IT Matters - Episode 3 - Mike Privette

Fri, Jul 29, 2022 5:54PM 48:49

SUMMARY KEYWORDS

security, people, ciso, company, organization, business, software, customers, mike, driven, passport, money, banks, general, technology, spend, assessment, iterating, secure, bit

SPEAKERS

Aaron Bock, Narrator, Mike Privette

N **Narrator** 00:07

Welcome to the IT Matters podcast, where we explore why IT matters, and matters pertaining to IT. Here's your host, Aaron Bock.

A **Aaron Bock** 00:17

Welcome everyone to the IT Matters podcast. I'm your host Aaron Bock and I'm joined today by Mike Privette who is the CISO of Passport Parking in Charlotte. Mike, how you doing?

M **Mike Privette** 00:27

I'm good Aaron, thanks for having me today.

A **Aaron Bock** 00:30

I'm excited for this one. I've been anxiously awaiting this one for a little while. Before we get into today's podcast, in case you hear a massive amount of rain or potentially thunder, it looks like we're about to get poured on today. And I'm sitting right next to a window so if you hear some noise in the background it might be that. Stay safe for all of you guys out there about to get hit with this. You included Mike.

M **Mike Privette** 00:58

Thank you, I'm also right in front of a window.

A **Aaron Bock** 01:00

Ok, so you might hear it on Mike's side as well. Mike, tell the listeners a little bit about yourself. You're currently the CISO at Passport Parking. Previously, you were at BB&T, which is now called Truist. Tell the listeners your story and what you do on the side, as I know you're also an entrepreneur. I think it will be good for them to get to know you.

M Mike Privette 01:21

Yeah, I'm currently CISO at Passports. I have been there for about eight months now building out their whole security program. Passports is all over the US and Canada as a mobile parking company. They also do tickets and enforcements, and really just enabling digital wellbeing for cities. The more digital and more equitable a city is, the better people live. And so it's a really cool mission.

A Aaron Bock 01:44

It's the beginning of 1984, right?

M Mike Privette 01:47

Yes, although I think we have a better, more altruistic goal.

A Aaron Bock 01:52

Ok, not controlling people's lives.

M Mike Privette 01:54

We just want you to just pay us some money and then we can help you do all kinds of stuff. Prior to that I spent most of my career in financial services, in some of the biggest banks like Wells Fargo or Wachovia, First Citizens Bank, BB&T, and now Truist. I also had a three year stint at MetLife, which was a gigantic company and I got some awesome global experience there. But you know, I've always kind of been around the highly regulated spaces, mostly in finance. So coming to Passport was a subversion of that, because we're a payments company. We facilitate payments, it just so happens that you're paying for parking, or you're paying for a ticket or citation if you parked incorrectly. Or you're paying for a permit giving you the ability to go somewhere. So it is a pretty natural fit in terms of the regulatory concerns and the compliance concerns, but also, being able to bring in some of the structure from a larger company who's way more established and has more people and building programs from the start. On the side I've had many entrepreneurial stints which I truly love. I jokingly tell people my hobby is monetizing my hobbies. So I like to find fun ways to make stuff. The one I like the most and that works best with my day job is my newsletter. It's 'Security, Funded' where I track cybersecurity funding and M&A events every week and summarize the news. And it's been fun to show that and watch it grow. It helps me stay on top of what's happening in the market. It also helps me see places I should be looking at closer. So yeah, that's me.

A Aaron Bock 03:38

Mike's being humble. He also deals with strength on the side. And this is one of his brands for strength lifters and power lifters. For those of you out there, we will put this in the show notes. Here in Opkalla one of the things we do is to evaluate upcoming vendors and new vendors. And Mike is doing that in his writing in Return on Security and Security, Funded. It's an early source for those looking in the security realm looking at what's happening and why. Who's being funded and what are big companies buying? Mike, thanks always for sharing those. And we'll get back to that in a little bit. I want to go back, so kick us off. At IT Matters we talk about what are IT matters why IT matters. Before we get there, I know you're CISO now and you've always been in security, but tell everyone if you started out of college or high school knowing you were gonna go into security or did it happen by accident? Or were you in IT before?

