



All delegates will be required to present their Position Summary on the first day of the Conference. It will enable each delegate to share with the rest of the Committee your assigned country's stand on the issue.

Please use the below template to complete the Position Summary and submit to us by 4 September 2015. The summary should be about 500 words.

## Position Summary

**Issue:** How can ASEAN states work together to better combat cybercrime in the region?

**Country Assigned:** Singapore

### 1. What is the current status of the 'Issue' in your country?

The sophistication of Information Communication Technologies (ICTs) in the last three decades has changed the way we live and work. Increasingly, governments and privately owned companies have turned to technologies like laptops and notepads which are purchased and used by employees in their day-to-day roles and responsibilities. Organisations communicate with one another via electronic mails, and the number of Internet users across the world have increased tenfold from 1999 to 2013. To give an even greater contrast: back in 1995, only 1% of the world's population was connected to the Internet; in 2014, this has risen to 40%. Unfortunately, the rise of the Internet has also given birth to what is known as cybercrime.

Singapore is one country that is very well connected to the Internet and the Cloud. By Dec 2008, Singapore's household broadband penetration rate was 99.9%. This indicates that Singaporeans are very reliant on the Internet, both for work and for play. More and more activities – whether professional or recreational – are being done online, and this has a profound impact on how Singapore functions as a nation. A public servant will have difficulties performing his job without access to his work email account. An online merchant may potentially lose thousands of dollars a day if the Internet server she uses is down for a few hours. The situation is made worse by fraudulent sellers and buyers online, as well as hackers who work to compromise the security of any organisation that they are targeting to discredit.

In the second half of 2013, there was a series of cyber-attacks on some government and government-linked websites. At the start of November 2013, the Singapore Press Holdings' main English newspaper *The Straits Times* online web-blog was hacked. On 20 November, the websites of 13 Singapore schools were also reportedly defaced between 3:30pm to 5pm.

These attacks have been linked to the organisation Anonymous, an online hacktivist that launched a cyber-war on the Singapore government. Singapore responded robustly and had the situation under control after performing some investigations and a thorough re-evaluation of the country's firewall capabilities and other security system flaws that may compromise Internet security.

2. What is your country's stand on this 'Issue'?

The fact that almost every household in Singapore has an Internet connection makes the country vulnerable to cybercrime. Even though some people may not think much about it, the dangers of cybercrime are very real, and this is something which Singapore takes very seriously in our campaign against hackers and other online criminals. There is a need to make people more aware of cybercrime and its repercussions to the civil service, private organisations and also the citizens in the island state.

Singapore hopes that a concerted effort in fighting cybercrime will deter cybercriminals from attempting to do what the hacktivist Anonymous has done. Because of the close ties between Singapore and the rest of the ASEAN member states, a breach in security for Singapore may also result in repercussions that would implicate more than just one country. The peace and security that we current enjoy in the region is not something to be taken for granted. Instead, it is something which we should fight hard to uphold and preserve.

3. State 2-3 solutions which your country will take to solve the 'Issue' in your country. (More solutions are also welcomed).

- 1) Singapore will step up on cybersecurity management in the country. Governmental agencies will work alongside private sectors to ensure that the cybersecurity networks of different organisations are up to date and can withstand possible attacks from hackers. Regular cybersecurity exercises will be conducted to test the system from inside, ensuring that measures put in place to counter such criminal activities are sound and impenetrable. Singapore will also engage more cybersecurity experts to help design a whole-of-country security network in the next 5 years which can stand up against attacks of all permutations.
- 2) The Singapore government will put emphasis on educating citizens, from public servants to private sector employees to retirees and young people, the importance of ensuring security in their work and recreational activities online. Talks, surveys, and workshops will be conducted to share strategies to counter cyberattacks, and personal awareness of cybersecurity will be promoted throughout the island state through a three-prong approach: via education, mass media, and workplace enrichment. Singaporean from all walks of life will be engaged in learning and understanding cybercrime in order to better deal with it when the time calls for it.
- 3) Singapore will strive to attain greater bilateral collaborations with our regional partners when it comes to cybercrime. Access to vital information concerning a breach of online security regarding government and other private organisations, as well as sharing of best practices when it comes to online security may help Singapore and the region to enjoy greater cybersecurity in the future.