IP Cybersecurity Show 2
COVID's Impact on Cybersecurity:
Primary Trends and What Makes For a Successful Company

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 the primary trends and what makes for a successful company in the cybersecurity segment.

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. **Ariel Evans, CEO/Founder, Cyber Innovative Tech**
4. **Christian Kameir, Managing Partner, Sustany Capital**
5. **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.

[00:15:46] **Hall Martin:** And so what do you see is the primary trend in the cyber segment today, what do you see coming up right now?

[00:15:54] **Greg Fitzgerald:** It's _____ on cybersecurity today. We're seeing, in essence, a trend around privacy, because now people recognize that their data is being used, not getting compensated for it and potentially being misused overall, protection of what they do have, and a big trend with coming forward is really about understanding from a from a corporation's environment, the understanding of the organization; and with COVID, in particular, the environment's gotten more sophisticated. So let me describe that. What used to be just five years ago, 10 years ago at max, where everything was very centralized, right, people were in offices and they had central offices; and if you're going to access the network of the office, you had a VPN, COVID just exploded that, and now people were not only working remotely, but they're working from a variety of places remotely, be at the beach, the mountains, their family's house and their house. They're using personal devices, not always their own, for example, they'd be using their kids' device that has games on it, that of course has malware, and basically, systems that might be calling out to servers that are nefarious of sorts from an IT corporate perspective. The exposure to the opportunity for bad guy to take advantage of that is now rampant, and the understanding of the corporate environment is more confused than ever, because they've lost some of that control and understanding. And that's everything from how someone buys a computer, right before it was like usually _____, now people are like, they just bought it online, bought a used one, or I went to apple.com, or I went on Amazon. Nope, not telling the IT department what they've got and just showing up with a computer. They got cloud apps that are coming out. Right now, _____ Office 365 is in the cloud, it used to be obviously a mail server on premise. That's changed tremendously with Zoom, great example. Everybody's got Zoom. But if you don't Zoom, you're using a Google Meet or you're using something else. And so that's, you know, the application environment is exposed, and so the dynamicism of change, and the exposure, everything, is really driving new cybersecurity solutions to adapt to that model. So what I see kind of summarizing the trend or what I see coming is we're seeing a very rapid lifecycle of cybersecurity technologies, that three years ago were brand new, game changing, transformative, they're already outdated for the today's environment. And so, there's a whole plethora of new ones. And one of the things that I've experienced in cybersecurity as a vendor is literally every three to five years, there's a transformation of an entire new category of products that need to be protected, or that the aging of technology has come forth. And that's where an opportunity for an entrepreneur, for sure to recognize those things, and that opportunity to say even if something started five years

ago, it's probably almost outdated now. And if they were successful, which a lot of them are, then the idea is, as a startup, you're nimble; as you grow, you become more entrenched into your inertia of who you are; you have a lot of technology debt, so to speak, that you can't change to the new environment very easily. And so, it's a great opportunity for an entrepreneur to come in there and kind of take over some market share of that.

[00:19:27] **Hall Martin:** Great. So what makes for a successful company in the cybersecurity world, what do they have to do to be successful?

[00:19:33] **Greg Fitzgerald:** I think, in particular, while cybersecurity is a relatively new field, I mean, again, in the late 90s, it was really software firewalls and usernames and passwords. Now, over the past 20 years, it's gotten to be a lot more sophisticated and everybody is – it's a very small world, so it's kind of who world. So meaning, what success is the people that are in it should understand the domain very well, in the sense of, kind of, what is its purpose as well as the context and knowledge of the history of how it's evolved. I say that because it's been so much mergers and acquisitions, so much of technology adoption, companies have changed names a couple of times, and so understanding how that has evolved over time is really crucial to see, again, the opportunity, as well as to avoid kind of getting run over by traditional technologies that may not have the technology promoted today, but maybe understand significantly how to just extend themselves and take over the market opportunity of a small company. I also think this is an industry of respect, meaning, people are very skeptical. In the past five years, in particular, an enormous amount of venture capital has gone into this market space, and everybody's got a great widget. The challenge is marketing, and I am a marketer, I've been part of the problem – we overstate our claims for what the products can do. And so there's a huge amount of skepticism on what a product says it can do functionally, as well as its capabilities and its future growth. And so, that's a key element of being more authentic, more sincere, more practical, and even proven it out is one of the key opportunities for success. And then obviously, it's just the market opportunity. There are lots of little niche areas that companies can play into. But as an investor myself and entrepreneur, people need to go after big market opportunities. The small ones are great, they might be great for a lifestyle type business. But if you're going after venture capital, obviously, they want to see a much larger market opportunity. So the key is to navigate that in a company that can say, yeah, go where the puck is going, right, always. And so, make sure that you you're targeting a big opportunity, you see _____ being transformed or, frankly, the traditional players are just outdated. That's the best opportunity that I've been playing in myself in the past 20 years.