M Mike Privette 04:38

It was it was really by accident. I came out of college, right when Sarbanes Oxley was huge along with the whole Enron scandal and the mismanagement of financial controls. There was quickly like a global concern around IT systems that move money and people who have access to them. So I started off at college as a consultant at a public accounting firm doing IT stuff. And when I say stuff, I mean I would rack and stack a server one day, I would configure a firewall the next day. I would do a Sarbanes-Oxley audit the following day, I would make a VBA app, because that's how old I am. We would do custom Visual Basic for Applications apps in Excel. I'm using the term app lightly. I kind of had a niche there in banks, because many of their customers were banking clients. You know, when you start asking about basic IT controls there's a lot that compliance frameworks like Sarbanes-Oxley leave to desire. It doesn't quite go a step far enough. I started probing more and seeing how I could get involved in the very early days of security assessments. And doing like, what people might call an external penetration test and to include physical assessments and trying to wardrive or break into buildings in a totally legal manner. That piqued my interest. I saw that there was more here, and I want to go a bit further. Then I left public accounting. I actually went to Wachovia right before the merger with Wells Fargo. And I was doing third party security assessments for all of their customers. So I got to learn a ton about how all these companies handled and dealt with bank data and what they did for them. And that really kicked my security mindset into drive. That was a contractor role and after that roll I really wanted to stop asking questions and I wanted to push buttons. I wanted to do some of this work. I had an opportunity to go jump into the engineering side of the world at First Citizens Bank from my previous boss who hired me at Wachovia. So I said, 'I'll reverse audit all these things until I learn it.' And that's how I got into security. And then like, that was like a breakout role for me which cemented my love for security and all things in that space.

A Aaron Bock 06:52

That's awesome. I have a funny story I remembered as you were talking. I forgot you were in public accounting. I was a finance major and I graduated in 2009 when there was no jobs. I thought I was taking a finance or accounting role. And I ended up taking an IT audit role. So I was auditing all of the people and what they were doing inside of the apps and databases. So that's similar to my start although I didn't go nearly as technical as you and now I'm on the

evaluation of vendors and solutions side. For those of you who don't know, Mike writes a ton. I already mentioned Return on Security. You also write a lot about the career path or the job path to get into not only security, which I would say is where you spend most of your time, but IT in general. Over the last couple of years, I think that conversation has been coming up more and more about how to educate and what's the education path to get into security. For someone that is interested in eventually getting into security, whether they're a student right out of college and they are looking for their first job or they're midlife, and want to switch into IT or security. What would you recommend to them? How do they get started at this point where we're at in 2022?

M Mike Privette 08:11

That's a conversation that's actually pretty highly debated on the internet like many things. If you look at any other degree or any other career field, you have to get a degree in it to show you have a competence level. That's the bare minimum expectation to join certain parts of the workforce. But for many, many years, security was not like that. In fact, the people who were doing the hiring were actually anti-degree because they thought, 'there's nothing you can learn in a four year college setting, or even a two year college setting that will be relevant into what you're going to be doing day to day in the security organization at a company.' But what's interesting is that's now shifting. So as a certain demographic of the workforce is aging out or retiring, the people who were doing the hiring are now the people who have degrees in cybersecurity. So they have more esteem for that and they hold it in higher value. So if you had no other background in security today, I would tell you to go get a degree to start because if nothing else it's a gate check.

A Aaron Bock 09:12

Just a general cybersecurity degree or something specific?

M Mike Privette 09:17

I would say start with a basic degree. A lot of people who have already gone through undergrad are getting masters now in the program. I would say that wherever you're at on the undergrad versus grad side, focus in on that degree. That will give you an orientation on what is even covered in the field because the education side has actually evolved tremendously. I've talked to many people who hire people in security and a lot of them are not looking for specific degrees skill sets, but instead they're looking for people to understand the concepts and the approaches to security. Which is something that can be taught and that's something that would be good for a classroom setting to help you talk through concepts such as: why is authentication important, why is authorization important? Why should we talk about lease privilege? Why should we make sure that applications don't get abuse on the internet? And how can we prevent that? These are conceptual ways of thinking that can be packaged. And then you can then take those learnings and say, 'all right, now I have my full time job setting, how can I apply these learnings to this situation? I would say start there. Don't rely on just the degree though. There is far too much free stuff on YouTube, and far too much free stuff on GitHub that you can learn just about anything you want. I would tell people to go deep on a topic. So instead of trying to learn all of security at once, maybe you are interested in security

engineering. Or maybe you're really interested in incident response. Try to learn as much as possible about how that works and why that works. And then get the foundations of that instead of like focusing on a tool or focusing on like a particular framework. That will help you get in right mindset because your foot in is the door.

A Aaron Bock 11:05

Do you think it's an organization's responsibility to train folks who are going into the security field? And should they pay for it and come up with the criteria for how you go through it? Or do you feel that is on the individual to train on what they feel is relevant and teach themselves?

