Elevate Live Episode 12 Transcript | June 24, 2020
Cybersecurity

Razor Suleman, Rounder & CEO, Elevate
Robert Herjavec, Founder & CEO, Herjavec Group
Claudette McGowan, Global Executive Officer of TD Bank

Razor - Welcome to Elevate live. We are at episode 12 from season one. Today is our last episode. It's been such a privilege. Being able to connect with our community. Talk about these important conversations we've been having. As we all move to home, have been navigating COVID and economic depression and systemic racism in our communities. So I am super grateful. I just want to take a little moment and thank our partners. When I think about the opportunity to be able to host season one, 12 episodes, we've had 30,000 people join us on Elevate over these past 12 weeks, making it the largest tech platform in the country. We're super grateful. Thank you so much. Garrick at Facebook, Canada, you and your team have done an amazing job around helping us create world class content. Claudette and Rizwan from TD bank. Thank you again for your support, encouragement, opening up your networks and guiding this our team and being able to deliver our friends in the government.

I mean, amazing job on navigating the health crisis and the economic you know, realities that we're facing. We're so grateful, Mayor Tory. Thank you for your continued support. You've been there on day one, day two. And now on year three of Elevate, we're super grateful premier Ford, Rob Phillips from the province. You guys are doing a great job. Thank you for continuing to support Elevate and again, our friends in Ottawa. Thank you, Justin Trudeau our Prime Minister for being responsive. I know you're going to come up in a future episode. I'm putting that hint out. Minister Bill Morneau, Minister Bains, Minister, Chagger, Minister Joly, all of you have been so gracious, thank you so much for your time, your coaching, your support. We wouldn't be able to deliver this experience to our community across the country. At no cost, thanks to the support of our partners.

So we are super grateful to be able to do what we do because those people are continuing to support Canada's tech ecosystem. Okay. We've got a great show for you today. We're talking about cybersecurity and now why more than ever, we need to double down on our strategy on our investments and making sure that our offices and our home offices are secure. We've got two incredible thought leaders on the topic of cybersecurity. Robert Herjavec from the Herjavec Group, and we've got Claudette McGowan from TD bank. So we're going to ask them what you need to do at home to stay safe. What heads of cybersecurity, what CEOs need to do to ensure that they remain safe in this new hybrid workforce revolution. And I know that there might be some people out there thinking, you know, cybersecurity, this doesn't really affect me, but I want to share a personal story that happened to me this week.

This week, my Twitter account got hacked. If you go to at Razor Suleman, it is not me, someone with a dot R U email address? I'm going to say Russian hacker has taken over my account. We're dealing with it with Twitter, but it happened literally on Monday. Elevate had over 600 attacks on our domain over the last six weeks. We're seeing a rise in cyber threats, cyber criminal activity around the world, and particularly here at home. And so if you don't think this topic is going to affect you, you are, have either been a victim of cybersecurity or you will be a future victim. So you definitely need to pay attention. We've got two of the world's foremost leaders on the show today. Very excited. Let's start with introductions. We have the one and only Claudette McGowan back again. This week, very excited to welcome Claudette.

Claudette McGowan is the global executive officer of cyber experience at TD Canada. You may have remembered her from the Elevate main stage right next to the one and only Michelle Obama. What a magical experience this past September on the Elevate Mainstage an incredible conversation that still gives me chills, incredible job Claudette. She's also been recognized as one of the hundred, most powerful women in Canada in 2018, as well as one of the top 50 leaders in FinTech in this country. She's a member of the US Canada innovation partnership. And what I love most about Claudette is how passionate she is about Elevate, how active of a board member she is. And I'm so grateful for her time and her friendship. We also have the one, the only Robert Herjavec is the founder and CEO of the Herjavec group. You know, definitely this country's maybe one of the world's most leading cybersecurity firms he's been doing cybersecurity before it was cool.

