**Project: Public Sector Future WWPS Podcast Series**

**Detail: Episode 59**

**Talent: Alvaro Vitta [host], Sami Khoury [guest]**

**TRT: 19:31**

**OLIVIA NEAL:** Hello and welcome to Public Sector Future. This is a show for anyone who cares about using technology and digital approaches in the public sector to deliver better outcomes.

I’m your regular host, Olivia Neal, and today we’re continuing with the second of our episodes focusing on cybersecurity. In our last episode we heard from Tom Burt, who shared the findings of the recently released Microsoft Digital Defense Report. If you haven’t listened to that episode yet, do go back later and check it out.

Today, we’re hearing from someone at the frontline of protecting a government, and a country, against cybersecurity threats. Sami Khoury is the Head of the Canadian Centre for Cyber Security,. Together with his team, he has been leading work in Canada to modernize approaches and use the latest technology to defend against these threats. Let’s join our guest host, Alvaro Vitta, for their conversation.

**ALVARO VITTA:** Hello, Sami, and thank you for taking the time to speak with us today.

Sami, for our global audience, can you provide a brief description of your role at the Canadian Centre for Cyber Security and what you and your team are responsible for?

**SAMI KHOURY:** Thanks a lot, Alvaro, for the opportunity to be on this podcast. It’s a great opportunity to speak about cybersecurity with a great partner of ours in Microsoft.

So the Canadian Centre for Cyber Security was established in 2018. We have been doing cybersecurity for a long time. But in 2018, the government, as part of its National Cybersecurity Strategy, felt the need or felt the opportunity for us to share our extensive knowledge with the rest of Canada. And as a result, the Centre was created, and now our capabilities and services are output to the service of Canada and Canadians more broadly.

So what we do is we respond to incidents. But I would hope that we are known for putting out advice and guidance, for putting out publications, for supporting folks during incidents, for developing world-class capabilities, and for building partnerships in the form of outreach to all sectors of Canadian society and Canadian economy. So it’s a busy organization, and we are here to support Canada and Canadians in their cybersecurity journey.

And another thing that the Cyber Centre does is also we are the information assurance arm of the government. So when it comes to cryptography, we are the authority on cryptographic standards that the governments use, and we use that knowledge to inform Canadians also the state of cryptography and its evolution.

**ALVARO VITTA:** Thank you, Sami, and thank you for the service you and your team do.

So when we look at the Microsoft Digital Defense Report 2023 that just came out on October 5, what we’re noticing, what we’ve observed is that there’s been cyber threat activity against organizations in more than 120 countries and territories. Now, 53% of all of that activity targeted specifically government and critical infrastructure organizations.

From your perspective, what do you believe is driving the intensity and emphasis on government and critical infrastructure organizations?

[02:28]

**SAMI KHOURY:** Because we’ve been working in the cybersecurity field for a long time, we knew that at least the Canadian government would be a target of nation-state actors. And we’ve had a number of incidents in Canada, where nation-state have gone after government organizations.

We have been warning about that in our National Cyber Threat Assessment document that we’ve put out in 2018, 2020 and 2022, that nation-state continues to pose a strategic threat to Canada, but that also they are targeting critical infrastructure.

And they’re targeting for many, many reasons. I think some of what’s driving the intensity could be some geopolitical tensions, maybe new opportunities that they’re finding in the West. Could be for pre-positionings, and we have been warning about prepositioning for some time. And the Joint Cyber Security Advisory with CISA, but also the work of Microsoft on Volt Typhoon, speaks to that prepositioning on critical infrastructure.

So there are many reasons why nation-state would go after that. Some of it could be traditional espionage. Some of it could be, intellectual property theft. Some of it could be economic information or business intelligence that they’re going after. But it is getting very sophisticated. And also, as you said, we are seeing more intensity because we live in a more and more connected world.

**ALVARO VITTA:** Just to your point, we’ve seen a lot of data exfiltration exercise and living off the land techniques, just to stay dormant and dwelling in the environments, to then, you know, later on, as you said, you know, preposition their for nefarious future activities.

Now, Sami, what unique challenges do government and critical infrastructure organizations face as they defend against nation sponsored cyber threat activity?

[04:31]

**SAMI KHOURY:** Nation sponsored cyber threat activity tends to be sophisticated stuff. So the challenge we face is that we have to be imaginative, innovative, and fairly sophisticated ourselves in our defensive capability because we have to defend ourselves against those sophisticated threats.

Also, you know, they tend to be very determined adversaries. The cybercriminal might try a few times, if it doesn’t work, will move on to somewhere else. A nation-state is a determined adversary that will keep trying until they find an in. So as a result, that is that is one of the unique challenges, a bit of their persistence in pursuing targets that have strategic interest to them.

So we have to be constantly vigilant, and we have to be on top of our threat landscape. And we have to be on top of our awareness of what the threats are, where are they coming from. Also, what are some of their interests in Canada, or whatever they are pursuing in terms of critical infrastructure?

