Hans Albrecht
Hello, welcome to the Horizons Generation ETFs podcast. I'm Hans Albrecht, Portfolio Manager and Options Strategist here at Horizons ETFs. Today we bring you part two of a conversation I had with Cameron Schuler, Chief Commercialization Officer and VP of Industry Innovation at the Vector Institute for Artificial Intelligence here in Toronto. In it, we focus a little more on the important topic of cybersecurity and how it all plays into the wellbeing of all areas of Industry 4.0. I hope you enjoy it.

Hans Albrecht
A little pivot here. I know that you have a little bit of an interest in cybersecurity and I do too. I think it's an area of concern. I almost see it as if we sort of look at the major pockets, big data, and automation, and robotics, and internet of things, and augmented reality, virtual reality, all these kinds of perhaps more interesting and fun things, I find in the middle of that there's this idea of security.

Hans Albrecht
I've explained it to folks as look, "All these other areas are going to have a difficult time growing without relying on this sort of on an increasing need for security." Again, Equifax is supposed to pay out a massive amount due to the breaches they had a couple of years ago. These breaches, these headlines of breaches are certainly frequent these days. So we're seeing a need for cybersecurity. From an investment standpoint, how do you feel about that area? Is there anything in particular about cybersecurity that gives it longevity, that gives it sort of heft?

Cameron Schuler
Yeah. So I think it's a perpetual arms race. I think it's always one side trying to keep ahead of the other one. So I don't think that's going away, and I don't think it's ever going away. I think it'll be continual. The dollars on the illegal side are huge. So the chair of ESET, which is a security company, said it's larger than all the other organized crime in the world.

Hans Albrecht
Wow.

Cameron Schuler
Part of it is because you don't physically have to be there. So there's a bunch of those aspects that there's a degree of anonymity, you can be in a different country, you can be around the world. But it's kind of funny too. Some of the big thefts have just been not good practices. So the one, I think it was Target, if memory serves me correct, where somebody came in and they went to their HVAC supplier and there's lo and behold, a username and password that they could use. So because there's so many dollars involved, it still had a cybersecurity component but they just kind of went through a different methodology. So if the prize is big enough, they'll create specific hacks exactly for that one. You may never see it again. So those are the things that make it riskier. So yeah, it's this perpetual, "How do you keep up piece?"

Hans Albrecht
The crooks seem to be ahead of the cops much of the time. I see that as an interesting sort of revenue. It has an interesting revenue implication for companies that are in cybersecurity, either in creating protocols, or specific software, or different approaches to cybersecurity. It isn't really something that gets solved, does it? I mean, it's sort of this cat and mouse thing that continues in perpetuity. It doesn't get solved, does it?

Cameron Schuler
No. This is something that I think really will go on forever. So about 20 years ago, I had a company that did network security and anonymity and that one I should have kept going. But the dot-com boom was not in our favor when it came to financing. Yeah, it's, it's one that I think we'll just go, and go, and go. The other interesting thing is too, if you look at it from a military perspective, there are companies that can get really good at cyber warfare in a very short period of time. So it's not that it doesn't have implications, but these aren't people on the ground. These are people staying in their own country, maybe yes, maybe no, but for the most part, staying in their own country and doing things. So yeah, it's definitely a changing world.

Hans Albrecht
It's a less obvious form of warfare, but it's happening almost below the surface. As you say, there's this anonymity to it. It's probably easier than ever to perpetrate these crimes partially due to the nature of the technology. The money being made is quite staggering. I remember hearing that some of these sort of crime conglomerates are being run very much like companies with various levels of management. I mean, there's so much money being made. A lot of these companies are being run very efficiently to accomplish what they're doing. Some of the dollar amounts are in... If you think of lost productivity and if you start to extrapolate into the various sort of areas that money is being lost, we're talking about trillions of dollars. This is not small potatoes.

Cameron Schuler
Yeah, most definitely. I mean, wasn't it the bank in Bangladesh that lost a huge chunk of dough? It was hundreds of millions?

Hans Albrecht
Is that right?

Cameron Schuler
170 million? Yeah. So these are things that they're certainly not victimless. There aren't a lot of teeth around financial crimes either. So there's a whole bunch of things that happen that are different. I think we'll see it when a large company goes out of business because of it. I think we'll see a big change at that point. I don't know who it will be. I certainly don't have that crystal ball. But unfortunately, I think that will happen at some point where there's a large company will lose such a large chunk of money, either their customers will or they will that would be pretty catastrophic. At that point, we might see a change in the way the world works.