Robert is a serial entrepreneur, started and exited several ITE, cyber and tech companies. You may have seen him on the hit show, Shark Tank, where he's been crushing it, giving entrepreneurs the much needed advice and financing. They need to grow their business alongside past Elevate guests, Mark Cuban, and our friend Kevin O'Leary. Robert has served on the cybersecurity advisory for the government of Canada and participated with the White House Summit on cybersecurity. He was sharing some some stories of his time at the white house spending both with Michelle and Barack Obama. I think Michelle, Claudette myself and Robert agreed that Michelle definitely steals the limelight in their presence. We are also going to have AMS, ask me anything. You can ask our thought leaders, anything you want to know your pressing questions on cybersecurity. They're here to get back to you to answer those questions.

Upvote the questions that you think are most relevant, and we'll get to the most upvoted questions. Okay. I'm going to go to our guests, Claudette. Let's chat about you. You know, when I think about you, you are a champion for Canadian tech and innovation. You are a leader in diversity, inclusive and making sure there are opportunities for all to exist in our country, but you love, you nerd out when you hear about cybersecurity, which I love how you are so excited about it. Tell me about how you think about cybersecurity at home in the office. What do we need to know?

Claudette - Yeah. Razor are here's what I'd say. You're going on vacation and you've got your bag packed and you're just, you know, you're, you're just feeling lighter and you're enjoying it and you're in this paradise and I call that physical paradise, but there's this place that I think we all want to be at, which is digital paradise. And when we're online, we don't feel that stress free. We feel stressed. We feel worried. Should I click the link? Is the camera watching me? That's why you got the little tape over the camera, is the system listening to me? So there's so many different things that give us anxiety and stress. And so my mandate is really to just help demystify cybersecurity and make sure that everybody understands that we need a cybersecurity mindset at home, at work from the top of the house, you know, your CEO to your, you know, frontline worker. Everyone has to be thinking about this and be vigilant about it because we may want to take a rest from time to time, but the threat hackers are not taking a rest and they're working overtime, defining new ways to make life difficult for all of us.

Razor - Yeah, definitely. I think our cyber criminals are working double time from home to attack businesses that are, you know, they're trying to make ends meat. They're trying to be productive members of society. And you have people that are preying on really the vulnerabilities and the changes that are happening so quickly. Let's start with at home Claudette, tell me what you know individuals can do at home. What are the three things that I could go back to today and implement in my home environment to protect myself and my family?

Claudette - Yeah. First thing is making sure that you have a healthy password kind of management in place. So ensuring that you're changing passwords on a regular basis and not using simple ones like the ever so popular “password123”, let's stay away from that. The second thing is running a VPN virtual private network at your home, and making sure that you've got insecure pathways into your work and secure pathogens to your competing kind of endeavors. The third thing I would say is to make sure that everybody in the home understands the importance of cybersecurity has sometimes I've heard, I've heard situations where, you know, mom and dad have it down pat, but then we give our kids an iPad or we give them a cell phone and then we connect to the wifi. And then all of a sudden, now we haven't really taught them any habits of what to do differently. So I think education is number one, making sure they think you're exercising, great password hygiene. And of course, you know, just being mindful of, you know, great tools you can put in place like virtual private networks,

Razor - Password hygiene, that's going to be the word for 2020. So let's talk about, you know, I'm, I'm at home, I'm watching Netflix with my family, but I'm also on a zoom call for work. Who's now responsibility is this and this new sort of hybrid workplace revolution that we're experiencing, whose responsibility or ability is it to protect the home environment, regardless of what you're doing. Does it fall on the employers? Should employees or individuals take more responsibility? How do we, how should we be thinking about that?

Claudette - Yeah. My personal view is that when it comes to me and my home, I am the person accountable for protecting the home and making sure we have the right tools in place. Your employer is going to help you to guide you the best practices, wonderful things that you should do, but ultimately you want to keep your home safe. It's the equivalent to saying, now who's responsible for putting the key in a lock on the front door. It's definitely the homeowner. So you want to protect your data. You want to protect your assets in the same manner. The other things that folks should be thinking about at home is really all the different people that you give your wifi password out to, I have this great set of family whenever they come over, they don't even say hello, first they go, “what's the wifi”. So it's one of the things that we try to encourage people to do is to be mindful of, you know, who you're actually allowing access to. And then how often again, you're resetting those passwords.

