**Public Sector Future WWPS Podcast**

**Detail: Cybersecurity mini-series podcast**

**Episode: TBD**

**Host: Alvaro Vitta (Microsoft)**

**Guest: Yeo Beng Huay (Gov Tech Singapore)**

**TRT: 21:35**

**Audio: Public Sector Future\_Cybersecurity\_EPTBD\_Yeo Beng Huay\_V2.mp3**

[TCR 00:00:00]

**OLIVIA NEAL:** 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. Today we’re bringing you the third in our set of cybersecurity episodes, with guest host Alvaro Vitta. For this episode, Alvaro is joined by Yeo Beng Huay from GovTech Singapore.

Singapore are frequently looked to as one of the governments leading the way in digital transformation. Beng Huay will be discussing the approach the Singapore Government have taken with moving to cloud and the ambitious targets which they’ve set. She’ll share she is using governance; agile approaches to policy making; and automation and digital tools, to manage cybersecurity and compliance on this journey. Over to you Alvaro.

**ALVARO VITTA:** Well, thank you for joining us,. And thank you for joining us to talk about government cybersecurity relations in the Asia public cloud. To begin with, can you tell us a little bit about your cybersecurity role in government and what you and your team do?

**YEO BENG HUAY:** Hi, I’m Beng Huay here from GovTech. It’s a pleasure to be here. Maybe let me first introduce what is GovTech to all of you. GovTech, what we call Government Technology Agency in Singapore is the lead implementing agency for digital government, and what we do is, we harness technology to make a difference to citizens and businesses.

So broadly, our work can be categorized into three areas: products, solutions, and cybersecurity and governance. Then for products, what we do is develop products for citizens, businesses, and the whole government.

And in terms of services, we manage technology for about 60% of the Singapore government agencies, and cybersecurity and governance. we are the sectoral lead for cybersecurity in Singapore government,

**ALVARO VITTA:** And for our international audience, and for context, what are these guidelines, what are these cybersecurity compliance and relation guidelines that you usually work with in GovTech?

**YEO BENG HUAY:** So in Singapore, we are working on the Smart Nation. in 2018, we developed our digital government blueprint as a statement of our ambitions in support Smart Nation. we advocate the Singapore government that is digital to the core. under the digital government blueprint, we set out our own KPI to say that at least 70% of the eligible government services to be on commercial cloud by 2023.

This is an ambitious goal. And with the acceleration of the cloud adoption, what it means to us from the governance group is to really make sure that there are proper clear security policies in place and tools to support the government agency in migrating their current solutions to cloud.

**ALVARO VITTA:** Can you tell us a little bit about why the acceleration moves to cloud and the cybersecurity element of it? So what is it in cloud that attracts the government?

**YEO BENG HUAY:** Well, I think in simple terms, it will be actually – allow us to deliver our services faster, in a more agile fashion. And in fact, COVID has actually reaffirmed our emphasis in this area. It allows us to deliver our digital services in a very – in a quick time, turnaround time, and during COVID where citizens and businesses are not able to contact us physically, and we are able to roll out digital services in a very short span of time.

That is really due to the benefit of cloud and having the necessary governance policy in place beforehand. So I’m happy to say that we had a head start.

**ALVARO VITTA:** one of the things that I liked that you said there was the governance element, which is, listen, before we move all of these quote-unquote appliances and digital clients from on-premise to the cloud, let’s ensure that we have the foundational elements, the governance elements

**YEO BENG HUAY:** I think that is important, because cloud was new to us, a few years ago. It is important to make sure that we have the foundation, we have the necessary tools and support to the agency while they strive towards moving their services to the cloud.

**ALVARO VITTA:** how did you manage, because usually what I see with global government organizations is that there’s opposing forces, right, as in digital transformation. So on the one hand, you have the champions that say, "Well, let’s go ahead and start putting all these workloads to cloud real quick," right? And on the other hand, there are folks like yourself that say, "Well, hold on, let’s slow down a little bit, let’s do things the right way. Let’s have the right governance, the right compliance elements, the right security elements, so that we don’t have a setback, because we didn’t do things the right way."

**YEO BENG HUAY:** Yeah, so we did it in a very agile fashion. So first, we put in place the cloud-first policy, to state what can go on cloud. We started with a smaller group. We say that for system classify as restricted and below, so it’s a smaller set that we allow to go on cloud, and we have a set of a policies that we developed for them. Along the way we fine-tuned it. In fact, we get feedback from the agencies to make sure that the cloud policies are feasible and easier to comply.

