

Organized by

Supporting Partner

Media Partners



16 March 2021
Virtual Summit
on Zoom

Malaysia Cybersecurity Summit

Preventing High Tech Crimes



Overview

As a saying goes intellectual solves the problem but geniuses prevent them. There is an alarming rise in cybercrime and there requires preparation at war level to prevent rather than responding to attack. Organization requires genius approaches, practices, people, procedures to prevent an incident and never let a disaster happen.

ASEAN has a vital geographic location. It is a transit point connecting east to west. It has been a hub of transnational crimes ages back and still remains to be. With growing technology usage and lax cross border initiatives to handle cyber-crimes.

Technology from drones and analysis and predictive methods to biometrics, to facial recognition help to track the crime but still businesses and enforcement lack in combat the menace as a team. Policy framework, processes, procedures, cross border investigations, intelligence sharing

are homegrown hindrances allowing transnational crimes to grow in cyber space.

“There were some 3000 plus complaints were lodged to the Cyber999 Help Centre during the Movement Control Order (MCO) period from March 18 to June 30, an increase of more than 90 percent compared with the same period last year.” This data is alarming that all ASEAN nation authorities should take a call and come on a platform to discuss this.

True prevention is not waiting for bad things to happen, it's preventing things from happening in the first place.

Don McPherson



DURING THIS CONFERENCE, YOU WILL LEARN

<p>The Latest tried and tested methodologies for dealing with current patterns of cross border hi-tech crimes.</p> <p>1</p>	<p>How criminals are using technologies to communicate and utilizing electronic data to execute the crime.</p> <p>2</p>	<p>How businesses are done in darknet space: Truth and myths about the darknet.</p> <p>3</p>	<p>Providing full proof IT and physical security solutions to protect your critical assets.</p> <p>4</p>
<p>About Modus operandi of cyber espionage that how they were planned and executed.</p> <p>5</p>	<p>Managing cross border investigation and forming a partnership with enforcement agencies and foreign agencies combining legal and technology to prevent crime.</p> <p>6</p>	<p>How attacks are being planned and staged by cybercriminals and terrorist network to bring losses to the country's image and business losses.</p> <p>7</p>	<p>About a new era of hacking and comparing your preventive measures with the level of hackers' tools and techniques.</p> <p>8</p>

WHO WILL ATTEND

- Investigative Analyst
- Enforcement officers
- IT Director
- IT Security Specialist
- AML specialist
- Facility Security Officer
- Forensic Investigator
- Forensic Scientist
- C.I.O.
- Lead IT Security Analyst - Forensics
- Digital Forensic Investigator
- Digital Forensics / Information Security Analyst

- Digital Forensics Incident Response
- Legal counsel
- Investigator
- IT Forensics Specialist
- IT Specialist (INFOSEC)
- Enforcement officer
- Forensic Examiner
- Forensic IT Specialist
- C.T.O.
- Chief Information Security Officer
- Digital Forensic Analyst
- Business continuity management head
- Digital Forensics Examiner
- Digital Investigator

ATTENDEES FROM

- Financial institution
- Police force
- High Commissions (Commercial counselor, defense attache)
- Airport
- Narcotics
- Companies commission
- App provider
- Business houses
- Customs
- Seaport
- Immigration
- Anti-Money laundering task force
- Law firms

For further enquiries or registration, please email to mradi@kasi.asia or wani@kasi.asia