M Mike Privette 11:26

That's a great question. I think there's got to be a mix of both. Most people who are in the field want to improve themselves in some way anyway. So there's a constant desire to kind of level up your skills in that aspect. And I think you have to be that way if you're going to be in that field today. It's already very hard to keep up with all the changing news, let alone the technology you need to figure out how to secure these things. So I think people need to take it on themselves to do some of that. But I also think from a corporate standpoint, you need to look at what would be the best level of education for people there in general. This may be a hot take for some, but paying for a bunch of people to go get their CISSP, which is a very classic certification, is probably not great for the employer. It is great for the employees. Instead sending them to get AWS Certified is probably more applicable if you're a cloud company who does a lot of work in AWS. Yes, they can use that elsewhere, but if you don't invest in them in that regard and make it specific to what your organization needs, then either they'll go somewhere that will give them that or they won't have the information. Or they won't be as prepared as they could be. So I think there has to be a fine line of doing both company and person.

A Aaron Bock 12:41

Speaking of that, you mentioned Passport being very digital with a footprint. I would say it's a tech company for all intents and purposes. Not that banks are not tech companies, knowing FinTech. They're just very different. Let's kind of dive into being a CISO and being in security. How is security viewed differently in those two types of organizations? Maybe you'll start with defining like, what does a CISO do? Obviously, it's security. But what does that mean all day for an organization? And what are the misconceptions in those two organizations you deal with, and you've seen?

M Mike Privette 13:24

They are very, very different. So CISO, in general terms, is the person who's setting the strategy and the direction on how you're going to secure the business as a whole. That's just a broad swath of it. But really it comes down to making sure you understand what does the business care about in terms of, what is critical to make the business run? What data do we need to actually service our customers? And then how do you secure all the things around that,

and the pieces and components that actually serve customers, or that people rely on today. If you think about it from inside out, it's protecting the company from inside, including employees, out to the world. And then from the outside in, what's the threats coming in? To then affecting us as Passport customers or as employees. It's an inside out and outside in role in general. Where that changes between like large organizations, such as banks in particular, or other highly regulated things; typically when a company gets to any size IT is like a whole nation of itself. It's so big that it moves independently of the business and the business moves independently of it. But this doesn't always happen in a positive way. It's so hard to coordinate across so many moving parts that typically those organizations just do whatever they want. And then they let the fallout happen wherever it happens. Especially in highly regulated places security gets to do what they want. And there does not have to be a direct business impact or driver to what they're doing.The fraud space is the exact same way. You can say, 'if I spend this much money, I can reduce this much risk.' That sounds like it's a win no matter what. But really your larger companies and more established companies, one, there's so many products and so many different ways that the business works. You're just bolting on security around existing things that people have to work with. And by and large most people don't have a positive security experience with their banks as customers. But people just accept it, because people feel that, 'well, all my money's there, so I guess I deal with it.'

A Aaron Bock 15:35

I guess it's better than under the mattress?

M Mike Privette 15:37

Yeah. So there's a certain level of people accepting it as customers. So we have to do it because security is important and that's what we have to do. Now, contrast that with a product company or with a company that does not have the same lens that financial services companies do, and then you can't afford to operate that way because that product is the whole reason you have a job there. And if that product didn't exist and you didn't service the customers, you wouldn't have a job. You have to be very methodical about how you help them securely deliver what they're doing. And it is a much more succinct piece of the product and the consumer journey. Which to me is honestly the most appealing part. Because when you're in a large organization, you often have zero knowledge about what your downstream impact is to the business side. And how is it impacting the revenue, positively or negatively? You have no idea. You just exist to pontificate about security. You can't do that at places such as Passport, or any other product company like that. You have to be a lot more thoughtful and a lot more collaborative across all aspects. Your goal is to make the business as successful as possible, as securely as can within the risks that they're allowing. And smaller companies have higher risk tolerance than industries like banks and insurance companies who have an almost zero risk tolerance approach. So you have to be a little more artful in delivery.

A Aaron Bock 17:06

You touched on something that I have heard recently. I won't say as an argument, but you talked about ROI on security. Obviously security is important. Turn on the news or any alerts you get and within a couple minutes some sort of breach, or some fallout from a breach. This

past year, we've had a few major ones. But for an organization, I think sometimes security gets a bad rap. Because in some people's eyes there's no ROI. For them the only purpose is to prevent risk inside and out. And it's 100% prevention, and then remediation if something happens. But there's not like an ROI to the business for them. Do you agree with that? And if not, help these listeners understand where the ROI is outside of prevention and remediation for an organization?

