue, they're interested in reducing costs, or reducing risk. Most of the security pitches are all around reducing risk and that's a very, very difficult sell. If you can change your product and say, "If you do these things, here's how you're going to save X amount of cost by configuration manager or whatever, or here's how you're going to drive revenue." If you can tell your customers that, now you can do this proactively and you'll differentiate yourself from your competitors to win more deals. That's the way to do it. So, I think the lesson learned is don't be reactive and don't try to sell it to reducing the risk. Instead be proactive and tie into solving your customer's problem to help drive revenue or reduce their costs.

Ashwin Krishnan: [00:05:21] Again that ties into a theme which seems to be pretty resonant in my conversations, which is the role of a CISO who has thus far been highly tech-oriented - that's how they come up the ranks - now they have to cross the chasm and have business conversations. Could vendors be the champions of how to help the CISO cross the border, and have you seen examples of that?

Tom McAndrew, Coalfire: [00:05:51] Absolutely. I think your first statement is CISOs are coming up, we've already seen that. I've got a lot of friends that are CISOs. The best CISOs have to be technical, but the reason they're the best CISOs is they're business-minded. They can simplify the messaging, they can turn

it into business language. Most CISOs are presenting to their boards and you have to take these very complicated things and simplify them. Definitely, business acumen is number one. The second part is as they're working with vendors, it's really not around hodgepodging solutions for I've never talked to a CISO that says, "I really just need a solution that does X, I really need three more, four more products." What they generally say is, "I already have more than enough products. My team is already super busy. What we need to do is simplify, prioritize, and get rid of other stuff that we're not using." And so vendors that can kind of come in and well, we think that the future is less point products, like you might have the best antivirus or best notability scanning or best database discovery, but you're going to see consolidation. Right now it's not a CISO going out choosing the best of a thousand products, it's groups of services that are industry specific: healthcare-specific, retail-specific, cloud-specific, you're going to see those bundles coming through. Even though that bundle may not be the best technically, if it makes sense that it's simple you're going to win those. So the advice, I think, for security vendors is don't choose products based on best security. If you take the business impact, you've got to think about all the costs and implementation. And a great product that doesn't get implemented, that takes too long, it's not as good as an okay product that can show ROI.

Ashwin Krishnan: [00:07:29] You mentioned something there that stuck in my mind earlier, which is become an advisor to prospects or customers. You gave the hospital example, these ten hospitals you've seen and this is what they're doing for HIPAA compliance or reduce ransomware attacks and so forth. Do you see members truly taking the time and effort and resources? Because it's one thing to come to a show like this and say you have got the best and most efficient product, it's another to say, OK anti-phishing for oil and gas, anti-phishing for utilities, that takes stamina. So is there a place for vendors to start saying, "Hey it's great to attend Black Hat, RSA, and other security-centric shows, but it's even more important to attend conferences or meet-ups of groups where customers are meeting their peers and their suppliers to understand what's really going on." That takes an enormous amount of time and effort,

which I have not frankly seen lots of vendors do, including all the vendors that I was part of. Is that something that's even feasible and possible?

Tom McAndrew, Coalfire: [00:08:42] So, Patrick and our marketing guys just did a great job, as we've thought about this. We work with over 3,000 companies, we've got 3,000 projects going on, and so as we're talking to folks and saying, "We're one of the largest labs groups, we're the experts," their response is, well, prove it to me. Most people's answers are let me get a smart person on the phone. If you're really a thought leader and we had that discussion, if we do have this, what is the knowledge that we get from our 3,000 customers? So, that drove one of the releases we started publishing, what we call secure realities with these thought leaders, which is exactly that. We looked, and we called this kind of our labs report, and said based on a sample set of 300-plus penn tests, what does this mean? Where are the common issues, what are the common areas? So we drove that, made that publicly available for folks, and that's something that we challenge other people to say, "Hey you know what, if you're looking at us versus somebody else, what's the thought leadership that they're creating?" So, research, R&D, and publicly giving back thought leadership was really critical in this function in a non-product way. Educating the customer and if you can educate them and they know it's not really a sales pitch, that's the best way to build that and get that meeting. We get that lunch with a CISO to say, "I downloaded your report, I saw the stuff, do you have anything else to add?" "Yeah absolutely, here's our specific challenges. Can you talk about, you didn't address this or you didn't address that." So, there's definitely ways to do it. I think we're trying to lead the way. You know we're looking at releasing things like voting machines. We're looking at releasing things on different industries, different technologies. If you listen to your customers, you'll get the inbound of what do they want and you should be you should be providing that in a variety of different things.

