IP Cybersecurity Show 3
COVID's Impact on Cybersecurity:
Participation in the Cybersecurity Segment
and What Investors Look for

This is Investor Perspectives, I'm the host of Investor Connect, Hall T Martin, where we connect startups and investors for funding.

In our new Investor Perspectives series entitled "COVID's Impact on Cybersecurity", you'll hear about participation in the cybersecurity segment and what investors look for.

As the COVID pandemic passes, we emerge into a new world. The cybersecurity space is now undergoing tremendous change as we shift from a centralized to a decentralized workforce. Every business is impacted by cybersecurity. We have investors and startup founders describe the changes coming up.

Our guests are:

1. **Greg Fitzgerald, Co-Founder, Sevco Security**
2. **Merrick Andlinger, Partner & Chief Investment Officer, Option3Ventures**
3. **Christian Kameir, Managing Partner, Sustany Capital**
4. **Andrew Morris, Founder, GreyNoise Intelligence**

I hope you enjoy this episode.

Our first guest is Greg Fitzgerald, Co-Founder of Sevco Security. Headquartered in Austin, Texas, Sevco Security is a company of cyber experts building services and products for cyber experts. They design solutions to solve hard problem(s) associated with quickly discovering the context for who, what, where, why and how network-connected devices relate on your network.

Greg, thank you for joining us.

[00:22:15] **Hall Martin:** Great. Well, tell us more about your participation in this segment, what have you done in this space?

[00:22:21] **Greg Fitzgerald:** So I've been able to see on the network side, so _____ as the whole environment has matured, everything used to be network centric. And then, so _____ protecting the pipe, so to speak, of the organization and how people got in and what happened traversing the internal network. Then I was able to go and work with the cloud security companies, as things started to transition out to that new hybrid model is some stuff's on premise, some stuff's in the cloud, and then transitioning very much into the endpoint security space, where the weakest link to get into an organization was a person's laptop, or their desktop at home. Obviously, the advent of that has gone now to mobility with iPads, and even your phone, which are incredibly capable for corporate use. So I've been seeing that side, and interestingly enough, most recently, I have kind of reverted back to the fundamentals, the basics, meaning, companies, in particular, have protected their endpoints to where they feel pretty confident with next new artificial intelligence based technologies. And then, they've gotten, say the data understanding of their environment, like, on the security realm, but what they're really missing is what, in a dynamic world that I've mentioned earlier, like, who has what devices with what on it, and how are they accessing my network, like, basic questions, frankly, are not able to be answered easily or accurately in today's technology world. So I've seen my cofounder and I, J. J. Guy, have seen this over the past 10 years, in particular, where we walk into an organization and we say, hey, we want to help you out, and like, tell us a little about your environment. And it's, like, I'm not quite sure, or, I don't have the _____ of exactly what's going on, because things are changing so fast that the traditional systems that used to do this on the IT management side are frankly outdated. They weren't really designed for the dynamic environment of users and devices and applications and hybrid networks, they just weren't designed that way. And then, on the point product side, they were built for a particular purpose, for example, antivirus or discovery of what's going on, on an endpoint, or your network firewall. But those technologies are being asked, I would say, from the IT guys, the security guys, like, hey, give me more information about what does Greg have as a computer, what's on it, is it configured right, does it have the right protections, where's he accessing from. And those technologies, while they have some of that information, is not comprehensive, and it's not over everything. You can't – so the biggest danger we're seeing is, companies just don't know what they don't know. And so we're solving that problem. It's a massively hard problem, but it is solvable, it's been done in the government space, and unique pockets, I should say. And that's one thing we see a lot of is commercialization of technology of the United States government,

which has spent an enormous amount to ensure that we stay ahead of the threat, so to speak, as a government agency, and then apply that to corporate world.

[00:25:37] **Hall Martin:** Great. So what should investors look for when they come to this space, what should they prioritize in their diligence and follow-up?