[05:44]

**ALVARO VITTA:** And one of the things that we also noticed is that because of their persistence and sophistication, they’re very well-funded, they are very patient, right? So we’ve seen sometimes campaigns that take a couple of years or more for them to actually come to fruition.

And so, how can national cybersecurity centers across the world assist these government entities and critical infrastructure entities in preparing for and responding to these type of persistent threats?

**SAMI KHOURY:** So at the Cyber Centre, you know, our job one is to protect the Canadian government. And for that, we’ve deployed an array of sensors and array of capabilities to make sure that the Canadian government is well protected. And that is in addition to the capability that are inherent in our desktops or in the cloud. So we add another layer of defense to protecting government.

But beyond government, we need to reach out to all sorts of communities out there. We need to encourage them to report incidents to us, big or small, to be vigilant.

Nation-state activities often can go unnoticed or can go – or sometime the artifacts are very sort of discreet, versus a ransomware incident where you know right away that you’ve been had.

So how can we encourage businesses to be vigilant, to be on top of their IT, like to report incidents, big or small, and then we would then work with them to decipher whether it is a nation-state or not.

So we put out a lot of publications, a lot of IOCs. We add our voice to that of other international partners to share information about campaigns that we are aware of. And we encourage businesses to follow the advice and guidance that we put out so.

And I hope that that’s a two-way street, that it’s not just us putting out information, but that they see the value in sharing with us whatever they see, so that we can then connect some dots and identify whether or not there is a campaign going on.

[07:57]

**ALVARO VITTA:** Yeah, I think that’s crucial, that bidirectional partnership between the public and the private sector is crucial, because we’re all in this together, right. So the more we share, the more we’re going to be able to mitigate these threats together.

So, as the leader of one of the most modern national cybersecurity centers on the planet, what guidance would you offer to other aspiring nations that may be looking to modernize their national cybersecurity centers?

**SAMI KHOURY:** So the Cyber Centre is about five years old. So as a result, we are still in that growth journey and that discovery journey. And prior to 2018, we were very much focused on protecting the government. And starting in 2018, we started to do an outreach beyond government.

So we are constantly learning about how do we reach to the various sector of the Canadian economy, the various sectors of society, how do we tune our message to the different audiences. each one needs a different type of engagement. And I think that is something that we are learning. So part of my guidance to somebody else is to make sure that you develop a capability to speak in multiple voices, depending on the audience to whom you are speaking.

The world is constantly changing, and you know, when we were established in 2018, there was no thing, such a thing as work from home. There was no pandemic. The pandemic has thrown all of that into a bit of disarray, and now we have a new reality out there.

So having the ability to constantly adapt to the new world order and tackle today’s threats, not necessarily yesterday’s, or five years ago’s threats. So we need to be very agile in the way that we respond to the role of the National Cyber Security Centre.

So and the other thing is, I would say, it’s about persistent engagement. It can’t be just one message and then move on. We have to constantly repeat the message, because, sadly, to this day, we see a lot of incidents that have been or can be prevented, which unfortunately, you know, businesses have not heeded our advice and fall victim to cybersecurity incidents. So persistent engagement is very important.

[10:24]

**ALVARO VITTA:** Thank you. No, that’s great advice. As you mentioned, right, this is a constant evolution, and you constantly have to innovate to stay ahead of the adversaries and attackers.

And in your opinion, what would you say, from a technology perspective, are some of the challenges that you’ve been successful at overcoming in this public and private sector partnership?

**SAMI KHOURY:** There’s a couple of things. One is, we have to be on top of our technology. So in a way, we have to be leading by example, and not give businesses the impression that for us in the government, we use special things. So it’s been very important that when we put out advice and guidance of our technology, that we demonstrate that that advice and guidance also applies to us. so that is one thing.

The thing is, we tend to develop a lot of capabilities in house. We like open source model to develop some of our own tools. And we, in turn, have shared these tools. We’ve open sourced many of them. We publish them on GitHub, and we encourage businesses to look at what we use. If it’s good enough for us at the scale of defending government, it should be good enough for many others.

And one example is Assemblyline, which is our malware analysis engine that we’ve put out of open source, and it’s used by some extremely big companies that have found value in deploying something like Assemblyline into their IT environment.

So we speak from a position of understanding and appreciating of technology. We have a strong partnership with Microsoft to try to stay on top of all of the innovation that’s coming out of Microsoft, but also we encourage our own teams to have hackathons, to have, collaborative events where we partner with the private sector to look at the latest and greatest innovations in technology, so that we demonstrate that we are masters of the latest and greatest.

Of course, we can’t take our eye off old things because not everybody adopts the latest and greatest. So we have to be on top of old technologies or legacy technology. But also, we have to be mindful of the fact that we want to work with the latest and greatest, so that if there are any security issues or vulnerability issues, that we can address them as quickly as possible.