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.

[00:08:26] **Hall Martin:** So what's the primary trend in the segment at this timeframe?

[00:08:31] **Merrick Andlinger:** Well, I guess, I like to say that security, in this case, cybersecurity, is an enabler for digital transformation. And so, if you think about that statement, we're moving, our society and our businesses are moving more and more to digital, whether it's online, and security is central to that. If businesses and people don't have confidence in their new ways of connecting and interacting, we're just going to have problems. So that's the foundation, and that's going to continue into '21 and beyond. Last year was a cybersecurity investment, was up about 15% from the year before. '21 is looking to be strong as well. I know from the pipeline that we have, we'll be making a number of investments this year. We're seeing rounds, funding rounds be much larger than they had in the past. So there's a trend. And if we look at some big hacks, SolarWinds, that massive hack revealed vulnerabilities in supply chains, for example. Healthcare systems, we've seen overburden by COVID, we've seen ransomware attacks on hospitals putting patients at risk. Think about the connected devices in a hospital, you might have an infusion pump or a respirator or something that's connected. Those are vulnerable, and companies are looking at putting in layered kinds of solutions. And so, I think we're going to see more security as a service also. So these are, there's not a primary trend other than up and more, but there are a whole bunch of things going on below the surface.

[00:10:24] **Hall Martin:** So what makes for a successful company in this segment, what do you look for?

[00:10:29] **Merrick Andlinger:** Well, I've been in a number of segments in my investment career, and what makes a successful cybersecurity company is much the same as in any other sector. There's good timing, so you have to be right, you can't be too early, you can't be too late. The team, you have to have the right team, you got to have the right technologies. So those all come in, come into play in what we look for.

Our next guest is Professor Ariel Evans, CEO/Founder at Cyber Innovative Tech and client of TEN Capital. Cyber Innovative Technologies is a technology innovator that provides an integrated cyber risk management platform that allows organizations, governments, regulators and their third-parties to become more cyber resilient.

Ariel, thank you for joining us.

[00:16:38] **Hall Martin:** 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.

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.

[00:07:24] **Hall Martin:** And so what do you see as the primary trend in the cybersecurity space coming up here?

[00:07:28] **Christian Kameir:** Yeah, so I think finally, after all this time, privacy has become its own discipline. And after law school, I taught privacy law for a short period of time, and that was back in the old world back in Europe. And so, this is finally also coming to North America, so definitely aware about things like GDPR, the general data protection rights in Europe, and this was to some extent, modeled here with CCPA, California Consumer Protection Act. But now there are six other states in the United States working on similar laws, so Connecticut, _____ Mississippi, New York and Virginia, they're all working on similar laws to protect their citizens. And there's also another movement and you probably heard about this lawsuit in this context against Facebook, because that was already filed in 2015, and it's based on Illinois's biometric law act, which has a really interesting name, it's called BIPA, so it's really easy to remember for those who like beer. And so, there's other states now that they are planning on passing similar laws. So specifically, it's on the shortlist for Maryland and New York. And Facebook had by themselves originally proposed a half a billion dollar settlement, and actually that was just revised, and it's now $650 million in settlement fees for that class action lawsuit filed on behalf of citizens of the State of Illinois. But they are still suing Amazon, Google and Microsoft for the same violations for using the biometrics of citizens to train their own AI, that was kind of the impetus for that. And you can clearly see how that might be relevant across the world. Right? So where now you got a lot more biometric implementations in airports and other

security sensitive areas, and one thing that we are _____ to some degree is _____ local law enforcement and cybersecurity agencies. And so they have, like, specific problems around the topic of things like police body cameras, i.e., what is a permitted use of this body camera, when and where can you actually run a query against your biometrics, and where does it come from, like, what was it obtained legally in the first place. And so, I don't want to go too deep down the law rabbit hole here, but you're probably familiar with the doctrine of the fruit of the poisoned tree, which is if there was any part of evidence obtained in violation of any law, right, it doesn't matter what it is, then any subsequent action is going to be deemed inadmissible. Anyway, so again, I don't want to go too far down that rabbit hole, but the overriding trend here is really privacy is fine, you have the _____ become its own discipline within cybersecurity, it's a huge growth area.

[00:10:33] **Hall Martin:** Cool. So what makes for a successful company in this segment going forward post COVID?

[00:10:38] **Christian Kameir:** Well, you've probably heard this old quote that's being attributed to Gretzky, that hockey player, I don't know anything about hockey aside from that crowd, but it's like you want to skate where the puck is going, not where the puck is. Right? And that goes back to what I said earlier, so there's a lot of laws that are being passed now that companies need to be compliant with and there's a lot of work to be done, because the current situation that we created is largely untenable. So what I mean by that, if you look back throughout history, and I think most people know about data breaches like the Equifax data breach, where basically every US citizen's data was stolen. So it's not something that you can take back. What I mean by that is, it's not like this data magically disappears from the web. Right? You can buy this everywhere. And actually, the credit agencies specifically have been charged with actively selling this data to crime organizations incidentally, or, like half willingly just ignoring the fact that they could have been identified and so forth. So if you know that, so skate where the puck is going, skate towards actually enforcing these laws using technology, right? So that's actually, to me, as far as I'm concerned, the more interesting part, because to go after the perpetrators is next to impossible.