Razor - Got it. Robert, how's your audio doing?

Robert - I think it's doing good. How does it sound?

Razor - You sound great. Okay. I'm gonna go to you. We chatted a little bit about at home and we're thinking about cybersecurity. Robert talk to me about the office, right? What are the new risks? What are the things that CEOs or the leaders of cybersecurity in the workplace should be thinking about in a, in a post COVID world?

Robert - Yeah, I mean, I think Claudette brought up some great points if I can just add to That Claudette. I think that the one thing that we're really encouraging people to use also is multifactor authentication. You know, there was a recent study that a home computer it's seven times easier to hack than a work computer or a, or a device within a corporate network. And one of the challenges that we see is, you know, to your point, Razor, you're at home, you're watching Netflix during your zoom call. You leave that open session for your teenager to come on and use that same device. And so we're really encouraging people to use a lot of those tools, you know, to your question, what is the new workplace like? What, what should people at work be thinking about? The first question out of that is what is the new workplace? I mean, once we're all allowed to go back and Toronto was just allowed to go back July 6th, well, we all go back. Will we work from home forever?

So I think the idea of remote access VPNs is here to stay. I don't see an environment where we go back to normal and everybody just goes back to the office. And along that line, I think that the idea of having a device that you've been able to lock down will become even more difficult, meaning we'll have to find a way to secure those devices without physically having them. And then the last part is where does the data reside? I think everything's moving to the cloud. All the storage is moving to the cloud. And I think we have to find a better way from a work perspective to control those, find those logs and make sure that there's an element of control with all these different cloud services.

Razor - Got it. So give me a sense, Robert, I'm gonna go back to you just around budgeting, right? What should, if I'm, if I'm a small business owner with 20 employees, how do I work in cybersecurity? Where should I be investing my money? You know, if I'm a mid sized company of 2000, how does that change? And then if you know, 20,000 employees give me a spectrum of how small, medium, and large companies should be thinking about investing in cybersecurity.

Robert - Yeah, there was an article just yesterday in the wall street journal that said 80% of small businesses below 500 employees don't have a security policy or security practitioner on site. I think everyone's, budget's been blown up because of COVID, you know, everything we thought pre COVID, it doesn't really exist anymore. And so I think it comes to, you've got to look at your company inside out. So if I was a small company, I would really worry about now where meaning, I mean, still to this day, believe it or not, 85% of malware still comes through phishing. And the smaller companies, it's easier to phish them. People, as Claudette said, people still click on stuff that they shouldn't. You know, we always tell people when we do training, you're not that sexy. There isn't a woman in Russia that wants to meet you. You did not win a lottery that you didn't enter, and you don't have an uncle in Africa who left you millions of dollars. So don't click on that stuff.

But interestingly, during this COVID time, people are stuck at home. They're lonely, they're, they're wanting to open mail. And so we've seen the rise of phishing go up and the rise of malware. So if you only can protect one thing and you're a small company, I will protect against malware, meaning I would have a good antivirus, something called EDR type of tool on my end point. That would be my number one thing. I would focus on the larger the company like Claudette's company. It really comes down to the critical data and what's more important. And of course then compliance, audit, all that kind of stuff.

Razor - Got it. So you're saying I should not rush home and send money to my Nigerian Prince, long lost uncle immediately. That's not a real thing, huh?

Robert - So I have a funny story. I was doing an interview on GMA when COVID first started and the interviewer before we went live, told me his grandfather just got phished. He, he got this email, supposedly from Apple support and even looked like an email from Apple. He knew it was phishing, but he still clicked on it. And so the reporter asked him, why did you click on it? And he said, well, I'm lonely. I haven't seen anybody for a month. I just, I was hoping it was real. And yes, you shouldn't be clicking on stuff like that. But I think it's very difficult because you're dealing with human emotion and great phishing campaigns, prey on either arrogance, fear, loneliness, basic human emotions.

