

SPEECH BY MR. K SHANMUGAM, MINISTER FOR LAW AND 2ND MINISTER FOR HOME AFFAIRS, AT THE 18TH GOVERNMENTWARE SEMINAR AT THE SUNTEC SINGAPORE INTERNATIONAL CONVENTION AND EXHIBITION CENTRE, 30th SEPTEMBER 2009, 0900AM

**Distinguished Guests,
Ladies and Gentlemen,**

Good morning.

Cooperating for Infocomm Security

1 In recent years, this event has brought together both the public and private sectors to discuss developments in infocomm security. The aim is to foster a good partnership.

2 This has become very important. IT systems are now ubiquitous in our networked world. There are more concerns about the reliability and security of our digital assets.

3 We will therefore need even greater cooperation between the public and private sectors. We need to continuously come up with better solutions to secure our infocomm infrastructures.

4 This year, there is again good participation from the private sector despite the difficult economic conditions. It is important that during difficult times, we be even more vigilant about IT security.

5 The 2008 McAfee Virtual Criminology Report stated that “the recession is proving a hotbed for fraudulent activity as cybercriminals capitalise on a climate of consumer fear and anxiety”.

SITSA

6 We take this message seriously. To achieve better IT security, we have decided to form the Singapore Infocomm Technology Security Authority (or SITSA). It will be the national specialist authority for operational IT security.

7 IT security has become a national security issue affecting numerous sectors.

8 The volatile IT landscape of today also demands that Singapore adopt a more proactive strategy that places emphasis on anticipating and neutralising emerging threats.

9 SITSA’s mission will therefore be to better secure key national interests in the realm of IT security. It will be the specialist authority to deal with threats to national security, especially external threats such as cyber-terrorism and cyber-espionage. SITSA will focus in the near term on capacity-building and engaging regulators and industry players in Singapore.

10 SITSA will also lead efforts in developing the operational capacities and technical expertise to deal with the challenges associated with the IT security threat landscape.

11 SITSA will be a unit within the Ministry of Home Affairs (MHA). It will be under the Internal Security Department (ISD). The ISD has been playing a key role in the protective

security of Government's IT systems.

12 SITSA is being formed at a time when the world has witnessed the Estonian cyberwar in 2007 and the Georgian cyberwar in 2008. In July this year, we witnessed yet another widespread cyber attack. This time, it was targeted against government and banking websites in South Korea and the United States. In this attack, personal computers, infected with a virus, were used in a distributed denial of service (DDOS) attack against the websites.

13 Such targeted DDOS attacks are gaining popularity. They:-

- a. do not have to be performed via sophisticated or costly means,
- b. are practically untraceable, and
- c. present little risk to the remote attacker, but yet can be used to inflict huge impact damages to critical IT infrastructure, such as e-banking websites.

14 In order to achieve its goals, SITSA is currently embarking on two initiatives. Under the National Infocomm Security Governance Framework, and in line with the strategic thrust of the second Infocomm Security Masterplan, the first initiative aims to harden national infocomm infrastructure and services. Of particular importance is the protection of our critical IT infrastructure within key sectors such as energy, transport, water, banking and finance, among others.

15 SITSA's second immediate initiative will be to work towards achieving a higher level of national preparedness against cyber attacks. It will develop a framework to provide a comprehensive incident reporting, response and escalation process to handle national level emergencies resulting from large-scale cyber attacks.

16 It will also conduct, from next year, on a regular basis, cyber security exercises aimed at enhancing Singapore's responsiveness to large-scale cyber attacks at the national level. Through the exercises, gaps can be identified and our capability and readiness to respond and recover from such attacks can be improved.

17 Today, much of the nation's critical computer systems and infrastructure are designed, developed and operated by the private sector. In times of crisis, it is almost inevitable that help from private sector professionals would need to be sought. SITSA will engage and involve the private sector through regular cyber security briefings, discussions and seminars, and exercises. Through these engagements, there will be more sharing and cooperation between the public and private sectors IT security personnel, which will in turn sharpen our cyber defensive capabilities.

18 This is in line with the theme of this year's Governmentware conference - Beyond Uncertainty, Collaborating for Security.

IT Security Challenges in the Digital Society

19 It could be asked: why is there the need for the public and private sectors to collaborate and cooperate? There are several answers. There is already evidence of higher levels of cooperation between cyber criminals. According to the 2009 Midyear Security Report by Cisco Systems, there was collaboration between the creators of Conficker and Waledac, where the Conficker botnet[1] was used to deliver the Waledac malware to the compromised victims.

20 Such cooperation amongst cyber criminals will create more uncertainties and difficulties for cyber defenders. The same report also stated that security experts expect more such joint ventures between malware writers to take place in the coming months.

21 The security community came together to respond to the Conficker threat earlier this year, in April. This was a good example of cooperation between the public and private sectors to address such asymmetric threats.

22 Securing our digital assets will also become increasingly challenging due to the novel IT technologies that have emerged in recent years. For example, cloud computing is a technology that is rapidly gaining popularity. However, with cloud computing, confidential business information is processed and stored within the cloud, and this opens up additional avenues for cybercriminals to steal sensitive information. According to a recent study from Deloitte & Touche and the Ponemon Institute, 45 percent of surveyed security professionals had purchased cloud computing services for their companies. But they had not established plans for managing the security risks associated with it. Unprepared adopters of cloud technologies potentially face a lot of threats.

23 It is essential that we pay attention to potential “show-stoppers” when adopting technologies. It may not be possible to prevent the ‘unknown-unknown’, that is, the emergence of new attacks. However, we can be vigilant and prepared, and more importantly, work together as a team, to be able to respond more effectively to such attacks and mitigate the impact.

Conclusion

24 I hope that this seminar will provide a spark for us to re-think security in a holistic, cooperative way. In this regard, I thank all speakers and exhibitors who have responded to our call to share their experiences and knowledge.

25 On this note, I am pleased to declare the 18th Governmentware seminar open. I wish all of you an enriching and stimulating seminar.

26 Thank you.

[1] Botnet is a jargon term for a collection of software “robots”, or bots, that run autonomously and automatically to carry out certain activities. The term is often associated with malicious software.