IP Cybersecurity Show 4
COVID's Impact on Cybersecurity:
Changes expected in the coming 12 months

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 changes expected in the coming 12 months and our guests' final thoughts.

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:

Greg Fitzgerald, Co-Founder, Sevco Security, 00:56
Merrick Andlinger, Partner & Chief Investment Officer, Option3Ventures, 07:23
Ariel Evans, CEO/Founder, Cyber Innovative Tech, 11:53
Christian Kameir, Managing Partner, Sustany Capital, 17:10
Andrew Morris, Founder, GreyNoise Intelligence, 28:41

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.

[00:28:58] **Hall Martin:** Well, what else should we know about this segment?

[00:29:02] **Greg Fitzgerald:** Well, I really take a look at a couple of key things, where the trends I've mentioned, are moving towards where they're more into visualization of the threat environment, to give an organization and even a person because there is a consumer play to this as well, to have better protection, better privacy of their data, and a better understanding of their organization. And I say that in the sense that, again, look at where things are going and where the puck is going, you got mobility. Mobility has always been one that, for some reason, hasn't truly been protected, not quite sure why that hasn't happened to date, but now the power is no longer server based, it's really at the endpoint base, just as much data as on your endpoint. So that's an area to look at. The privacy element is really key about where the data is, and there's enough regulation with GDPR in Europe, and now the California law about knowing where your data is, and being able to personally request to the people that are holding your data to delete it, get rid of it – that is a key area that I think is going to be continuously growing as we go forward. And obviously, Facebook and YouTube, and all these companies that are using our data, have been able to take advantage of that for a long time, but I think people are waking up, obviously to, whoa, like, that's just not right. So I think there's a great opportunity in the privacy space. And then, like I said, the visualization space of what really is going on in my environment, like, please help me out. Because in the end, for organizations, whether they be small or large, they're making critical decisions about their business based on data, and that data needs to be more than just facts. It needs to be analyzed, it needs to be a package, so to speak, and visualized in a way that they can digest it very, very quickly, right, because they got to really make decisions at speed of business, and move businesses flying along right now, due to the advent of all this technology that's being incorporated. And so, they need to make right decisions, and it's hard to make a good decision on incomplete or not truly comprehensive data. So there's a, I think there'll be a huge move into that area.

[00:31:24] **Hall Martin:** Great. So what changes do you expect to see in the coming 12 months?

[00:31:28] **Greg Fitzgerald:** Well, I'm seeing really, I think people have gotten very comfortable working from home or remote, I'm not too confident that people are very excited to go back into an office, which puts a huge amount of pressure, a continuous pressure on the IT environment, which, again, has to be decentralized in so many ways. The second thing is I see, you know, there are more than 4 million technician jobs open in the IT space, and they're in the cybersecurity space, so I don't know, there's a last statistic that was like, in America alone,

there's 300,000 jobs in cybersecurity that are wide open. We just don't have enough people and enough talented people that are skilled. And so my point being is I think we'll see in the next 12 months and 18 months, because the job market has gotten so difficult, some people are being very strategic and saying, wow, now's a better time than ever to go get a little bit of education, maybe in the cyber world, to go get some skills in that area. And we'll start seeing more opportunities, I think, for the cybersecurity space as a vendor, also, as buyers, because more people understand it, they can understand the technology they need to use to solve the problems that they have. And that's on the positive. On the other side, there's so many cybersecurity technologies in the space. I think we're seeing a very difficult buying environment today, I mean, you just can't get out and show your technologies as easily as one could. So some technologies are taking off because of that remoteness. Others that were dependent on kind of the older environment, like I said, they are struggling. And so, I think we're going to see some consolidation. We're kind of moving to an oligopoly of big guys, right? Like, you can name now the big boys in the world, like, Palo Alto Networks' classic, that's an undeniable fact. They're one of the biggest. But you can name them. You got Cisco and Palo Alto, Semantics falling behind, but you've got others that are stepping up. And so, I think you can see some consolidation on one level at the higher end space, and then you're seeing a lot of little ones that are either going to pop up through the wheat and the chaff, so to speak, of that whole opportunity, and some are going to make it, some aren't. There's just, the volume we have today in the space just cannot sustain itself, so that's going to be a unique opportunity and loss for some.

[00:34:03] **Hall Martin:** Great. In the last few minutes that we have here, what else should we cover that we haven't?