Razor - Yeah. I can see that. While we were having a conversation around cybersecurity and threats, we did go to our live audience to poll them asking them what they thought the number one threat of cybersecurity was for businesses in COVID are. So the number one answer that came back, what 57% was fake websites. Number two, the answer was phishing with health info at 17%. So those according to our home audience are the ones that most people should be concerned about. Let's talk about protection. Okay. So there's some practices you should do. What about cyber insurance? Is this something, is this a real thing or is this just another money grab insurance companies want to sell you fear? Should companies, individuals be buying cyber insurance?

Claudette - Yeah, it's definitely a thing. And while I'm not an expert, what I will say is that you should take all the steps possible to protect yourself. So I encourage you to take a look at it and see if it's the right thing for their business to do. If you think about it right now, Robert talk about phishing. From a study, there was 6.4 billion fake emails sent every day. And there's a bunch of reasons why we might do things, Robert highlighted a few of the reasons that, you know, people are tapping into. So I think you have to protect yourself and have multiple lines of defense. So, so that would be my thought Razor.

Razor - Okay. So buy the insurance. Okay. Let's talk about the amazing need that we have. You know, there are 3.5 million open jobs in cybersecurity. Okay. So for those of you thinking of going to university or graduating or being re-skilled, lots of demand, not enough supply, let's talk about what companies, what can we do to help fill those roles? Claudette, I'm going to start with you. How do we solve the talent gap on cybersecurity? Robert, I'd love to then go to you, Claudette, your thoughts.

Claudette - Yeah. Again, I would, first of all, tap into the pipeline and go really deep. So there are amazing roles in cybersecurity. Some are more around blocking. Some are around tackling. Some are preventative, a ton of work being done right now in data and analytics. And you know, we're working on some really key initiatives around really understanding the data and pulling that out to be used for insights and key decisions. So when you think about cybersecurity, it's not one type of job. It's not just eyes on, on, on a pane of glass. There's multiple opportunities. Whether you're doing things around incident response, you're doing things like threat hunting. You're, you're, there's a whole industry around intelligence and making sure that you've got the right Intel at the right time. So I think I will be tapping into like middle schools to let people know about these types of opportunities to, to use co-op programs.

We did something really fascinating with Seneca and building out a curriculum to get people, to embrace and understand more about the opportunities and learn more about cybersecurity. So tapping into, you know, youth, but also recognizing that there's five generations in the workforce. And so people interested in a career pivot. I know companies like ours and welcome, you know, bright, brilliant people to come in and join, join our team. So I think, you know, don't, don't count yourself out if you're, you have a healthy sense of curiosity and you know, you really like to get to the bottom of things you love getting to root. Cause then this is a, the right industry for you.

Razor - I love it. Middle school, all you TKS students out there, focus on cybersecurity. There's lots of open jobs. It's never too early to get into it. Robert talk to me about how do we deal with this talent gap? Are there rules in the organization that could be retrained or maybe split for a company that maybe not have somebody dedicated to cyber?

Robert - Yeah, I think not to be self serving, but this is one of the reasons we've seen so much growth in our business from a managed security perspective is because companies are waking up to the fact that there is this huge shortage of gap. And the other problem is people don't want to do the non a glamorous part of work. You know, Claudette talked about threat hunting but to have a great threat hunting program or a great IRR program, you do need those people that are looking at screens 24 hours a day and doing the basic rudimentary stuff. And so what we do is we encourage companies to take the staff they have and train them into higher value propositions and outsource that non-glamorous work, but still critical work that needs to be done. You can't analyze and provide value to data unless you're actually collecting the data in a very cohesive and stringent kind of way.

But in terms of education, we do the same thing. I mean, we have a program with Seneca where we bring people in and train them and get them going. Cybersecurity is a super fun feel to be in, it pays well for all those people that are looking for a field. More than that, it's something where you can actually affect change, provide value and stayed with your whole life. You know, to Claudettes point. You could start in logging and move to IRR and move to threat and then move to remediation. So for somebody like me, it never gets boring. It's always exciting. And what we're now seeing is certain education. So like we're working with the university of North Carolina, they have a threat hunting program. So a few years ago we were to hire students to do general security work. We're now hiring them into our pen test team right out of school. And they're great because they're being taught a very narrow, specific skillset and we can fill in the rest.