Programme

16 March 2021 | Virtual Summit on Zoom

9.15am	All Role-Players and Participants on Standby Mode
9.30am	WELCOME SPEECHES BY Tan Sri Michael Yeoh, President, KSI Strategic Institute for Asia Pacific
9.40am	OPENING KEYNOTE ADDRESS BY YB Dato' Seri Hamzah bin Zainudin, Minister of Home Affairs, Malaysia (<i>to be confirmed</i>) Fighting cyber and high-tech crimes during pandemic COVID-19: The way forward for Malaysia <ul style="list-style-type: none">• Highlighting Malaysian government approaches and stringent steps against evolving threats• What are the amendments and new initiatives proposed in order to prevent cyber-attacks on critical and non-critical assets
10.00am	KEYNOTE ADDRESS BY Royal Malaysia Police (PDRM) (<i>to be confirmed</i>) Tackling the growing menace of cyber terrorism and how and what kind of threats terrorist organizations are posing to brand, customers and data <ul style="list-style-type: none">• Highlighting difference between cybercrime and cyber terrorism and how both go hand in glove• Current nature of threats and vulnerabilities being noticed by law enforcement agencies• Underlining steps that agencies are taking to mitigate terror-related activities and expectations, they have from businesses• What are the gaps being noticed in the legal and policy framework of Malaysian businesses and what they must do to chasm those gaps
10.20am	Session 1 : Strengthening Organizational Preparedness For A Resilient It System Secure by design: Designing and development of a world-class robust ecosystem while embedding security into technology processes <ul style="list-style-type: none">• Top 5 areas that are commonly neglected by Information technology expert during the designing phase that later becomes a threat• Explaining the process of integrating security control into your tech ecosystem design so as to bring down the vulnerabilities• "Test everything" - Leveraging a proactive cybersecurity approach using the right kind of penetration testing and deciding which pentest is right for you
10.40am	Panel Discussion (I): Cyber Security Talent Management – Developing A Strong Cybersecurity Workforce in Order To Augment The Returns On Investment On Technology <ul style="list-style-type: none">• Recognizing the difference between Information technology talent and cybersecurity talent• Pinpointing out of the box hiring approaches and what characteristics and non-technical expertise comprise a "perfect candidature" for IT security role• Harnessing a culture of proactive and green light thinking and practices to cultivate a "creative" culture in cybersecurity team• Best practices to retain best-in-class talent, empowering your employee while redefining their career planning and path
12.00pm	Session 2: Unveiling The Dark World of The Crime and Criminals, Deep Web and Dark Web Dark net an underground economy - myths v/s reality and how the darknet is affecting your businesses <ul style="list-style-type: none">• Looking into operational factors like how and why of darknet invisibility, anonymity and non-traceability• Modus operands of the criminals on the darknet and how they are different from hackers like cybercriminals• What is kind of threats the darknet is posing and Staying away, staying awake, staying safe from unearthing threats
2.00pm	Panel Discussion (II): Exploring recent developments in cybercrime criminologies mainly computer crimes related to integrity, network, and contents <ul style="list-style-type: none">• Elaborating "not so widely known" social engineering techniques and attack cycle• "Putting old wine in new bottles" - studying types of generation-old cybercrime conducted in new settings• Revising criminological and psychological theories evolving in the digital landscape• Tracking and tracing "that black sheep" while knowing the appearance and behavior of a habitual criminal in your team involved in cyber espionage and theft
2.45pm	Session 3: Fighting Criminals in The Connected World and Digital Spaces Machine v/s machine: Using AI, ML, robotics like advanced technologies to detect crime and attack assets in a digital terrain <ul style="list-style-type: none">• What is Artificial intelligence, machine learning, and robotic tools being used by cybercriminals• Evaluating the dark side of digitalization and how novel technologies can be used to build responsive strategies to protect the organization's technological assets• What are the drawbacks and limitations of AI, ML, And Robotics and how to overcome them
3.00pm	Panel Discussion (III): Turning to Public-private partnership and deriving upon a model to combat cybercrime <ul style="list-style-type: none">• How global pandemic and upswing in remote work have created a target-rich milieu for cybercriminals and what are the looming threats that can be curbed using PPP• Why and how a partnership between law enforcement agencies and businesses fails - understanding the distractions and eliminating misunderstandings• Cultivating the "culture of collaboration" through intelligence sharing and techniques to bridge the gap between agencies and businesses
3.45pm	End of Summit

Notes

- The Organizers reserve the right to alter the content and timing of the Programme in the best interest of the Summit and is not responsible for cancellation due to unforeseen circumstances.
- The Organizer accept no responsibility for statements made orally or in written material distributed by any speaker at the Summit. In addition, the Organizer is not responsible for any copying, republication or redistribution of such statements.
- Copyright © KSI Strategic Institute for Asia Pacific (KSI) 2020.
* All rights reserved.





