uberknowledge

Sergio Caltigirone, VP Threat Intel., Dragos

A Digital Geneva Convention

Sergio talks about the cyberspace power vacuum, the challenge of ICS cybersecurity, and mental health issues in an incredibly pressured industry.

02:42   ICS cybersecurity is one of the most important and preeminent challenges we face because of the direct relationship to lives.

07:10   There are significant mental health issues in the cybersecurity community. We need to be more open in discussing this and helping each other.

13:27   We face a policy and power vacuum in cyberspace. We need a digital Geneva Convention.

20:43   Cyber professionals have to hold each other to account — we should be nice to each other personally but fight each other professionally to find the right answer.

Ashwin Krishnan: [00:00:32] So with me, I have Sergio C, I won't even attempt to pronounce your last name...

Sergio Caltagirone: [00:00:37] No problem.

Ashwin Krishnan: [00:00:37] Who is the VP of Threat Intel at Dragos. For the purpose of our listeners, I'm going to read your LinkedIn profile and then have you talk about it. It seems like a journey that is very non-traditional. You've been tracking hackers and malware. You followed your passion into computer science and information security at NASA, briefly, and then the NSA, then left the NSA to become the director of Threat Intel at Microsoft — launching the Microsoft Threat Intelligence Center in 2016 — and you joined Dragos to start the world's only dedicated ICS threat intelligence team, focused on uncovering cyber threats to ICS.

[00:01:12] But the thing that I found most interesting was the passion to fight evil took you to become the Technical Director of the Global Emancipation Network, using technology to counter human trafficking and working to save millions from modern-day slavery. That's a lot!

Sergio Caltagirone: [00:01:27] Yeah.

Ashwin Krishnan: [00:01:27] And a non-traditional LinkedIn profile. It actually speaks to what you believe personally. Talk a little bit about your journey and particularly about how you straddle what do you do at work and what do you do outside of work. They all seem to merge together.

Sergio Caltagirone: [00:01:41] They're all one and the same. So, the personal philosophy: I think that what we do, whether it's from the smallest things to the largest things, impacts the entire world; I really do. I feel like a small kindness paid to somebody on the streets, saying hi and recognizing and acknowledging maybe a homeless person who's sitting down, is a small kindness that you should pay and that pays dividends to everybody. And I feel very passionately that, I think it was Mother Theresa who said, "Not everybody can do great things, but you can do things with great love." I think that's really the fundamental of it, right? I drive very hard to try to make my life impactful to others in the world and in a joyful and loving way.

> "I think that what we do, whether it's from the smallest things to the largest things, impacts the entire world."

[00:02:42] For me, cybersecurity is one of those things. A lot of people see it very differently or in a lot of different ways, but for me, it's fundamentally about being a helper and solving a problem. Many people in this world use the internet just for their daily lives, to pay their bills, to talk to their families, and I believe in a safe environment allowing people to do that. It means that, you know, when you walk into a room, you can flip on the light switch and electricity is there, that you have access to clean and safe drinking water, that toilets flush and you have sanitation. These are all important things because without them, we know people die.

Ashwin Krishnan: [00:03:27] Right.

Sergio Caltagirone: [00:03:28] And so to me, industrial control cybersecurity is probably one of the most important and preeminent cybersecurity challenges we face because of the direct relationship to livelihoods and lives that we can impact with it.

Ashwin Krishnan: [00:03:42] Wow! I'm going to double-click on something because there's a passion in what you do and why you do, which is rare. I have to acknowledge that. The second thing is we keep talking about cyberskills shortage. We keep talking about how we need more people and interns and recruits, which is great, but how many people do you think will get into cybersecurity for the reason you got in? How do you chronicle your journey to let others find what their true calling is? Unfortunately, many people, they never get to that point.

Sergio Caltagirone: [00:04:13] Yeah. Here's the other thing though, I think many people do follow their true calling; they may not acknowledge it.

Ashwin Krishnan: [00:04:17] That's true.

Sergio Caltagirone: [00:04:19] And it's also not just what you do, it's how you frame it and what you prioritize when you do something. Like I said, it's everything from the smallest interaction you have with somebody to the most important thing you do in your career. And those are all important. For industrial in cybersecurity and for those getting into it, I think what you need to realize is that when you get into cybersecurity, you become a helper, that is your job. I think that everybody in cybersecurity finds that eventually somehow.

> "Industrial control cybersecurity is probably one of the most important and preeminent challenges we face."

