Micro Focus Reimagining Cyber Episode #38 Taylor Hersom

Thu, 7/21 3:51PM • 23:04

SUMMARY KEYWORDS
security, people, sock, cyber, cso, business, started, startup, cyber insurance, customer, automate, realize, reimagining, taylor, organization, virtual, companies, tied, data, stan

SPEAKERS
Rob Aragao, Stan Wisseman, Taylor Hersom

Listen | Read

Taylor Hersom 00:00
Oh. So, the way I describe security in general is it's very much a loop and not aligned. So, I think people need to realize that as soon as they start it, they can't stop it there is whether you're pursuing SOC 2 or you are doing customer security assessment questionnaires. Those don't just happen once and then they're done. You have to maintain that SOC 2 at a station, you have to answer those questionnaires every year for the same customers. And so first realizing that that this is something that once you start, you can't technically stop.

Rob Aragao 00:37
Welcome to the Reimagining Cyber podcast where we share short to the point perspectives on the cyber landscape. It's all about engaging yet casual conversations and what organizations are doing to reimagine their cyber programs while ensuring their business objectives are top priority. With my co-host, Stan Wisseman, Head of Security Strategist, I’m Robert Aragao, Chief Security Strategist. And this is Reimagining Cyber. So, Stan, who do we have joining us for this episode?

Stan Wisseman 01:04
Hey, Rob. Taylor Hersom is joining us today. He is the CEO and founder of Eden Data, a cybersecurity firm that focuses on the next generation of businesses that are ready to build security and privacy into their DNA. Now, Taylor started his career at Deloitte, where he focused on Fortune 500 companies and their security compliance needs. And from there, he went on to be CSO at Renaissance Systems, and soon thereafter identified a market opportunity that led to his launch of Eden Data. And that's what we're going to be talking about today. Taylor, it’s great to have you with us. If you wouldn't mind expanding a little bit more on your background for our audience.

Taylor Hersom 01:41

Absolutely. Stan, and Rob, thank you so much for the opportunity. First of all, you did a great job, Stan, I don't have too much more to add. I sold my soul to the Big Four, started there and was doing IT audit, realized how awful that was and transitioned into cybersecurity, right when it was becoming pretty popular, and was able to learn a lot of things in a short period of time and touch a lot of cool brands in the Fortune 500 space. And then when I took my position at RSI as a CSO. I was definitely learning as I was drinking through a firehose, essentially, and was able to work on internal security, and then also start to get a taste of building security for other programs in another company, so I made the brilliant decision of quitting my job the week before COVID started. And that was, that was a fun adventure. So, Eden Data kind of spurned by accident from that, and I had started to figure out I had built on Upwork, and realized, Oh, my goodness, the startup space, specifically, there's just a lot of opportunity here, there's a lot of companies out there that need the help with security, they don't want to pay for the Big Four, they don't want to pay the big corporations. And there's this issue of consulting firms that you might want to work in.

Stan Wisseman 02:57
As you said, you sold your soul, and you're working for one of those big firms that pretty much, you know, serves that larger enterprise. And, you know, I guess that's the gap you identified, right? The fact that you had these smaller firms that have similar needs, but just can't afford those kinds of consulting rates.

Taylor Hersom 03:16
Exactly, yep. Yeah, and even just the “I'm gonna charge by the hour and take as long as humanly possible to do everything,” that model doesn't work. So well, either, whether you're Big Four or even the boutique consulting firms that are doing that.

Stan Wisseman 03:29
But specifically, I think, you know, what we'd love to talk to you about is that service that you're providing, you know, that's been labeled by yourself and others as the virtual CSO. And so, can you expand on what that is and why you think there's a need, especially for the SMB market?

Taylor Hersom 03:52
Absolutely. So, the way that I look at it is now in the 21st century, we're in this weird stage, where just about every data, or every company in the world is a data company. It doesn't matter if you're a SaaS provider, or you're a flower shop down the road, you're collecting some kind of sensitive data on your customers. And so, because of that, you need access to some kind of cybersecurity help, whether that be just consulting or have F professionals on staff. And so that that suddenly opens the market up to just countless brands out there that need help with security. And a lot of them either don't see the value in investing in a full-time resource, or they can't find a full-time resource, or they simply can't afford a full-time resource. And so, this fractional model, it's not new. I didn't invent it by any means. The fractional model works really well in those scenarios. And so basically what that is, is you're getting access to someone part-time instead of full-time to be able to come in and give you the security leadership and the security guidance that you need to be able to establish a security program internally at your organization.