[00:34:07] **Greg Fitzgerald:** Well, I think I'm pretty happy with the space that we're in. I would encourage people to continue to look at it, both as entrepreneurs as well as investors. It is a wonderful space. It is not going away. It continues to grow exponentially in terms of the market opportunities. We've seen so much of that being in kind of the B2C space a lot, right, with social media and all those. I think cybersecurity is one that, you know, it's an infrastructure place, so it has a little different approach to the investment as well as to the return. But it's more assured, because it's like a brick, once a brick starts getting laid, there's a lot of bricks that need to be laid down and we're in a space that cybersecurity continues to need this focused and attention by the market in terms of the investor community in particular, and from a personal experience, it's not going anywhere, it's just going to continue to grow. So I think that's really where we feel things are looking pretty good.

[00:35:14] **Hall Martin:** Great. Well, thank you for taking time to join us today and hope to have you back for a follow up soon.

[00:35:19] **Greg Fitzgerald:** Thank you very much.

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.

[00:16:56] **Hall Martin:** Well, so what else should we know about the cybersecurity space?

[00:17:01] **Merrick Andlinger:** It's a whole lot of fun. But we like to think of cybersecurity as it's horizontal so that it crosses through all of the other sectors in my investment career that I've worked on. It crosses through energy and through consumer products and through government services and through media, and you name it – it's something that is central to our economy, central to the functioning of all those different sectors. So one of the exciting parts is seeing where the companies we invest in can tailor their solutions to those kinds of companies across the industry spectrum.

[00:17:49] **Hall Martin:** Well, great. And so what changes do you expect to see in the coming 12 months in this space?

[00:17:55] **Merrick Andlinger:** Well, looks for speed, so fasten your seat belts. One of the areas that, it's our newest investment, but that we're excited for the sector as a whole is connected car security. And if you think about it, in the automobile sector, cars are increasingly computerized, there could be 60 to 80 separate processors in your car doing different functions. Some of them are self-contained, but many of them are connected into networks, and many of those are connected outside to the internet in one way or another. And you don't have to wait for autonomous cars for this to be the case. Think about your information system in your car, your warning system – if you drive off the road, it sends out an SOS. This is only being accelerated, and cars last a long time. People need to feel secure that when they're driving along at 60 or 70 or 80 miles an hour that there's not some problem, there's not a ransomware problem, they're not working with faulty security, that their automated cruise control will actually slow down when it detects a car ahead of it. This kind of thing that is using the right types of code, these are exciting areas, these are ones that I think people on the street can relate to because everybody's in a car doing something. And so, we're very excited about what that can mean and look to see a lot more for that in the coming 12 months.

[00:19:33] **Hall Martin:** Great. Well, what else should we cover that we haven't so far?

[00:19:39] **Merrick Andlinger:** I'm going to draw a blank on that one Hall. I think we talked through a number of, a number of things here. So I got covered about everything I want to cover unless there are any other questions you want to ask me or something you think, I know they're going to edit this part out that anything else you want to comment on.

[00:20:02] **Hall Martin:** Yeah. So I've heard that in the cybersecurity space, every three to five years, there's a whole new set of care-abouts: platforms, technologies, devices or whatever. How do you manage it in a situation where every three to five years you got a whole new set of things to do?

[00:20:20] **Merrick Andlinger:** That's a really good question, and it relates exactly to the velocity of investing in the sector that I've talked about. And so, some of the solutions layer on top of one another. So just because there's something new coming down the road in the way of a problem or in the way of a solution, it may be incremental, so that the old solution can still stay in place or it can evolve. In some cases, you have legacy systems where they might have a 20 or 30-year life, think about the factory floor, think about our electrical distribution system. So again, those things can be incremental. Some of the newer things like you're talking about, quantum computing, and what that means for cryptography, and what it means for security measures is going to blow wide open just about everything that we're working on. So it's a matter of being nimble, picking the right spaces, but that's the nature of this fast moving sector.

[00:21:22] **Hall Martin:** Great. Well, appreciate your taking time to join us today, and hope to have you back for a follow-up soon.

[00:21:29] **Merrick Andlinger:** Good. Thank you. Anytime, enjoy it.

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.

[00:20:56] **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.

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.

[00:21:05] **Hall Martin:** So what changes do you expect to see coming in the 12 months in the cybersecurity space?