Razor - Great lots of opportunities to get trained, lots of career opportunities, well paying jobs. If you were thinking about a future in cybersecurity clearly is a big opportunity. Let's talk about, we touched a little bit about some of the tools, you know, we've been hearing that zoom, isn't safe. People have been hacking it. Some companies have abandoned. Give me, I'd love you to give me your sort of your top, maybe two or three tools that you love, both Claudette and Robert. And maybe if you're comfortable, maybe one or two that people

Claudette - Yeah. So, so I won't, necessarily call it brand names, but I'll say around themes and what they do. So endpoint you know, small, large companies, you all have laptops, phones, printers with, with hard drives and the multifunctional devices. Making sure that you've got tools and solutions in place to ensure that all your end points are protected, you can detect anything that's not, you know, where it needs to be, you can remediate it. And having things like automated remediation tools are very key intelligence tapping into what's happening around the world through different agencies and services to know, just because the threat that didn't happen to your company or your organization doesn't mean you shouldn't be interested in what happened, how it happened and how you could prevent that from happening in your organization too. So having tools around intelligence are very key.

And then the last thing I can't reiterate it enough is to have threat hunting capabilities, where you are in primly employing folks that are searching your systems and understanding what types of threats are out there. And are you truly resilient when it comes to those things coming to your doorstep? So those would be the three things that I would highlight. And just keep in mind when we look at like data breaches, 4.7 million dollars is the average cost to a company in Canada that have the data breach. You want to be as resilient as possible. This is why I'm so passionate about this because I know just a little bit of effort upfront will save you so much in time, money and resources. So that's my, that's my 2 cents Razor.

Razor - Robert, before we go to you, let's talk about what can we do to improve our cyber resilience at home and at the office?

Claudette - Definitely, again, employing those tools, the education components of things, Razor is very key, but I, I think there's so much to learn from why things went wrong. So there's a bunch of big cases that we cite, whether it's, you know, a big box company, whether it's an information credit reporting agency, we know things are happening. Every company needs to spend some time understanding what happened and why. And as an individual, you know, when you understand what happened with your Twitter account, socialize it. Is there something that you could have done differently? Is it just, you know something that happened? Where you targeted? Sharing information because many times when people are hacked, they keep it quiet. They feel embarrassed. And this is the stuff that we have to talk about. So we can all be stronger for the day.

Razor - Well, listen, I definitely felt embarrassed, but I do have a big mouth so I can't keep it quiet. I was hacked on Twitter this week. Oh my God. Robert, over to you, your favored tools around what people can get immediately to protect themselves.

Robert - Oh please Razor, you were hacked on Twitter. Can you imagine how often people are trying to hack me on Twitter and all the fake Robert Herjavecs you see on Twitter, Instagram stuff. You know, it's funny. One of the biggest challenges we have on Shark Tank is people are constantly standing up fake websites and using video enhancement.

So apparently I promote some, I'm promoting so many different products on the internet right now that I've never seen, never touched. And the video quality looks very real. So it's very personal to me obviously, but it's, it's a big challenge for everybody. So you shouldn't be embarrassed if it can happen to us or Shark Tank or ABC, it can happen to anybody. In terms of tools. I echo what Claudette said. So you have to have a great end point tool, whether it's an agent or some type of an intelligent end point device, the traditional McAfee Symantec tools, aren't doing it anymore. I think that basic antivirus is way too basic. So my number one recommendation, if you're going to invest in something it's in a better end point tool, I mean, of course I'm going to say manage services, not only because we do it, but I also think it's very difficult to bring that expertise in house and an outside party is probably going to do a better job at it then than you are.

