Cybersecurity Risks and Business Context

Jeremy Snyder
Hi, I'm your host Jeremy Snyder, and I am delighted to welcome you to today's episode of the Ask A CISO podcast.

I'm the founder and CEO at Firetale.io, but on today's episode, we are delighted to have Fausto Lendeborg from Secberus joining us today.

Fausto is the co-founder and Chief Customer Officer of Secberus, a cloud security governance platform. Fausto has always been involved in cybersecurity. He was employee number 14 at Prolexic, later acquired by Akamai.

He co-founded Zen Edge, which helped secure critical IT systems deployed via cloud, on-prem, or hybrid hosting environments, and he served as the SVP of security before creating and becoming CEO at Secberus.

Fausto began his career 20 years ago when his self-made entrepreneur father mentioned that cybersecurity would be the most in-demand industry in the next millennium, and his mother's career at Cisco provided him with an excellent learning resource as well.

At the age of 14, Fausto became fascinated with the inner workings of computers, networks, and hacking. Fausto's uncle even invited him to his computer engineering seminars at Miami Dade College, so he's a natural-born technology enthusiast who's been polishing his talent for decades.

Fausto, thank you so much for taking the time to join us today.

Fausto Lendeborg
Thank you, Jeremy. Thank you for the invite. It's a pleasure to be here.

Jeremy Snyder
Awesome, awesome.

And it sounds like you've had, you know, great family support in kind of pushing you down this entrepreneurial path in the cybersecurity domain.

I'm really curious to kind of get into some of that as we go but to kick things off, this is our first episode of 2023. I'm really curious to know from your perspective, and I asked this of everybody that I'm talking to, kind of in these weeks, what was 2022 like for you, and how were you feeling going into 2023?

Fausto Lendeborg
Wow. 2022 was a very interesting year.

I mean, overall was great. I mean, we embarked on the journey of truly understand the problem we were solving.

So for us was to see people transition from always at home, remote working, to actually start having some face-to-face meetings.

So we were able to transition ourselves into the pandemic and out of the pandemic, and 2022 was the catalyst of that transition back out to the real world, right?

So, still living in a hybrid world where everyone can choose either to conduct business remote or not. I think it really helped us to understand that now everyone has a choice of how they want to conduct business.

So, for us, it was a lot of learning of that, learning about the customer, learning how the customer wants to get spoken to.

And in a personal, you know, manner, it was a great year. It was an amazing year. Very successful and just super excited for what's coming. And I think now transitioning to 2023, there's a lot of changes. And now we live in a different world, you know, and now it's, it's adapting ourselves to that, to that new world.

Jeremy Snyder
Yeah. I think that adaptation is exactly, you know, one of the things that I'm seeing from everybody around us, kind of adjusting to the new normal.

We've been talking about that for a couple of years, but, you know, kind of, post-pandemic if you will, but it really does feel like the last, kind of, the last half of last year is when that started to become much more of a thing.

I'm curious: in all of that transition and all of that adjustment that you observed. What's kind of the one big cybersecurity learning that you had from that?

Fausto Lendeborg
I think the big cybersecurity learning is there's going to be a revolution of how enterprises and consumers interact with business when it comes to cybersecurity.

We now see the consumer is more aware than anything else of their data, and I think that consumer education is actually going to change the way we interact with systems and the way applications are built and cybersecurity solutions are built, right?

I think going into the pandemic, everyone started to being attached to their phone more than anything, so it became this true digital world that wasn't there before, right?

That wasn't the underlying, but because it became a digital world from a consumer perspective, now the consumer has high expectations of data security.

So with that education and awareness of the customer today, I think that's going to change the way every technology company thinks about security so I think that's a big, big plus.

Jeremy Snyder
And do you think that consumers understand, let's say, their side of in, you know, their responsibility in that data security or data privacy equation because, you know, you and I work in the cloud and with cloud providers, cloud providers often talk about this shared responsibility model where they give you a secure environment, but then what you do with it is up to you, and you're responsible for securing your data.

