Professor Ariel Evans of Cyber Innovative Technologies

[00:02:17] **Hall Martin:** Hello, I'm the host of Investor Connect Hall T. Martin, where we connect startups and investors for funding. Today we have joining us Ariel Evans, CEO, founder at Cyber Innovative Tech, and client of TEN Capital. Ariel, thank you for joining us.

[00:02:36] **Ariel Evans:** You're welcome Hall. Hello everyone.

[00:02:38] **Hall Martin:** Great. Well, let's talk a little bit about today, your thoughts on the impact of social cybersecurity and what's happening with SolarWinds – can you give us a little bit of background there on that?

[00:02:52] **Ariel Evans:** First of all, SolarWinds is a very significant issue that we are facing today, and it's something that's been overlooked for quite some time. But now it's coming front and center because it's impacted over 18,000 companies, particularly all of the US federal agencies as well as the Fortune 500. And SolarWinds is a vendor, they're a third party who produces software. The software they produce though is what's important in the context of what they do, in terms of what they do digitally is important. So SolarWinds is actually monitoring and managing the infrastructure and the firewalls of an organization, and so what that means is that your entire infrastructure of your organization is in scope, if there's something wrong with SolarWinds. What happened with SolarWinds was that they did not have a type of program that permitted the ability to have vulnerability scanning and penetration testing done on their development environment. _____ think of SolarWinds, what's important to know about SolarWinds is that they provide patching every cycle to the organization that has their software. And if there's something wrong with that patch, then that patch is going to have malware in it, and that's exactly what happened in the instance of SolarWinds. So now what you have is a situation that's probably taking a number one position to the NSA hack that happened a few years ago, where this is now in every single federal agency in every single Fortune 500, and they have to go back and do forensics to see what kind of backdoors these guys left.

So we need to understand cybersecurity and context is my point. And if we don't understand what SolarWinds is, they're not a cloud service provider, they're not storing and processing your data, you don't need a SOC 2 report, what you need to understand is what the heck these guys do. And then you have to look at that in the context of what could go wrong, which is that their entire software development lifecycle could be a mess, and frankly, it was obviously if this happened. So that's what we're focusing on in cybersecurity, and cybersecurity in context of digitization and how it impacts an organization from a business perspective.

[00:05:08] **Hall Martin:** Great. So how did this happen at SolarWinds, what went wrong in this process?

[00:05:14] **Ariel Evans:** Well, two things went wrong. One side, one thing that went wrong on the side of the SolarWinds, and one thing that went wrong on the side of the organization that uses SolarWinds. So let's talk about the second one first. You use a vendor, a third party vendor, you use a software vendor. Right? What do they do? They supply you with patches to update the software to make sure that vulnerabilities are not exploited. So in the case of the vendor management program of the organization, they were not looking at SolarWinds in the context of what it did. They were looking at it very, very haphazardly. They were not seeing that this was something that you needed to check the actual ability to protect the development environment. So SolarWinds, what did they do wrong? Well, they didn't establish a good governance program around their secure software development. They did not pen-test their development environment. They did not do vulnerability scans on their development environment. And therefore, this was a very sophisticated attack actually that was well, well planned, whoever did this was quite genius frankly. What they did was they said, okay, goodie, how can I get to the entire federal government and the entire Fortune 500? Well, I can go in through a third party to get to them. And that was their motive was to get to these organizations so that they could then exploit these organizations, either steal data, intellectual property, ransom them, whatever their nasty nefarious activity would be. SolarWinds needed to have a good SDLC governance structure in place around their development environment which they didn't have. So we need to look at this in the context. You've got the responsibility of the software vendor and you've got the responsibility of your organization that uses the software vendor, and they are not mutually exclusive, they're interdependent on each other frankly. We're not looking at it that way. We're looking at like, okay, let's just look at a checkbox report and see what they did. That doesn't work. And SolarWinds is a prime example of what can happen when you do that type of behavior.

[00:07:24] **Hall Martin:** It seems like a lot of major hacks occur because they went through a third party vendor and not directly through the company. Everybody's looking at the company but nobody's looking at these third party apps or programs. Is that a common situation, and what do you do about it?

[00:07:40] **Ariel Evans:** I think there's two parts to that. One part is that there's no way that you can slide under the radar when something happens between you and a third party. It is reportable, and there's no way you cannot report it. There's a lot of things that happen in a company that don't involve a third party that people say, well, don't ask, don't tell. Right? We don't have an obligation to report a business interruption until now but laws are changing. But in the past, they didn't have that obligation, so why report it? So if you got ransom, maybe you wouldn't report it. If you had a DoS attack, maybe you wouldn't report it. So the context of this is that third parties are more visible. So we had targeted, they were the poster child of bringing cyber into the boardroom.