And my third point is the move to the cloud. So we really like tools like Netskope around CASPI, something called CASPI. People are moving to the cloud, the idea of a physical perimeter, it's just going away. And then my last tool recommendation would be in some type of a correlation engine. We're big fans of Splunk. We think there's a lot of intelligence you can gather, but again, these are just tools. It's the old hammer and carpenter. You can buy the best hammers in the world. I still can't build anything. I need an expert to help me do it.

Razor - Robert I'm now concerned. I just bought the Robert Herjavec miracle hair growth formula, because you were endorsing it. I'm like, I gotta do it.

Robert - Look at this hair. It's unbelievable. No, but it's true. It goes back to your point around phishing Razor, like the quality of the phishing campaigns and the quality of these fake videos is unbelievable. I mean, it's really difficult to tell reality from something fake today. And I think it's to Claudette's point, you have to have constant training. You have to constantly be educating people and don't be embarrassed if you've been phished or your Twitter has been hacked. Let your company know, let people know it's a constant vigilance and training.

Razor - Got it. I will share one tool that I'm a big fan of. It's CloudFlare started by Michelle Zatlyn, she’s Canadian, she's the co-founder and COO of a very valuable cybersecurity firm. So check out, clearly the Herjavec Group and then CloudFlare as well. I'm a shameless promoter of all things Canadian and Michelle and Steve are doing a great job. We are going to go to our live Q and A. Over to you Robert. The question is why do we always react? Why do we always react to incidents, reactively? How do we get out of this cycle? How do we go to this trap?

Robert - Say that three times in a row Razor, reactively. We're competing against an enemy that is moving faster than we are. And somebody gave me the best analogy. You know, if you think about our companies, we have to protect a very wide perimeter or very wide footprint. The attacker narrows in on a very small chink in the armor and the tools are constantly evolving. The threats are constantly evolving and we're fighting something that we don't really know about today. And I mean, from, from Claudette and my perspective, that makes it very interesting in a theoretic way. But from a protection perspective, it's very difficult to protect the guests that are in attack that you haven't seen before. And so most of the tools today are reactive. And the general feeling, insecurity is it's not about protecting you in a way that somebody can't get in. I mean, yes, you want to do that, but it's about reacting as quickly as possible. And I always say to people, it's your responsibility to react quickly. A lot of the previous breaches, if you go back to the target and so on, he attacked her. The attackers were in that network for something like 18 months, that's inexcusable. That is the responsibility of the company. And I think that's where you really want to focus on is being able to detect as quickly as possible and react as quickly as possible.

Razor - Okay. Next question is actually to both of you Claudette, I'll ask you first, in our new world when it come to cybersecurity, what keeps you up at night? What's the one thing that you are most worried about?

Claudette - Yeah, the thing that I'm most worried about is I'd have to say as we move to cloud and we're, we're very agile about our desire to move to cloud. This is to all organizations, that we need to take the time to do the fundamentals, make sure that we get brilliant at the stuff that helps us to run our operations. And have we thought about every single kind of endpoint or every single kind of device in the ecosystem. So for me, I'm very, very bullish on cloud. I think it's the right thing to do. But I want to make sure that we measure a few times before we cut and every organization should be asking themselves the same thing. Do we have all the right fundamental foundational elements in place so that we can truly move with speed,

Razor - Robert, same question to you other than your two young twins, what keeps you up at night?

Robert - I was going to say that that's what keeps me up at night, the two year old twins, but besides that, I think it's the rogue device. As long as we have human beings in networks, we will fundamentally have insecure networks because the greatest defense in our network is human beings and the greatest weakness in her networks as human beings. So what keeps me up at night is that one person that's found a way around our security controls or logs on with the device that's not approved or download some applications that we don't want them to. That single rogue device and controlling the user community, not from a kind of control perspective, but from a sticking to policy and enforcing our security policies across the entire surface.

Claudette - Yeah I would like to add to that. Long gone are the days where you're just kind of protecting the perimeter and trying to prevent anybody from the outside of getting in. We've had to think about insider threats as well. And making sure that we're doing all the right things to understand user behaviors in your organization, whether it's adding a new device or, or going to places that they don't have access or should not be going to. So having good controls in your interior is very, very important, just as important as your exterior.