But do you think that consumers have a similar understanding about what they can and should do from their side with regard to data privacy or data?

Fausto Lendeborg
The short answer is yes and no.

I think there's a generation that will never truly understand their role, right? And I think we've seen that.

And I think there's a new generation that truly understands their role and what they do is not only understand what they need to do, because that's going to rely on the

adoption rate of solutions, which is really complicated behind the big tech wall, but I think what that does is going to push companies to be better at data privacy, right?

Because now, the consumer doesn't have to understand the technology behind it, but now understands the law behind it and the compliance and regulation.

So I think we're seeing a highly regulated, you know, we're living in a highly regulated era, pushed by the consumer's demand of data privacy, and then that's flowing to big tech to actually secure the data.

So it's a, it's more of a, it's a top-down approach coming from the consumer point of view.

Jeremy Snyder
Yeah, and it's so interesting. There is this tension where, you know, companies are collecting more data, and so you would think that they would automatically take steps to secure that data.

Unfortunately, we've seen that's not always the case, but I think to your point, they're getting better at it. They do understand that consumers don't have all the awareness.

And then, I think also to your point, I agree consumers are getting at least a little bit more aware. Certainly, they're being made more aware by, you know, some of the breaches that get announced and so on.

So, let's shift gears for a second. I'm curious, you know, we talked in your introduction about, kind of, this long career in cybersecurity.

I, myself, am a lot newer to the cybersecurity space. I was an IT practitioner early in my career. Then I kind of went away from it for the mid-part of my career and came back about, I guess, about 10 years ago.

But you've been in cybersecurity pretty much your entire career.

I'm curious, you know when your father said to you that cybersecurity would be the most in-demand industry in the next millennium? Tell us that story. How did that happen, and you know, what else kind of pushed you down this path?

Fausto Lendeborg
It's a great story.

So my dad was a, he was in the entrepreneurship of his whole life, but he was in the telco business 20 years ago.

So he flew to Vegas for a trade show. And he, you know, now he recounts the story that he saw this guy talking about IP telephony security. And he was doing this demo with an IP phone, and he was the only guy in the entire trade show that was speaking about cybersecurity, but everyone was super intrigued by what he was doing.

So my dad really didn't know the domain, but he said, look, this guy looks like he knows what he's doing, and definitely there's something here.

So he flies back home. I'm 16, 15, 16 in my room reading some sci, you know, science fictional books, and he walks in and goes, whatever you do, you need to do cybersecurity because that's the future.

He shuts down the door and just walks away. You know, he just, I just had a foresight, right? He told me years later that he, this guy, inspired him.

And at an early young age, I started doing traffic analysis, building applications to understand how, you know, breaking systems and hacking systems and just even building, you know, just little pieces of code. And to me, it was such a new world.

And, you know, people say luck, but it was, you know, pretty lucky to get in there early and to truly understand the insights of the market.

Jeremy Snyder
Yeah, it's so interesting. I remember, you know, one of my first training courses after I graduated from undergrad and then started working in the IT space. Up until that time, all the computing that I did was really on, you know, just like one computer.

And, we got into the computer lab at school and started to see a little bit about computers connecting to each other. But that was all kind of black magic to me.

And then I went to work for, you know, for a corporation, and the first training course that they sent me on was TCP/IP, and it was so fundamental, and it's crazy, but here we are, you know, so I don't mind dating myself.

That was 25 years ago. It's still the same, you know, it's the same fundamentals, you know?

Traffic is traffic. IP packets are IP packets. It's, but it took me a few years to kind of realize how foundational and how important that was. It sounds like you latched onto traffic analysis as one of the first things.

So what made you realize the importance of networking at such a young age? Because for me, that was, you know, 10 years, 15 years later.

Fausto Lendeborg
Wow. No, the TCP/IP bit is funny.