M Mike Privette 17:59

That's a tough question. In 99% of cases, security teams don't have any kind of revenue impact. They're just a call center.

A Aaron Bock 18:07

Unless they are a security product.

M Mike Privette 18:10

Yes, and then it's a direct correlation. It's really hard to block all things. You can't prevent all risk, that's impossible. But the consumer expectations are so high that if you don't spend this money, then you're just negligent. It's not that its just a cost sink. It's more a course of doing business. It has to be done. And you can't do business without it today, at least not very long. It's one of those things that you have to be able to spin on its head and say, 'well, okay, knowing that it's maybe not a direct revenue driver, how can we then enable security to be a reason someone picks us?' How can we improve their process? And that's what I'm trying to do at Passport today. Most of our customers are governments and DMBs. They're extremely regulated and very particular about all their frameworks. So I want to have our program in tip top shape for them to the level they expect, such that say, 'okay, wow, that was actually really easy to deal with you guys, thanks for making that simple.' The way I'm trying to layer it in on Passports is to enable the RFP process and our customer outreach process to say, 'yeah, we do what you expect, but we also do more. Check this out, we really take your privacy seriously. We do all these things for security above and beyond of what we're being asked to do.' Yes that costs money but there is almost a goodwill factor that you're creating a reason for people to come and say, 'I like them better because they're a security minded organization, or a privacy minded organization.' While there are tools out there to help you do a little bit of attribution in terms of security helped sell this or we helped close this deal in some way. And maybe you get an attribution in Salesforce or something.

A Aaron Bock 19:57

It's really a pat on the back.

M Mike Privette 19:59

Yeah, a pat on the back. But you have to do it. And everyone knows the importance. If I'm being honest, it's doing it internally and externally, such as you're not an inconsiderate group

being honest, it's doing it internally and externally, such as you're not an inconsiderate group. You have to think about the user experience. You've got to think about the people aspect of it. And you've got to make people want to do it. And then some of those conversations about, 'oh, you spend money' disappear when you make it nice and easy and simple, or collaborative.

A Aaron Bock 20:27

I agree with you. I've seen customers lose RFPs totally unrelated to what IT and security as an organization. Except as part of the RFP they have to answer security related questions and IT related questions, and they lose. They can't even put their name in for the RFP. I agree with you. I think it's good for people to understand that. Before we go into trends, because I'm very excited to talk to you about trends - by the way, I feel like Mike's going to be on this podcast a couple times because there's so much trend analysis he does. But for the first time, let's talk about basics. Before we get there though, I understand you've been in different types of organizations doing security. You just talked about the differences. From a lens of a CFO, an accountant, a salesperson, or generally someone who doesn't have to deal with you. What's a misconception that people have about IT in general? And what IT is for a big organization? And specifically security. What are some of the misconceptions? What do you think they don't understand that you wish you could just tell them?

M Mike Privette 21:30

I think a lot of times those groups see IT in general as a big cost that doesn't work. Or it doesn't get them what they need. Everyone has a preference on how they want a system or how they want to operate. A lot of groups see that just as a barrier or as a guardrail. And they make work hard. It should never be that way. I wish that I could tell them, 'if you feel that way, bring it up a couple of levels and let's have a different conversation about what is it that you're group's not getting? And how then can it help you solve that? Or how can security help you solve that.' I think a lot of those IT and security groups don't have the best feedback methods. Especially from a business side. Or maybe they find low value in feedback from the business because in some large businesses they're a business under themselves and they do what they want. I'd say ask more often than you think is normal. Go talk to them and have a real question. If someone mentions poor experience, tell us about it. Because most people in general want to help, but IT people and security people want to fix your problem. Give them the shot to fix it. I think that's a big important piece that I wish they could say. Another piece of it too is that no question is too small. Especially on security, if there's something weird, let me know. I don't care how small it is. If you got a weird text message, I want to know about it. Because I'd rather you be in that mode of being forthcoming with the information and quick and collaborative with me. So then I can say, 'Oh, you know what, I actually know this is a non-event and you can safely ignore it.' Or, 'Actually, I would have never known that until it was too late. Let me dig in a lot deeper on this.' I know sometimes they speak different languages between finance and accounting and business, and it's kind of hard to understand what the others are saying. And sometimes they they miss each other a bit. I would say to try to be more open. That goes for the IT people as well. Try to be more open and ask more.