Robert - That's a great point. You know, the largest data breach in the U S government was from an insider attack. It wasn't from an outside agency. It wasn't from some third world country. It's the insiders. And so Claudette's right on, you have to be able to protect core applications because every company has some crown jewels that are critical to them, but they don't want to get out into the world, whether it's financial information, customer information, mining information, manufacturing information, all of that stuff is valuable.

Razor - The, the inside threat and inside job around cybersecurity is a, is a real risk as you pointed out, Robert, okay.

Let's talk about opportunities in cyber to our young. Tech founders out there that are looking to getting into this space. What advice do you have for them? Where are the opportunities for the sort of a next great Canadian startup to be to be in the cybersecurity ecosystem?

Robert - Well, I, I think what a golden time to be a Canadian and be in tech, if Canada, wasn't a great place pre COVID, what a great place it is now because the entire idea of an office or coming on site is completely gone. And Canada has unbelievable tech talent. I mean, I, I started there, Claudette's there, there's so many great companies and the idea of physical, national borders has gone away. Razor, we have 350 people roughly in our company. I haven't seen another human being from our company or one of our offices in over four months. Think about that. And we're running large corporate networks and keeping them secure, what a great opportunity that is for somebody trying to start a business in Canada or learning about cybersecurity. I really think that this is the golden time because the other thing we know coming out of COVID is cybersecurity is here to stay. It's not going away. It is an essential service and business for many companies.

Razor - Yeah. We've long talked about how now is a great time to start a company. You know, I think Aaron Levie said it best when he said, when there's a lot of disruption, a lot of changing happening in the world, it creates a whole bunch of new problems, which you need a whole bunch of new solutions and new opportunities. So clearly with this new hybrid workplace revolution, we're seeing the need for startups to sort of fill that gap. Claudette, You are a very, I mean, you're a, you're a big company executive, but you are also an entrepreneur at heart. Tell me about what you would tell a founder looking to get into cybersecurity. Where should they focus on?

Claudette - You know, whether we're borrowing from TKS or we're borrowing from Elevate, it's about solving the world's most challenging problems and our most challenging problem worldwide globally is his COVID 19. It's remote working. It's, you know, people being healthy and well. And so if you were asking me what type of company to create, imagine you were the person who came up with that, you know, solution in a box so that people could work from home in a remote way and securely, that would be a big win. Everybody would want to speak with you. Imagine you were the person who created something to ensure we knew the health and wellness of our employees at all given times or of our family. So not so much as who's ill, but how are you doing living in this new context? I think having, I envisioned heat maps, analytics, and different types of graphs, so I know where to focus on as a leader.

I think that would be a great opportunity, but also I, I keep going back there and I know people are tired of hearing it, but the cyber literacy, the digital cyber fluency of a nation is so critical. The most at risk folks are being targeted. Whether we're talking about our seniors or we're talking about newcomers, people from all walks of life are being targeted in ways that it's heartbreaking. And so I would love to see folks really wrap their heads around how do we get to all of those different communities and make sure that they have what they need so that when they are online, they do experience that digital paradise.

Razor - Yeah. Thank you. Thoughtful that thoughtful answer. I agree with you, the health and safety, the wellbeing of our employees has gotta be a paramount concern and a great opportunity around starting a company around that. More on that later, Robert, over to you you know, we saw the, you know, the sort of rise of this, bring your own device to work happening even prior to COVID. Now that we're relying on home printers your own cell phones. Talk to me about what we could do to further secure the, sort of bring your own device that we're seeing it happening in the workplace. What can we do to make it?

Robert - Yeah, it's an interesting problem because even companies that were prepared for BYO Device, bring your own device, weren't prepared to have every employee working from home. We had an interesting phenomena here in the States where some of our customers, laptop orders, we're actually taken by the government for first responders.

