

**APT Symposium on Cybersecurity 2019**

8-10 October 2019, Kuala Lumpur, Malaysia

**CONCEPT NOTE**

1. **Background/Context**

The widespread use of ICT brings with it a rise in cybersecurity concern. The cybersecurity has a tremendous impact on our lives as various services including utilities rely on information infrastructure that could be target of attacks, let alone huge amount of data that needs to be protected.

Traditional approaches to secure cyberspace are not always successful while providing cybersecurity has become elusive. The cyber-attack develops rapidly and head-to-head in various forms with security measures. Without confidence, users may hesitate to enjoy ICT services fully and accordingly, cybersecurity is at the heart of digital economy. It is also a cross-border issue which requires collaborative efforts and engagement from all stakeholders in every level.

Recognizing the importance of cybersecurity, the APT has embraced the issue as one of the strategic pillars in the Strategic Plan of the APT for 2018-2020 under Strategic Pillar **C – Trust: Promoting security and resilience through ICT**.

Last year, the APT Symposium on Cybersecurity 2018 was held in Seoul, Republic of Korea, with the active participation from APT Members, Affiliate Members, International Organizations, and other organizations. The participants supported to organise the symposium in the following year with new emerging topics related to cybersecurity. The 42nd Session of the Management Committee of the APT (MC-42) held in Mongolia in October 2018 also approved to hold the APT Symposium on Cybersecurity 2019.

In addition, the **Singapore Statement of the Asia-Pacific ICT Ministers on Co-Creating a Connected Digital Future in the Asia-Pacific** adopted by the Ministers from Asia-Pacific on 26 June 2019 in Singapore, has reflected the importance of developing a safe and trusted telecommunication/ICT enabling environment in Strategic Goal **D - Digital Trust**. Key aspects under such Strategic Goal include: Data Privacy and, Free and Secure Flow of Information; Cybersecurity; and Online Safety and Well-being.

The APT Symposium on Cybersecurity 2019 is therefore designed to be result-oriented and capture relevant topics in line with both the Strategic Plan for 2018 - 2020 and the Singapore Statement. The Symposium aims to provide a platform to discuss issues around concerning cybersecurity and approaches to address them. It also features cybersecurity initiatives from private and public sector including policy and regulatory aspects, recent development in cyberthreats and available cybersecurity tools, measures against identity theft to secure digital identity, critical information infrastructure protection, challenges in managing cybersecurity when building smart cities, data privacy and free and secure flow of information, blockchain and its role in cybersecurity, and some of the best practice or guidelines for the safe use of network.

The Symposium on Cybersecurity 2019 will also include a panel discussion to encourage and identify avenue for national and international collaboration. The participants will have the opportunity to learn from each other, exchange views and ideas, and more importantly, collaborate at all possible aspects in order to achieve secured cyberspace in Asia-Pacific region.

1. **Objectives**

The objective of the APT Symposium on Cybersecurity 2019 is to bring APT members to a common platform for a dialogue on cybersecurity issues and to provide them an opportunity to share and address key issues of concern, as well as to facilitate intra-regional collaboration as required. Industry leaders and other key stakeholders also share their views on various cybersecurity issues facing the sector.

The specific objectives are to:

* Assist members to collaborate to build and strengthen trust and confidence in the use of ICT;
* Provide a platform to exchange information on implementation of polices/regulations in cybersecurity measures, including best practice or guidelines. To share experiences and lessons learned in the field of cybersecurity;
* Share information on the cybersecurity threat landscapes in the digital economy environment and suggest plausible solutions;
* Discuss and share knowledge and experience in secure entity of digital identity and protect from identity theft;
* Raise awareness and exchange knowledge in critical information infrastructure protection
* Discuss and share knowledge and experience in managing cybersecurity in smart cities and use of blockchain technologies in cybersecurity.
* Address data privacy issues while keeping free and secure flow of information including cross-border;
* Encourage initiatives through international collaboration towards the secured cyberspace in Asia-Pacific

1. **Expected outcomes**

The APT Symposium on Cybersecurity 2019 covers relevant and up-to-date themes in the field of cybersecurity addressing the key regulatory and policy issues relating to cybersecurity and data protection. As an output-oriented symposium, it urges policy makers, regulators, and industry representatives of the ICT sector in the region to generate new ideas and collaborate to transform them into practical implementation and initiatives. The tentative programme is annexed to the Concept Note as **Attachment 1**.