I have a funny story, so when I was at the age of 18, 19, I joined this company called Prolexic Technologies you mentioned earlier, and the solution was we needed to look at internet traffic in real time doing a TCP dump, which is a way of actually reading the TCP packets at all the layers, like layer two to layer seven traffic.

And the training alone to actually understand the traffic patterns in the wire was about six, seven months. I remember someone came with this giant TCP/IP book and just slammed it on my desk and said, read that until you, you know, until you read that, you can't start working.

And, you know, I was just very fortunate to be at the forefront of traffic analysis 15 years ago, actually. So, you know, it was truly understand the foundational concept of communication, of computer communication, and then how attacks were layered on top of that.

So one of the initial cyber attacks in the market was Distributed Denial of Service, so it was a way of overloading a web server with TCP or application request. That's before the internet was completely decentralized, mostly how it's decentralized in traffic today.

So, you know, I spent six, seven years there fighting cyber attacks. I mean, I probably fought over 50,000 cyber attacks over the course of my first seven years in the career.

So it was truly understanding how they think, you know, how they operate, what motivates them. So it was from that side of the fence that I started just falling in love with security as a whole.

Jeremy Snyder
That's really interesting.

I think one of the interesting conversations we had on last season of the Ask A CISO podcast was with a guest who was talking about incident response. And we talked about and another guest actually talking about cybersecurity training.

And one of the things we talked about is that a lot of people who work on the defense side don't have the mindset to understand the attacker. You know, they just really focus on what they do from a defensive perspective.

So I'm really curious, because you worked on this at such an early stage, you know, before DDoS was a very common thing that you could just throw around as a saying, like, oh yeah, we got DDoS, et cetera.

That wasn't a thing back then. That was still new at the time. What did you learn? How did you learn to put yourself in the mindset of the attacker, and how has that skill stayed with you as you've gone forward through two or three companies and now into Secberus?

Fausto Lendeborg
Yeah. I think starts with understanding their motivation.

I mean, I remember fighting against Anonymous, and we infiltrated into some of their chats and their private channels to understand the communication. So, you know, it's motivation behind what they're trying to do, understand the actual crown jewels of the company, understanding how they're structured.

So, you know, the way that attacker thinks is the attack that you're seeing at firsthand is not the actual attack, right? So there's a lot of distraction, illusions, and on the way they operate.

And when it comes to kind of blue team, the defense team, it's about understanding you cannot secure everything, but you have to know exactly what you're securing and then stick to the crown jewels of security.

So when an incident response team is actually operating, it's not about the current event. It's about what else can be happening right now. Where's the data? Is any other data moving? So, you know, I think that is very, you know, useful to understand

and one of the challenges we are having as an industry is that we have, this market is extremely segmented.

Segmented between like the red team and the blue team, and the vulnerability team and the misconfiguration team and the cloud team, and the ops team and the SOC and incident response and all these segments that are happening are creating these giant gaps.

So, you know, for me it was actually looking at this 360 problem of there's gaps everywhere. How do we start closing the gap? How do we start closing this business and operational gap, these security gaps?

And you know, I think over the ... that happened the last 20 years. In the next 20 years, I think what we need to start focusing is in company solutions and technology that can close the gap, that can close any type of gap.

Because it is not about who has a better mousetrap anymore, right? Like the detection, detection technology has been done and solved. You can find any vulnerability management and you can build almost any detection company, right?

So I think the focus of, for us as an industry and as innovators and technologists, is not just building detection technology, detect another attack.

Like it's, yeah, we've detect all the attacks and clearly, they haven't been solved, right? Let's look at it from an operational business perspective. How can we close the gap in the entire market?

So for me, transitioning from my early engineering security mindset to founding a company that builds technology is to start discovering the gap that us as an industry have actually created into the market, right?

Because I think we're also at fault for building so many different technologies and confusing the customer. But now it's about just closing that gap. And that's truly my focus, as a person.

Jeremy Snyder
Yeah. There, there's so much there that I want to get into.