So I have dinner with the head of cyber crime here every couple of months, and so the first thing that I learned is that these poor guys are totally overwhelmed. He's like, well, I'm in charge here for cybercrime for Southern California, but I'm essentially fighting the entire Eastern Bloc with my little department. But there's really no good way to move this back, and maybe some anecdote from my early days in technology, when we still needed to buy server _____ and put these into datacenters and so forth, once you start looking at these server logs, you actually get really afraid. So what I mean by that is like, one random example, a third of the World Wide Web is run now on the CMS, content management system called WordPress, and it has a very particular structure. And so, what it does though is if you have a very particular structure that's identifiable, you can write script to go after those installations. And either hackers will just do this for sport, and/or because there's actual financial gains to be had. And it doesn't really matter to the script at the end of the day. So what I mean by that is, there's very typical attack vectors that you will see in your server logs. So if you have, let's say, a WordPress

site, there's a typical login file, if you don't change that, you will just create an enormous amount of traffic to that. So it's just like simple best practice that people simply don't know, because they never had to do these type of installations that are being ignored. So if you can install the software yourself, but you don't know those details, you're very prone to make these very, very simple mistakes. That's why it's good to know the basics of these installations and how they work.

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.

[00:08:33] **Hall Martin:** Great. So what's the primary trend in this segment going forward?

[00:08:37] **Andrew Morris:** So I expect to see a lot of cutting edge technology that's going to come up that is looking at historical problems that the industry, that the buyer has seen through new lenses. I expect to see more companies that are focusing like, again, on the basics. I expect to see more companies taking more positions in quantification of the returns to the user and to the customer. I expect to see the security industry start borrowing more and more from a lot of the major technology companies that have been wildly successful that use product led growth, which is to say, instead of the flow being, hey, I'm a firewall vendor and you have to – you call, you know, your chief information security officer calls us and say, hey, I'll take a 1000 firewalls, please. Instead of seeing something like that, I expect to see more and more user based, you know, you could call it freemium, but kind of product led growth of kind of like companies like Slack and Datadog, these companies where there are people that are practitioners signing up to use services, cybersecurity services. And then that kind of dovetailing into enterprise products and offerings, and I expected to see much more focus going after practitioners and growing that way, as opposed to kind of the traditional top down sort of targeting the very top executives and trying to sell massive, massive accounts to those, because I think that the world just prefers it that way, and I think that that's going to be – so that's going to be the kind of one of the number one things that I expect that we're going to see a lot more of is a lot more product led growth.

[00:10:48] **Hall Martin:** So what makes for a successful company in this segment?

[00:10:51] **Andrew Morris:** Oh, that's a good question. There are a lot of things that dictate a successful cybersecurity company and things that I think are problematic for cybersecurity companies. A successful company is always going to have traction, I mean, it sounds obvious, but it's always one thing to look at is that it doesn't even necessarily have to be customers, but you need a really good barometer, especially if you're not a practitioner, and if you don't

understand cybersecurity, just look for social proof from lots of other people that use it. So the first thing is like, look for products that have lots and lots of use. Obviously, that can break down sometimes, because there are some products that have lots and lots of use and services that have lots of use that people despise using. But I would say that generally, products that have more use are going to have more metrics that the vendors can use to iterate on quickly. So adoption, I would say, the ability to quantify returns to, so any cybersecurity company that can tell their customers how much money or value they're actually generating for them, instead of just saying, hey, the breach didn't happen again, so I guess you should keep buying us. Right? Instead of saying that, you're going to find more and more cybersecurity companies that are really going to have to justify their value proposition to the buyer and to the renewer, so to speak. So I think we're going to see, I would look for that, look for companies that justify their cost, and that justify their value. And I would be very skeptical of companies that feel like they're making up problems that they're solving. The cybersecurity industry is certainly – certainly it is a complex industry and a complex set of problems. But a lot of the time, security companies have a tendency to sort of make up problems, scare you and then believing that they're real problems and then offering you a solution. I think that that worked for a little while, and now I think the market is kind of wising up a good bit, and so there's going to be more and more scrutiny on companies to really justify that they're actually solving problems and providing value. Aside from that, people love open source technologies, people love anything that have lots and lots of users or a community, people who have used it and people who are excited about things. People like products that where there's a lot of explainability and transparency on how the product works and what it does, as opposed to kind of black boxes. I expect to see more of that. Those are some of the things that I think make good, effective cybersecurity companies in general.