[00:21:10] **Christian Kameir:** So, one of the largest things that we focus on is the new implementations of money that people are proposing. And so, they are specifically things like digital bearer instruments, so digital cash, in the form of _____ digital currencies. So 80 some percent of all countries are working on that, and have been working on that, and we talked about that. And so, to the extent that they come into being, they create new honeypots, because your bank account is one thing, it's insured and it's being protected by a corporation and their resources, but it's a whole different thing if you have a digital bearer instrument that you store on a digital wallet that either resides on your phone or on your desktop, coming back to, as I said earlier, the whole cryptocurrency space is a very tempting honeypot for hackers, because you don't have to interact with anybody or you don't have to go to a bank, you don't have to do anything physical, but you got all these addresses out there, they're literally addresses in cyberspace that you can address and attack. And so, it's not going to be different for CBDC. So it's China's estimate now, like, they're going to issue _____ this year, and then other nation-states have to follow suit. So expect that a large part of the population within the next 12 months around the world will have additional digital wallets that they're not used to. So it's just something new that they need to secure, secure your physical wallet in one way, but you don't necessarily think about your phone as something that holds the equivalent of digital cash. So I think that's going to be a large inflection point. The other large inflection point is, as we

start to travel again, there's going to be a lot of attempts to track people's health data. So there's already things being proposed, like the health passport and so forth. So there's an enormous amount of fraud possible around this particular data, either in a way where, well, if I want to conceal a certain status, I can conceal it and/or I just want to cause havoc on a certain system and just cause false flag operations for the LOLs, you probably have heard that term, for the laughs. Right? And that's a huge motivation overall in the hacker space.

[00:23:41] **Hall Martin:** So that's great. Well, in the last few minutes that we have here, what else should we cover that we haven't?

[00:23:46] **Christian Kameir:** Yeah, so I think the thing that's largely not understood and that's recognized at scale yet is that the World Wide Web, as we know it, the internet, as we know, it, is about to undergo change, and it needed to undergo a change for a long time, and it has been a long time coming. What I mean by that is, so for centuries, we've facilitated commercial activity using paper, right? So up until the early 60s, all commercial activity had some physical paper attached to that, you had file folders and _____ and paper in that regard is good for security, because you have it in your own possession, and if I wanted to have that paper, I have to find where you keep it and break into your house and take it from you, and that holds true for things like bearer instruments, something like shares or otherwise securities, but it also holds true for anything that pertains to your certifications and identifications like passport, for example. Right? So identity theft is a huge problem. Well, before databases were created to do identity theft, i.e., if I want to get a hold of your past, I'd have to find where you live and find out where you live and then break into your house and steal it. So that's a huge feat. So it's a much smaller attack for focus, so it's kind of a decentralized system organically by the virtue of that particular technology. So fast forward to 1960, we started introducing databases, which introduced a lot of efficiencies, but a lot of surface structure, a lot of the attack vectors. And then, what made it much, much worse though, which increased the tech vectors by orders of magnitude is to attach these legacy databases to networks, including the internet. So the larger point here being databases are actually not suitable to protect your data, so you can't protect data that's in a database. Any engineer will tell you, it's basically impossible, because at some point in time, you have to retrieve it.

So what's the retrieval mechanism? Most likely, for the vast majority of databases right now, you got one or typically a lot of systems administrators and/or just simply users at the company that's maintaining those data silos. So like, typical example, as you call your credit card company, and some person in some lower wage country will answer your phone call and will ask you for specific information that he/she can identify seeing on their screen, right? So that this is possible should strike you as very suspect, because a worker in these context will often make something to the equivalent of $5 an hour, that's not very unusual. But your data, your individual data on the market is worth about as much. So if and when and where these people then leave their jobs, there is a significant likelihood they will take some of that data with them. But moving on to what we need to fix, we essentially need to avoid using databases altogether for personal identifiable data and for assets. And so, the obvious solution, well, obvious for people that technology investors in that space with all background, all of this, this information

needs to be cryptographic primitives. And so, what I mean by that is that people usually have heard about blockchain, so blockchains, to some extent, deal of that, but it's more likely acyclic graph based solutions that point to these. So, to make it very simple, think of it as a digital unique bearer instrument, so that you have your passport, the thing that I referred to earlier, but in a digital form.