I mean, one of the things that you said, I've been saying myself for a long time, which is that, actually, the volume of data that you collect isn't nearly as important as the

context of data that you collect from a security perspective. It's the correlation of data across these different, you know, whether it's let's say vulnerability plus endpoint or vulnerability plus cloud infrastructure or what have you.

It's bringing that data together that I think is most interesting and so, you know, you're hearing a lot about security data lakes and all these things starting to evolve, very similar to what we went through, let's say in the 90s, and the 2000s with, you know, different database silos and then all of a sudden, data warehousing became a thing, right?

And so I'm curious, like, how has that informed your thinking at Secberus, and what you guys are building over there? Does that play into the design of your product or your architecture?

Fausto Lendeborg
A hundred percent. Jeremy,

I think you mentioned the biggest keyword is context and people over, you know, they over, they over-see that word.

I think let's break that down for a little bit. I think my personal belief and foundation is that the risk foundation, the risk context which comes from the business is one of the biggest problems at the core of any cybersecurity solution or any solution, right?

Because you can correlate as much as you can correlate. They're still missing some element of context from multiple aspects, right? You know, you can say this vulnerability in this data is high risk, but the moment you have 1,000 critical alerts, it's the same thing as having no critical alerts because you cannot remediate them all, right?

So I think there's two major foundational columns that we build with at Secberus, and I think every product should get built, which is: find the context, but what context are we trying to find? It's not just security context.

We need business context, right? You can have a production application that's facing the internet, and you can have a testing application that's facing the internet, right? The one different context differentiator between the two applications is that there's dummy data, and then there's production data, right?

So that's a risk context that somebody from the business has to add, right? I think that's the first thing: it's understanding what context we need to add to the data.

And then the second thing is, from an operational perspective, how and when, and from whom do you gather the context?

Because, machine automatically, right now, and we can get into the AI and all these advancements. I think the technology has advanced a lot, but when it comes to security context, I don't think it's there yet to understand a 360-degree from a business perspective.

So I think solutions have to be smart enough or intelligent enough to gather context from the right user at the right time that fits the data. I can actually take this data lake into a remediation kind of timeline because it's not about eliminating the risk as a whole. It's pretty much almost operationally impossible.

But it's about reducing it over time, making sure that you're having the right technology to prioritize, and, kind of, is working together with the solutions to the people.

Jeremy Snyder
And how do you recommend customers think about, kind of, making progress there because I know from my own work, and you know, I've spent the last five, six years working with customers on their cloud security journey.

A lot of customers, they get hung up on trying to solve everything at once instead of kind of reducing over time, as you just said there.

What's some of the learnings that you could share? What's some of the thinking that you could share with our listeners about, like, how to measure progress or how to approach this problem and not like try to solve it all at once and get frustrated when it doesn't get solved all at once?

Fausto Lendeborg
Yeah. I think the transition from, for CISOs, cloud security architects, VPs, and directors, and CTOs, is understanding that security is no longer only a security problem, but it's also a business problem, right?

I think that's the first thing that we talk about. So when you think, what does actually, what does that mean? Well, it means that you have to look outside of the

security data of what the solution is giving you. You have to look at the business data the solution is giving you, right? We often say we are not solving a technical security problem, we're solving an operational problem.

So when you start thinking about what does that mean to solve an operational problem, let's understand what business metric and what business value is this solution providing, right?

Can I see a reduction over time? Can I see who's working on what? Can I understand how is the traffic or the data, or the alerts being managed across my pool of employees, right?

So that's kind of the first main concept that we talked to CISOs about, which is: think business first and then blend and merge the technology around your business thesis on how you're gonna get this job, right? And that's the first thing.

Now, when you take that outside and say, now I need to construct my security program, you have to start picking solutions that fit within a stack of solutions to build an entire program, right?

It's not, I'm not going to pay one product that does it all, right? And that's what, that's the easiest route, but it's never the best route. Because one company can do something very, very well as a core solution and have a feature that you need that doesn't work very well. And you need a company that has developed an entire solution out of that one feature, right?

