**Public Sector Future WWPS Podcast**

**Detail: Cybersecurity mini-series podcast**

**Episode: 1**

**Host: Alvaro Vitta**

**Guest: Tom Burt (Corp. VP, Customer Security & Trust)**

**TRT: 28:50**

[TCR 00:00:00]

OLIVIA: Hello and welcome to Public Sector Future. This is a show for anyone who cares about using digital approaches in the public sector to deliver better outcomes. I’m your host, Olivia Neal, and together we discuss technology and trends, as well as the cultural aspects of making change happen.

October is Cybersecurity awareness month, and today we’re kicking of a set of episodes, which you’ll hear throughout this month, on the topic of cybersecurity. To help steer us through these, I’m delighted to be joined by Alvaro Vitta. Alvaro is the Worldwide Public Sector lead for cybersecurity here at Microsoft.

Alvaro, great to have you here.

ALVARO: Thanks for having me, Olivia! It’s Great to be here!

OLIVIA: Can you tell us a bit about your background?

ALVARO: Sure. Olivia, I’ve been in the cybersecurity industry for the last 18 years in a variety of roles in security, including; security architecture, consulting , strategy and other areas.

Throughout my career I’ve helped private and public sector organizations at the regional, national and global levels with the planning, design, implementation and operationalization of security programs.

Currently I am leading the Worldwide Cybersecurity Strategy for Public Sector at Microsoft

OLIVIA: Why is public sector important to you?

ALVARO: Olivia, Public Sector Organizations are the backbone of our societies. They have the people and infrastructure that provide critical citizen services that ensure the well-being and safety for all of us at the local, regional and national level .

It’s my mission to ensure Public Sector Organizations across the Planet, are empowered to do more to protect their digital ecosystem in this complex and ever-evolving cybersecurity landscape.

OLIVIA: Thanks Alvaro for joining us. Our first guest in this series of episodes is Tom Burt. Tom is Microsoft’s Corporate Vice President for Customer Security and Trust. He and his team are responsible for protecting people, businesses and governments who use Microsoft products from cyberattacks.

Tom's team will be launching the Microsoft Digital Defense Report later this fall, which will share trends and insights from the past year of cyber defense.

He and Alvaro are going to be discussing the trends he’s seeing, how he’s been working with the government in Ukraine in relation to cyber defense, and how public sector organizations can be better prepared.

Over to you Alvaro!

[Music]

**ALVARO VITTA:** Hi, Tom, thank you for joining us, and welcome to the show.

**TOM BURT:** Well, thanks for having me.

**ALVARO VITTA:** Today we’ll be talking about cyber-resiliency in government and what does that really mean?

So to start with, Tom, for our international audience, can you start by telling us about your role at Microsoft and what your team is responsible for?

**TOM BURT:** Sure, I’m corporate vice president for Customer Security and Trust, and in this context, that means I have in my organization, teams that are responsible for doing what we can, what Microsoft can uniquely do to improve the security of the digital ecosystem.

So I have a digital diplomatic team that works with government officials around the world to advocate for enforceable rules of nation-state conduct in cyberspace. We have teams that work on our cybersecurity policy. But we also have teams that work to disrupt nation-state actors, through both technical and legal means.

I have our Digital Crimes Unit, which really leads the world in combating digital crime online, and a number of other teams that in other ways contribute to the security and safety of the digital ecosystem.

But most specifically, over the last six months, we’ve been directly engaged in assisting the Ukrainian government in its efforts to defend against the cybersecurity parts of the hybrid war that they are fighting with Russia.

**ALVARO VITTA:** Who benefits from this work and these programs?

**TOM BURT:** The work that we do I think benefits the digital ecosystem in general. And in particular, you know, the work that we’re doing in Ukraine, we’re doing to help the Ukrainian government in its efforts to defend against the war there.

**ALVARO VITTA:** So Tom, can you tell us about the Microsoft Digital Defense Report and why does Microsoft produce this report?