Preventing High Tech Crimes

16 March 2021
Virtual Summit on Zoom

WELCOME ADDRESS

SESSION 1

STRENGTHENING ORGANIZATIONAL PREPAREDNESS FOR A RESILIENT IT SYSTEM

SESSION 2

UNVEILING THE DARK WORLD OF THE CRIME AND CRIMINALS, DEEP WEB AND DARK WEB

SESSION 3

FIGHTING CRIMINALS IN THE CONNECTED WORLD AND DIGITAL SPACES



Tan Sri Michael Yeoh
President, KSI Strategic Institute of Asia Pacific



Khadir Fayaz
Vice President, Global Enterprise Architecture & Cyber Security, CBRE



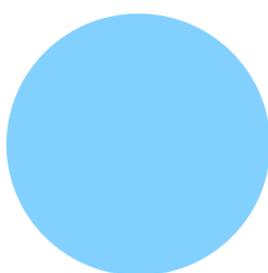
Bob Schi
Founder & CEO, Cyberlitica, Inc.



Steven Sim
President, ISACA Singapore

PANEL DISCUSSION (I)

CYBER SECURITY TALENT MANAGEMENT – DEVELOPING A STRONG CYBERSECURITY WORKFORCE IN ORDER TO AUGMENT THE RETURNS ON INVESTMENT ON TECHNOLOGY



David M Clarke
Trustee, the Fraud Advisory Panel Charity, Director, Group Head of Integrity and Multilingual Due Diligence Services, the Queens Award winning company, Guildhawk

Maz Mirza bin Mohd Aminurashid
Head Information Technology, Mass Rapid Transit Corporation (MRT Corp), Malaysia

Col Ts Sazali bin Sukardi
Senior Vice President of Strategic Research, CyberSecurity Malaysia

Rupesh Bhuran
Security Solution Designer, Sony Electronics (Singapore)

Darron Sun
Chairman of Cybersecurity Committee of CMA Australia/
Chairman of Cybersecurity Committee of IPA Australia/
Vice Chairman of Institute of Financial Technologists of Asia (IFTA), Hong Kong

PANEL DISCUSSION (II)

EXPLORING RECENT DEVELOPMENTS IN CYBERCRIME CRIMINOLOGIES MAINLY COMPUTER CRIMES RELATED TO INTEGRITY, NETWORK, AND CONTENTS

Dr. Mohammad Khaled
Adjunct Professor for Doctorate and MBA, Abu Dhabi University

Parag Deodhar
Director - Information Security, VF Corporation

Soumo Mukherjee
Head of Strategy & Architecture—Cyber Security, PETRONAS

Ir Dr. Daniel Ng
Director, Kun Hang Group Limited

Micky Lo
Managing Director, Chief Technology Risk Officer APAC The Bank of New York Mellon

PANEL DISCUSSION (III)

TURNING TO PUBLIC-PRIVATE PARTNERSHIP AND DERIVING UPON A MODEL TO COMBAT CYBERCRIME

Rear Admiral Dato' Shamsuddin Bin Hj. Ludin
Assistant Chief of Staff - Defence Communication and Electronic Division, Headquarters

Sivaruban Balachandran
Enterprise Security & Cloud Security Architect - Cybersecurity / Strategy and Architecture, Digi Telecommunications