A Aaron Bock 23:27

It drives me crazy when I see projects, whether it's an initiative in finance, or an initiative with

some sort of product. And maybe its not directly being driven by security or IT like we talked about, but when you look at the project committee, or the steering committee and there's no one on IT, or no one in security, at least not even once a month or not in any part of it. And then all of a sudden they get through it and they ask IT to do things. But you should have them in there because they might be able to enable some of those things you're trying to do faster, easier, or quicker by just knowing that. So the good organizations view that as a part of the team, versus just as break-fix like you said. And I'm sure security's even worse. Sometimes I've heard terms like, 'The CISO is just the person that says no.' It's just, 'How do I get this past the CISO.' Well, there's a reason they do that. And you can look on the news and see why you might want to listen to them. We talked about big organizations, security, and IT. For folks out there that are part of smaller companies with 10 people, or 15 people where the big bureaucracy has nothing to do with them. You could look at this online but I'm curious of your thoughts. At the most basic form, if I'm starting my own little company and I want to make sure I'm secure, what should I do in security to make sure that like the basics are covered and at least most of the risk has gone on off the bat?

M Mike Privette 25:01

I'd say for a company like that, don't try to do anything yourself is where I would start. Stick with the basics. Don't overcomplicate your business. Stick with the Microsoft's or the Google's of the world. Turn on every basic feature they tell you to turn on. For example turn on two factor authentication in most places, use SAS apps and make sure they're always authenticating through your Google or other authentication provider. Those extra steps can help beat phishing attempts, which is still the most common attack in the world for businesses of all sizes. And they are the easiest way to compromise a business or fraudulently move money. Get some of those very basic things out of the way first, and rely on SAS providers and service providers to help you do a little bit more. You don't have to wing it all yourself in a spreadsheet and slowly figured out. The industry has come too far for companies of that size, of up to the 100 person range, especially if you're cloud based, to have to anything yourself. I would say look for those platforms that can help you lean into a compliance framework. Although we know compliance is not security, it's at least a roadmap. And it can at least give you some basic things that make you better off and not negligent. It helps you get there and it can then help you secure other parts of your business as you go. So then you can focus on growing or making money and not having to run security as a full time job yet. That time will come if you grow as a company, but you don't have to overthink it. That is what I would say.

A Aaron Bock 26:40

So let's go on the flip side. Let's say you're taking over security at a large organization, a couple 1000 people. This has no correlation to anywhere you've worked for in the past. This is not insinuating any of those companies are not secure. But say that you walk in and it's a dumpster fire, the processes are bad, the tools are outdated and nothing's updated. The people are really not qualified. So you're now taking over CISO. And someone says, "Mike get us secure." I've seen a lot of debates online saying, "Well it depends, security is about people, or security is about process. It's not about tools and things like that." But I also have seen these same organizations get hacked, because over time they can't get stuff figured out in time. If you walk into a situation like that and the people, the process, and the technology is all a mess,

what do you do first? Like how do you start sleeping at night as a CISO in that type of organization? Like where do you pull the triggers to get the most secureness in an organization like that?

M Mike Privette 27:46

That's a tough one. And that's not an easy job. But I do not want that job by the way.

A Aaron Bock 27:51

Hopefully, no one has to take that. But I know that there are companies out there that just haven't focused on it.

M Mike Privette 27:58

Honestly, you'd have to start doing an inside out review and ask, 'what is it that we actually have in terms of the people, process, and technology.' I would do a thorough evaluation of your talent at first. And then you also want to look to see what have we already committed to as a company and as an organization? Which compliance frameworks that we're looking at? Which regulatory bodies do we have to answer to? What do our customers expect? Basically reverse engineer what the full scope of security is at a company like that. I think that's where the nuance is going to come from. Security's is going to look a bit different at most places depending on your business model. And depending on how many people you have, where IT sits, whether it's a sales driven organization or not. But a thorough vetting of, 'what do I have'? Especially from a people standpoint, that will help you determine, "alright, based on what I've heard and based on what I've seen, are the people I have in the seat right now the right ones to solve it?" And if they are, why aren't they solving it? And if they're not, then we need to fix that. But rarely is it ever going to be a, "let's buy a bunch of tools." And rarely is it simple enough to say, "Oh, we just have to to fix a bunch of processes." That's a nightmare in a big organization because things are so ingrained in the process and policy, even if they're not right. They will still be ingrained. I would also suggest a company like that quickly hires an outside counsel or outside consulting firm to come give them a maturity assessment. Then that way you can have the ability to lean on fresh eyes from another company's perspective who's seen a bunch of companies, presumably like yours. And they can give you some focus areas to work on. And then you use that to determine what your risk levels are. Then that risk level and that get better plan is going to drive your whole roadmap. That's what you're going to have to go back to your leadership with and say, "here's where we are, here's where we need to be, and here's the delta between those things." In order to do that, we're going to have to invest in this kind of technology, we're going to need to hire this kind of people. Maybe we need to stand up our own security operations center, or maybe we need to outsource it." But without that general assessment it's going to be really hard for you to make a gut call. Especially when you're faced with all of those things happening at once, you're not going to know which dial to turn. You don't have to do it yourself is what I would say. So I'd quickly look to bring in that. I would also say, on that same vein, figure out how to do incident response. If you don't understand how that process works, you're going to have to do it in an unfavorable position when it's a real deal. And nobody wants that, nobody wants to know that you don't know what you're doing at

