Welcome speech at ABS-MAS Technology Risk Conference on 17 November 2016

1. Introduction

- Good morning Mr Aubeck Kam, Permanent Secretary, Ministry of Communications and Information, distinguished guests, ladies and gentlemen.
- A very warm welcome to Singapore, and to the 4th Technology Risk Conference, jointly organized by ABS and MAS.
- This year, the Conference is organised as part of the inaugural Singapore FinTech Festival week. For good reason, as the topics are closely linked. I encourage you to participate in the activities this week, if you have not already done so.
- Back to our gathering, it's a forum for industry players to share expertise and best practices on technology risk management and countering cyber threats to the financial sector.
- The work that you do is all the more timely and critical in this day and age.
- And the large audience here shows the keen interest in this serious topic. It's a topic which continues to rapidly evolve, and perhaps to evade us, at times.

2. Cyber threat landscape

- Indeed, the world we are living in is increasingly volatile and complex. The global economy is struggling for growth even as geo-political dynamics are shifting.
- Amid the uncertainties in the political and economic landscape, we are seeing increasing threat on the security front. Financial crimes, cyber-crimes and terrorism are on the rise. And we may only be seeing the tip of the iceberg.
- Advances in technology and innovation have led to greater speed, ease and convenience. These have opened up huge borderless opportunities for everyone…but not everyone has good intent.
- Innovation and disruption – buzzwords in the world of fintech - take on different meanings when applied with ill intent.

- Internet and mobile technologies have allowed crimes to be committed quickly, easily and on a large scale. With significant impact on individuals, industries and countries.
- No one is spared. Whether it's the SWIFT payments network, popular websites or mainstream media. Just last month, Twitter and PayPal, Wall Street Journal and New York Times, were among those subject to D-DoS attacks. One of Singapore's telecom service providers has also been hit.
- The frequency, scale and sophistication of such attacks are on the rise.
- And so are the costs.
- A McAfee report estimated losses from cyber risks to be between USD300 billion to USD 1 trillion a year. This is much higher than losses from natural disasters, which averaged USD 200 billion a year over the last ten years.
- To guard against such risks, cyber security spending is growing. Global spending increased almost 4 times from USD22 billion in 2008 to an estimated USD81 billion in 2016. And is forecast to double to USD170 billion by year 2020.
- The consensus these days is that cyber attacks are inevitable. It's not 'if' but 'when', and how frequent and significant the impact. So the focus is not just to prevent, but to detect and respond promptly to such attacks. Advanced capabilities using machine learning and big data analytics to automate and proactively search and detect threats are becoming necessary for the industry to be agile in responding to cyber threats. Defence is no longer reactive but proactive.
- In short, as banks continue to innovate and digitize to stay relevant to customers, we must concurrently step up on cyber security in our more open and connected world.

3. Managing cyber risks - banking industry & regulatory initiatives

- How are we doing so?
- In the Singapore context, our Prime Minister announced last month a Singapore Cybersecurity Strategy to strengthen resilience, through a focus on infrastructure, cyberspace, eco-system and partnerships.

- ABS welcomes such leadership, which paves the way and further supports the many programs which the industry is and will be undertaking.
- Since our last conference in 2015, the banking industry has taken steps to strengthen its cyber security capabilities, building upon the foundations established in previous years.
- The approach is multi-pronged. Let me briefly share some updates:
  (i) Recognising that criminals often exploit the vulnerability of customers in a highly mobile, connected world, ABS and MAS stepped up efforts to engage and educate the public on cyber security.
  (ii) Sharing of information, expertise and best practices, within and across countries, is key to fighting cyber-crime. Among other initiatives, the ABS Standing Committee on Cyber Security, in collaboration with the MAS and Israeli Ministry of Economy, did a study trip to Israel earlier this year. You will hear more about it later today.
  (iii) We all know there is a global shortage of cyber-security professionals. MAS and ABS are working with local schools and tertiary institutions to groom young cybersecurity and Fintech talents, through curriculum development and internships. The aim is to nurture a pool of skilled manpower for these growing sectors.
  (iv) Regulatory guidelines have been developed to keep pace with the fast moving technology and innovation landscape. In June this year, MAS announced the regulatory sandbox initiative to encourage innovation within manageable risks. ABS also published a set of Cloud Computing Guidelines for its members to ensure consistency and controls.

4. Putting in perspective

- A strong regulatory framework and effective supervision are fundamental. But to counter the threats more effectively, we also need collaboration among industry

players, striking a balance between data privacy laws and the need to share information, within and across countries.

- Whether it's fighting terrorism, financial or cybercrimes, sharing of intelligence and best practices as well as coordination in monitoring and responses are crucial.
- Teamwork is key. We are only as strong as our weakest link.
- It's an ongoing challenge to catch up, if not keep pace, with the criminals. The risks today are not the same as yesterday. Neither will they be the same tomorrow.
- It's also an ongoing challenge, to find the optimal balance when investing efforts and resources for such purpose. To be vigilant and protect businesses on one hand, while promoting enterprise and growth on the other.

  As commercial enterprises, we have to find pragmatic solutions. Risk management is part and parcel of our business. We can't afford to be paralysed by security threats.
- Ultimately, it boils down to people – our ethics, values, integrity. Having the common belief that every one of us has a role to play to make the world a better place. It's a collective responsibility.
- Your gathering here is an encouraging sign of such teamwork.
- If such spirit of collaboration can be multiplied across industries and countries, I believe it will be more difficult for criminals to succeed.
- On this note, I thank you all for joining us today, and the distinguished speakers for sharing their valuable insights.
- Have a fruitful conference and enjoyable day of sharing.
- Thank you.

7.11.16