Opening Speech by Mr Heng Chee How Senior Minister of State for Defence at the Second Cybersecurity Awards and Gala Dinner

08 Nov 2019

SPEECH BY SENIOR MINISTER OF STATE FOR DEFENCE MR HENG CHEE HOW, FOR THE SECOND CYBERSECURITY AWARDS ON 8 NOV 2019, 08.00PM AT SAND EXPO & CONVENTION CENTRE

Chief Executive, Cyber Security Agency of Singapore, Mr David Koh

President of the Association of Information Security Professionals, Dr Steven Wong

Distinguished Guests

Ladies and Gentlemen

1. A very good evening. I am delighted to join you this evening at the second Cybersecurity Awards and Gala Dinner. I do thank you for this kind invitation. On behalf of Minister Iswaran, I convey best wish to you.

2. We have gathered here to celebrate the contributions and achievements of the cybersecurity community, and I offer my heartiest congratulations to all the award nominees.

3. I would like to also congratulate AiSP for successfully organising the Cybersecurity Awards with the support of the Cybersecurity Agency of Singapore (CSA) and nine other professional and industry associations. This event is testament to the strong partnership that exists within the cybersecurity ecosystem. It is also testament to the passion of the many volunteer leaders that are present this evening.

Challenge in Tackling Cyber Threats

4. With cyber threats increasing in scale and sophistication, it is important that we develop cybersecurity capabilities and professional competencies to protect our increasingly connected digital economy and society. Everyone has a role to play in strengthening our cybersecurity and resilience. To heighten this awareness, earlier this year the Ministry of Defence introduced Digital Defence as the Sixth Pillar to the Total Defence Framework. Government agencies such as the CSA, GovTech and MINDEF’s Defence Cyber Organisation have also been working towards strengthening our cybersecurity resilience.

5. The government cannot do it all alone. Committed industry partners, and a robust, motivated and capable cyber workforce are also key and critical in building a secure cyberspace.

6. Singapore is confronted with a shortage of cybersecurity professionals. This shortage is not unique to Singapore, though it is quite a serious one. According to the ISC2 Global Information Security Workforce Study 2018, there is an estimated shortage of 2.15 million cybersecurity professionals just in the Asia-Pacific region. Globally, the shortage is estimated to be around 3 million.

7. The demand for cybersecurity professionals to defend our cyberspace will remain high for years to come. Some cyber professional job roles that continue to be in-demand include threat and vulnerability assessments, security management, and incident and crisis management.

8. To address this shortage and meet tomorrow’s demand, we must make maximum efforts to continue to build a robust cybersecurity workforce in Singapore. We also need to recognise organisations and individuals who have made valuable contributions to the ecosystem. Allow me to elaborate.

Building a Robust Cyber Workforce to Meet Tomorrow’s Demand

9. Over the past few years, the government has rolled out specific initiatives in partnership with the industry to grow the size and competency of the cybersecurity workforce. The Cyber Security Associates and Technologists programme, or CSAT for short, is a good example. Launched in 2016, the CSAT programme is on track to equip more than 900 info-comm fresh graduates and mid-career professionals with relevant skills to take up cybersecurity job roles through a combination of training and industry attachments by 2021. So, we create a supply [of cybersecurity professionals].

10. In the Ministry of Defence (MINDEF), to strengthen the cyber defence capabilities, last year we launched the Cyber NSF scheme to allow full time national servicemen (NSF) with the requisite aptitude and skills to be deployed in cyber roles. Cyber NSFs with higher aptitude and skills are offered the opportunity to take up the Cyber Specialist Award. These Cyber Specialists will undergo a work-learn programme with Singapore Institute of Technology (SIT). The programme provides deep technical training, and prepares the Cyber Specialists for technically demanding cybersecurity jobs in the MINDEF ecosystem. Approximately about 80 to 90 Cyber NSFs will benefit from this scheme in subsequent years. With the training that they have received, these Cyber NSFs play their part in national defence, and after completing their national service, we hope that they can continue to contribute to Singapore’s cybersecurity as NSmen, or as Cybersecurity Professionals in the industry.

11. At a more general level, the government has also undertaken efforts to grow the size and quality of the cyber workforce. First, educating youths early on cybersecurity and outlining career prospects will help inspire them to join and to stay in the cyber workforce. In July this year, CSA introduced a Singapore Cyber Youth Programme to guide aspiring cybersecurity professionals in their career pursuit. The programme includes training bootcamps, learning journeys and career mentoring sessions, and it will reach out to some 10,000 secondary and tertiary school students over the next three years.