that point. I'd say focus on those two areas first, and then that will show you where a lot of failures happen in process and tech and skill set. And then you have to keep iterating on that. But that could take years at a big company, you know.

A Aaron Bock 31:05

You sound very qualified to take a role like that, I'm gonna be honest. But we'll say you're not in the market for it. You mentioned iterating at the end. And this will be my last question before we wrap up with some of the trends, because that's what I know you're more interested in talking about anyways. But iterating. Say it's the company we just described, they're a mess. Let's say over the first year and a half that you do your assessments, you figure out your maturity, you start implementing either tools, processes, or you hire the right people. You're working off an assessment that was done, let's just say 18 months ago. How frequently do you feel companies should get assessed? And is it the same full assessment every two years? I think people don't understand assessments and the frequency of them.

M Mike Privette 31:52

It depends because some regulated industries require internal self assessments, which are very subjective. How can you really trust that some of the time? I think at a minimum, even for your audit committee, or for regulatory filing reasons, you should do an annual assessment of some sort. It may not have to be like a full blow the doors off the place assessment, but you should at least have an understanding at a strategic level. And at a capability level. And when I say capabilities, I mean security capabilities. Do you have the ability to do incident response? Do you have the ability to contain a malware outbreak? And then what happens from that standpoint? And do you have the ability to recover your assets? And do you have resiliency in the business? You need to stay on top of that constantly. What often happens in large organizations, and this is the challenge, is that you have to spend multiple years fixing the sins of the past. And it's extremely hard to do the new things, or fix the things that should be fixed. Because you're filling up all your time with large projects to solve first principle problems that should have been solved long before anyone's time there. But for one reason or other businesses grow into a Frankenstein monster, and then that's what you have. And so you're left to secure around that system that's too big to fail. So getting that updated is often going to be good. If nothing else, it'll help you have orientation about how you're tracking. You can report that to your executive team and to the board. So you can then see, "Are we spending our money in the right places, still? Have we improved, number one?" And you can ask, "Can we divert money to different places or focus on different areas?" And it will give you an idea of how the outside competitor set is doing on that as well. This is a very common exercise in banking, where banks pay an external search firm to help them understand how much money other banks are spending on security as a part of IT budget every year. There's value in that. Just so you understand that they're growing at X rate, we're growing at X rayed. Maybe they're a 5000 IT person company, and we're 2000 IT person company. This gives me an idea of where my budget probably should be in relation to theirs, in terms of spending. It's not always a rubric you have to follow, but it gives you an idea of, "Am I keeping pace with customer expectations and industry expectations?" You should look to try to do iterations at the smallest level possible outside of the assessments. If your incident response team can do an after action report after every incident that happens and they get better each time then that's progress. If your engineering team figures out ways to make the software deployment process or the image

creation process or the server imaging process simpler, easier, or faster then that's a win. You have to encourage that and set the tone of the top of that, as a CISO. That's the kind of outcomes you need. Once you start iterating on that, you'll create a good flywheel, and then you'll start to slowly catch up in areas and even surpass places where you expected to be. It really comes to controlling your energy and controlling where you can turn the dials up at that point. It's very little about security and more about, 'where can I make incremental, gentle progress'?

A **Aaron Bock** 35:31

It's the get 1% better each day, that applies very much.

M **Mike Privette** 35:36

That's very much a security mantra. If you're interviewing for security, say those words because that's good. People like that. You want to fight the good fight and play the long term game with long term people. That's positive.

A **Aaron Bock** 35:48

There's free advice on how to interview. I have couple a couple questions before we go, so lets switch gears. You write Return on Security, and Security, Funded. You write about companies that are getting funded. You gain a lot of insights, and we gain on insights from seeing, "Last week I emailed you and said, holy crap I can't believe they just got half a billion dollars of funding for this tool." I'm curious right now, we are filming this May 6. If you're going to go on a show on CNBC or MSNBC about the forecasts for 2022. What is the security tool, or hot trend forecasts for 2022 that you're seeing and what people are investing in? And what you think you're going to see more attacks or breaches on? Tell me about general trends and security for the remainder of this year?