So in the technology landscape, it’s a bit of a broad swath that we have to cover, but we are here to share as much as we can through our open source collaborative environment on GitHub.

[13:05]

**ALVARO VITTA:** Now, that’s great that you’re open to sharing your learnings, your technology with others, so that they have similar capabilities of defense.

And so, talking about technology, right, and the evolution of technology, I mean, over the last few months, when we talk about 10 months ago, we weren’t talking about generative AI at all, right? And now we find ourselves here whereby, you know, cyberthreat actors are using, and cybercriminals are using these generative AI technologies, and they’re weaponizing them, and they’re monetizing them, right, across the world. So they’re early technology adopters and are operationalizing a lot of these advanced, sophisticated tools.

So how can government organization counter these technology adoption advantage and sophistication as they look to protect their digital assets?

**SAMI KHOURY:** You’re absolutely right, I think, Alvaro. The ChatGPT, OpenAI, all these capabilities hit the society like a storm about a year ago. We have been well informed about artificial intelligence for many, many years. We use it at the Cyber Centre for the triage of many of our flows of data. So from that perspective, we understand it, but it has taken off in a completely different scale a year or so ago.

So it’s important that we appreciate the risk of what this technology brings. It brings lots of opportunities, but also there are some risks. And those risks, we know that, for example, cyber criminals are using some of these capabilities to craft very sophisticated, very well authored phishing emails. So you can interact with many of those engines to craft an email that is well tweaked, or well-tuned to the person to whom you want to send it to. And it will be written very well, very eloquently.

And so unfortunately, while it has brought many opportunities, it has also given an opportunity or given a space for a cybercriminal to use it in a way that maybe have accelerated some of the phishing attacks and made them a little bit more sophisticated.

We have published some generative AI, information, advice or guidance, on our web site, so others can go and read what it is that are help to identify some of the risks that those capabilities bring.

The opportunities have to be assessed on a case by case. Every business will look for how to leverage OpenAI, or how to leverage those LLM models to their own business model. But it’s important to understand that some of the risk, and some nation-states are working hard to at least to maybe find opportunities to exploit these language models or find vulnerabilities or find weaknesses in them.

So it’s a double-edged sword. And as we also explore how to better understand them, the good thing is was talking about it. So that’s the good thing. But I think we have to proceed with caution, and until we get to a space where we understand a little bit more, what are some of the practical risks that are out there in terms of these generative AI capabilities.

**ALVARO VITTA:** Well-articulated, yeah, and I think we’re in a race, right, in this cyber-AI race, but we’re always in a race in cybersecurity, right, whereby, you know, the adversaries and the defenders are always trying to, get a leg up on each other, right?

And I think these, just like you mentioned, there’s a lot of challenges with AI. But there’s also a lot of opportunities for government and private sector to be able to work together to have an advantage to be able to defend effectively against these new threats.

So, Sami, we look to highlight and celebrate and share the good work of public servants from around the world that others can replicate. Are there any examples in cybersecurity from some of the other governments that you work with that inspire you and which you consider to be worthy of replicating?

[17:35]

**SAMI KHOURY:** I would say in the cybersecurity space, it’s all about partnership, and you want to partner with folks who can complement you in a way. So we each have sometimes different mandate, different scopes, different domestic realities. So it’s difficult to compare, you know, one country to another.

But in that partnership, and I would look to, you know, our closest partners, the U.S., the UK and the Five Eyes, but beyond that, I mean, we have partnerships with more than those I just named. And in each one of those partnership, we have something to contribute to the partnerships, and also we learn from it. None of us can solve cybersecurity by ourselvesand cybersecurity knows no borders. So an attack or a cyber campaign that was targeted one country can easily end up in Canada.

[18:33]

**ALVARO VITTA:** That’s great. You know, I love that that partnership is based on collaboration where each of you are augmenting each other’s capabilities, and as a whole, the sum of its parts is greater than each of the parts on his own. So that’s fantastic.

Well, Sami, we want to thank you for your time today and for the relentless service that you and your team do around the clock to keep us all safe and allowing us not only to survive, but to thrive in this digital era. Thank you so much.

**SAMI KHOURY:** Thank you, Alvaro. Again, it’s a great opportunity to talk about cybersecurity, to get more folks aware of what the Cyber Centre is up to, and to reach out to us in case they need any help.

But also, I would say thank you for the partnership. I mean, we – we’ve had a very longstanding partnership with Microsoft, and it’s important that we celebrate it. I again thank you for this opportunity to be on this podcast.

[19:29]

**OLIVIA NEAL:** Thank you to our guest, Sami Khoury, and thank you to you for joining me today on Public Sector Future. Visit our website at aka.ms/publicsectorfuture to find more insights and material on cybersecurity. As always, please do send us your questions and feedback, you can find me, and Alvaro, on LinkedIn, or email us at ask-ps@microsoft.com. Thank you and see you next time.

END