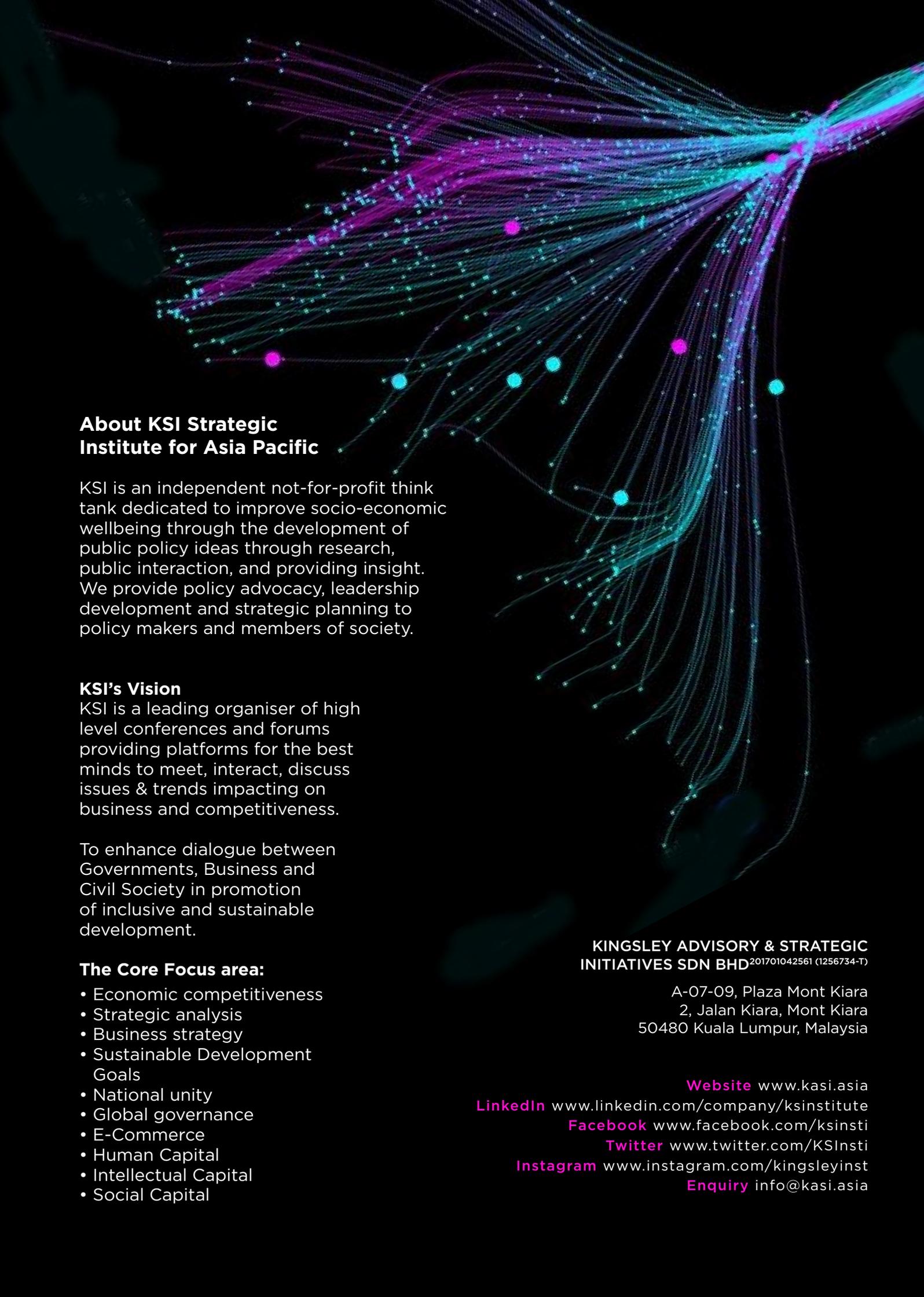
Jairam Ramesh
Heads, Group Cyber Security, AIA Malaysia

Anshul Srivastava
Global Chief Information Officer, Large Sovereign Fund

Moderator

Associate Professor Col (R) Dato' Dr Husin Jazri

Member of Board of Governor, University Malaysia of Computer Science and Engineering (UNIMY) /Editor-in-Chief of E-Security and Privacy Media Channel (ESPC)



About KSI Strategic Institute for Asia Pacific

KSI is an independent not-for-profit think tank dedicated to improve socio-economic wellbeing through the development of public policy ideas through research, public interaction, and providing insight. We provide policy advocacy, leadership development and strategic planning to policy makers and members of society.

KSI's Vision

KSI is a leading organiser of high level conferences and forums providing platforms for the best minds to meet, interact, discuss issues & trends impacting on business and competitiveness.

To enhance dialogue between Governments, Business and Civil Society in promotion of inclusive and sustainable development.

The Core Focus area:

- Economic competitiveness
- Strategic analysis
- Business strategy
- Sustainable Development Goals
- National unity
- Global governance
- E-Commerce
- Human Capital
- Intellectual Capital
- Social Capital

**KINGSLEY ADVISORY & STRATEGIC
INITIATIVES SDN BHD** 201701042561 (1256734-T)

A-07-09, Plaza Mont Kiara
2, Jalan Kiara, Mont Kiara
50480 Kuala Lumpur, Malaysia

Website www.kasi.asia

LinkedIn www.linkedin.com/company/ksinstitute

Facebook www.facebook.com/ksinsti

Twitter www.twitter.com/KSInsti

Instagram www.instagram.com/kingsleyinst

Enquiry info@kasi.asia

PARTICIPANT REGISTRATION FORM

16 MARCH 2021
VIRTUAL SUMMIT ON ZOOM



Please fill in **BLOCK** letters and print with **BLACK INK**. One form per person.