So, it's understanding you need to pick a different set of systems to actually build security programs part of your stack.

And then the last thing is understanding the architecture building blocks of applications that can actually be blended together, right?

Instead of looking for companies that just have a one-feature in the micro world, let's look at API architecture. Let's look at companies that can integrate with each other, right?

So it's going beyond just the normal set of requirements and look outside of the box, from a business perspective.

Jeremy Snyder
Yeah, I think that's such great advice.

I mean, trying to remind customers again and again that you have to look outside of the security context, look at the business context, what's the overall impact?

And to me, it kind of goes back to your statement around what are attackers after? They're after the valuable data, the crown jewels.

So try to, you know, try to put that in your own mindset when you're thinking about measuring the impact of a cybersecurity program on your organization.

Well, we've got just about five or six minutes left, and I've got three topics that I still want to get to with you today, Fausto, so I hope you don't mind the abrupt transition.

I know that you have talked a lot about alert fatigue in the past. What advice do you give to anybody around alert fatigue, whether it's somebody implementing a tool for the first time, or somebody responding to alerts and starting to experience this alert fatigue?

How should customers think about managing the volume of alerts better?

Fausto Lendeborg
So I think the first thing is to understand: alert fatigue is drowning a team with false positives, right? I think that's the first thing you know.

That is what causes alert fatigue. So I think the first thing is the mitigation and the, in solving the alert fatigue, the false positive problem, right?

So it is having solutions that can find context, generate, fit the data, and eliminate the false positive rate, at least 80%, right? Because now you have an alert that can actually be actioned upon, right?

So once you start thinking about false positive rate, which can be solved with customization and technology, now it's understanding that the alert that comes out of any system has to be put in the right person's hand, right?

So, it's a layer approach of getting the context, eliminating the false positive, and then landing and making sure that systems are smart enough to take the alert to the right person, right?

So I think that's kind of the main concept, which is building a system that can find the context and then can route the alert to the right person. And that starts reducing the fatigue issue that we have.

Jeremy Snyder
Yeah, so again, that contextualization is so, so important.

So when we think about alerts, one of the things that always comes to my mind is, you know, a lot of companies, they only focus on kind of managing the alert, you know, let's say resolving the alert, but they don't necessarily focus on the meantime to detection or the meantime to respond.

I know you've worked with companies of large scale over the years in kind of implementing cybersecurity programs and in responding to incidents and so on.

How do you think about introducing those concepts to cybersecurity organizations? Because, historically, these are concepts that are very often associated with application development and with developers, and looking for, let's say, bugs in code more on the application logic side than on the cybersecurity side.

But I do think they're relevant for a cybersecurity context. So how do you explain them to people, and how do you advise people to embrace those concepts and make them part of their operations?

Fausto Lendeborg
So I think we no know now that we, you know, we potentially walking into a recession here in the economy. I think it's finding solutions that can be completely automated and can have business value.

So when you talk about median time to remediate, it's one of the big business metrics that we can have in this cybersecurity world, right?

It’s how long it's taking my team to solve the problem, right? So if you eliminate false positives and reduce alert fatigue, and you have a solution that can actually track the state of an alert bi-directional, right?

We're not in the world where we send the alert and we forget about it. We have to understand what happens, who's solving it, and how long does it, how long did it take between detecting the problem and solving the problem, right? So, that aggregated over time is one of the big business values that we can offer.

So the way we educate CISOs is understanding that's the metric that saves you hundreds, if not thousands of dollars, right?

So when you think about a methodology of continuously assessing, continuously remediating, one of the big terms we use in the methodology we use at the course called CARTA, which is a Continuous Adaptive Risk and Trust Assessment, right?

Which is a bidirectional methodology of detecting the alert based on business requirement, pushing it down to the right person to remediate.

Now the person can either accept, reject or mitigate risk or add context to the risk which actually comes back to the top.

So this bidirectional methodology of flowing from a top-down and from a bottom-up actually provides CISOs the overall business architecture to take to the board and say, now our Median Time to Detect is real-time.