12. To complement the Singapore Cyber Youth Programme, I am pleased to announce that CSA will be organising a Singapore Cybersecurity Education Symposium in February next year, a first of its kind in the region. The symposium will equip teachers, academics from institute of higher learning (IHL) and career counsellors with a better understanding of the cybersecurity professions and its career prospects. With that, we hope that they will be better equipped to guide and inspire our youths to join the cybersecurity workforce.

13. Women make up half of our population but they only form a small part of the cybersecurity workforce. Therefore, encouraging more women to join the workforce is an important strategy to reduce the shortage of cyber talents.

14. In this regard, CSA is partnering with professional associations and non-profit organisations to drive the SG Cyber Women initiative to encourage girls to pursue tertiary education in cybersecurity, and inspire women to take on technical and non-technical cybersecurity roles.

15. Since January, our local partners have reached out to at least 3,000 women and girls through career talks, mentoring sessions and competitions. For instance, at the sidelines of the fourth Singapore International Cyber Week last month, CSA and the High Commission of Canada, supported by the Australian and British High Commissions, co-organised a Women-in-Cyber event. It was a great success, and saw the participation of more than 160 foreign delegates, professionals and students.

16. Through these efforts, we hope to inspire more women to take on leadership roles in cybersecurity and follow in the footsteps of excellent examples, such as Dr Ong Chen Hui. Dr Ong, Senior Director of Emerging Technologies in Trustwave, a cybersecurity company, attended cyber courses and earned accreditations as a GIAC Certified Forensic Analyst and GIAC Reverse Engineering Malware (GREM) technologist to complement her career.

17. To guide more women to succeed like Dr Ong, I am pleased to share with you that AiSP will be launching the Ladies in Cyber Mentorship Programme later this month. The programme will see at least 35 girls from tertiary institutions individually matched with industry mentors to advise them on cybersecurity career opportunities. It is heartening to see industry partners voluntarily stepping forward to drive such women-targeted initiatives.

18. Besides expanding the size and skills of the workforce, it is also important to ensure that the knowledge of the workforce is up-to-date and relevant. To this end, I am glad that AiSP has taken the initiative to update the Cybersecurity Common Body of Knowledge or BOK for short.

19. Over the last two years, AiSP members with the support of volunteers from the industry have invested significant time and effort to update the BOK to the current version 2.0. Emerging technological development such as Cloud Security, Internet of Things (IoT) and Industrial Control Systems (ICS) are now included in the BOK. The revised BOK is being validated with the industry and academia. Such voluntary community efforts exemplify the passion of our cybersecurity practitioners and bode well for the development of the cybersecurity profession. It also complements CSA’s national initiatives like Singapore’s Operational Technology (OT) masterplan that was announced by Senior Minister Teo Chee Hean at this year’s Singapore International Cyber Week.

Recognising the Valuable Contributions of Organisations and Individuals

20. In building a robust cyber workforce, it is equally important to give due recognition to organisations and individuals who have made valuable contributions to the cybersecurity ecosystem.

21. RSA is an example of such an organisation. Together with Ensign and Republic Polytechnic, RSA has set up a cyber-threat intelligence centre to enable Republic Polytechnic students from the infocomm security management faculty to manage realistic cyber threat scenarios. RSA provides technical support and experts for these trainings. Similarly, RSA works with other higher learning institutions to train and nurture cybersecurity talents. It also frequently conducts outreach programmes in the region to raise cybersecurity awareness among the public. These multifaceted efforts by RSA are indeed commendable.

22. To boost the recognition of such organisations as well as individuals, the inaugural Cybersecurity Awards and Gala Dinner was initiated last year and it was a great success.

23. To recognise cybersecurity end user organisations for their investment in internal processes, people and technology for cybersecurity as well as their broader contributions to Singapore’s cybersecurity ecosystem, this year we have introduced a local award category for end user organisations.

24. We have also introduced a regional award category to honour organisations that have contributed to the region’s cybersecurity development. This includes impactful contributions towards professional skills development, the promotion and adoption of best cybersecurity practices and knowledge, and growing the cybersecurity talent pool.

Conclusion

25. In closing, we can agree that it is critical that we continue investing efforts in building a robust and motivated cyber workforce for a secure cyberspace. The cybersecurity awards are an important way to recognise organisations and individuals who have done well, and to encourage our community stakeholders to continue contributing to the ecosystem.

26. Once again, I want to congratulate all award nominees. Thank you for your valuable contributions to Singapore and the region’s cybersecurity landscape.

27. I wish you a pleasant evening. Thank you.