Yes! I would like to attend Malaysia Cybersecurity Summit.
Please make a reservation for the following:

PERSONAL DETAILS

Name:

Organisation:

Designation:

Address:

Office Number:

Mobile Number:

Email:

Fax:

REGISTRATION FEE

PRICE PER PAX (Please tick (✓) your choice)

Virtual Conference

RM400 (Pricing listed inclusive 6% SST)

The registration fee includes conference material, coffee breaks and lunch.

FOR THE PUBLIC OR GOVERNMENT SECTOR

A Local Order (LO) or letter of approval to participate must be presented before the event.

Service tax number

B16-1903-32000112

Effective date

1 April 2019

PAYMENT METHOD

MODE OF PAYMENT (Please tick (✓) your choice)

Cheque / Bank Draft

Payment by cheque or bank draft must be made payable to:
Kingsley Advisory And Strategic Initiatives Sdn Bhd

Bank Transfer

(kindly email or fax the payment slip to the Secretariat)

Account Name Kingsley Advisory And Strategic Initiatives Sdn Bhd

Bank Name Malayan Banking Berhad

Address B-13, Garden Shoppe One City, Jalan USJ 25/1, USJ 25
47650, UEP Subang Jaya, Selangor Darul Ehsan

Account Number 518617007256

Swift Code MBBEMYKL

- Registration will only be confirmed when the full payment is received. Please send your payment to the Secretariat at the address above.
- Admittance may be denied upon failure to make full payment

PARTICIPANT REGISTRATION FORM

16 MARCH 2021
VIRTUAL SUMMIT ON ZOOM



Please fill in **BLOCK** letters and print with **BLACK INK**. One form per person.

CANCELLATION/SUBSTITUTION POLICY

Upon registering, participant(s) are considered successfully enrolled in the event. Should participant(s) decide to cancel/transfer their enrolment, a cancellation/transfer policy shall be applied as follows.

- a) Written cancellation/ transfer received less than three (3) days from the date of the event:
- A refund (less administrative charge of 20%) will be made
 - Unpaid registrations will also be liable for 20% administrative charges
- b) Written cancellation/no show on the day of the programme:
- No refund will be entertained
 - Unpaid registrations will also be liable for full payment of the registration fee - Partial cancellation is not allowed

You can substitute an alternate participant if you wish to avoid cancellation/transfer charges. Any difference in fees will be charged accordingly.

BILLING AND APPROVING AUTHORITY INFORMATION

Organisation/Company:

IF DIFFERENT FROM ABOVE:

Name:

Designation:

Department:

Address:

Office Number:

Mobile Number:

Email:

Fax:

Purchase Order # or other reference:

DATA PROTECTION STATEMENT & PERSONALITY / IMAGE RIGHTS

By filling out the registration form, the participant gives consent that KSI Institute can process the personal information provided, whether now or in the future, may be used, recorded, stored, disclosed or otherwise processed by or on behalf of KSI Institute for the purposes of facilitation and organisation of this or similar conference, research and audit, maintenance of a delegate database for the promotion of this or similar conference, and such ancillary services as may be relevant. This includes the placing of photographs in the KSI Institute's social media platform, in the KSI Institute's newsletter or selecting some for articles on the conference in a journal or newspaper, or in any other web/printed publication.

DISCLAIMER:

KSI Institute reserves the right to change the speaker(s), date(s) and to cancel the programme should circumstances beyond its control arises. KSI Institute also reserves the right to make alternative arrangements without prior notice should it be necessary to do so. Upon signing the registration form, you are deemed to have read and accepted the terms and conditions.

REGISTRATION

Contact

Mobile

Email the form

Mohd Radhi Puteh

+6013 757 2395

mradhi@kasi.asia

Noor Syazwani Md Amin

+6017 405 0102

wani@kasi.asia

FOR ENQUIRY

Kingsley Advisory & Strategic Initiatives Sdn Bhd 201701042561 (1256734-T)

A-07-09, Plaza Mont Kiara, 2, Jalan Kiara, Mont Kiara, 50480 Kuala Lumpur, Malaysia
T: +603 6419 9698 F: +603 6419 9683 E: info@kasi.asia