In this digital age, where everyone and everything is connected, there are various risks and threats that could happen to an organisation. The number of attacks on those working in the supply chain has increased, heavily targeted, more vulnerable and at risk than ever before. Some of the threats to the supply chain are sabotage, tampering, counterfeiting, piracy, theft, service disruption or destruction, exfiltration, infiltration, subversion, diversion, export control violations, corruption, social engineering, insider threat, pseudo-insider threat, and foreign ownership.

Supply chain attack is difficult to handle due to its malware design which stays hidden among the infected system and user's device. Especially in today's environment, nations are slowly recovering from the pandemic and starting to move towards digital transformations. While cybersecurity practices and awareness has been increasing but the frequency of the attack has also been getting faster and more sophisticated.

Currently, the cybersecurity landscape has been moving towards new environment and new technologies. As the current policies and law are being reviewed, the new ones being studied to accommodate future landscape. However, the three aspects of **people, process**, and **technology** are still lacking as there are some industries that are still using legacy system and referring to old policies instead of creating new ones for today's environment. Furthermore, the people's aspect of cybersecurity that still contributes as the main cause for these cybercrimes occurring.

There are also individuals who have problems with new security practices, poor digital hygiene, and poor cybersecurity implementation at workplace. People aren't learning from their cyber mistakes and, more disturbing, they aren't equipped with the knowledge on how to prevent repeated mistakes.

Cybersecurity strategies need to be embedded into manufacturing operations from the start, spanning across Information Technology (IT) and Operational Technology (OT). It needs to ensure the security of future manufacturing production operations, throughout its lifecycle. In ensuring security across the ICT Supply Chain, acquisition requirements and service level agreements should include relevant security requirements including the ISO/IEC 27001.

Dato' Ts. Dr. Haji Amirudin Abdul Wahab ("Dato' Dr. Amir") is currently the Chief Executive Officer (CEO) of CyberSecurity Malaysia, the agency that monitors e-sovereignty of the country. He has approximately 30 years of ICT working experience in the telecom and IT sector in the Government as well as in the semi-government and private sectors.

Dato' Ts. Dr. Amir holds a Doctor of Philosophy (PhD) from the School of Information Technology & Electrical Engineering (ITEE), University of Queensland, Australia. Dato' Ts. Dr Amir also holds two Master degrees, a Masters in Business Administration (MBA) from the University of Duqubue, Iowa, USA, a Masters in Information Technology from National University of Malaysia (UKM) and a Bachelor of Science Engineering in Electrical Engineering from the University of Michigan, Ann Arbor, USA.

During his leadership, Dato' Ts. Dr. Amir also spearheaded various national and international Cyber security platforms such as serving as the cyber security co-chair in the Cybersecurity working Group for Council for Security Cooperation in the Asia Pacific (CSCAP) since 2015, as Permanent Secretariat to Organisation of Islamic Conference Computer Emergency Response Team (OIC- CERT) since 2013, Deputy Chair to Asia Pacific Computer Emergency Response Team (AP-CERT) for 2015 - 2019 and current chair to AP-CERT since 2019 till now. Dato' Ts. Dr. Amir is a Canadian-based POLCYB (The Society of The Policing of Cyberspace) Non-Executive Board of Directors for year 2015 to 2018. He used to serve as an OIC Task Force Member on ICT and Cyber Security and currently a Fellow at Malaysian Institute of Management (MIM) and Fellow of Academy of Sciences Malaysia. He was also appointed as Vice-Chair of OIC Science and Technology Committee and Executive Committee Member of Annual Coordination Meeting of OIC Institutions (ACMOI) during the Thematic Committee on Science, Technology and Information Technology meeting which was held in conjunction with Inaugural Annual Coordination Meeting of OIC Institutions on 7 December 2015 at Jeddah, Arab Saudi. He was also ratified by APEC ECSG on 27 February 2016 as an Expert Members for the 2nd APEC E-Commerce Business Alliance (ECBA) Expert Council (2016-2018) in which he was one of its Deputy Chairman. Dato' Ts. Dr. Amir was also appointed as Advisory Board Member of The Economist Intelligence Unit on Asia Smart City Program 2016. In January 2021, Dato' Dr Amir has been appointed as Microsoft Asia Pacific Executive

Council Member and CyberEdBoard Member. He has been appointed as Advisory board of CIT-CERT Coordination Center (C4P) Pakistan in August 2021. Most recently, as Member of Consultative Council on Foreign Policy of Ministry of Foreign Affairs starting 30 August 2021.