CYBER DSA 2023
15-17 AUG 2023 | KUALA LUMPUR CONVENTION CENTRE

IG TAN SRI ACRYL SANI BIN HJ. ABDULLAH SANI
INSPECTOR - GENERAL OF POLICE, MALAYSIA

I am honoured and delighted to be part of this very timely event that addresses a critical issue we have long been facing; cyber security. Cyber security threat is very real and has rapidly become a widespread challenge faced by all countries. Ransomware has become the most popular type of malware that attacks computer security systems to get confidential information from companies, governments, and even individuals.

Ransomware attacks have been making headlines worldwide, and it is also on the rise in Southeast Asia as a form of digital hostage-taking.

In March 2022, an Asia-based personal computer manufacturer was attacked by ransomware with a ransom set over $50 million. Recently in the US, a software firm took more than a week to restore its servers after being hit by ransomware which crippled hundreds of companies worldwide. Such an unprecedented attack affected about 1,500 businesses and demanded a ransom of US$70 million.

When big-scale cyber-attacks are committed, it poses a threat to national security and the country's economy. Not only valuable information is compromised but countries also stand to lose billions. It has been reported that global losses from cybercrimes are now over USD $1 trillion and rising continuously.

Cybercrimes are often unpredictable and can strike at any time, therefore it is important for all to be vigilant and to get the best protection available.

In a recent report, 70 % of commercial crime cases in Malaysia now can be categorised as cybercrime cases. A total of 71,833 commercial crime cases were reported involving losses amounting to RM5.2 billion from 2020 to May this year. Of the total of cybercrime cases, some 48,850 cases, or 68%, involved online fraud.

Online fraud and threats can undermine any efforts to promote economic development and stability.

As with other online criminal networks, the threat of cyber terrorism cannot be taken lightly whether in the form of direct attacks against Critical National ICT Infrastructures, the spread of political or militant propaganda and even recruitment of potential members.

RMP has over the years monitored closely online development, particularly in relation to the spread of online propaganda. To date, various numbers of such websites that are suspected have been taken offline or blocked with the cooperation of the Malaysian Communication Multimedia Commission.

Therefore, it is critical to implement policies and regulatory framework in combating such activities.

The Malaysian Government recently announced the adaptation of the Internet of Things (IoT) and the implementation of Industry4WRD: National Policy on Industry 4.0. From a law enforcement perspective, we should be prepared for the road ahead to serve and protect the people of Malaysia.

CYBER DSA 2023
15-17 AUG 2023 | KUALA LUMPUR CONVENTION CENTRE

On that note, I would like to congratulate the organisers of Cyber DSA and I wish all participants an encouraging session over the three-day program. The outcome of this programme would enable us to further strengthen the foundation of Malaysia's cyber security landscape.

Thank You.