Specific outcomes include:

* Collaboration to build and strengthen trust and confidence in the use of ICT;
* Exchange of information on implementation of polices/regulations in cybersecurity measures, including best practice, guidelines, and lessons learned;
* Exchange of information on cybersecurity issues including threat landscapes and solutions, digital identity and identity theft, critical information infrastructure protection, cybersecurity in smart cities, and the use of blockchain in cybersecurity;
* Data privacy issues and free and secure flow of information including cross-border are discussed and addressed;
* Initiatives through international collaboration towards the secured cyberspace in Asia-Pacific

1. **Timing and location**

APT Symposium on Cybersecurity 2019 will be hosted by Ministry of Communications and Multimedia Malaysia (KKMM) and Malaysian Communications and Multimedia Commission (MCMC), from 8 to 10 October 2019 in Malaysia.

1. **Participation**

All APT Members, Associate Members, Affiliate Members, and International/Regional Organizations can participate in the symposium.

1. **Contact persons:**

|  |  |
| --- | --- |
| **APT Secretariat** | **Local Secretariat** |
| **APT Secretariat:**  Asia-Pacific Telecommunity  12/49 Soi 5, Chaeng Watthana Road  Bangkok 10210, Thailand  Tel: + 66 2 573 0044  Fax: +66 2 573 7479  Ms. Elisha Rajbhandari  Assistant Project Coordinator  Email: [apt-sc@apt.int](mailto:apt-sc@apt.int) | **Nur Risyah Musa (Ms.)**  Communications Technology Division  Ministry of Communications and Multimedia Malaysia (KKMM)  Tel: +603 8911 7521  Fax: +603 8911 5642  Mobile: +601 2359 5865  Email: [risyah@kkmm.gov.my](mailto:risyah@kkmm.gov.my)  **Syahniza Md. Shah (Ms.)**  International Affairs Department  Malaysian Communications & Multimedia Commission  Tel: +603 8688 8492  Fax: +603 8688 1000  Mobile: +601 9325 8801  Email: [syahniza.mdshah@cmc.gov.my](mailto:syahniza.mdshah@cmc.gov.my) |