Why? Because they had an H _____ vendor that they had, that gained unauthorized access to the organization through the misuse of credentials. So that was one of the first attacks that became on the front page of The Wall Street Journal and The Washington Post, because it was so prolific. And it's shined the light on third party relationships between organizations and their vendors. And so, that's been something that's been monitored, and there's a lot of data on that. We now know that 63% of reported data breaches are due to third parties, but one of the reasons for that is because it's required that you have this monitoring relationship.

With that said though, think about the whole idea of cloud first. What is the cloud? It's a vendor. And when you go cloud first, it's like you're outsourcing the data processing and the data storage to this third party, you are responsible for some of the controls and they are responsible for some of the controls. And that dance is not well understood at Wall. A lot of folks think, oh I outsourced it to the cloud. No, no, no, no, no, you didn't outsource your risk, you just move things around a little bit. The other aspect of that with the third parties is when you're looking at what they do for you, what's the context of the third party, you've got cloud service providers that are processing and storing; and then you've got third parties like SolarWinds, they're a technology vendor, they're a system vendor, they're providing you a system. So their cyber responsibility is around the integrity of the patch, making sure that there's no nefarious malware in that hatch. So we have to understand again the context. So vendors, yeah, we see a lot of this, and I just explained why. But also think about the fact that you integrate. So you're sending data to a data processor. They're processing it on your behalf. They're sending out to your bank, so that the bank can go ahead and do the debits and credits. So you've got this whole supply chain, distribution chain that is dynamic and integrated with third parties. So this is how business is done today, and it's not just you as an island doing business. No, you're taking data here, you're moving data there, you're processing data there, it is very dynamic, and it is very interdependent.

[00:10:47] **Hall Martin:** You think we'll see increasing federal regulatory over this area based on this and other hacks like it?

[00:10:54] **Ariel Evans:** _____ following this for the last few years. No, I wish.

[00:10:59] **Hall Martin:** Why not?

[00:11:00] **Ariel Evans:** Well, the states, like the COVID, let's take that as an example. See how the states have authority over COVID and who gets vaccinated and how they get vaccinated. It's the same thing with privacy. Right now you're seeing more and more states enacting privacy laws. Matter of fact yesterday, Virginia enacted their privacy law. So Virginia. We see this slowly, right? So we are starting to understand how important this is at the state level, but the states have their own legislative process, it has to go through committee, it goes to the Senate, it goes into the House, just like it does in Congress at the federal level. The federal government has opted not to go that route for

whatever reason. The FTC is still the top cop and privacy, as you saw with Facebook with their $5 billion fine, but they pick the big Kahunas, they picked the 800-pound gorillas to go after, which is good, but they're not legislating and enforcing on the rest of the market which is 99.9% of the world. They're going to pick and choose their battles. So we don't see that. We see slow millimeter movements at the state level, which is good, don't get me wrong. But there isn't going to be any overarching privacy level unless one of the Presidents steps up and understands this level that needs to be understood and says, listen, no more nonsense, let's do this at the federal level, and then they have support for that. We don't see that happening. We talk to legislators on a regular basis. We talk to people in the privacy industry who are at the government level on a regular basis, and they say it's not happening.

[00:12:42] **Hall Martin:** So what do you think might happen that would actually spur changes at the top level and make it a priority?

[00:12:52] **Ariel Evans:** Well, it's funny, because the NSA, that tool breach that they had a few years ago, you think that would have spurred people into complete action. It didn't. I don't know, to be honest, Hall. I mean, I would have taken action a few years ago. I think they're too distracted by other national priorities. Obviously, COVID is completely distractive. But from a cybersecurity perspective, we've been inching towards trying to get better federal regulation in place. But when you look at the federal agencies, I just had a conversation with some ex-GOD guys who are running a couple of new, different boutique, federal based cybersecurity firms. And they're basically saying, listen, there is no impact on the federal side. There's likelihood, but there's no impact. Nothing happens _____. You're not losing cost per record, like you do in the commercial side. There is civil penalties, but they're not enforced. So it's like what's the downside. There is no downside. So you've got a mechanism in place. It's ineffective. So something has to happen at a very high level to come from the top down and say, hey, we're reorganizing how this is going to work, and we're going to treat this more like the commercial space where there's impacts which they're not. So it's a huge issue, to be honest with you, in terms of how the federal government operates in cybersecurity. And we would think that they would have the highest level, which unfortunately, according to everyone that I've spoken to, and what I've seen, that's not the case, which is unfortunate.