Patrick, Coalfire: [00:10:18] And I would add to your point that sharing that information, the common vulnerabilities that we're seeing, is all done in the context of a particular vertical. It's not a generic set of findings it's very much

couched in the context of the business process, the business problem, and the most common things you need to worry about. That, ultimately, is a differentiator for us as a business, and I think the more vendors and service providers can do that same type of work the better off they're going to be.

We see the best organizations realizing that their approach to compliance, their approach to security, ultimately can be differentiators in the market. Some of the best organizations are very proactively marketing their security posture and their successes and seeing enormous results. One organization, as an example, has seen a 33% improvement in their pipeline yield after they promoted a white paper that talked about the security of their solution. After they started to have collateral that their sales reps were leveraging in conversations with their customers. So, it's just an awesome example of a company that has harnessed their security posture, their privacy posture, and is using that from a go-to-market perspective to really have a dramatic impact on their sales and all of that very much tailored per vertical as well.

Ashwin Krishnan: [00:11:52] That's an amazing example that you bring because one of the big challenges that I've heard, and I been through that myself, is as a vendor if you start talking about how you approach your competitors will use that as fodder to come after you. The one thing is you've got to be truthful. And if you have a code of conduct about what data you're going to collect about your own employees what are you doing with that. It's an amazing feat. I mean it absolutely builds trust with the customer, saying, "OK you are doing things that you are pontificating." At the same time, how do you get vendors to see what this is the right thing to do? Even though for some short-term there could be some some challenges, especially with your competitors who could sau “these guys don't do this, don't do that”. You want to be transparent so that people trust customers, at the same time you do run the risk of getting into this pissing match that you don't want with competitors who are much more short-term focused. How do you balance that? It’s a great posture you are talking about here.

Tom McAndrew, Coalfire: [00:13:14] If you're worried about that I think you've got a crappy product, right? Which is if you really believe that you are the best solution, not necessarily the cheapest, you are the best value for whatever niche, and you're better than your competitors and you know that, then you have an obligation to educate the customer within that vertical within that field. What they should be looking for, what features, functionalities, and how they should return them. And if you're worried about what your unique approach is, your pricing is too transparent, your features are too transparent, then you really are in a shortcoming. That's where I think most salespeople in junior organizations are frustrated because they can't get the time with the CISO. If I'm going to meet with one or two people, I'm going to meet with the one or two people who are going to talk about the industry, who I know is going to promote their product, but they can talk about the top competitors. Why is your solution different? Why is your solution right for me as a retailer versus a cloud provider versus a government agency? Why is it the right fit? I think understanding the product is one. But understanding the size of the business, understanding what vertical they are in, and understanding what technologies they're using is the sweet spot. If you can go to a CISO and say I've worked with 100 organizations exactly like you, exactly your size, exactly with your problem, exact technology staff. I know the best practice, I know what's failed. I guarantee you're generally going to be able to get that. If you're another vendor that says I'm the best endpoint solution, it's hard because people aren't looking at them.

Ashwin Krishnan: [00:14:37] I know you mentioned this thing about tabletop and tabletop for the boards - what does that mean? It's a great analogy. Just for our listeners, talk about where that came from and what that's helping you drive.

Tom McAndrew, Coalfire: [00:14:51] Yeah. As we've moved a lot of the security, most of the security discussions have historically been at the CISO level, CIO level, VP of Risk, Compliance, or whatever, they're buying that and then just reporting the information back. Cyber security is starting to become, it's not there yet, we want it to become a board-level discussion. Boards are taking it much more seriously, they're including it quarterly. But boards generally don't

have cybersecurity experience. They're considering trying to pass a law that mandates at least one person be designated that. But many of the boards we talk with they don't have any cybersecurity. What we find is many of them are afraid to ask questions because they don't want to feel stupid. Going through a simple tabletop exercise of spending 30 minutes and saying, all right we just got notice, we have a malware attack and we've got 24 hours to pay a ransom; what do we do? Just to walk through that exercise where everyone can kind of understand we find is really helpful that makes the theoretical cybersecurity a more actionable thing, it helps the board understand what the gaps are, what their real capabilities are, it really drives funding everything. So, it's one that we really recommend everybody do. And they are taught from instant response around malware, around business strategy, and it will reflect what would happen if this company acquired this. Also, there's a game changer: there's lots of ways that can happen and in cybersecurity the two things that people are worried about are the digital transformation of disruption and then the cybersecurity breach liability.