[00:04:53] One challenge we have in it is that as people are becoming interested in the field and the career, I like to try to tell people, don't let technology be the thing. It's not the thing. It's the people using the technology that are important. So, don't get yourself wrapped too much into the technology. And when we talk about, say, industrials, we talk about disrupting a power plant or disrupting a water sanitation unit, the hackers who are trying to do these things don't care about the power plant. They don't care about water sanitation. They care about the people; they're attacking fundamentally the people that are using those. The technology is just a means to an end. I think in cybersecurity we get too wrapped up in, it's the technology, it's the thing, it's all we care about. When it's really the users and the people and everything that's relied on.

[00:05:47] At NSA, what I learned very much was the role of technology and national security and how bad people use technology. And how, as a nation, as a whole world of nations, we all have to work together to not let the bad guys win. I think it's a career path. One thing I love about InfoSec and cybersecurity is that almost everybody in it is good. I actually feel like it's a gigantic extension of my family to some extent ...

Ashwin Krishnan: [00:06:27] [Laughs]

Sergio Caltagirone: [00:06:27] And it's weird because most of us are, including myself, fairly dysfunctional, sometimes it's a weird family. We yell at each other on Twitter and

all this stuff that we do but, fundamentally, we get together. You know, I was at a place last night with a bunch of people and it felt like ... I mean, I was sitting across the table from people, and we yell at each other on Twitter about each other all the time, but at the same time, we love each other's work. And we recognize that these fights that we have are really the method of problem solving. It's like nobody's right or wrong. It's really about battling ideas to the extent that we can find the right solution between us.

[00:07:10] So in cybersecurity, I think that I found that the community, in almost all cases, tends to be one of people who care. I think it's also a challenge of we have significant mental health issues in cybersecurity because it's driven from people who care. Right?

Ashwin Krishnan: [00:07:26] Right.

Sergio Caltagirone: [00:07:26] And I myself have dealt with them. As I've chronicled in my blog posts about my depression and stress and challenges, I've had with that.

> "We have significant mental health issues in cybersecurity."

And I think that in cybersecurity, we need to recognize that part of being a helper is that you take on problems of others to help solve them. And in cybersecurity, I think we need to recognize that we do that as a community and that we also need to protect and help each other.

[00:07:52] In cybersecurity, people are horrible for being sarcastic. You know, we are really sarcastic people because we're constantly taking on problems. We are problem fixers. And sarcasm in the cybersecurity community, it's the outlet.

Ashwin Krishnan: [00:08:07] It's a pressure valve.

Sergio Caltagirone: [00:08:09] Just laughing about and finding joy in the problems, you know. But the challenge I want put to folks who are listening, the challenge I want to pose is, don't let the sarcasm become you. It's hard; as therapists say to people, if you keep telling yourself how bad you are, you're going to believe how bad you are. So, we can't let that part of our community become us. That is a challenge, and we do struggle with that from time to time. So for those stepping into cybersecurity, welcome! I welcome you with open arms. I love that you want to take this journey but take it joyfully and just be careful that you are part of the solution, and don't try to drag others down with you. When you have hard times, look for the joy in it and not the not the pain and sorrow that so many of us focus on.

Ashwin Krishnan: [00:09:03] Yes. You mention something which you talked about in the article that you wrote on dealing with stress and depression. Now, that's not something that is typically talked about at all, much less in cybersecurity, where it's all about how do we fight the bad guys. And your problems are your own, but you have made it very personal. You've gone into great detail about how you discounted it and then dealt with it. How has that helped you become a better individual, a better human being, and ultimately, have you seen positivity come out in others as a result of reading that?

Sergio Caltagirone: [00:09:41] Absolutely. I get an email almost every day from people who, one, are recognizing that they're seeing the same issues, or two, that because of

what I said, it helped them find help. Writing that post, it was because I met with several other of my friends, who very personally confided their challenges with me. And I recognized that I needed to say something because too many people are struggling and not saying anything. I honestly don't care if you say anything or you don't; I would love you to get help, whatever your challenges are.

[00:10:23] If I can at least express what we're challenged with, then I'll know, I'll do my best. I think the issue we have there is that no matter what we try to do, mental health is a hidden issue. Unlike, and I said it in my blog post, if you have a broken arm, people send you cards.

Ashwin Krishnan: [00:10:51] Correct.