[00:25:45] **Greg Fitzgerald:** That's a really good question. I'm going to fall back on the three main things that I see as well as an investor in any company, which is, first of all, the management, the management team. Is it solid leaders? Do they understand the domain? Do they have the experience and, frankly, the skillsets to just really be understood in that particular domain? The second one is the market, like I said, is the market big, big enough, for the way? As an investor, I'd want to have a return on my investment, and each person has their own preferences of what they would like to do, whether you're an angel investor or venture capital or private equity. But is the market big enough to really take hold of that and not be pushed out? And frankly, the last piece I see is what kind of money is behind it? In cybersecurity, it does take funding to get a lot of these technologies to market. It's not as extensive as, say, pharmaceuticals or medical devices or things like that, which has a lot of FDA regulations. Cybersecurity doesn't have that, but the technology itself takes some time to get done. So you need to have some pockets with some depth that can get you the runway you need to, again, go back to what is most critical, which is a product that works. Right? So being very careful that the marketing didn't overextend on the capabilities of the product, and in a skeptical buyer market, being able to really fulfill the promise of what is being stated about the product, and then, of course, have a little bit of money, where it's not just the money itself, but the influence of the money, the people that are holding it is, can they help you either with connections, obviously, network, open doors, relationships at technology partnerships. That is a critical piece of the, I guess, the operator, like we are, to who we would want to invest in us. And the last piece that I would even really emphasize is culture. I mean, in my almost, gosh, almost 30 years of work, it really has come down to where the culture of a company and the investor backing has to be synergistic, because when there is inevitable discussions, debates, difficult situations, if people are aligned on the philosophies of life and management and structure and returns, then that ends up being a very successful relationship and one that anybody will get through together, where, when it's not, you see powerplays, you see struggles, you see people not getting fair shakes, and it really destroys the organization. And that's not, that's unfortunate, is what it is, because in today's world, there's money everywhere, in my personal opinion. Is it at the right price, in the right terms? That's all to be debated. But there's more money now than there, frankly, has been ever, and so, there's a great opportunity to invest, there's a great opportunity to be an entrepreneur, and there's enough variation on both sides to make a fit, have a really happy fit.

Our next guest is Merrick Andlinger, Partner & Chief Investment Officer at Option3Ventures. Headquartered in New York City, New York, Option 3 Ventures specializes in finding and developing attractive investment opportunities at the frontiers of cybersecurity and

immediately adjacent technologies. It brings a unique perspective to these industries, integrating the expertise and experience of its management and advisors in the United States National Security Community with their extensive operations and investment expertise gained in the technology industry and on Wall Street. The Option3Ventures team has worked together for the past five years, invested in five companies and successfully exited from two of those investments.

Merrick, thank you for joining us.

[00:10:57] **Hall Martin:** Great. So you mentioned some of the deals you've been doing so far. But can you tell them more about your participation in this segment?

[00:11:03] **Merrick Andlinger:** Sure. We're focused on several sectors within cybersecurity, and we like to think of those as a frontier. And they might be a frontier from a technology perspective or they might be frontier from a market perspective. So the first one we're looking at is automation, and if you think about it, given the explosion of attacks, the explosion of threat, intelligence, and threat information, there just aren't enough humans to work fast enough to analyze everything. So automation is a very important sector that we're looking at. The second sector that we're looking at is we'll call them impactful technologies, and these cut across all different industry verticals, that could be something like an application of blockchain to keep the information secure. It could be a cryptography, it could be, oh, another technology like quantum computing, for example. But not just the technology, per se, but the technologies applied somewhere. A third area that we're looking at, and we've invested in, it's one of my favorites, is we call it cyber physical systems. And if you think about what that is, it's where the internet meets the real world. So instead of trying to protect your information, because there might be an identity theft thing going on, this is where the internet or someone via the internet can come in and jump into the real world. It can make a car crash. They could make a factory blow up. They could stop the power or regulate the power on an electrical distribution system and burn out particular circuits. So this is an area of increasing focus for us. And the last one is cyber insurance where maybe people don't think about that, but you can do everything. Think about it like your car. You wear your seatbelt. You drive safely. You follow the rules. That doesn't mean you won't get into an accident, even if you do all the right things, and so you have some insurance for that. Cyber insurance is the same kind of thing that companies need to take steps to protect themselves in this layering kind of protection that I've talked about. But they're also increasingly looking for insurance and the insurance world, with all the technology and data and actuaries that they have, hasn't caught up yet with how to analyze, assess risks, and price insurance. And so that's an opportunity for us as well.

[00:13:45] **Hall Martin:** And so what are you looking for in these companies in order to make an investment?