Patrick, Coalfire: [00:16:22] In working with boards we see organizations at all different levels. The minimum level typically being just focused on compliance and meeting the kind of the minimum requirements that are out there, which does not translate typically to security. The next level being one where the organization is focused on their maturity, and they are able to evaluate objectively their competencies in the security domain and benchmark that against others. Then the third and ultimate level is where they're very much risk oriented. They have an appreciation for the business risk and the impact of security on business risk and they can quantify the risk within the organization and track how that's happening and improving over time. So a lot of the focus to best practice organizations that we work with and support is really helping organizations and boards towards that continuum. Ultimately get to the level where it's a quantified discussion not a compliance discussion and helping them grasp it from that perspective.

Ashwin Krishnan: [00:17:32] This goes back to what you were mentioning about great CISOs, successful CISOs having good business acumen. But this speaks to a different level, which is you want to be able to talk about the hard stuff in front of a board, right, because this is not like a marketing campaign, it's not like an acquisition thing, this is going to impact. Let's talk about what that will look like. So it does take a different level of courage to go to a board before an attack happens and say, this is what it's going to look like if we don't do A,B,C, and D. What percentage of CISOs are doing that today?

Tom McAndrew, Coalfire: [00:18:14] I think a lot of them are doing that now. This is what an internal resource can't do, most of them can't provide benchmarks to other organizations when they haven't been there long. So when a first CISO comes on board, his or her opinion is great because they can say, "With my previous organization the best there her to do is … This is where vendors, consultants, third parties can really help coming in, because it's one thing for us to provide back a phishing report, a penn test report with all the vulnerabilities. It's difficult for them to process, I got 130 and I had 140, are we better or are we worse? It's much easier say of the 20 organizations exactly like you guys, you guys are the bottom two. That changes that or say you know despite all these risks that look really bad you guys are in the top 10 percent of everyone we're seeing. And so being able to translate that to the relativeness of where they're at makes a huge difference along with prioritized recommendations of how they can close the gaps. As we looked at that for our penn test reports, it's not a technical finding so it should never go to the board. It's a technical finding that's a result of business process that provides risk, and then turning that around into how is that relative to everybody? Boards are worried about being negligent. They're worried about not investing in what their peers are doing. And they should be equally concerned about overinvesting, into becoming too secure, too lock down that they don't stay nimble enough and they can't bring up with it. So that pivot is starting to happen now, and it's different across different industries.

Ashwin Krishnan: [00:19:41] Very cool, so any last comments on what do you expect out of Black Hat? What would success mean for you at Black Hat, if you could look at one thing and say that makes it worthwhile?

Tom McAndrew, Coalfire: [00:19:55] I think in general what I'm looking at here at Black Hat is known for being the technical base. And there's this kind of pooh-poohing that, you know, if you're not a hacker, you're not the deep technical person, you're a no-no. You're a vendor, you're a sales guy or whatever. I think this understanding, this mutual respect that the technical knowledge and the technical expertise is really critical in this field, as well as making sure that the solutions get simplified to make a difference. We're all here fighting the same fight. People are bringing different skills. And I think the more that we can bring everybody together that would be great.

Ashwin Krishnan: [00:20:29] Patrick, anything from you?

Patrick, Coalfire: [00:20:30] Just part of what we're promoting is the insight from our most recent research and that highlights the common vulnerabilities at the application level, network level, internal level, so that the community can take advantage of our insights and others that other vendors and service providers are sharing here just to elevate at the macro level. We are still not winning this battle. Hopefully through the education, through the training, through research like ours that collective wisdom and knowledge will take us to the next level.

Ashwin Krishnan: [00:21:07] Very cool, thank you for your time.

Main discussion topics:
01:31 Three areas customers want high levels of assurance in.
03:47 A proactive approach not only educates your customer, but differentiates you from your competitors
06:54 The trend for industry-specific security products
8:59 Thought leadership and sharing information

13:14 The importance of understanding your customers and then educating them.

15:10 Make cybersecurity a board position.