M **Mike Privette** 36:44

I think there's a couple of key trends that are happening this year that have already kind of started earlier in the year, but are going to increase. Anything related to IoT and operational technology is going to continue to skyrocket. The Russia-Ukraine situation exacerbated that. And there's a big need for that now because people realize how insecure and vulnerable critical infrastructure is. Same for public works, city water systems, or sewage systems. It's scary how old the technology is that runs all the services and how immature or non-existent security is around it. Even for IT, because some of these systems don't even have IP addresses, if you can believe it. It's scary to think of what could happen and the potential human impacts of that. Anywhere in that space that crosses the physical and cybersecurity realm is going to continue to a huge investment spot.

A **Aaron Bock** 37:40

Let me ask you really quick on that. You said the Russia-Ukraine conflict is pointing out a lot of

Let me ask you really quick on that. You said the Russia-Ukraine conflict is pointing out a lot of inefficiencies or inadequacies. Is there something else driving it besides just more monitoring and IoT being better technology? Or is there another breach or attack that you would point to that you think is causing people to focus on it more?

M Mike Privette 38:03

There's been a couple of local cases in the US states where people are attacking water treatment systems. I think that happened more than once in Florida. It is becoming more opportunistic, either driven via nation states or driven by individuals whoa are looking to cause some form of chaos. The world is getting more volatile in some ways. I would expect there to be repercussions in a different manner, or even domestic terrorism happening in some way through cyber methods as well as physical methods. It's a continuing trend. And intelligence agencies are also heavily tuned into that as well. But that's a growing area of concern. I think people are just now realizing how fragile some of these systems are. Looking at what happened in Texas when they had the big winter storm and their power grid failed. And that was just a mother-nature calls situation. It probably wouldn't be that difficult from a technology standpoint to make that happen again. It's important to ask how to build more resilient cities in light of climate change and all of these other external factors, in addition to human factors and tech. I think a lot of that's been driven by a multitude of forces.

A Aaron Bock 39:18

So IoT security is huge. What else do you think people are going to be asking about buying in 2022? And why?

M Mike Privette 39:29

Software supply chain security is another major topic. You might hear software bill of materials or SBOM. If you look back at the SolarWinds breach and how the attackers injected themselves into the code delivery process for SolarWinds. They got bad actions set inside legitimate software. And that's how they are able to compromise everything. Before these events understanding what libraries you use, or what third party services, whether it be open source or otherwise, was never that much of a concern because it was never turned against them as an attack vector. Going back to the Russia-Ukraine situation, there's increasing 'protestsware'. People are now injecting geographic specific attacks or maybe they're disabling the service based on where a person pulls the repository from. Or from where their repository goes. And so they can say, "Hey, we don't support what you're doing to Ukraine, so we've now disabled the software in your country." And corporations can't stop that because many of the things that run such as corporate software or enterprise software is run on open source software and is managed by like one or two people. Trying to safely ingest software and use it for commercial use all around the world is a challenge. I think the concept of treating all software that the company itself did not create as hostile will become a pervasive thought. It might be where there's only certain repositories they can come from, and they're all copies of the original. And maybe the originals are inspected to an nth degree before they're allowed to be into the organization's copy.

A Aaron Bock 41:07

I assume these are enterprise technologies, because we haven't seen these necessarily as much in the mid-market space. Do you think it's coming? For people that are sitting here listening for a 150 person company, what can they do if they can't afford a software supply chain technology or investment to review?

M Mike Privette 41:32

I'd say it is coming for this small to mid-size market. My general business advice would be: don't run the software all on your own, use a SaaS product. Let somebody else handle that. But if you have to bring in the software, or if you have to develop it yourself and you don't have the means to interrogate the software lifecycle around that, then it's going to be a challenge. The attackers have proven that the size and the organization doesn't matter. And neither does the monetary value associated with them. They are often just opportunistic. If they can find that a small business uses a particular piece of software that they can exploit, they'll try to exploit you and everybody else who uses it. It's more along the lines of casting a wide net. Even in just the last five years, small and medium businesses have realized that they're not safe from the attacker net anymore. I would say to be smart, and try to get a better handle on how your developers are bringing in software. And the concept that many startups are built off of a combination of many different software's is relevent. That goes back to the Frankenstein set of systems. But if you can streamline on only developing in Go, or only developing in this form of JavaScript, or these types of libraries then you can limit your blast radius a little bit. But you're still going to be dependent on those upstream systems and updates. So having a strong technology team, or a strong developer team who can understand the risks and trade-offs with delivery, is going to be really hard. And I won't even lie, it's gonna be hard to do, especially when you're in the mode of growing. It's something I think will cascade down. But in the same turn, I think the commoditization of that kind of software is gonna get cheaper.