[00:14:35] **Hall Martin:** Well, it sounds like it will take something on the catastrophic level to actually achieve change. And so, I guess, that's the next level is when something catastrophic happened, we had an ice storm in Texas two weeks ago that shut down the electric grid for a week. A week we were out without diversity in many parts, not all but many, and I can tell you there is now a change underway. People are like, oh legislators are doing nothing but fixing it.

[00:15:02] **Ariel Evans:** What level of critical infrastructure is there at the federal level, right? I mean, there's nuclear power plants. We certainly don't want to see something

there. That would be absolutely disastrous. The electric grids are not federally regulated. They're not at the federal level. So what does that mean? Like, what's the critical infrastructure that would impact it? To me, it's the financial system itself. We've already had, not a cyberattack on the financial system, but a physical attack on the financial system with the World Trade Center. I mean, that devastated the whole Wall Street economy for years, and it's still working on recovering from that. But from a cyber perspective, if it was a financial system, if we had a run on the banks as an example like 1929, yeah, maybe we would have people pay attention to this. I don't know. It's a great question.

[00:15:58] **Hall Martin:** Yes. Well, I appreciate the discussion on that. Let's just talk about you for a moment. What is your background?

[00:16:07] **Ariel Evans:** I am a serial entrepreneur with two successful exits in software, one company sold to BMC, the other two Kleiner Perkins company. My background is in nuclear physics, moving into IT, and then moving into cybersecurity about 12 years ago. I moved to Israel seven years ago to work with the innovative companies, and got very interested in this area that I thought was underserved, which is cyber risk, and wrote a book about it, two-three years' worth of research, and then started to develop a solution around it which is why we're talking today.

[00:16:38] **Hall Martin:** Great. Well, so what is the primary trend in cyber risk, cybersecurity risk, where is that going?

[00:16:44] **Ariel Evans:** Quantification and defensible metrics. No one is quantifying cyber risk well, except for us, we have the only known defensible set of algorithms that look at cybersecurity in the context of the digital asset. Today, 85% of your businesses digital, which means that 80% and 5% plus of your value is digital, 20 years ago 10% was. And the explosion to digitization is parallel to the explosion in cybercrime, and this is what the cyber criminal attacks. They're going to steal data, they're going to cause business interruption with ransomware and denial of service, and they're going to cause you regulatory fines based on the type of data you're processing and storing in the systems and technologies. So if you look at it from a digital perspective, you can quantify it accurately; and when you can quantify it, there's a lot of use cases that come out of it: prioritization, insurance limits. So we service both the insurance industry and the corporate industry as well as the vendor communities. So we have quite a broad level of service, because everyone is impacted in a slightly different way, but they're impacted nonetheless. And then you can prioritize your cyber program. It's very hard to understand, when you have a vulnerability threat or an incident, where you should start, if you have multiples; and companies do, they don't have just one, they have multiples. So how do you prioritize? Where do you start? What kinds of risks do you accept? What kinds of risk must you immediately remediate? How does that look? And how do you communicate that very high level cyber jargon to a board of directors who has the fiduciary duty to protect those digital assets? You have to do it in the language of

metrics, and this is what we provide for companies. It's a way to level the playing field, to connect the technology people and the decision makers so they can see data the way they need to see it, and to ask the right types of questions.

[00:18:41] **Hall Martin:** I assume if you understand the risk, then you'll be able to mitigate it. Is that true? If you have a certain score, you know what to do to fix that?

[00:18:51] **Ariel Evans:** You'll know what to do, but the question is priority again. You only have so much budget and so much resources. So you have to be mindful, and do it in a very strategic way, so that you're getting the most for your money. And this is something where we see companies doing percentage of IT spend for cyber budgets. We think that's not very effective. And the reason that's not effective is because one has nothing to do with the other. You need to look at it in terms of risk mitigation, and understand what level of risk is acceptable to you, and then budget, reverse-engineer the budget, back to what makes sense for your company, and how to get to where your goal is. And that's what we allow companies to do is to understand the return on investment on their cybersecurity program, their people process and tools, and to be able to look at that as an asset and not a cost center. This is a big mistake that companies are making, but this is how the industry has evolved, and we're here to change that because you've got to do something different. And what you need to do differently is understand that this is a value to you. When you look at protecting the business, it's a value to you, it's going to increase your stock price; it's going to increase your ability to acquire companies and understand how they fit into your strategy and your infrastructure from a cyber risk perspective. So this is important part of what we do.

[00:20:11] **Hall Martin:** You think your quantifiable metrics would ever become a marketing tool, just like people's social impact metrics often help a company sell and become a trusted brand, so their cybersecurity metrics would also do the same thing?