Rob Aragao 05:01
So, Taylor, you know, that's a great niche, right? Because the SMB market has kind of been neglected from a cyber perspective for quite some time. We had some conversations, actually recently, we spoke with Ty Sbano, who's the CISO at Vercel. It's interesting, right? So, he's worked for some very large organizations through his career. And over the past few years, he's kind of pivoted into being the startup CSO, so we talked to him about, you know, just the speed of these of technology-oriented companies. So, the speed of technology, the go to market, the time to drive and deliver new service capability or new products, and security having to be attached that. So out of curiosity, what are you seeing on your end? Are you getting pulled in? I guess, from a customer perspective, are there certain verticals that you're seeing yourselves align more with and supporting them? Are there similar kinds of blueprints that you can apply to at least kind of get them started and continue moving them along the way and obviously, realizing each businesses is different, and you have to maybe make some kind of nuances changes, as you're going along the way and working and engaging with them.

Taylor Hersom 06:04
I think you've touched on such an important point, as it relates to security across the board, whether you are a startup or a huge organization, a lot of security applies the exact same across the board. And I think vendors will try to convince you otherwise. But if you go look at the cybersecurity trends of 2022 and 2021, and further back, they're always the same. It's always people clicking on bad links, it's always cloud misconfigurations. It's always ransomware. And a lot of the attack vectors are the same. And so, I think that back to your point about blueprints, absolutely. Eden Data's found this, this niche of us serving SaaS startups, mostly, that are in all industries, but they are all in the same vertical in the sense that they provide a software service to other businesses, a lot of the technologies they use a lot of their processes is all the same largely. And so being able to take a lot of the complexity out of out of building a security program and just bring in “Hey, this is exactly what you should do. This is the technology you should use to do it. This is how often you need to execute on it.” That's the guidance they're looking for. And that's what we're building, it can be commoditized to a certain extent, because a lot of the risks impacting a healthcare startup are impacting a Fintech startup as well.

Stan Wisseman 07:25
So, is one of those blueprints are recognizing that most SaaS offerings have to go through a SOC 2 add a station? Are you looking at, for example, SOC 2 controls and saying, “Hey, this is at least a minimum set of things you need to be thinking about?”

Taylor Hersom 07:42
All day, every day, Stan. Yes, SOC 2 is huge in the startup community, I think basically in the US at SOC 2 beyond the US it's of course, ISO 27,001. But everybody and their mother is asking for a SOC 2 out of station report these days. And so, these poor startups down to even just a few employees are already being demanded of their customers and their prospects that you need to have a SOC 2 report in place. And I'm sure you guys have experience with the SOC 2 language from the AICPA. But I mean, it's like reading Pig Latin, and then you go into ISO 27,001. And it's even more confusing. And so it's just, it's a weird time that we live in, where you can be a startup that has, it’s some guy and his dog, and he's selling to GE, and like, it's just, it's a cool era in terms of entrepreneurship, but that also creates implications from a security standpoint, where you have to focus on security from the get go.

Stan Wisseman 08:39
So go ahead, Rob,

Rob Aragao 08:41
I was just gonna say, so I think Taylor you're going into a direction I wanted to delve into a little bit deeper, which is, you're absolutely right, it's kind of the easiest time to be able to spin up your business, right. And there's so many different platforms to be able to take advantage of many of the different types of businesses coming to market are doing so by leveraging, you know, SAS solutions, leveraging cloud service providers, and so on. I wonder how many times are you guys kind of getting pulled in after the fact what I mean by after the fact is, you know, this organization has come up online, they're using, you know, pick a CSP, they think they have kind of the quote, unquote, inherent security controls all covered, and they're in great shape. And they don't have any worries about cyber. And then all of a sudden, they realize, “whoa, this is a shared responsibilities model. I do have some skin in the game.” And they make the call to someone like yourself and your organization and now come back and like, you know, what's kind of that trigger point that you're seeing out there and how much of that ties back into what their initial thoughts were with like a CSP doing it all and covering the security aspects as well and then realizing, “I actually on the hook for some of the stuff myself?”

Taylor Hersom 09:50
Yeah, that's honestly that's the majority of our business, I think very, very few times is someone being proactive about security, and fundamentally, it makes sense. You don't want to go put your money into something that you don't understand the returns for and in a lot of people think that security is purely a cost center, and therefore there's no return on their investment. So usually what happens is they think that, that they've got security dialed in, like you said, Rob, or some people, if I had $1, for every time I've heard, “hey, we use AWS and their SOC 2 certified so I'm covered.” It's, it's like, once they have the realization that they're not covered, and they lose their first deal, or they get hit with their first angry customer email. Or they even get some kind of scare from a regulator than they're usually suddenly shifting their focus on what's important and what's not. Interestingly enough, it's usually not the first deal that they lose, it's got to be like the third or fourth, they start to realize that, oh, my gosh, “I'm starting to lose a lot of deals, and they're all coming in at once.” And all of a sudden, everybody's talking about SOC 2, and, and then they talk to vendors, and they realize this is a four to six month like investment for you to be, and you're just so far behind the eight ball, that you're jeopardizing a lot of deals, and it seems like it happens instantly. So that was a long-winded way to answer your question, Rob. But it usually is reactive instead of proactive.