So the policy is evolving, as we go along, to make sure that it stays relevant, it is continued to be able to support the agency easily, and they are able to comply with, and more importantly, they are able to put in place controls.

**ALVARO VITTA:** I like where you have a baseline, and said, "Okay, here’s some quote-unquote compliance guiderails that you stay – you have to stay within, but let me get feedback so that I can then refine, continuously," and then I would assume that includes, you know, you have a process by which you monitor and you measure drifting, right, and that allows you to then go back and say, "Okay, we need to remediate this."

**YEO BENG HUAY:** Yeah, indeed. Actually, our policymaking is a quite extensive process. Before we’re able to roll out, we will have to seek consultation from the engineers, the business users, and CIO community, deliberate over there before we can get the approval and launch. But having said that, it doesn’t stop us from checking out to make sure that they are okay. Agencies are able to operationalize what we put in place.

So we do have a feedback channel. And we look at that and we have a process to say that "hey, look here, something is not quite here." Everybody is asking questions about this particular statement. We should fine tune it. look back and refine and improve along the way.

**ALVARO VITTA:** As you started that journey of going to cloud and continuing that journey, what would you say are the – the most common needs that government organizations and the agencies that you serve with GovTech have in terms of how do I address compliance in an automated way with limited resources that allows me to not only be compliant, but ensures that I’m continuously compliant, not just point in time?

**YEO BENG HUAY:** Yeah, spot on. So having a policy is not enough, actually. And we do training, as well, but with the increasing adoption of cloud, we are now looking towards automation to try to improve auto-tracking, as well as streamline the governance process.

So this included putting in place some auto-tracking, we call it CloudSCAPE, which stands for Cloud Security and Compliance Automation Platform Ecosystem, but what it does is that it monitors deployment on the government cloud to make sure that it actually complies with our policy.

It includes also the automated scans to monitor and send alerts where the system does not meet the security baseline, and also, it actually provides some remediation guides, to our guys to say how they can secure the cloud resources.

So this is rolled out, 1.0, and we are working towards refining it. More than that, just last year, we also implemented a digital governance platform, where we pull into the relevant datapoints, provide a dashboard to the agency, say their cybersecurity engineer, to have a dashboard view of their compliance status, including the asset tracking, as well as patch management progress.

So this allows them to take action earlier. And we are continuing to improve to provide more insightful dashboards for the various stakeholders so that they can know ahead, what are the potential risks and be able to take action earlier to remediate ~~some of~~ them? So automation is a way to go, moving forward.

**ALVARO VITTA:** And I like that you provide the agencies with their dashboard so that they can see for themselves, okay, here’s where you are, you’re 80% compliant, or you’re 90% compliant, and here’s the remediations you need to do, and let them – I would assume you have some kind of a timeline that says, "Hey, listen, you know, you have 30 days to remediate this before we need to take action." Is that how you do it? How do you enforce the process in a way that doesn’t disrupt their operations?

**YEO BENG HUAY:** Yeah, so yeah, right, so at the policy level, at the standards level we did set for critical vulnerabilities you have to remediate by a certain time when the patch is made available.

So the purpose of this is really to provide an environment, a platform where a lot of the various stakeholders, whether you’re our cyber engineer or you are the CIO, to allow them to have more awareness of their risk for the ICT system. And then they can do more to uplift their compliance level. Yeah, so patch management is one. We are looking into possibility – integrated risk management, where they can do their risk assessment for their systems to be embedded into the system as well.

So all these various datapoints will actually create a lot of useful insight for the stakeholders.

**ALVARO VITTA:** when you look at in contrast, right, a perspective of, you know, having this set of compliance frameworks and compliance relations you need to adhere to in an on-premise environment versus a cloud environment? What are some of the challenges that you’re able to mitigate in the cloud and say that you weren’t able to do in an on-prem environment?

**YEO BENG HUAY:** I would say that speed is definitely one of them. For example, if I have a government service where I look at seasonality of a transaction, for on-prem services with on-prem system, you will need to install with the hardware capacity to be able to manage the surge and load, whereas in cloud, it can be done pretty easily. You can actually do the autoscaling, and you can scale down when you don’t need it.

If you don’t need the services, you can even shut it down, from the cloud. So I think we – we do see the beauty of cloud versus on-prem.

**ALVARO VITTA:** I think you mentioned up to restricted, you have in cloud, but then higher than that, you have on premise, is that correct?

**YEO BENG HUAY:** Well, we started with restricted systems, and actually, after a few years, and – and as we progress on, we actually are now scaling up to another class of the systems to be onboarded to cloud, and we call it confidential cloud eligible

**ALVARO VITTA:** So it looks like you’re progressing towards moving more and more to higher levels of classification of systems into cloud.