Hans Albrecht
I almost wondering from an insurance standpoint, if you're going to have trouble at some point being insured, if you don't have a certain protocol in place, if you can't prove that you are doing your absolute best and you're not spending a certain amount of your IT budget in cybersecurity, you might even have trouble getting basic insurance for your business. Could we get to that point where it's considered that critical a part of the way we do things in the future that we all have on a personal basis, from a business level that we have these things in place to protect us?

Cameron Schuler
Yeah. There's certainly products now that you can get on a personal basis. If you look at corporate director liability, this is one that if you're not paying enough attention... When you go through your risk register, so what am I looking at for risk in the business? All of a sudden, if you're not taking those seriously, it really could be something quite catastrophic. So yeah, I think it will definitely go that direction.

Hans Albrecht
I think there were a couple of cities in Florida recently, I think one of them paid the ransom. It was ransomware that they got hit with. It was so disruptive, the only solution they came up with was, "Let's pay the ransom." You know, Baltimore was hit as well and they said, "Well, we're going to fight it." We'll see how long that lasts because it's costing them money every day to have certain aspects of their system paralyzed by this. So it's a very serious thing. I almost wonder if all these other things have moved so quickly, the way that we use the internet, the way the companies are being pushed to adopt technology, is that leaving vulnerabilities because it's happening so quickly or combining legacy systems with new systems and in somewhere in between, something gets lost in the shuffle and that creates an opportunity for cybercriminals to kind of poke a hole and find an entry to their system? Is that...

Cameron Schuler
Yeah. It was actually over Twitter, I asked somebody who was a cybersecurity expert, "What are the big problems left to be solved?" He was like, "People." So if you look at a bunch of those types of attacks, somebody clicked a link and that's what launches it through your organization. Because once it's on the inside, it has much more freedom to move because for systems to be able to communicate, you have different protocols. So it's really that piercing of that safe internal environment to external, certainly a piece of that.

Cameron Schuler
There's some balance in between having the freedom to do things and having something totally locked down. So the way you ensure that your systems aren't hacked is you just are not connected to the internet. Right?

Hans Albrecht
Right. Right.

Cameron Schuler
So that's not particularly practical. So then you start looking at it saying, "Okay, so what level of risk do you accept?" It's really that trade-off. Good people that are good in cybersecurity, you create honeypots and all sorts of other stuff where people can then go get caught or at least you see how people are probing and you learn about it. But there's certainly a push with academics too to create sandboxes to play with things. So there are actually some areas where you do need to explore these.

Cameron Schuler
My challenge? So think about it from an antivirus perspective. So 20 years ago, I created a virus. It was a system called sub seven. So you could actually create a virus with that really easily, package it up, and send it. So I sent it through Hotmail at the time. Three weeks before it caught it, I sent it to myself every day. Eventually, it's like, "Oh, well there's a virus in this." So traditionally, they've been saying, "Okay, you now have a virus," rather than being proactive and trying to protect you from it when something new comes out.

Cameron Schuler
So when you think about self-propagating worms, when those came out, nobody was prepared. I remember I was in grad school and all of a sudden, my computer's acting funny. So I take a look, see what's going on in the ports. "Okay, I've got a virus." Disconnect, system restore, and it went away. But yeah, these things will continue to change over time. I think it's about having good corporate practices and having people well-educated. Again, if you look at fraud, there's still frauds that happen where somebody sends a fax to wire money and somebody wires money to the wrong spot. There's all sorts of these things, but I just think that awareness on the financial crime side is just so much greater now because there is a lot of money available for it and it's easy for people to send stuff off.

Hans Albrecht
Do you think part of the issue is that IT departments aren't getting the support that they need? Perhaps I want to use the word respect, right? It used to be that, "My computer's frozen, let's call IT. I've got a problem. Okay." But now, the ramifications of cybercrime are so serious. Some of the reports are showing the IT departments aren't getting enough of the budget to be allocated to cybersecurity. Is it this disconnect between the reality of what's going on and upper management not realizing that, and making that connection, and involving IT, and giving them the power and the budget to do something about it? I think there was a study that showed that around 46% of CTOs admitted that their companies weren't ready for a major cyber hack. That almost feels to me like there's a little bit of a disconnect happening there, a divide that needs to be dealt with.