Rob Aragao 11:18
Yeah, exactly. No, it makes sense. I think I think it's just people come in and use it, right? They look at it as perceiving it as cyber specifically being a cost center. But I think there's certain elements that you can pivot into showing how it can be a competitive differentiator, it's going to enable them to win more business, as you said, right? It's that second, maybe third, maybe fourth contract that they just lost and realize that we're losing, because we're not beating the security requirements needed of that organization. Hence, that's a great example of saying, you know, let me enable the business and support you this way.

Taylor Hersom 11:48
Yes, and I think the only thing I would add to Rob is another element that oftentimes we see in it, it breaks our heart is that they will think they can take on SOC 2 by themselves. And so, they will, and this is like, actually SOC 2 is just an example, I think they think they can take on security by themselves. And suddenly, if you go through a SOC 2 audit, and you have a material finding, and your report is qualified, like that loses deals, that ends up being even worse than then saying, “Hey, we're preparing for SOC 2, and we're investing in it. And we'll be done by this date.” We see that quite a bit where someone already comes to us with a black eye and asked to fix the fallout that was created by that.

Stan Wisseman 12:30
So, circling back to the virtual CSO role, I had the opportunity to serve as a CSO, but it was a larger organization. Where do you see folks making that decision of either, you know, finding somebody to fit in the role full time versus leveraging a service like yours as far as a virtual CSO kind of role, or more of a transactional thing? Again, if what they need is a SOC 2 add a station report, then is that all they need to do? Or to your point, they recognize they need to do other things, too, and they need to have more of a continued support?

Taylor Hersom 13:10
Yes, that's a that's a fantastic question, Stan. So, the way I describe security in general is it's very much a loop and not a line. So, I think people need to realize that as soon as they start it, they can't stop it there is whether you're pursuing SOC 2 or you are doing customer security assessment questionnaires. Those don't just happen once and then they're done. You have to maintain that SOC 2 at a station, you have to answer those questionnaires every year for the same customers. And so first realizing that that this is something that once you start, you can't technically stop, I think the way that we describe it, and I realize I'm bias here, but any time you're under 500 employees, I think that there is actually value in going the virtual route or the vendor route. I do think that as companies get past that 500-employee mark, you need to have some kind of internal stakeholder, it doesn't necessarily need to be a CSO. We've seen people get by with compliance manager coupled with contractors, we've seen people with just senior security analysts. And then I think that the way we'd like to describe it as your security team needs to be about 1% of your total headcount. Point five to 1%. And people don't realize that that's like that's, that's a pretty significant investment. So, you go look at the salary of a CSO and a data compliant or a data privacy officer compliance manager. They start to add up a lot and I think I truly believe that especially for the startup and scale up market, you can replicate and use a lot of the you can usually get more value out of contractors than you can out of hiring full time. And the reason I say that for the security industry specifically is because there is a ton of volatility there is the whole issue of people getting poached left and right. And people being unfulfilled because we're all humans that that you've is exacerbated in the security space and then of course, the fact that people get overworked in this area. And so, you start to invest a lot of money into resources that aren't all that reliable. And I don't mean that to knock on CSOs or security professionals by any means. But it's the reality that we're seeing. And so, at least with vendors, you have that ability to get dedication, people will, I guess, always take your money for lack of a better term. And so usually the smaller companies can get by for a long time with using third parties.

Rob Aragao 15:29
Taylor, one of the things that I'd like to kind of get your, your thoughts on, and I'd be interested to hear how you're working with your customers on this is around the topic of cyber insurance. Right. And we've seen such major changes in this past year and the cost associated to policies, and you know, they're really turning up the screws and increasing the requirements, right, of course, but also like, you know, now that means these organizations, a lot of them that you're working with, are now needing to put further investment into some different tooling, and so on so forth. What role do you play, you come in and kind of even negotiate some of those different policies do you go through, and you work out of curiosity with maybe some other third parties that kind of have, you know, time with cyber insurance plus solutioning tied together, just out of curiosity, kind of what's the world of cyber insurance as relates to the customer base you're engaged with?

