OPENING ADDRESS BY SMS DR JANIL PUTHUCHEARY
AT THE AiSP IOT SECURITY SHARING AT NTU
ON 3 NOV 2023

Building a Safer and more Secure Internet of Things (IoT) for Tomorrow

Mr Andre Shori, Vice-President, AiSP

Distinguished Guests

Ladies and Gentlemen

Introduction

1. Good morning. Thank you for inviting me to join you for the AiSP IoT Security Sharing today. Today's theme, "Empowering Tomorrow's IoT: Unveiling the Shield of Innovation and Igniting Lifelong Learning", is well-chosen. It captures two components that are key to developing a stronger ecosystem well-equipped to handle the emerging IoT security challenges of today and most importantly, tomorrow.

IoT security is important

2. In fact, today if you say Internet of Things, people pause and look at you because it has become a thing where you just talk about the acronym IoT, right? IoT has brought about unprecedented connectivity and greater convenience, a shift in business models, a shift in operating models, but also, it has become very ordinary. It's just how the world works. It's how you do research, how you do business, how you live your lives.

a. Whether it's smart TVs, wearable fitness trackers, voice-activated speakers, these don't surprise us anymore. They are just part of how we live a modern life and it has improved our lives. Our lives are not the same, they are better.

b. It's not just the personal level. This has changed how we do things in business. There are industrial uses of smart devices. Smart grids have enhanced operational efficiency, and many other things.

3. But the greater connectivity and convenience also come with much greater surface area and that means greater risks and threats.

a. Malicious actors can exploit to compromise our network and steal our data.

b. We are also seeing malicious actors infecting IoT devices to leverage its scale of the space to launch distributed denial-of-service (DDoS) attacks to disrupt operations and services.

4. To make matters worse, IoT devices are traditionally designed with lower costs and user convenience in mind. So [when] we think back, the devices were a target, and they are then being used to target other parts of our digital ecosystem. Individual device cost, scale, convenience have been the priorities of manufacturers. Security, which would likely increase costs, and in the history of these devices, is often an afterthought, because from the perspective of business, speed-to-market and profitability would likely be the key considerations.

5. With this context in mind, more definitely needs to be done to create a safer and more secure IoT for all.

Raising the security of IoT devices

6. We will need to tilt the balance towards having better security for IoT devices. How do we do this? One way is the Cyber Security Agency of Singapore (CSA)'s **Cybersecurity Labelling Scheme (CLS)** for IoT devices. It was launched in 2020, as part of efforts to improve IoT security, raise overall cyber hygiene levels and better secure Singapore's cyberspace. We continue to adapt it, drive it, [and] deepen its effects over time.

7. The CLS is more than just a simple sticker affixed on the packaging. There is a sticker, but it's not just about the sticker. The sticker is just one tiny part of the value proposition. What we want to promote is the development of safer and more secure IoT devices by shifting the behaviours and mindsets of end consumers and manufacturers.

a. The label on the product reminds consumers about IoT security, and hopefully influences them to consider their needs and buy a more secure product.

b. Manufacturers can also turn security into a competitive advantage. They can offer better security and security features to differentiate themselves from their competitors. This is especially since consumers can see this difference clearly on the box.

8. The scheme has found some success.

a. Since the launch of the scheme, CSA has received applications for more than 550 devices, and more than 350 devices have received a label to date.

b. We have also gained international traction. People around the world are paying attention to what we are doing here in Singapore. We have achieved mutual recognition with Germany and Finland. What does that mutual recognition mean? It's not again like a sticker on a piece of paper. Mutual recognition means that our processes are recognised by the counterparties in Germany and Finland. We recognise them, they recognise us. That means if they test a device and put their sticker on it, we will accept that testing process and certify that device as meeting our standards. Much more importantly for us, they recognise us, so our manufacturers based here now have the opportunity to use that labelling, that framework and the security that is assumed to be part of that as a means of accessing their markets. So this is very important. And I think that approach of mutual recognition, [with] more and more markets that take on this approach, we hope [we] can shift the view of manufacturers, retailers, vendors, consumers, and then over time, improve the security and safety of the IoT ecosystem.