And our Median Time to Remediate, we now understand what every engineer is doing, how they're doing it, when they're doing it, and how much money we can save from an operational perspective.

Jeremy Snyder
Yeah, I think that's such an important point.

People don't often think about kind of ROI on their cybersecurity investments because it's very hard to measure.

And I know lots of people have tried approaches with like, oh, let's look at the cost of one record or one data breach and all the IBM data around 3 million per incident, et cetera.

But I think, you know, kind of thinking about the ROI on the time invested into a cybersecurity activity and making that a repeatable process that, to your point, through automation can return, you know, tenfold the amount of time back to your engineers and your organization to work on other things that are also crucial to the organization.

That's so important.

So, couple other things I want to follow up on there. So we talk about automation. We hear a lot about kind of, automated response. We hear about SOAR, but we also hear about, you know, Infrastructure-as-Code, Policy-as-Code, Security-as-Code.

Can you help us understand, from your perspective, as somebody who's been in this space for a long, long time, what's the difference between Policy-as-Code and Security-as-Code, and what's the importance of each of those?

Fausto Lendeborg
I think the big difference between Policy-as-Code and Security-as-Code is the intent.

Policy-as-Code: the intent to build something customized with coding language is to what type of intent you want this code to assess. It can be an operational intent, it can be a compliant intent. You can code anything into a policy.

When it comes to Security-as-Code is Policy-as-Code derived and focused on only the security intent of that policy, right?

So we are going into a world where we can modify it and customize the policy, but it's about understanding what intent you would want to give to that Policy-as-Code.

Jeremy Snyder
Got it. Got it.

And so if we think about, kind of, all of that in the context of cloud security, I guess, what are some of the lessons that you would leave with our audience today as a takeaway?

You know, how should you think about incorporating either Policy-as-Code or Security-as-Code, or even concepts like Meantime to Detection and Meantime to Repair?

How do you think about incorporating those into cloud security strategies?

Fausto Lendeborg
I think every cloud security strategy should have, at the core, a cloud governance platform that is powered by Policy-as-Code. This Policy-as-Code gives you the flexibility and the extensibility of creating any intent to the cloud.

When you think about what the cloud is, the cloud is a big blob of code that's completely ephemeral. So the only way to actually solve for that problem is to have complete solutions that can be extensible from a code perspective.

So it's looked beyond the nice graphs and the nice charts from a demo. And look on to understand what business problem is actually the solution solving.

Jeremy Snyder
Yeah, I think that's, again, such a key point. Let's always bring it back to the business.

So, Fausto, we've got, you know, just like one or two minutes left.

I'd love to ask you for two closing thoughts.

So one is high-level advice on security for the cloud going forward into 2023.

And then, second is: if customers want to learn more about Secberus, give us just a quick overview on what Secberus does, where they can find more information.

Fausto Lendeborg
So I think the big advice from a security perspective is to just truly continue to innovate and push the boundaries beyond the box.

And from Secberus, you know, we are a company that truly solves cloud security challenges. I think we've seen the market fluctuate, but it's about helping CISOs build a cloud governance solution to solve multiple problems that they have today.

You know, we can definitely always have conversations and what we want to understand is what problems companies are having at scale, and truly understand how our product and platform solve for those use cases, right?

We built something that could be extensible to so many different use cases, so for us is listen, learn, and then provide a solution to the customer that just fits the problem.

Jeremy Snyder
I think that's a fantastic note to leave it on.

Fausto, thank you so much for taking the time to join us today on the Ask A CISO podcast, and for sharing your deep experience in this space through many iterations

of the internet, going back to, you know, IP telephony, security, and some of the inspiration that started it all.

It's been a real pleasure speaking with you and hearing about your journey. Thanks so much for taking the time.

And to our audience: please join us on the next episode of Ask A CISO.

Thanks for listening.

Fausto Lendeborg
Thank you, Jeremy.