So what that did is it for some of our customers to have to work on devices that weren't secured and nobody had ever seen them on the network. I think there's some great tools out there. Claudette talked about them from an endpoint agent tool, the need to be rolled out. That's one of the reasons we're seeing the growth of something called EDR and endpoint tools knowing what's in your network is really the first key and having a way to authenticate into the network. So one of the areas that's really growing in cybersecurity right now, his identity, something we called I am. So this is a niche space right now, but growing very quickly, because if the idea of the perimeter is gone, your identity, who you are, because becomes as critical and authenticating to the network. So I think if you're a large company, you've got to look at identity tools, how people think, how they come onto the network and what applications, multifactor, all that kind of stuff.

Razor - Yeah. It's an interesting and changing field, lots of acronyms, lots of things to learn. It always feels like this, like cat and mouse game of this, continuing to evolve on that cloud. We've had a question from zoom coming in around how you think machine learning and AI will affect the future of cybersecurity.

Claudette - Yeah, that's a great question. We are thinking about data and analytics and predicting things. So seeing things before they happen, seeing, you know, hearing that Canary in the coal mine, or seeing some of the trends or the patterns that can help us to detect things before they happen, just because it looks like it might be a dot, dot dot we're doing things around user behavior and analytics. So, you know, Razor, you log in, you've got a nice flow to how you log in every day. Well, then we see a login and it's a little bit different than what you normally do. Those different keystrokes are being analyzed to say, Hey, that's a sign, that's a potential threat. So there's, there's many ways that you can use machine learning to get better insights, but it's around identifying threats faster, detecting things that may look like anomalies, but also pulling out things. So to say, where do you put your investments, where you put your dollars? We talked, you're getting more lift out of this versus that. So we're already beginning to use it. We've been using it actually at TD for some time now, but, but I think we're doubling down on it. And so you'll see some more things coming through, but every organization should not just be doing things in the traditional way, but let’s use AI and machine learning to really help us move that needle a lot quicker that it is today.

Razor - Yeah. I know. I definitely think it's going to play a key role in helping keep us secure. That is all the time we have today. Claudette, Robert, thank you so much. I learned so much on this call on this conversation, I'm super grateful for both of you and your time as a small token of our appreciation, we have planted Robert and Claudette a forest of trees. As I mentioned every week, we, once we beat COVID, we have a climate crisis to deal with and know that you are both doing your part. You are right next to each other in a cyber secure place, in the Great Lakes Region. So thank you so much for your time today.

Claudette and Robert - Thank you very much. Pleasure. Thank you.

Razor - Awesome. We'll be sending out follow up items, action items linking on our blog around the great wisdom that Claudette and Robert shared following today's conversation. I wanted to thank everybody at home. It's been a pleasure again, when we heard that there was over 30,000 people over the last 12 weeks joining us, I was so grateful that you have tuned in, you've given us feedback every week. We love what we do, and we knew that Elevate had a role in communicating and connecting with the Canadian tech ecosystem. I'm super grateful to the talent, the thought leaders, the people that when we reached out to, you know, Mark Cuban and I emailed him to ask him to come on the show and he immediately said, yes, 12 minutes later, Mark replied. Scott Galloway was so thoughtful. His response, Brian Halligan, jumping on the white board talking about founder friendly financing and how to preserve the economics for entrepreneurs.

We had some great conversations there. It's been an absolute pleasure to be your host. Over these past 12 weeks, 12 episodes, season one is now complete of Elevate Live. We will be posting all of this to YouTube, cutting up our favorite parts. Please watch your favorites, share them with your friends. And we will be taking the summer off. We will be back again in September. We've got five incredible episodes of Elevate Live with special host Commander Chris Hadfield leading the conversation with the global leaders around social innovation, sustainability, and what we can all do to create a better world. That is the end of season one. My name is Razor Suliman, special thanks to my team. Executive producer and co founder of Elevate, Lisa's, Dennis, Misha, Audrey, Megan. Thank you so much for your help. It's been a pleasure coming live to you every Wednesday at noon for the past quarter, let's stay healthy. Take care of yourself. Take care of each other. Thanks so much. We'll see you in September. Bye.