1. Foremost, I take this opportunity to record my heartfelt appreciation to the European Union – Malaysia Chamber of Commerce and Industry (EUMCCI) and TÜV Rheinland for the privilege of addressing this forum today.

2. Let me share with you my thoughts on "the role of cyber security in securing innovation in paving the way for industry 4", which I believe is a great concern to every one of us in today's Digital Age.

MALAYSIA COMMITTED TOWARDS CYBERSECURITY
Ladies and Gentlemen,

3. The International Telecommunication Union's 2017 Global Cybersecurity Index has ranked Malaysia as the third most committed country towards cybersecurity, after Singapore and the United States.

4. This is recognition of Malaysia's plans and strong cooperation among its government agencies. The Ministry of Science, Technology, and Innovation (MOSTI) is committed towards generating a secure cyber environment for individuals and corporations in Malaysia.

5. This shows the Malaysian Government's commitment in strengthening our cyber security aspect in accordance with our aspiration for Malaysia to be a developed country.

6. But there is still more work to be done. I don't need to say but the economic prosperity in the 21st century will very much depend on effective measures to protect our cyberspace and infrastructure.

7. It's a fact of life today that cyber security acts as a shield for the nation's economic development and societal well-being. The challenge therefore is to ensure Malaysia becomes a safe cyber place for business and a developed nation by 2020. According to Accenture, 65% of companies in Malaysia are still vulnerable to cyberattacks as they are not sufficiently protected.

8. At national level, the Eleventh Malaysia plan has identified cyber security as one of the technology focus areas, which has a strong emphasis on Information Communication Technology (ICT) investments to prepare the economy for Industry 4.0 and create conducive cyber physical systems.

9. The development of cyber physical systems will enhance Malaysia's position at global economy, allowing the country to move from being a technological consumer to a technological producer. ICT is set to grow and contribute up to 18.2% to Malaysia's GDP by 2020.

HISTORY AND THE LATEST DEVELOPMENT IN INDUSTRY 4.0
Ladies and Gentlemen,

10. Cyber security is crucial in ensuring innovation and sustaining future global trade between European Union and Asian region including Malaysia. It is useful for us to go back into history and review the journey that has brought mankind to where we are today: The Industrial Revolutions.

11. Historically, the first industrial revolution started in Europe, more specifically in Great Britain in the late 17th century. The revolution was the culmination of development in machine tools and factory system on the back of invention in steam power and iron production at that time.

12. While the First Industrial Revolution spurted the growth of industries, from coal, iron, railroads to textiles, the Second Industrial Revolution witnessed the expansion of electricity, petroleum and steel in the late 19th century and the beginning of the 20th century. Indeed, the 2nd industrial revolution brought about much prosperity to Europe, North America and later expanded to Asia and rest of the world.

13. By the second half of the 20th century, a third industrial revolution appeared with the emergence of a new type of energy whose potential surpassed all its predecessors: nuclear energy. This revolution also witnessed not only the rise of electronics from transistors to microprocessor, but also the rise of telecommunications and computers.

14. As telecommunications continued to advance, the arrival of high-speed Internet at the dawn of the third millennium sparked the digital revolution that ultimately brings about the latest game changer.

15. So as I stand before an elite group of business leaders and entrepreneurs from European Union and Malaysia today, a fourth industrial revolution is underway, which builds upon the digital revolution.

16. But all these come at a price. The trends of technologies have introduced new vulnerabilities and opportunities for cyber attackers, hence adding more risks of cyber threats.

17. As technologies evolve, the criminals and other malicious actors also emerge. Therefore, there is a growing concern of increasingly insidious threats at various levels of societies. The trends of technologies have introduced new vulnerabilities and opportunities for cyber attackers, hence adding more risks of cyber threats.

18. We have also see how classified networks and industrial control systems were being compromised and how such attacks have affected businesses and government abilities to functions.

19. It is not an exaggeration to say that cyber-crimes are fast becoming the crime of choice and they are gradually replacing traditional crimes.