Cameron Schuler
Yeah. I mean, you call it nerd in the corner, right? So you need that person, so you go find them. It tends to be very reactive. It's expensive to replace hardware too. So when you think about if your office runs on Windows, what version of Windows are you running on it? There's those sorts of things. Yeah, I think there's a combination. So one is the talent's hard to come by. So you can certainly use managed services and if they're good, they should be up and running on a bunch of different areas. So you certainly could farm stuff out that makes it more effective. But yeah, I think in general, it's looked as a cost center, and they are, but they're also not a profit center. But if you think about disruption, it really is a profit center.

Cameron Schuler
There are systems that I've seen that have been created that if something happens that looks nefarious, it'll shut everything down. It's backing up every couple of minutes so you might lose 15, 20 minutes worth of work. I mean, I still remember when the original Citrix systems were around where it's like rather than updating your computer, you just run on a terminal and it's your Microsoft Office and things are all in the back end.

Cameron Schuler
I've been a banker as well. So when I worked for a bank, all of a sudden they switched us over that. We're still on Windows 95 machines in 2003. But all of a sudden, the whole branch goes down and there's 150 people not able to work for an hour till they can get up and running. So there's no ideal state. The cool thing about being in the AI space is everything looks like an optimization problem. You have extremes on both ends, and you have to find the pieces in between there that is the right spot. It's like lots of things, they're not black and white. There's many different shades along the way and it's finding that.

Hans Albrecht
Right. Right. Yeah. I find that area quite interesting. In the internet of things category, we're looking at this incredible exponential proliferation of devices that are going to be created and maybe partially because 5G is going to enable that to happen much faster as reliability improves. We tend to think of cybersecurity as a piece of software that protects our PC. Even though some people say that mobile phones are the next area of vulnerability, we tend to think of it as software. How do we address all these devices, all these what is essentially hardware, your fridge, your toaster, your car, your phone, your watch? All these things, I've heard that a lot of these things are being created with cybersecurity as an afterthought. Does the area of cybersecurity have to kind of resolve that problem of, "How do we integrate security into your fridge because that may represent an area of vulnerability to a hacker"?

Cameron Schuler
Yeah. It's the weakest link, right? So I can't remember who it was, but they got hacked through a fish tank. Yeah. So it goes back to it's the weakest link in the whole chain. So you might have a company with 10,000 FTEs, but somebody's like, "Hey, let's connect the dishwasher."

Hans Albrecht
Right.

Cameron Schuler
Right. So yeah, I think there is some process of afterthought for these going, "Let's build this as really cool. Oh yeah, and security." Part of it is the protocols you have to do for security are incredibly expensive and they're time-consuming. Take a look at Blackberry. So their argument always was, "Yes, our apps are hard because they're more secure." But people didn't care about the security side. It was, "I'd like to be able to get out an app in three weeks," versus developing a software program. So that customer-driven, "Yeah, we got to get this out," really can impact things in a much bigger way than people anticipate.

Hans Albrecht
And those were different times. I mean, we hadn't seen the full impact that we're seeing today in that area of cybersecurity and cyber hacks. So suddenly, it's an area where there's this revelation that, "Uh-oh, we'd better focus a lot more on that aspect of it." You can look for improvements in all these other areas using big data and perhaps some form of automation, and you're looking to improve margins and find deficiencies in areas of extra productivity. To throw that all away by not focusing on securing all these things that you're creating and securing the data that you're acquiring seems irresponsible in a way, but maybe not a top-of-mind realization for some companies.

Cameron Schuler
Yeah. When you think about the criminal element, they have a lot of time. So, I don't know if you know what the Captain Crunch whistle is, but back in, I don't know when it was, the '80s, the Captain Crunch whistle was at the same 2,600 Hertz a dial-up modem was. So you could hack into things using a whistle you got in a box of Captain Crunch cereal, and you're like, "Okay, so who actually thought of that?" Somebody with way too much time on their hands. So yeah, I think there really is that you can focus on margins and everything else. But when you think about how things flow to the bottom line, you have one expensive event that happens and your profits disappear, right?

Hans Albrecht
Right.