So in this case, if you're the one that has control over it, well, you're the one that needs to _____ to divulging it. So it's not an unlimited number of people who have a copy of it right now, so it should invalidate all the copies. So the larger point here is this to me is the main infrastructure change to what we call web 3. So getting rid of database, specifically, getting rid of databases for the use case of storing personal identifiable data, I think that will simply not be viable. So the new topology, that's how I called it, the new network topology for the World Wide Web will be reversed. So right now, the way I like to explain is you, as a person, as an individual, you from the network's perspective, you're like an Oracle. So an Oracle is a thing that spews out data that the network observes and then stores and does something with it. So that paradigm needs to be reversed to where, if you look at things like GDPR, GDPR tells you that you have to forget data. Well, that's really not a practical thing to do. Once data is digital, you have millions of copies floating around, it doesn't matter if you tell one company to forget it. And that's actually, for the most part, even not possible for that one company, because they have, whatever, tape backups and otherwise, backups is a really, really hard thing to do from a technical perspective.

So what really needs to be happening and I expect this to happen all the time is that the laws will be revised to the extent that you have the right to not be observed, because the only way to protect data is to simply not have it, so to just leave it with you. And I think that is a crucial, moment in technology development and cybersecurity history that we need to acknowledge, like, we did these mistakes in the past, so let's make sure we don't double down on these next mistakes, and I see this every single day. So I see every single day that people still create what I call account based systems, so when you have a username and password to access their system, it tells you there's some form of database. And maybe there's actually kind of a blockchain or graph based solutions behind that, but then there's like a crude recovery mechanism that falls back to that paradigm because it's very tempting, and it's like, a lot of engineers have been so indoctrinated in this paradigm, that you have to have a username and password account based system. So the larger expectation from you is that we get rid of account based systems, so they won't be databases that entail stories, so that at the end of the day, you're no longer an Oracle in the World Wide Web, but you are an actual agent, you actually have agency. So what I mean by that, in order to have agency, you need to actually be able to control who gets to even observe your data before it even gets stored. And that should default to none. Right? Because as soon as you have detected these technologies, by the way, a lot of things that are legal right now should become illegal.

So what I mean by that is, let's make one simple example. Right now, if you're opening up a bank account, what happens? People at the bank do a process for you that's called KYC, know your customer, which is a window-washing term within the laws and regulation of anti-money

laundering. But the reason why you do this is at account opening, and opening up an account, obviously, you didn't do any transaction yet. So why do we need to disclose the information? The reason is the legacy technology, so the current laws were written towards the legacy technology, so they are specifically database solutions. So if you have a different solution, if I can attach a _____ your name and address and so forth to a transaction, only if that's added, only if there's a specific requirement for that, then this dragnet approach that financial service providers are doing right now, should be unlawful, because of what fits the definition of illegal search and seizure. So you can typically just walk into a store and take out your wallet and hand over cash and get your merchandise, but by virtue of legacy technologies, by the virtue of database solutions that have been custodied by financial service providers under certain obligations, we actually got into a situation where we extended government functions to these pilot service providers. That shouldn't be possible in the first place, but again, it's mostly, in my opinion, an externality of legacy technologies that didn't allow for a different mechanism in that regard.

[00:32:30] **Hall Martin:** Great. I want to thank you for joining us today, and hope to have you back for a follow-up soon.

[00:32:34] **Christian Kameir:** Of course.

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.

[00:16:03] **Hall Martin:** And so what changes do you expect to see in the coming 12 months in the cybersecurity space?

[00:16:09] **Andrew Morris:** I think while the markets are the way that they are right now, so most people would agree that a lot of tech stocks are artificially overvalued by a lot of the fundamental levels. And so, while the Fed policy is what it is, and bond rates and interest rates are really low, you've got a lot of investors that have a lot of money, that would have gone into bonds, but there's no growth there, and so they're putting them into growth stocks, tech stocks. Right? And so, a lot of tech companies I think are pretty overvalued right now, and while these companies are still pretty overvalued right now, I think that they're going to want to hoover up as much intellectual property as they can, buying up and consolidating other companies as much as possible. So I expect to see a lot more acquisitions, major acquisitions, many $100 million and many billion-dollar acquisitions. I absolutely expect to continue seeing this. I expect to see more companies coming back, coming up – I expect to see fewer companies that are using AI and ML to solve problems. I expect to see more companies that are targeted towards to solve cybersecurity problems that is. So we see more companies that are bringing in trust,