**YEO BENG HUAY:** Yeah, so as I mentioned, we will go progressively, as we learn and as we improve our governance processes to get control, and that’s where we can move on to the next level.

**ALVARO VITTA:** I love that. That’s a good model to follow because you’re doing it with baby steps, right, and you’re saying, "Well, you know, once we have the governance in place, we would restrict – but let’s say, we want to learn, you know, the whole lifecycle, and as we get more and more comfortable, and we optimize the system more and more, the compliance framework in cloud, then it allows us to then onboard higher levels of classifications once we’ve gotten comfortable with this system.

**YEO BENG HUAY:** Yeah, right, and now we are putting in place automation to enable them to do auto-tracking, as well as the digital governance platform that I mentioned, to give them more awareness of their risks areas.

So actually there is a lot of training that we have to put in place to refocus. First, we need to make sure that our officers are well equipped with the necessary skills to govern the cloud, and you do a higher-level task. And for some of them, you can actually retrain to do other aspects of the work. So it is actually indeed a transformation, not just in terms of digital services.

**ALVARO VITTA:** Absolutely, yeah, what you’re talking about is modern service management where you are saying, "Well, listen, it’s one thing to transform the technology aspects, but the way our organization functions, the roles that they do, , it’s going to allow us to operate in a different way. So you’re modernizing not only the technology, but also the people, the functions, the processes and the organizational structure of these programs.

**YEO BENG HUAY:** So in terms of this, it’s not just roll out digital services, moving up to cloud. You have to make sure you have the setup processes. You have to make sure your people are ready to be able to handle them, support them well. So it comes together as a total package that we have to manage.

**ALVARO VITTA:** In your experience, what is some advice that you can give organizations in terms of maybe pitfalls to avoid when implementing a cloud cybersecurity compliance program?

**YEO BENG HUAY:** Well, one of the things that we need to do is really to make sure that there’s a clear policy in place. So I mentioned earlier that sometimes agencies may be rushed to do certain things, without – aware of what should not be done, and this is where we want to caution there, first making sure that the policies and processes are clear enough so the agency can comply. And the next, we go back to training, but being in cloud, more importantly is about the agility, and this is where we are looking at how we can do automation that (inaudible) code to help them, a template.

Another potential pitfall that we see is the cost containment, so when you can go cloud, and it can go scale, but it’s also important for the agency to know how to contain the cost to manage the services as (inaudible) in the cloud, so that they have visibility, they know how to optimize it as they move along.

**ALVARO VITTA:** I see a lot of government organizations globally leveraging public cloud to accelerate the cloud transformation journey, just like you are doing in Singapore, and – and they do this, of course, like you said, right, to provide faster and more modern services for their citizens. As we wrap up this episode, could you share with our audience practical actions that government organizations can do as they start their cybersecurity compliance journey in public cloud?

**YEO BENG HUAY:** I will just say that, first start with what you have, looking at your assets and what are the scope that you can roll out in managed scope,. We have a certain set of processes in place to guide the agency forward. Also have in place some automation to help to trigger certain exceptions that didn’t meet the baseline or certain with critical risks. This is so that you have a safe environment for the agency to do their startup.

As you progress, then you can refine the policies and do more complex cloud services, and you can move on to the next level. So I will say that the first step is to start small. Make sure you have the necessary compliance processes in place and automation to help trigger any risk area before you go into and do more on cloud.

**ALVARO VITTA:** That’s, that’s great. Thank you. So make sure you use a crawl, walk, run approach and take your time and you continuously learn as you go along before you take on bigger tasks.

**YEO BENG HUAY:** Yeah, right, you’re right.

**ALVARO VITTA:** That’s great advice. Well, thank you so much. There has been a lot of insight, a lot of information, a lot of experience that you’ve shared that will be very beneficial to our audiences, globally. We appreciate your time and you sharing the knowledge with us. Thank you so much

**YEO BENG HUAY:** Thank you. It’s my pleasure to be here. Thank you.

[Music]

**OLIVIA NEAL:** We hope you’ve learned something new from the ambitious targets, agile approach to policy making and using of digital tools to manage compliance which Beng Huay has shared. You can find more content on cybersecurity on our website, at wwps.microsoft.com. Please do reach out and send us your questions and your feedback. You can find me on Twitter @livneal, or on LinkedIn, and you can find Alvaro there too. Or you can email us at ask-ps@microsoft.com. Thank you and see you next time.

END