Cameron Schuler
So all those things, they're scary from a business risk perspective.

Hans Albrecht
Are there areas of AI, all of these various areas we've been talking about, are there areas that get you a little bit excited that you feel that perhaps people are not looking at but you're seeing a lot of potential? Or, perhaps people are looking at, and you think that this is an area where it's going to particularly change peoples' lives? Or, this is going to be an area where companies can monetize and sort of find ways to find consumers and do well? Anything that kind of comes to mind that you've been looking at?

Cameron Schuler
So definitely a lot of efficiencies. I mean, I think health care will have dramatic changes. I think environmental, we could see some really dramatic things change too, the way that we solve those sorts of problems. I really mean in terms of pollution from automobiles and things like that. So DeepMind has a great case study where they used a particular type of learning called reinforcement learning were able to reduce the usage of the electricity by 40% in their server farms. I mean, that is a meaningful change. So it's those sorts of things that do excite me because it's, again, we turn on a light and we leave it on...

Cameron Schuler
Historical knowledge, so I still remember buildings where all the lights were on because it was more efficient. Because if you turn them off and on then it could damage the grid. By turning them on, it takes more energy, all these falsehoods that somebody said that made sense at the time. Daylight savings time is another thing. During World War I, they were trying to save energy. Well, what it looks like is it actually costs 1% more energy. So all of these things that seemed logical at the time aren't proven with data. So that ability to prove things out with data I think is pretty exciting.

Cameron Schuler
Then, you start looking at areas that are so complex that you can't actually program them. So autonomous vehicles, so if you and I are driving in a car, I'll make a fair assumption, you don't think about where to put your steering wheel. But if you're driving in a zone with lots of people, or kids, or a highway, you're going to put your car in a different spot in that lane. We just do that automatically. But if you think about an autonomous vehicle, now all of a sudden, you have to decide, "Where should it be in the lane and to do that, where do I put the steering wheel?" That's just one thing, and it's based on the environment around it. So when you start thinking about being able to program that, it's effectively an impossibility. So the learning systems will allow it to do that. That, to me, is the really cool part that, again, they're hard to do. But over time, I think we'll see some pretty neat things coming out.

Hans Albrecht
So how are they able to develop these systems for autonomous cars? Is that just a sheer amount of data that it just learns from? Is that a paper bag flying across the street? Is that a sign? Is that a truck? Is that a person? Is that the sun's glare? Is it just the sheer amount of data that is going to get us to a level-five autonomous car where we can trust something like that?

Cameron Schuler
Yeah. I think level five is actually quite a ways away, just for a bunch of... I mean, living in Canada, we have snow, and ice, and things that get obscured. In a talk that I do, I actually found a picture online of somebody painted a Bugs Bunny Road Runner tunnel and a car ran into it. Autonomous vehicle actually wouldn't do that but the human did. So I think there's lots of opportunities in multimodal data. So autonomous vehicles are an incredible example where you use GPS to find out where you are in the world. Things like mapping tends to have a resolution of under one inch and an X, Y, Z coordinates. So once you find out where you are in the world then here's your map. Where are you on that map?

Cameron Schuler
So you use a bunch of different systems. They run at different frequencies. They're selecting data at different speeds. So your vision system may be selecting data at 30 Hertz, something else might be one. So it's 30 Hertz is 30 times a second. So all these different things are... The ability to take that and make sense of it is incredibly hard. So it was Sebastian Thrun, who used to be a professor, he has something called The Udacity. He ran Google X. I think it was his team that actually won the DARPA challenge with autonomous vehicles. But a bunch of that was actually highly engineered. If you take a look at some of the weapons systems, they're so highly engineered, you'd think they're learning but they're not.

Cameron Schuler
So the first attempt at intelligent weapons was actually World War I. World War II, there was stuff they could actually fly by wire. They weren't necessarily missiles, but they were bombs they could actually steer. Vietnam is when it really came to systems that could do that itself. Now, there's things like bullets that can do that. So it's interesting to see that progression. Some of those are engineered systems, and some of those are learning systems depending on what they are. But again, that's probably a much longer discussion.