**TOM BURT:** So the Microsoft Digital Defense Report is something we started two years ago, and we’re continuing to issue annually, each year.

And what it is, is our effort to assemble from across the entire company, everything that we have seen in cybersecurity over the prior year, and see what insight we can draw from pulling all that information together, communicate to our customers, to officials, government officials, policymakers, as to the threats we’ve seen across the entire ecosystem.

And then in the Microsoft Digital Defense Report, we always include our best advice about what to do to be prepared for and defend against the cyberattacks that we’ve seen in the prior year.

**ALVARO VITTA:** How has the cybersecurity situation evolved since the publication of this report and previous reports that you’ve done before? And what were your main findings?

**TOM BURT:** Well, the thing that we’ve seen over the last couple years, and I think you’ll see again when we publish this year, is that, unfortunately, the scope, the volume of cyberattacks, the sophistication of cyberattacks, the impact of cyberattacks, both in terms of cybercriminal activity, as well as nation-state activity, continues to increase over time, and that the work that we all need to do across the ecosystem to better defend against this, against cyberattacks of all kinds, we need to do better.

The encouraging part is that we do see a continued investment in improving cybersecurity capabilities and building new tools and systems to help customers be secure, but we still need to do better as an ecosystem in terms of policy, in terms of how governments react, and right down to the basic cybersecurity hygiene that every individual and every corporation and every organization needs to practice to make sure that the entire ecosystem is safe and secure.

We have the tools. We have the tools we need today to be much more secure and to prevent a significant volume of cyberattacks, both – and especially cybercrime, but we aren’t utilizing those tools to the extent that we need.

**ALVARO VITTA:** And Tom, do you think this is because of lack of awareness? Could it be because they just under – don’t understand the capabilities that they – that they own? Is it a combination of both? It’s a skillset? What is your opinion as to why that continues to be a trend?

**TOM BURT:** Well, I think it’s a trend in part because we see incredibly sophisticated actors behind the cybercrime attacks and behind the nation-state attacks. And so, they continue to evolve and expand the techniques and the practices they use.

And in terms of cybercrime, it is so lucrative that we see more and more participants. And we now see an increasing trend, which we reported on in our last Microsoft Digital Defense Report, of cybercrime-as-a-service where the cybercriminals actually offer to others the ability to use their tools, their systems, their technologies, and even a full end-to-end service in order to engage in cybercriminal activity.

So you can go buy that on the dark web, for example, ransomware. You can find ransomware-as-a-service on the dark web, And so, you know, there’s an increasing volume and sophistication of attacks.

But on the side of – of defending against these attacks, there’s a number of things that need to be done. There are some basic cybersecurity hygiene practices, like patching your system with the most up-to-date security patches from every vendor. And that’s true for Microsoft, as well as all of our competitors. We all work to keep our – our systems as secure as possible. And that means you need the most up-to-date technology, which we all provide through security update packages.

You need to apply those patches. We see the bad guys; they see the new patches coming out, so they know there’s a vulnerability, and they exploit those vulnerabilities, the ones for which there are patches, because they know that most people in the ecosystem are not applying the patches. Typically, it’s only about 30% of the devices in the ecosystem are actually having up-to-date security patches applied, and that’s just not good enough.

We also need everyone to use multifactor authentication on every account. You know, Microsoft Teams published a blog, now it’s almost three years old, where our study determined that over 99% of all attacks in the prior year that was studied would have been prevented if multifactor authentication had been present.

And again, it’s not to say that multifactor authentication is perfect. But it is still an incredibly valuable and effective defense against the vast majority of cyber-criminal and nation-state attacks

And then the third part is, move to the cloud. Every vendor, and especially at Microsoft, our most innovative defense, our best security, our best security services are the ones that we are innovating for in the cloud.

And of course, when we need to apply a security patch, Microsoft takes care of that, and it’s taken care of for you across our cloud services. And so, the cloud services are always up to date with the most secure technologies that we have.