[00:13:51] **Merrick Andlinger:** We look for strong management teams. We look for distinctive technologies, where they're addressing important and large problems. We need to see successful deployments with reference customers. So that means we're not at the seed stage where it's just an idea in an entrepreneur's head, we need to see the product more developed. Increasingly, we want to see reference customers or quality relationships, and it could be an investor, it could be a channel partner that we can work with. So several of our more recent investments, we have had notable investors or industrial companies or others alongside of us that can help actually grow the business in addition to just providing funding. And we look for a trajectory in the business that can lead to a successful exit. And in our sector, in cybersecurity, that's more rapid than it may be in some other sectors. The velocity, the speed at which companies mature, is quicker than what I've seen. So, for example, our fund, we're looking at a seven-year fund, not a 10-year fund – we're expecting companies could be exiting in three or four-year investment cycle, not longer. Many won't make it to IPO, many will be bought up earlier, much like an analogue in the drug development, the biotech drug development area where you see many smaller companies advancing solutions and they won't get them all the way to market; a larger company will come in, acquire the solution when it's evolved enough through the regulatory process. Well, kind of the same thing here that we've seen many exits sooner in cybersecurity to larger strategic companies. So those are the those are the kind of things that we look at, given its cyber, given that there's a government angle, given that our own firm makes investments sometimes from that community. We like to see US developed technology, US owned technology, especially, if there's the opportunity for the government to be a customer, not the only customer, but a customer. There are other parts of the world, Israel has a wonderful ecosystem to develop cybersecurity companies. But California and the sort of Washington-New York corridor would be number one and number three in terms of where the companies come from as well. So the heritage and the location of the company is also important for us.

Our next guest is Christian Kameir, Managing Partner at Sustany Capital. Sustany Capital is a blockchain venture fund headquartered in Newport Beach, California. Aside from investing in blockchain-related projects, the firm lends its expertise to existing companies interested in 'security token offerings'.

Christian, thank you for joining us again.

[00:13:50] **Hall Martin:** Great. So what is your participation in the cyber segment so far?

[00:13:54] **Christian Kameir:** Yeah, so the topics that we focus on, as I mentioned earlier, is value transfer, and they are kind of in our head, the keylock systems. What I mean by that, you've got two things, you've got an asset all right on one end, and you've got, let's call it the identity on the other. And to that extent, there's an unlimited number of assets all right, that still need to actually be property – people usually use that term digitized or tokenized, and I don't really prefer the term. But you need to put in a way that they're easier transferable. And we see these come online bit by bit, so we've made a number of investments within that space.

So on one hand, as I mentioned, is the identity side, so we have a couple of biometric investments, and then they are specifically with an eye towards how this data is being secured. And identity is, quote-unquote, onboarded, and that same holds true for assets. So if you do, quote-unquote, asset tokenization if you bring it into a digital bearer instrument landscape like your provenance and Figure, you want to understand how these systems work. So that's why we also put our chip and sort of Figure specifically just went public to a _____ so they're now listed on NASDAQ. It's a super interesting company, and a really good example, really, on how these type of securities should be stored today. And we will go into that a little more high level, but maybe we'll just move _____ to the next question.

[00:15:28] **Hall Martin:** Great. So what do you look forward to invest in cybersecurity in the coming months?

[00:15:34] **Christian Kameir:** Well, so the most interesting call, in my opinion, again, like, call to action, that I really have been putting out for the past five years is, like, develop the technologies that actually allow to enforce the current laws and regulations, because that's sorely missing. We have a lot of let's call it data protection rights, privacy protection right, but it's really hard to enforce. And to make, like, very simple example, like, so you probably hear about this type of class action lawsuits that are going on against companies that lose your data every year, right? So they happen all the time, they will continue to happen for some time. But a lot of these claims, they are not actually being cashed, about 40% of these claims against companies and user data are not being cashed. The reason being is because there's more often than not some form of evidence required. So I always make it a point to push back against any settlement. But I have my own procedure for that, and I have my own email address for that, and I push it back against any settlement. Because to me, this shouldn't have happened in the first place, it was foreseeable, it was avoidable; and as far as I'm concerned, knowing that the technology landscape, you could have avoided this with the proper application.