safety, explainability into the ML and AI process, which is a little bit different, and obviously, it's not a cybersecurity thing. I think that when the market's correct, I think that we will probably see a lot of the companies that don't have strong value propositions, kind of, fire sale or fail is what I expect to see when budgets get tight, because right now it has been historically – it's been pretty easy to sell security products, I think, in general. Trends, that's, I mean, I would say a lot of that is mostly going to be obviously on the market side in the industry, specifically. I expect that we're going to continue to see lots of specifically of, in the context of cybersecurity happenings, we're going to continue to see lots of nation-state activity. We're going to hear about a lot of this kind of stuff. A lot of people heard about SolarWinds. We're going to continue to hear things like SolarWinds. I think there's going to continue to be a lot of high profile vulnerabilities in common enterprise software that a lot of people use, and I think that that's going to really scare the pants off of a lot of people and that has a tendency to make people buy security products, so I expect to see that continue. There's every major happening, there's going to be a company that's going to pop up that's going to say, hey, if you bought us that wouldn't have happened. Right? And that may or may not be true, but they can still say it.

And I think that we are going to continue to see lots of pretty, pretty nasty ransomware. I think that's going to continue for some time, and certainly as the economy is more and more unstable, but the price of things like cryptocurrency, Bitcoin, Ethereum, etc., continue to go up, certainly I think that there's going to be – there's a lot of reasons for ransomware to continue, so I expect to see a good bit of that. I hope to see good effective consolidation. I hope to see more companies focusing on doing fewer things and doing them better. And I think that it is possible though I don't expect that it'll happen this year, but at some point over the next few years, I think that the industry is going to look at itself in the mirror and really ask the question, how much of these problems can the industry really address, especially as it relates to big scary nation-state attackers, like all of the large geopolitical enemies of United States. I expect to see more and more, – I expect that sometime in the next few years the private sector, the cybersecurity industry is going to, at some point, ask the question, how much of this are we going to be expected to be able to defend against and how much of this literally has to be the role of the government, the Department of Defense, the military, etc., so there may be some kind of shift of burden from the industry over to government. But honestly, I'm not really sure, that's more of a policy thing, so I'm not sure. I would expect to see more consolidation though. Certainly, I expect to see more companies coming up that are looking at the basics, more companies that are built around building trust in AI and ML, and hopefully more companies that are built towards sharing information and sharing data between organizations to help them make better security decisions. That's one thing that I haven't seen enough of that I would really, really like to see more of. Any security company at all, that is strictly trying to help different companies share information with one another to try to protect themselves, I haven't been wildly impressed with a lot of those companies. And so, I would like to see more of those over the next year or so.

[00:21:47] **Hall Martin:** Great. Well, what else should we cover that we haven't?

[00:23:23] **Andrew Morris:** I had one thing that may be worth touching on, on how COVID changed cybersecurity.

[00:23:39] **Hall Martin:** What's your take on that?

[00:23:55] **Andrew Morris:** Yeah, so COVID-19, and the whole pandemic, I think, really accelerated the rate of change in a lot of things that were inevitably going to happen on the cybersecurity front. So all of a sudden, you had, instead of a subset of people who are working from home, you've got almost everybody who are in the offices who have the ability to work from home or working from home. And so, what that means is that from a security perspective, this entire idea of the perimeter, of the network perimeter, the safe enclave, the safe perimeter is completely gone. You now have work devices on home networks, Starbucks networks, I mean, on tons and tons and tons of networks. And so, you're seeing a lot more attack surface, and a lot more places where things can go wrong. And so, I think that that was going to happen eventually. At some point, it was inevitable, where we were going to realize that for a large amount of the work that we do, there's really no reason for us to be sitting in the same room with each other. And so, I think that that was already going to happen. But I think that more organizations were more prepared for that than others, and I think that an entire new set of companies popped up to try to help businesses deal with that as it happened. But it was certainly really interesting, and it was really, I think it was really illuminating on all of the problems that we'll have with this dissolving of the idea of the security perimeter, etc. So I thought that was incredibly interesting.

[00:22:49] **Hall Martin:** Thank you for joining.

[00:25:53] **Andrew Morris:** Thanks so much for having me.

[00:25:55] **Hall Martin:** Thanks. Have a good one.

[00:25:56] **Andrew Morris:** You too, bye.