Sergio Caltagirone: [00:10:51] And everyone is so sympathetic and so hopeful. But if you tell somebody, "I'm feeling depressed," and honestly mean it, nobody wants to talk to you anymore. I think the challenge here is a couple of things. One is people, and I get back to my philosophy, people tend to be good and love each other and want to help each other. The challenge we have with mental health is we don't know how to help each other. It's hidden. And so in some ways, me speaking out was my way of trying to express to others that it doesn't have to be hidden. And what it taught me personally, very, very personally, is empathy. I think a challenge we have is we want to help others, but if we have not walked in their shoes, we don't know how, or how it feels. I think that many people have expressed this. One of the things I hate in our community, and this is technology and honestly society as a whole, how we very fundamentally almost lionize or aggrandize working hard.

Ashwin Krishnan: [00:11:55] 24/7

Sergio Caltagirone: [00:11:55] That's stupid. I'm sorry. Why? What it comes down to is eventually you end up killing, literally killing, yourself. And that is not fair to your family, your friends or yourself or the industry. If your job is to help and solve problems, you're not going to help anybody by becoming mentally disabled or physically exhausted or things like that. So what I learned personally was, one, be empathetic to others; two, listen for people who are using words that say that they need something from you; and then the third is that as a community, we have to stop aggrandizing, killing ourselves. That's not OK. So if you're a manager of somebody, and I'm speaking to all of your listeners, if you manage people, manage them as humans, not machines, and recognize that you're asking a lot in cybersecurity and that you need to help each other.

> "If you manage people, manage them as humans, not machines."

Ashwin Krishnan: [00:12:53] Yeah, it's a great point. In fact, one of my earlier podcast guests, Diana Kelley of Microsoft, was equating cybersecurity to cancer research.

Sergio Caltagirone: [00:13:02] Yes.

Ashwin Krishnan: [00:13:02] It's an ongoing battle. There'll be good days, there'll be bad days. But you have to realize that you're never going to have mission accomplished.

Sergio Caltagirone: [00:13:09] Exactly.

Ashwin Krishnan: [00:13:09] But you'll get better at identifying mutations of cells and identifying how to go in. So that's a great point.

[00:13:16] Changing gears a little bit; in your Time interview, you were quoted as saying that we need a cyber Geneva Convention to protect civilians from state-sponsored cyberattacks. Talk a little bit about the theory behind that.

Sergio Caltagirone: [00:13:27] Absolutely. Right now, we face a policy and power vacuum in cyberspace. The smallest states to the largest states can effectively commit the exact same operation with almost the exact same outcome. If you're a state power with a few hundred thousand million citizens, you can cause a power outage in the most powerful country in the world, like the United States or Japan or so forth. That is a fundamental change in the world. Where, fundamentally, it was your geographical position, whether you had access to the sea or the air, or how much land, how many people you had, what your technological resources were that determined your power projection in the world. Now, fundamentally, that doesn't matter as much.

> **"We face a policy and power vacuum in cyberspace."**

[00:14:24] What we're finding, importantly, is that this is causing a large number of actors to enter into a very offensive space, which has impact on millions of people and businesses and so forth in the world. I'd just like to say, what if a country with a few million people decided that they didn't like what was happening, and they attacked AWS or Microsoft Azure, and all of a sudden, knocked millions of people offline and businesses can't make money, and the bad things happened. That's not OK. And the fact is right now that while you and I can sit here and say that's not OK, there is no common framework for understanding that that's not OK internationally. Nobody knows what anyone would do if somebody did that, what the response would be or should be. What if somebody went after a hospital? Everyone around us says that's not good, nobody should do that. But interestingly, that is not considered armed conflict and therefore does not fit within the Geneva Conventions.

[00:15:28] What if they went after a power plant next to a hospital because the power plant also provides power to a military installation? Right now, technically, even if we call that armed conflict, it's considered proportional because they went after a military target. It just happened that the hospital was attached. Let's say that they kill civilians, in the current framework, nobody cares. Basically, that's considered legitimate.

[00:15:52] Now, those are the questions we need to address. We've talked a lot about how earlier in our histories, we had carpet bombing and firebombing and nuclear weapons, and they are all fairly well understood between ethical and not appropriate uses of warfare. But now we've got very targeted weaponry. So it's like, "Oh, I can hit this military facility without hurting the hospital." In cyberspace, we don't have that yet. And so effectively, in many cases, what we're afraid of is the equivalent of carpet bombing on the internet, harming a lot of innocent people. And that's why I

say we need a digital Geneva Convention that says what is acceptable and not acceptable in this new landscape, before millions of people die because that is the path we're on if we don't address it.

Ashwin Krishnan: [00:16:45] And have you found any supporters for that?