Hans Albrecht
Well, I mean, I love that area, the area of autonomous driving. To me, it brings in these interesting questions of ethics. For example, I did a talk on just general Industry 4.0, and sometimes I mention that imagine this situation where a car has a choice to hit two people on the right to avoid something in front. It can two people in the right. It can hit three people on the left. Tragically, it has to make a choice. How does it make that choice? Or, perhaps the choice might be to run straight ahead and sacrifice the driver. I thought, "What an incredible thing to have to sort out." How do we arrive at that kind of conclusion?

Cameron Schuler
So one of the auto manufacturers did say that the thing we can control is the car, so we're going to save the driver. So you do pre-program some of these rules. It's always been posed as the trolley problem, or lifeboat, or however you want to look at that. So we've always had these moral conundrums of, "How do we deal with them as humans?" I think we have to be prepared that autonomous vehicles will make mistakes, but they'll make different mistakes. So do you need them to be overly cautious that it is a bag blowing across the road so you stop? But if there's lots of tumbleweeds, for example, does everything halt and you got to wait for the tumbleweeds to go away? So those are really hard decisions. That's why I think level five's a long way away. But that human augmentation of, "Okay, now the human needs to take over and make judgment," will be a big piece of it.

Cameron Schuler
Yeah. We have to be prepared. So there's somewhere around 3,300 or 3,500 traffic accidents per day that are fatalities in the world. So reducing that down to 1,000 is pretty cool. But the second you have an autonomous vehicle killing somebody, people are like, "Wait a minute. This seems pretty awful." So it's hard to take that into context. So yeah, it's going to make different mistakes. If it was you, you'd feel differently about it. So that's kind of the preparation we have to make. I think we do get very comfortable with intelligent systems, and it's kind of how I like to frame things more than AI. So if you think about autopilots. So this year was different. There was certainly issues of one of the manufacturers. But, was it 2018 or 2017? There were no fatalities with commercial jetliners that year, which is pretty cool.

Cameron Schuler
So if you showed up at the airport and they said, "Hey, our computer systems aren't working, but we're going to fly anyhow," You're not going anywhere, and you feel pretty uncomfortable. But there's a mix. What they did find that if the autopilot did too much, when something happened, the pilots weren't engaged and they made more errors. Still, the number one cause is pilot error in terms of accidents. But it's that combination of keeping them engaged enough that they're always connected to what's going on, but taking the mundane stuff away where we tend to stop paying attention. It really is that mix that's pretty cool, I think.

Hans Albrecht
Yeah. Your point, pilot error. I think it's quite clear that most fatalities on the roads are due to some version of driver error. I'll be the first to admit, when I heard about autonomous cars the first time, it made me nervous. I thought, "Well, there's this sort of idea that if we control our destiny, we feel better about it." So the idea that a machine or a computer might control our destiny is a little bit unsettling. But all I needed to know was that the possibility that autonomous driving done successfully could reduce the number of fatalities out there by a significant amount, braking for people when they're perhaps not aware of a stop sign that's coming up, or a turn, or a sharp turn that's coming up.

Hans Albrecht
I mean, we're all just human. We make mistakes. The possibility that technology can reduce the number of mistakes that are being made and save lives is quite an amazing thing. But you're right, all it takes is for that one single statistic that shows, "Well, the car screwed up, and it may not have done things correctly." That is what's going to capture people's attention. So you're right, we're going to have to struggle with that over time. How much do we let technology take over at the same time realizing that the benefits are, in all likelihood, going to outweigh that one incident every so often that unsettles us because it was beyond our control?

Cameron Schuler

Yeah. So I went to grad school with a guy who was a doctor, and he said there's people he went to medical school with that he'd rather go on his own than to see them. I said, "Bollocks. Because you're a doctor." He goes, "No. If you had no medical training, you'd still be better off." So you think about the medical system and how... Or, think of paramedics. People who need to see them are pretty happy when they show up. So they're not going to be perfect. Things are going to go awry sometimes. But those sorts of things where you really see it as a help to your life, I think it'll make it pretty dramatic difference.

Hans Albrecht

Amazing times ahead. Well, I want to thank you, Cameron, for spending some time with us today. It was very enlightening, and hope to have you back sometime soon to talk more about things. Things are happening so quickly that it seems like there's always something to talk about. So thanks very much for coming.

Cameron Schuler

Thank you very much, and I'm grateful that you provided the opportunity. I'm happy to come back.

Hans Albrecht

Great. Thank you.

Cameron Schuler

Thanks.