A Aaron Bock 43:23

It seems like it could scale. An enterprise would review a vendor. And once you review one once it feels like you could push that down to others. I could see that over time getting less expensive for mid-markets.

M Mike Privette 43:33

I think so, especially if you leverage any of these cloud hosted code depository platforms such as GitHub, GitLab. There's often things that the tech industry as a whole has to level up. For example, back when Amazon Web Services was out, every other day you'd see a breach in the news from a company who didn't configure AWS correctly. Over time, they built in either checks to say, "Hey, this isn't configured correctly, you should turn this on." Or they default activated some of these services so you don't shoot yourself in the foot. I think there needs to be a broader lift of industry level in the same way that Microsoft forces updates to computers everywhere now. You can't opt out of it because they know the tech service they bring. It's a general public service. They have to do the right thing for the world.

A Aaron Bock 44:30

My computer was trying to restart about five minutes ago. That's why I was looking down into the corner and I was like, "No, don't do it right now, wait till tonight." Relating current trends, and I'm putting you on the spot here, in the United States inflation is a big topic right now. People are speculating a recession, etc. Do you see any security risks that will come out of that?

M Mike Privette 44:56

I think money is always a driver for any kind of attack. And that's what drives most cyber attacks in the world. It would not surprise me if there was an increase in phishing or business fraud related things around inflation relief. Or around some kind of debt relief. These attackers are always very opportunistic. But that happens with any news cycle. There's always going to be attacks related to those kinds of things. I'd say on the investment side, people are probably going to stop investing on super new, or untested technologies as much. It'll still happen but I've already seen this year that there's been an uptick in acquisitions. Way more so than last year already. And I think that's largely due to the fact that investors are a bit nervous with where the markets going, and they're a bit nervous with their money. But they still have a lot of money to deploy so they try to look for ways to make safer bets and safer acquisitions. So why not acquire a business that's already making a lot of capital, as opposed to trying seed or Series A round on this startup that may or may not make it through this downturn. But even still, there's no slowdown in overall funding. It's still picking up and going extremely fast. I keep a leaderboard, but there's already been around $7 billion of funding just this year already. That's just in what I've been tracking. And there's been around $29 billion in acquisitions. It's definitely not slowing down, it's just shifting.

A Aaron Bock 46:32

We'll have a whole nother episode dedicated to the funding and why and how. But for the sake of time, I want to let you go and let listeners go. For my final question, it's the question I ask everyone. We've been talking a lot about security, big organizations to small ones and how to get secure. If Mike Privette gets to give a State of the Union and he's speaking to multi-millions of people, because everyone's going to come out and see you, what do you tell them?What's the message you would want to tell the most number of people, whether it's personal, about cyber cybersecurity, IT, or career-wise, what would you tell them?

M Mike Privette 47:12

If I had this kind of audience I don't know what I'd say.

A Aaron Bock 47:15

We'll say it's the common man or woman.

M Mike Privette 47:18

I would say to be wary of what you're trading off for ease of use. In general be more vigilant than you think you should be. You can't get some of this stuff back. Once your information and data is out there, your best bet is to limit the blast radius of it. So be careful and beware of the trade offs. If you're not paying for the product, you are the product. So think about that.

A Aaron Bock 47:45

One of my customers has that T-shirt, by the way. I'll wear that the next time. If you're not paying for the product, you are the product.

M Mike Privette 47:54

I think people are generally more aware. But don't stop now. Keep it up.

A Aaron Bock 47:58

Yeah, that's good advice. Mike, thank you for joining the show. For the listeners out there, thank you for joining. We look forward to having you on again. Thank you for all the writing that you put out to the world. If you have not or you do not subscribe today, I highly recommend subscribing to Mike's newsletter Return on Security and Security, Funded. We will put it in the show notes. Mike, thanks again. Have an awesome rest of the week. Have an awesome rest of the week to the listeners out there. We'll talk to you soon.

M Mike Privette 48:27

Awesome. Thanks for having me today.

N Narrator 48:28

Thanks for listening. The IT Matters podcast is produced by Opkalla, an IT advisory firm that helps businesses navigate the vast and complex IT marketplace. Learn more about Opkalla at opkalla.com