Taylor Hersom 16:19
Yes, we are pulled in on the cyber insurance discussions, because we usually are the ones filling out the application, at least on the supplemental side, so filling out the questionnaire on what's in place today. And then we're typically working with the cyber insurance provider to say, "hey, what do we need to change in the near term to be able to lower this rate." And then we're usually using the discretion of the insurance provider to be able to provide a quote on how much coverage a customer needs. And it's kind of tied, ultimately, people think it's tied to revenue. And the way that we look at it is actually tied to how many records you hold how many production records have PHI PII that you hold. And there's a calculation that we do to be able to produce an estimate on how much insurance you should be holding. We also help with like HIPAA, this is something that people need to look out for. But a lot of the cyber insurance claims have gone up dramatically, and they're removing coverage benefits. So, a lot of them are trying to remove the clause about having an incident response team and being able to have like some of them will offer you discounts on endpoint solutions on security solutions in general. But there as cyber insurance providers are losing their bums on all of these breaches, they're starting to get smart with their language and what they will cover and what they will not. We've seen some horror stories there. So, we usually get involved on the postmortem as well.

Stan Wisseman 17:49
So, Taylor, our podcast name is Reimagining Cyber, and you've already discussed some of the aspects of where you think cyber is going. Right? Your service around virtual CSOs is an example of rethinking what's needed and how to provide that as a service to customers, right? Where else do you think, you know, the next phase of growth or change is occurring, and how you're going to help address it?

Taylor Hersom 18:17
Oh, my goodness, I could probably go an hour here. But I'll talk a couple things, Stan. So, one of the big trends that I am looking forward to is automation in the sense of automating controls and procedures. So, the biggest issue to security right now is human error and negligence. And so, if we can remove some of those factors all together and have a computer have AI or having that be automated in some facet, that would be ideal. And that's the direction we're moving. So, you're starting to see a big push of GRC (Governance, Risk, Compliance) tools. You guys have been in the industry long enough to know like the former GRC tools were awful. They were no offense, if they're listening to

today, and I won't say any names, but today, you can get a GRC tool for as little as 500 bucks a year, like their GRC has become very commoditized. And you now have the mechanism to build controls, policies, procedures, but they are also integrating into your AWS environment. They're integrating into your HR into your background check provider, and they're starting to do automated checks and balances to see that you're facilitating and completing

Stan Wisseman 19:21
Giving you that visibility then write the bill. Is your hygiene really where it needs to be?

Taylor Hersom 19:27
Exactly. And so, another example is like internal audits. Internal audits are needed, especially if your cloud environment so going and testing your configurations periodically. And oftentimes that happens on an annual basis. We, and other companies, have worked on ways to be able to automate that and to do more continuous internal audits, because internal audits, I know the word auditor scares everybody away, but those are the good guys and gals, because they can report a red flag before you go through the real test of an external audit. And so, it's starting to see a trend in that direction as well. I would say outside of that I think that technology is expanding rapidly, of course, as we all know. And so being able to have more insight into third party applications, and what their security posture it's coming around the bend, we're not there yet. Right now today, you send people on SAQ (Self-Assessment Questionnaire) and you have them fill out hundreds of questions and make their life miserable. And you hope that they answer it truthfully. There is going to be a time when we are able to automate a good portion of that and check for the things that are actual risk objectives. Surprisingly, a lot of those SAQs haven't been updated in years. They're not tied to current risks at all. They're just asking every question under the sun, and honestly, there are legal coverage there, CYA more than anything. So that's another trend that we're seeing in the industry is all.

Rob Aragao 20:55
Yeah, I think you hit some key points there, especially the topic of automation, right? Where the more that we can do to just kind of facilitate the customer requirements and ensuring that they're really being much more efficient overall. GRC was a great example of that, right? It's kind of so repetitive, why do we continue to do these things. And there's so many more opportunities to hook into these systems like HR, as you said, as being part of the whole kind of ecosystem of what GRC really should have been all along. So, Taylor, you know, talking about something that we've not discussed in all the different episodes we've done, which is really more of the SMB space, what the needs are of that space, right, and the business model that you've been able to develop, and then take forward, right, I think it's just a great topic. It's a great service that you're offering backup to clients in that particular market segment. So, we appreciate you coming on and sharing the story and sharing the path and journey you've taken on one that was very risky at the time, right when you did it. But obviously, it's worked out very well for you. So, thanks again for coming on and sharing with us.

Taylor Hersom 21:52
Rob and Stan, thank you so much for the opportunity. It seriously means a lot.

Stan Wisseman 21:55

Thanks, Taylor.

Rob Aragao 21:56
Thanks, Taylor. Thanks for listening to the Reimagining Cyber podcast. We hope you enjoyed this episode. If you would like to have us cover a specific topic of interest, feel free to reach out to us and you can find out how in the show notes. And don't forget to subscribe. This podcast was brought to you by CyberRes, a Micro Focus line of business where our mission is to deliver cyber resilience by engaging people process and technology to protect, detect and evolve