**Attachment 1**

**APT Symposium on Cybersecurity 2019** **(APT-SC 2019)**

**Tentative Programme**

|  |  |
| --- | --- |
| **Time** | **Tuesday, 8 October 2019** |
| 08:30 – 09:30 | Registration |
| 09:30 – 10:00 | **Opening**   * Welcome Address – Ms. Areewan Haorangsi, Secretary General, APT * Inaugural Address – Malaysia *(tbc)* * Presentation of Token of Appreciation   (Group Photograph) |
| 10:00 – 10:30 | Coffee/Tea Break |
| 10:30 – 11:15 | **Session 1 –*Introduction***  *The session sets the scene for the Symposium by providing information on APT activities relevant to Cybersecurity.*   * Outcomes of the 42nd Session of the Management Committee of APT * Outcomes of the Asia-Pacific ICT Ministerial Meeting 2019; * Implementation Status of Strategic Plan of the APT for 2018-2020; * Outcomes of APT Activities on Cybersecurity.   Q&A |
| 11:15 – 12:20 | **Session 2 - *Initiatives on Cybersecurity from Public and Private Sector***  *This session invites high-level policy makers and regulators as well as industry representative to shares information on initiatives from APT Member Administrations in the area of policy and regulation particularly cyber legislation. It also features initiatives from private sector to ensure secure, trusted and resilient ICT networks and services.*  ***Session Chairman:***  ***Topics:***   * New cyber legislation including policies and regulations in the field of Cybersecurity. * Initiatives from Member Administrations and Private Sector   ***Speakers:***   * Member Administrations; * Affiliate Members   Open Discussion and Q&A |
| 12:20 – 14:00 | Lunch Break |
| 14:00 – 15:30 | **Session 3 – *Recent development in cyber threats and measures***  *This session focuses on emerging threats in Cyberspace. These include new threats on the network and cyber-attacks on IoT, Social Network, and Cloud.*  *IOT makes up of huge number of edge devices. More often than not, these devices are not rigorous in their design. This makes IoT vulnerable to hackers as they can easily gain access from the weakness of these devices.*  *As Social Network becomes popular, so is the social network hacking. Social Network is an easy source for hacker to collect all user information shared on social media. Social Network Hacking can require little technical skill. This can involve both technical and psychological technique to win trust over users in order to steal key information that could lead to security breaches. How do we raise awareness of user on the secure use of social network?*  *Data are asset. Multitude of data stored in the cloud are undoubtedly attractive to hackers. What are the tools used to protect data from hackers? What should service provider and CERT do to protect user data against these attacks?*  *The session also aims to report on internet security landscape including profiles and statistics on cyber-attacks and risks in the region.*  ***Session Chairman: (TBD)***  ***Topics:***   * Emerging threats in Cyberspace: IoT, Social Network, and Cloud * Internet Security Report, Profiles, and Statistics * Approaches from CERT in cybersecurity * Tools used for cybersecurity and their applications   ***Speakers:***   * Member Administrations; * Affiliate Members   Open Discussion and Q&A |
| 15:30– 15:45 | Coffee/Tea Break |
| 15:45 – 17:00 | **Session 4 *– Digital Identity and measures against Identity Theft***    *Digital identity is one of key drivers for Digital Economy as it helps identify socio-economic transaction of individual such as in financial or public services. Digital Identity is not limited to person level, but also to device level. The rise of Digital Identity has brought along the problem of Identity Theft. This session discusses digital identity and identity theft. What damage can the identity theft do to our economy? What are the measures against it? What do we learn from countries which already introduced digital identity?*  ***Session Chairman: (TBD)***  ***Topics:***   * Digital Identity and its security   ***Speakers:***   * Member Administrations; * Affiliate Members   Open Discussion and Q&A |
| **Time** | **Wednesday, 9 October 2019** |
| 09:00 – 10:30 | **Session 5 –*Critical Information Infrastructure Protection***  *Critical Information Infrastructures of modern services sit on networks. Example are information and telecommunication networks, network of banks and financial institutions, transportation networks, smart grids and power plants, government network and data centre, Cloud services, etc. Attacking critical infrastructure can pose serious threats to national security. This session provides the insights into critical infrastructure and its protection. What are the weak points or channels to launch the attack and how to prevent it? How do we proactively protect our critical infrastructure? How to make our infrastructure resilience to the attack?*    ***Session Chairman:******(TBD)***  ***Topics:***   * Examples of threats in Critical Information Infrastructure * Critical Information Infrastructure Protection and Countermeasures against threats * Resiliency in Critical Information Infrastructure   ***Speakers:***   * Member Administrations; * Affiliate Members; * International Civil Aviation Organization (ICAO) *(tbc)*   Open Discussion and Q&A |
| 10:30 – 10:45 | Coffee / Tea Break |