TO SAFEGUARD THE NATION CYBER SPACE FROM CYBER THREATS
Ladies and Gentlemen,

20. Cyber-attacks can happen anytime, what more with the imminent rise of 4IR. The expansion of cyber security ecosystem requires organizations to develop cyber resilience the ability to powerfully resist, react to and recover from potentially catastrophic cyber security threats, and reshape their environments for increasingly secure and sustainable cyber operations.

21. Cyber security would remain as national security concerns in years to come. Cyber threats are evolutionary and we have seen how they are growing in sophistication, hence Malaysia's approaches towards cyber security must continue to be revolutionary and innovative.

22. Malaysia in particular, with its aspiration of becoming an advanced nation driven by digital economy, must cope with the new dangers posed by new cyber-attacks in the light of 4IR.

23. Digital revolution has introduced malware as a criminal tool with Internet acts as a medium. In most cases, malware serves as the initial step to cyber-attacks and most of our computer systems now are exposed to various risks of cyber-crimes.

24. Amongst the disastrous Ransomware attacks was Petya, first seen in March 2016, and continued in 2017, ransomware variants, WannaCry had affected more than 230,000 computers in over 150 countries.

25. From Malaysia's landscape perspective, we received numerous reports on ransomware which being categorized under malicious code. In 2017, there were 814 malicious code incidents being reported to CyberSecurity Malaysia and this year, until February 2018, 58 were reported.

26. Clearly, cyber security will underpin the future growth of any digital economy and Malaysia is well positioned to capitalize on this impending trend.

27. As such, we need to develop a national cyber security innovation ecosystem that will transform cyber security challenges into new opportunities, ideas and solutions. A new mind set is vital if any economy is to survive and thrive in the coming decades.

28. The government of Malaysia will continue to give priority to cyber security for the next five years where the development of home-grown cyber security products and services will be emphasised to enable self-reliance.

INTERNATIONAL COOPERATION IN CYBER SECURITY

Distinguished Guests, Ladies and Gentlemen,

29. Whilst at the same, as part of global community, we will also aim to further strengthen our international cooperation to respond to global cyber challenges in order to protect its regional and global common interests. With such holistic approach, we hope to create and sustain a secure, resilient and trusted environment for 4IR to thrive.

30. There is a need, now more than ever, to collaborate with our key international partners, since cyber-attacks are borderless and beyond geographical boundaries.

31. Homeland security and traditional threats in the past were confined within physical boundaries. However, we have already seen today, the affairs of homeland security are no longer relevant in the case of cyber dimension.

32. To the military and in modern warfare, Cyberspace is recognised as the fifth domain apart of land, seas, air and space that need to be safeguarded.

33. One of the ways to address this would be through science diplomacy whereby international cooperation in cyber security detection, response and recovery should be emphasized.

34. My government understands the need to strengthen communication, enhance mutual trust, and promote regional cooperation to build a peaceful, secure, open and cooperative cyberspace.

35. So far, we have witnessed successful international collaboration and MOSTI thru CyberSecurity Malaysia intends to play a major and active role in developing close relationships and partnerships regionally and globally.

36. For example, at international level, EU-ASEAN collaboration project called **YAKSHA Horizon 2020** aims to use EU know how and local ASEAN expertise to develop a solution tailored to specific user and country needs.

37. Cybersecurity Malaysia is one of the ASEAN partners in collaborating with seven European partners.

38. The YAKSHA project will allow for heightened cyber security progresses and improve the competitiveness of European security industries in all ASEAN countries.

39. It also aims to develop innovative methods to pinpoint cyberattacks and create a system to store and analyze the collected data from occurring cyberattacks in the long-term.

<u>CONCLUSION</u>

Ladies and Gentlemen,

40. In conclusion, I hope cyber security will always remain a national security priority in Malaysia and certainly for many years to come. Therefore, I call upon all stakeholders in the cyber security ecosystem to adopt a more coherent and holistic approach to overcome cyber challenges in the era of 4IR.

41. With that, I would like to wish you all success, thank you for your presence, and hope you have a pleasant and an enjoyable afternoon. Thank you.