And as we’ve gone through everything from the Ukraine attacks to what we’ve seen happening in the cybercrime world, each of these basic fundamental principles has been proven again and again to be the solution to significantly reducing the vulnerabilities that we see in the ecosystem. If people would move to the cloud and apply basic cybersecurity hygiene in their on-premises environments, they would find that they would be way more successfully defended against cyberattacks than we are today.

**ALVARO VITTA:** And that’s a good point. And I would assume that the primary reason for that is because if you have, like you were saying, ransomware-as-a-service organization, so for-profit organizations with deep pockets, and, you know, purpose for revenue, obviously, and our customers are found in, you know, whether you’re a government agency or a defensive intelligence agency, you’re not really for-profit, so you’re not investing the same amount of money or capabilities, or you don’t have the same kind of purposes as these organizations.

So what you’re saying is, if you bring it to Microsoft, we have a dedicated set of teams, and infrastructure, and services, and hyperscale to be able to do that on your behalf.

**TOM BURT:** That’s absolutely right. We recognize that a lot of what I described as basic cybersecurity hygiene, in any given environment, it takes time, it takes money, it takes effort, it takes budget that an organization would rather spend on other activities and other priorities, rather than spend it on cybersecurity.

And that’s one of the huge advantages of moving to the cloud is you now have the very best security technology, the very best security experts working to keep your data and your computing as secure as it possibly can be in the cloud.

It’s existential to cloud services that they be secure. So we invest our very best people in making sure that it’s secure. And you, as a customer, get the benefit of that investment and of that commitment to security, so that you don’t have to find the budget yourself, you don’t have to find the people yourself, which is one of the huge challenges we have in the cybersecurity spaces is how many unfilled jobs there are because we just don’t have the people who have the training expertise to do this work.

Well, we have those people at Microsoft, the very best security experts, and they are committed to keeping our cloud services as secure as possible. And so, you get all that benefit by moving to the cloud.

**ALVARO VITTA:** And I would assume that, you know, the rationale also, or the benefit for a customer, a government customer or a defense intelligence customer for moving from an on-premise environment to the cloud is that all of that amount of people that we have, the great technology, the great intelligence that we have, you cannot leverage that unless we are able to gain visibility into your environment. So having an environment that is not connected these signals that allows us to then help you is counterproductive.

**TOM BURT:** At Microsoft, we get 47 trillion signals a day that come into our environment from our global ecosystem. And our teams are increasingly using those signals, using our ability to hunt in those signals for adversary activity, and increasingly utilizing AI and ML technologies to look through that data for anomalous activity or for indications or hints of action by an adverse actor.

And we have the capability, using that data system from our hyperscale cloud, to detect and see and protect customers against attacks. We had that happen in one specific instance, in the war in Ukraine, where most of the customers in Ukraine have not migrated to the cloud. An exception is government. They changed the law a week after the war started, so that they could move to the cloud. And we immediately jumped in and helped provide, for free, a range of services to help move the Ukrainian government. We moved I think it’s 16 of 17 government ministries have moved their data or their compute to the cloud, to help provide greater resilience against the Russian attacks.

And so, in one instance, one of our private sector customers that was utilizing one of our cloud security services, that cloud security service, that Defender for Endpoint detected an attack from Russia, one of the wiper malware packages that they were utilizing, detected that they were installing that, had managed to get access to the network, and were in the process of installing that wiper, and the service detected it, blocked it and stopped the attack, all with no human intervention at all, utilizing the algorithms that we had in place in that service to detect that kind of activity.

So that’s the kind of thing that we can do in the hyperscale cloud that customers can’t possibly do on-premises. One of my colleagues referred to trying to defend against the attacks coming from criminals and from nation-states on-premises as hand-to-hand combat. And you don’t need to engage in hand-to-hand combat. You can come to our cloud, and we can use the technology, the expertise, and the data that we have to help protect you in a much more robust way.