[00:20:26] **Ariel Evans:** They already are. We do have customers that are using that, exactly that, to show return on investment on, so say they sell 65 different cybersecurity tools. It's like, okay, which types of risks do they reduce. If you have an IoT credentialing tool, it's going to reduce IoT access risk. Okay, what's the return on investment on that, and how can I go back and make a business case out of it? Absolutely it's one of the things that we are very committed to doing for companies because we think that is the future.

[00:20:56] **Hall Martin:** And so after the SolarWinds hack, what do you think will happen in the next 12 months, do you see changes of any kind coming up?

[00:21:03] **Ariel Evans:** Yes, we're seeing them slowly. So there's been four new regulations that require vendor risk management programs, CCPA, GDPR, New York State Part 500, and NAIC. They are saying you have to have a vendor risk program in place.

What we're seeing is that they have to understand what that means. They have to understand the context of what you need to do. And we are providing that with our _____ solution. So we show you, okay, what type of vendor it is, it could be multiple types, it could be a cloud service and a system and a processor. We don't know. But the question that we will ask is appropriate to that level of what the vendor does for you digitally. And then you can decide how to protect and how to work with the vendor. Vendors are partners. You must dance with them. I throw the ball to you, you catch the ball. Right? It's like, okay, now I run with the ball. Now, I throw the ball back to you. It's like, it is a dance. It's like the Super Bowl. It's like you have to, without Jell-O, unfortunately. It's like the Super Bowl where you're completely like competing against the other team, and you're moving and they're moving, and then you're moving back, and it's like – and it's cool, I mean, cybersecurity is fascinating. My husband doesn't like it, I don't get it. It's like, I think it's so amazing. It's like, I could talk about cybersecurity till the cows come home. I talk to him about it and he falls asleep. It's like, don't get it. Where I see it going is it's going to blossom, it's going to get context around it. It's going to get thought leadership. It's going to get understood by the business. There's so many places that this can go. It's not just about point solutions, oh I've got a firewall, oh I've got a SIM system, oh I've got a DMS. Great, you need those. Absolutely. They identify, protect, detect, respond, recover, absolutely have those. But what you really need to know is how this impacts you from the business perspective, and that's what we're here to do.

[00:23:01] **Hall Martin:** Great. In the last few minutes that we have here, what else should we cover that we haven't?

[00:23:06] **Ariel Evans:** What else should we cover? So I guess, maybe a couple of things that are interesting to investors. We are working with managed security service providers to align with their offerings to their current customers, and we're becoming an additional layer on top of them, to provide them with business process automation and security assessments, the risk management protection piece, of course, the quantification which is important in all the use cases that Derisk provides. And this is an area that we've been committed to for the last six months. Derisk is now looking at AI and looking at use cases that are going to be pivotal to the executives to do natural language processing. In other words, I look at the Wall Street Journal, I say SolarWinds. Oh gee, what does that mean to me Derisk. Derisk says, George, don't worry about it, you don't have SolarWinds in your digital asset inventory, you're good; or George, call your attorney, disconnect all your systems from SolarWinds, call your forensics team, call your cyber insurance company and take a deep breath, you need to deal with this. Right?

We're going to be advising, from a risk advisory perspective, those that need to understand this clearly and concisely, in a language that they can understand. We're also going to be looking at the loss events in terms of predictability. When you look at Equifax, it's over $5 billion worth of loss, 1.4 billion from the shorttail. The cost of the

record, the number of records and the business interruption losses, longtails of legal side, it's the class actions, its the attorney general coming at you. It's the _____ actions, and that's the longtail. So we're going to do the predictability around that because there's lots and lots of available data there that will help us to show companies, okay, how do you avoid the longtail. Because longtail is 80% of the nastiness, the shorttails 20%. The shorttail hurts, believe me, it hurts. But the longtail is going to hurt more. And you got to look at this in perspective. So we're going to really hit the ground running with that. We're excited. We're looking for the right investor. We want somebody who understands what the heck we're talking about frankly. We can do or we can teach. We want to do. So thank you Hall very much for having us.

[00:25:35] **Hall Martin:** Well, great. So how best for listeners to get back in touch with you?

[00:25:39] **Ariel Evans:** I'm available, of course, on email, that's the best way to get ahold of me because I'm usually running behind on emails, but I will get to you. It's Ariel@cyberinnovativetech.com or you can call me on my mobile phone which is 610-334-6914. I prefer the email because then I don't lose you in the morass. Thank you very much.

[00:26:04] **Hall Martin:** Great. We'll add that to the show notes. I want to thank you for joining us today, and hope to have you back for a follow-up soon.

[00:26:10] **Ariel Evans:** My pleasure. Thanks so much, Hall.