| 10:45 – 12:15 | **Session 6 – *Cybersecurity in Smart Cities***  *In Smart Cities, data and information from network are collected, analysed and converted to convenient services to improve quality of lives of their citizens. However, as we rely on more on network and information for services, more vulnerability and threats can also be expected. This session touches on smart city and its cybersecurity aspect. Will smart cities be an easy target for cyber-attack? How do we ensure safe and secure environment in smart cities? What are the lessons learned and precautions to be taken when building up smart cities?*  ***Session Chairman****:* ***(TBD)***  ***Topics:***   * Security threats and challenges in Smart Cities; * Experiences in managing cybersecurity in Smart Cities;   ***Speakers:***   * Member Administrations; * Affiliate Members   Open Discussion and Q&A |
| 12:15 – 14:00 | Lunch Break |
| 14:00 – 15:30 | **Session 7 – *Data Privacy and Free and Secure Flow of Information***  *Data Analytics and free flow of information have been used to improve personalized user experience in many services which optimizes benefit for users. However, some privacy concern has been raised. What level of data exploitation is considered appropriate and comfortable for users? How shall we strike balance between free and secure flow of information and level of privacy? What will be the ideal free and secure flow of information? This session discusses the issues around the free and secure flow of Information while protecting data privacy.*  ***Session Chairman****:* ***(TBD)***  ***Topics:***   * Data Privacy Framework and Policy and Regulation in free and secure flow of information: National and Regional Perspective * Initiatives for secure cross-border flow of information: Cases from Multinational Platform/Service Provider, International Organization, Government * Defining the right data privacy level / Balancing data privacy with free flow of information for optimal services: User vs Service Provider Perspective   ***Speakers:***   * Member Administrations; * Affiliate Members * Multinational Platform/Service Provider * International Organization * Consumer association   Open Discussion and Q&A |
| 15:30 – 15:45 | Coffee / Tea Break |
| 15:45 – 17:15 | **Session 8 – *Blockchain and Cybersecurity***  *Blockchain is a viable technology to strengthen cybersecurity and make the network less vulnerable. Decentralized in its nature, Blockchain-based solution is suitable to be applied for distributed storage service such as Cloud or even DNS for which hackers cannot access data from single point of entry. Neither can they access entire data in one instance. Blockchain can also find its use in IoT security where it can make IoT devices smart by making security decision through consensus within the network and exclude suspicious node without central control. Lately, there is also application of blockchain to secure cross-platform communications among different messenger services.*  *Apart from advantages offered by blockchain such as decentralization, tracking and tracing, fraud security, there are some disadvantages to be considered such as high cost, irreversibility and adaptability issue, etc.*  *This session looks into use cases of blockchain in strengthening Cybersecurity, and pros and cons that need to be factored when implementing blockchain.*  ***Session Chairman****:* ***(TBD)***  ***Topics:***   * Use cases of Blockchain in Cybersecurity * Pros and Cons of Cybersecurity through Blockchain   ***Speakers:***   * Member Administrations; * Affiliate Members   Open Discussion and Q&A |
| **Time** | **Thursday, 10 October 2019** |
| 9:00 – 10:30 | **Session 9 – *Best Practice/ Guidelines/ Raising Awareness on Cybersecurity***  *Human error is the leading cause of data and security breaches. Unintended human error can cause mishaps and has repercussion to organization and often even cause issues on a larger scale. Education and awareness raising on best practice or guideline for Cybersecurity is an effective approach as it stops the problem since the inception. This session focuses on best practices/guidelines/awareness raising activities on national or even organization level that can be shared among members*  ***Session Chairman****:* ***(TBD)***  ***Topics:***   * Best Practice / Guidelines in Cybersecurity from Member Administration * Success Story and Lessons Learned in Cybersecurity Best Practice and Awareness Raising   ***Speaker:***   * Member Administrations; * Affiliate Members   Open Discussion and Q&A |
| 10:15 – 10:45 | Coffee/Tea Break |
| 10:45 – 11:45 | **Session 10 *– Panel discussion on National and International Collaborative Effort Towards Cybersecurity***  *The panel discussion session invites stakeholders representing international communities or organizations to discuss how to leverage the synergy in cooperation and collaboration in addressing cybersecurity threats.*  ***Moderator****:* ***(TBD)***  ***Panel:***   * International Organizations * Member Administrations * APT Secretariat   Open Discussion and Q&A |
| 11:45-12:15 | **Session 11 *–Wrap-up and Closing***  *This session will conclude the Symposium with a brief summary of the sessions and discuss issues on way forward.*   * Way Forward * Any other matters   **Closing** |
| 12:15 – 13:30 | Lunch Break |
| 14:00 – 16:30 | ***Site Visit***  *MyCERT and Telecom Malaysia* |