Sergio Caltagirone: [00:16:47] Yes. So, the U.N. is not doing all it could right now, and that is unfortunate, mostly due to several countries that just have too many challenges, I think, in communicating with each other. Cyber diplomacy is one that is not being placed high on the list of things to do for most countries and that's bad. We're doing more cyber diplomacy through business than we are through diplomats, and that balance needs to be found. The G7, the Group of Seven countries, does have a side topic for cybersecurity. There is some movement happening in there.

"We need a digital Geneva Convention that says what is acceptable and not acceptable in this new landscape."

[00:17:27] I was very personally honored to be part of the group of experts at the International Committee of the Red Cross last year, where we got together to talk about the implications of cyber warfare in international humanitarian rights. We talked about things like what if somebody could target a humanitarian camp in a border that was maybe harboring terrorists? What would the OK things be? What would the not OK things be? Could you target hospitals? Is that OK or not OK? That was literally the first conversation of international experts who got around the table to ask those questions.

Ashwin Krishnan: [00:18:01] Wow.

Sergio Caltagirone: [00:18:02] And there was a paper released by the Red Cross that I highly recommend anyone read because it is just the first step in the conversation. But we have to have it because too many times in our human history, we've responded to the worst atrocities. This is one where we can look forward in time and say, bad things are going to happen; we should do something now to prevent atrocity. And that's what I want us as a global community to do.

Ashwin Krishnan: [00:18:26] OK. So one last question. We're probably, what, day four of Black Hat, depending on when you arrived?

Sergio Caltagirone: [00:18:34] Something like that. There are no windows here, man, who knows anything!

Ashwin Krishnan: [00:18:38] [Laughs] Most people are saying, "Have you checked in for DefCon?" So already, it's like Black Hat is passé, right?

Sergio Caltagirone: [00:18:42] Yeah!

Ashwin Krishnan: [00:18:42] What was one thing that surprised you at Black Hat 2019 this year, and what was one thing that you hoped would have changed but hasn't?

Sergio Caltagirone: [00:18:49] Absolutely. One thing I loved is that it's been a thought, a hypothesis, a conjecture for the last three years of mine that defenders are getting

better, much faster than adversaries.

Ashwin Krishnan: [00:19:05] Oh wow! OK.

Sergio Caltagirone: [00:19:06] And that's not a majority opinion, but I think it's true. I think that our cynicism and our negativity and some of the vendor issues that we've seen in the industry have driven us to a myth that we're way behind, and we can't do this without this blinking box or something like that. What was, I think, probably a watershed piece of information that was released by Microsoft showed how the changes that they made in the operating system made operating system exploits effectively nothing anymore. Like the number of zero days that they're dealing with are close to zero on the OS layer. What it shows is that we can do it; defense is doable, right. People are making big changes, and these changes take time but they're having big impact. I mean, operating system vulnerabilities, I have to stretch my mind to remember the last widespread OS vulnerability; they've all moved up, writing applications in some application-level protocols and stuff. And so, to me, that should be a huge signal to the industry that, oh, my God, we can do this. It really does happen. And I think that that is super powerful. And I loved that they stood up and they talked about the defenses that Microsoft has put in and that they showed data of what the impact was to the security of their platforms and to those of all their users. If there's anything in this that people take away from Black Hat, it should be that. This is real data that shows we can do this, and that should be very important.

[00:20:43] The one thing I wish that Black Hat changed or wish that the community as a whole changed is that we don't take as much of an engineering or fact-based approach. I wish that we, as a community, were stronger about saying when things are not OK. What you just said was not supported by any data or fact.

Ashwin Krishnan: [00:21:11] So calling each other out.

Sergio Caltagirone: [00:21:13] We absolutely should. We have to do that respectfully because you might be wrong, and man, I don't have enough fingers to tell you how many times in my life I've been wrong. We have to be OK. We have to be humble about that and accept that sometimes, you know what, we say stupid things or maybe we took the data too far, but we have to call each other out. I don't see that at all in our community. We let people run with whatever the hell they want to say and do, and nobody mentions anything at conferences or at presentations. Honestly, I feel like we are, as much as I love it, we're too nice to some extent to each other professionally. **We should be nice to each other personally; we should be fighting each other professionally, right, to find the right answer.** And I think that's where I want to see a Black Hat or an RSA really drive better us to be better.

Ashwin Krishnan: [00:22:10] Wow, we can't top that, so we have to stop there. This has been great. Again, thanks for your time. You, in particular, have brought a very personal feeling to this whole conversation, but also to what you're doing in the industry itself. So I salute you for that, and good luck!

Sergio Caltagirone: [00:22:27] Thank you.