Anyway, so what I look for to invest in is we need to clean up the digital landfill that we call the World Wide Web. So really build applications that serve that purpose. _____ be proactive, right? So at the end of the day, unless we clean up the mess that we created, then these things will happen again. Right? So on average, it's been predicted that the identity, quote-unquote, of a US citizen will be stolen anywhere between three to four times for each US citizen in the next decade. And that's an externality of those data breaches, right? So you can buy these complex datasets for pennies on the dollar, and that's just step one. So that's where regulators finally are catching up to. There's a much bigger topic here that no one yet talks about, which is this whole social engineering as a service disaster, because, if you look at the Cambridge Analytica example that had made widescreen spread news, it's really just the tip of the iceberg. It's not like companies that sell these type of solutions have stopped selling them. They're still selling them, they're still selling them the same way, and they're training their customers on how to use them. That this hasn't been stopped is a real disaster, but my suspicion is a huge reason for that is because it's really complex and hard to provide evidence for these wrongdoings. So provide tools and, like, on a simple level, provide user tools, provide these browser plugins that track certain behavior, so you can actually track it back. And the usual example I typically make for

that is, and that's something that's the most, like, needed missing layer for the web today is we don't have an agency attribution there. What I mean by that is, right now, you can stumble across information online, and people will and they will act on it. And think about an example where someone, let's say, drinks bleach to cure virus infection, because that's the information that he found on some website; so while you could say that this person was just really unintelligent in his behavior, or that it's no one's fault, but we have sort of evidence to the contrary. What I mean by that is, so if and when you actually do something that can be attributed to you that leads to other person's harm, it will actually, you will actually forfeit your right to free speech. The typical example that the Supreme Court made for that, I think decades ago at this point in time is shouting fire in a crowded room, in a theater people run out, people get trampled and hurt, and so that person was, at the end of the day, held liable for that particular action.

So I think that translates really well to this world: the problem is online, it's really hard to create attribution. So if you find this information and, as a result of using this information, you get harmed, there's no way for you to right now track back how you actually got there. And I think if we provide this type of, let's call them, evidence tool, you would be able to do that. And it would be really, really useful, and I think it really needs to be done, because it's the typical thing, where if you, right now, want to find evidence for anything, you can go to your favorite search engine and ask is the world flat and the search engine will provide you with websites that confirm that particular idea. And that's true for basically anything, so this is possible and this is not being penalized, that seems to be at least questionable. So the call to action is _____ provide these type of tools that track causality, because then you give the lawyers the weapons to actually enforce the laws that we already have, which we don't do right now.

Our final guest is Andrew Morris, Founder at GreyNoise Intelligence. Headquartered in Washington, D.C., GreyNoise helps security analysts save time by revealing which events they can ignore. They do this by curating data on IPs that saturate security tools with noise. This unique perspective helps analysts confidently ignore irrelevant or harmless activity, creating more time to uncover and investigate true threats. Andrew, thank you for joining us.

[00:13:37] **Hall Martin:** Great. So what is your participation in this segment so far? What exactly are you doing here?

[00:13:42] **Andrew Morris:** Yeah, so GreyNoise specifically plays in the security efficiency space. What we do is, we're very much trying to, we come in and we will – analysts can use our product to quickly figure out if something that they're investigating is something that they should be really concerned about, or if something that they're investigating really doesn't matter that much at all. We take a data driven approach; we're very, very explainable; we are very transparent in how we come with our conclusions. And so, we firmly play in the security efficiency space, specifically, selling to the security operations center of the Fortune 1000, any organization that's large enough to have their own security operations center. And the way we

do that is similar to a lot of the methods that some threat intelligence vendors provide. So companies like FireEye, etc., instead of us providing you intelligence on where the bad guy definitely is, we're actually providing intelligence on where the bad guy probably is not.

[00:14:46] **Hall Martin:** Great. And so what do you look forward to invest in this space?

[00:14:50] **Andrew Morris:** I would look for, to invest in this space, look for traction, look for excited users, look for anything that any cybersecurity company that, if they're a smaller company or a younger company, look for companies that do one thing and do them really well. Don't look – I would be turned off by companies who claim to do it all or solve it all, because I find that incredibly unlikely. Any companies that collect and analyze data uniquely that other, that buyers and other security product companies can buy access to, I think is something that's going to be valuable. Those are some of the things that I would look at when I am investing in companies right now.