**ALVARO VITTA:** I see the other benefit is that, in the case of what you mentioned with Ukraine, right, or any other similar situation, is that you have a data center, and a data center is a physical asset. And you know, in these geopolitical situations, that becomes a prime target, to eliminate that. When that is then dispersed and distributed through a hyperscale environment across all the data centers, across the planet, then you get redundancy, you get disaster recovery capabilities that you wouldn’t otherwise have in your place.

**TOM BURT:** That’s a really important point, and it’s one of the insights that we’ve gained from all the work we’ve been doing working with Ukrainian government to help defend against the cyber-war that they are facing in Ukraine, which is that not only do you gain cyber-resilience and cybersecurity by moving to the cloud; you also gain physical security by moving to the cloud.

We learned from one of the Ukrainian government officials that we’ve been working with, that one of the first missiles launched by Russia, when they began the physical attack in Ukraine, one of the very first missiles targeted the government data center. And at that time, all of the Ukrainian government workloads were kept on-premises and operated from that data center.

And that’s one of the reasons why they rapidly, why President Zelenskyy rapidly signed into effect a law that had just been passed in Ukraine, to enable Ukrainian government ministries to move to the cloud. And we helped them do that because once you’re in the hyperscale, cloud, your data is now located in multiple data centers, and likely many, if not all of them outside your country.

And so, when you’re engaged in a conflict, in a hybrid war, like we see happening in Ukraine, you are physically more secure, because your adversary can’t actually go in and destroy the data center where you are housing your compute.

So that’s one of the real insights is, especially for a government agency, public sector customer, how important it is to think about the physical security of where this data resides, as well as the cybersecurity. Both of those things are significantly improved by moving to the hyperscale cloud.

**ALVARO VITTA:** Now, one of the things I’ve noticed is that the transparency trend your team has shown in, for example, almost on a weekly basis, I see that you’re posting, Microsoft Threat Intelligence Center information around vulnerabilities or common threat vectors that you’ve either stopped or prevented from happening, or just awareness in general, so that people can look at indicators of compromise and take action and be prepared and be informed.

**TOM BURT:** We really have two motivations for the work we do and that others at Microsoft do to publish the threat intelligence that we see, when we think that that’s a valuable contribution we can make to the ecosystem.

One is exactly as you described, to provide the indications of compromise, and the other threat intelligence that helps customers that are working to defend against these attacks, to observe these attacks, to be prepared. And we often provide information about how to defend against them, or how to recover if you are attacked, in those publications.

In addition to that, we do publish this information, especially about nation-state attackers, because our view is that, as I mentioned earlier, we need a much more robust set of international rules governing how nation-states act in cyberspace, restricting attacks on civilians and civilian enterprises, in requiring governments not to look the other way when they know cybercriminal activity is being engaged in by actors operating from their geography.

Rules like that need to be established by the international community. They need to have enforcement, even if that enforcement are things like economic sanctions and the like, the same kinds of things that the international community does to enforce a wide range of rules that we have, whether they are formally international law, or customary practices that nation-states engage in, so that when those are violated, other nation-states take action to punish the actor who isn’t abiding by those established rules of nation-state conduct. We need those rules in cyberspace, and we don’t have them.

One way to get there is to be public, to talk about what we’re seeing, to do attribution. You may have seen that at Microsoft, we’ve been willing to call out actors from Russia and from China, and from other countries where we have active business, because we think it is critical for the international community to be aware of what is happening in the cybersecurity space, so that action can be taken, and these international conversations can occur.

**ALVARO VITTA:** So Tom, any examples of work that you have seen undertaking by a government organization, or a public sector organization that has either inspired you or has impressed you that others can benefit from?

**TOM BURT:** I’ll hit a couple of different examples that I think are worth public sector organizations who care about cybersecurity really looking at closely. One is Estonia. Years ago, was Estonia was the target of Russian cyber-attacks. And that country recognized the importance of having cyber-resilience and adopted a range of practices across their public sector and private sector workloads and became incredibly resilient to cyber-attacks.