c. What else are we doing? We are also working in specific industries because the cybersecurity labelling scheme, at its outset was generic. It was about Wi Fi routers and box exchanges, the generic

> foundations and platforms, but [for] IoT devices, some of them are deployed in very specific domains. CSA is also working with the Ministry of Health, Health Sciences Authority and Synapxe to extend the CLS to medical devices. This is so that consumers and healthcare providers could identify and select medical devices with better in-built cybersecurity. And you know, it's not something you think of practically as a practitioner. In medicine, it's not something that you have considered when you are thinking about the devices. And what we need is for people to then think, if there is data being shared out of this device, take into account cybersecurity in your decisions. And so we have to apply the cybersecurity labelling scheme, that mindset, to domain-specific devices.

9. We hope to build on this success and encourage more manufacturers to adopt cybersecurity measures in the design and development of their products. Two weeks ago, I announced that CSA will be developing with the industry a **Cybersecurity Implementation Toolkit** at the Singapore International Cyber Week. This will make things even easier for manufacturers to develop and build devices that are secure-by-design. We have to take this approach all the time to see what the industry players need and especially the small and medium players as they are innovating and developing new products. How can we help them to do cybersecurity by design?

Encouraging training and innovation

10. So that's a lot about the devices and the manufacturers. But the other thing that we need to do is training for innovation. We need this innovative cybersecurity ecosystem to then make sure that we have the confidence that we can address the needs of tomorrow, innovation and lifelong learning.

11. First, on innovation. We need to be innovative. It's the nature of the space that you are looking at - the threat actors, your adversaries, the people who are trying to counter, they are driven to innovation, like perhaps no other industry and when securing these spaces, we need to do the same.

a. In this regard, CSA's CyberCall is an important effort to encourage innovation within the cybersecurity ecosystem. It provides a platform for companies to innovate on challenges articulated by large, trusted end-users in Singapore, and we want to capitalise the development of cutting-edge cybersecurity solutions.

b. IoT is one of the areas that we are seeking proposals for this year's CyberCall. I encourage all of us in the community to participate.

12. Second, on lifelong learning. You can think about lifelong learning in two ways:

a. One, we need to support the upskilling of our existing cybersecurity practitioners, regardless how senior or how experienced they are. All of us, will need to ensure that we remain relevant. The threat landscape is evolving. We need to evolve just as fast and that means that lifelong learning for all across the personnel stack from the most junior to the most senior.

b. But the other thing that we need to do in parallel is support non-cyber professionals. We have a dearth of personnel, we need to attract more and there is a growth opportunity in this space. And how we are filling that is attracting people in adjacent industries and adjacent fields to learn about cybersecurity and join. This is quite key for us as the demand for cybersecurity professionals still outstrip supply greatly and likely that is going to be so for some time to come.

13. Minister Josephine announced two months ago that CSA will be investing $50 million in the Cybersecurity Talent, Innovation and Growth Plan. Under this plan, CSA will be expanding more opportunities for mid-career conversions, and help the cybersecurity workforce raise professional standards.

14. I am therefore pleased to hear that NTU is complementing these efforts and launching a new **Work-Study Degree Programme** for working adults looking for an upgrade to their qualification or to pivot into the Information and Digital Technology industry. This programme will focus on developing skills and competencies for industry application, and students will be able to undertake full-time on-the-job training within the programme.

Conclusion

15. Let me conclude by thanking everyone for making time to be part of this event. Cybersecurity is a team effort. Today is a great opportunity to

bring the community together to exchange ideas to see how we can do better to improve our IoT security. Doing this, as I have outlined in my speech, it requires our efforts at the device level, at the individual user level, at the manufacturer, at the consumer and within the profession, new entrants as well as experienced professionals. We all have a very important role to play in government, enterprise, academia and industry. The organisers have put together an exhibition and brought together a line-up of speakers from both the public and private sectors to share their perspectives and efforts towards the advancement of IoT security.

16. I wish all of you a fruitful day ahead. Thank you.

****