And when we wrote a blog earlier about what we were seeing happening in the aftermath of the hybrid war in Ukraine, one of the things we discussed was how we had seen in the second, third, fourth month of the war, we saw Russian actors beginning to engage in espionage activity across the border countries, the Baltics, as well as Nordic countries.

And what we saw was that while the other Baltic countries were being successfully attacked by Russian actors, and we provided them notification and threat intelligence to help them defend themselves, there were no similar attacks against Estonia, zero. That is consistent with what we’ve seen over the years, which is that nation has done a remarkably good job in establishing resilience. They’re moving to the cloud. They’re taking the steps they need to take to defend against cyberactivity.

And then I’d point to the United States, where over the last several years, with new leadership in place that understands the critical importance of cybersecurity to our government and to our critical infrastructure, we’ve seen a number of steps taken, whether it’s the leadership of the CISA organization in the Department of Homeland Security that is publishing regular alerts to the community and to segments of the economy saying, here’s a specific threat or a character or a type of threat, and here’s the steps you should be taking to protect against those threats. That’s one organization that’s active.

We saw the adoption by the President of the Cybersecurity Executive Order, which was really targeted at government agencies, but more broadly, was we’re going to require the technology industry to take steps to enable those government agencies to comply with that Executive Order by building in the concept of a software bill of materials, for example, with every product, and by taking other steps to help government move to the cloud.

There’s work to be done still to get that Executive Order in place and operative, but we’re working with government to see what we can do to move that forward quickly, because each of the steps required by that Executive Order would significantly improve the security of government agencies. And so, that’s a great model for the public sector to look to for the kinds of steps that should be taken to secure the public sector against these kinds of attacks.

And that takes me back to something I said earlier, which I think is an important thing, which is, we actually do have the tools in place today that would remarkably improve the security of the ecosystem, if we could get them deployed, you know, moving to the cloud, patching your endpoints, deploy multifactor authentication; where you have on-premises networks that for whatever reason, you can’t move to the cloud, or you can’t move yet, you know, applying zero trust principles to how you administer your on-premises network.

These tools are known, they’re well developed, they’re easily accessible. Will they take time and effort? Yes, of course, they will. But they would greatly improve the security of the ecosystem. If we could get 80, 90, 100% of the ecosystem to apply these – these tools and these practices, we would almost stop cybercrime in its tracks.

But instead, we see patch rates at 30%, we see the application of multifactor authentication at only in the high 20s, or low 30% across the ecosystem. We see many workloads that should be migrating to the cloud, where instead, private sector and public sector customers are choosing to engage in hand-to-hand combat. And maybe they think that they’re not going to be targets, but increasingly we see, you know, unfortunately, and this is a horrible thing, but we see again, and again, both on the public sector and private sector, we see those who thought they would never be targeted, become victims of ransomware attackers, or nation-state attackers who are trying to steal your intellectual property, or engage in espionage and learn what you and your government agency are doing.

So these are steps that need to be taken and can be taken today, and then Microsoft can really help you with, if you want to develop a strategy to get yourself into a more secure environment.

**ALVARO VITTA:** Those stories are great examples to follow, and the tips that you provided seem, you know, like common sense to me. So I think a lot of people would take away these great insights and implement them and they’ll be better off for it.

Thank you so much for joining us today and giving us these – these thoughts and this insight, and we look forward to hearing what Microsoft has next in terms of security, so that we can continue to protect the world against these cyberattacks.

**TOM BURT:** Thank you.

[Music]

OLIVIA: Thank you to our guest, Tom Burt, and of course to our guest host, Alvaro Vitta. And thank you to you for joining us today on Public Sector Future. We hope you’ve learned something new and been inspired to focus on the steps you can take to improve cybersecurity in your own organization. The Microsoft Digital Defense Report will be out later this fall, and you'll find the link to it on our website. You can get to our show page, and directly at wwps.microsoft.com

Please do reach out send us your questions and your feedback. You can find me on Twitter @LivNeal or on LinkedIn, or you can email us at ask-ps@microsoft.com. Thank you and see you next time.

END