

CYBER SECURITY ASIA 2022

Developing Cyber Resilience for a Future Ready Organization

15-16 August 2022 | Sheraton Imperial Hotel Kuala Lumpur

Cybercrime and cyberattacks continue to rise with ever more data breaches and crippling ransomware attacks. A broader security strategy is needed as the attack surface grows, and we rely more on digital technologies in all areas of business and industry. With the support of forward-thinking security strategies and technology solutions to match, the modern business can minimize potential risk and step into a digital future confidently.



Dato' Ts Dr. Haji Amirudin Abdul Wahab
CEO
CYBERSECURITY MALAYSIA



Daniel Norman
Regional Director
ISF



LCol Francel Margareth Taborlupa
Battalion Commander
PHILIPPINE ARMY



Dyma Budorin
CEO
HACKEN



Abhinav Mishra
Founder
ENCIPHERS



Shamane Tan
Chief Growth Officer
SEKURO



Philip Victor
Managing Director
WELCHMAN KEEN



Mohammad Imran
Founder
PRACITCAL DEVSECOPS



Pengfei Yu
Cybersecurity Associate
GOVTECH SINGAPORE



Farrell Tirtadinata
Business Solutions Director
AVERTRO



Justin Chong
Ethical Hacker
PRIVASEC



Nivedita Newar
Head of Cyber Security Strategy
UNSW



Robert Laurie
CISO
UNIVERSITY OF NEW ENGLAND



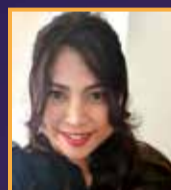
Leonard Ong
Regional CISO
GE HEALTHCARE



James McLeary
MD Cyber Security Risk
KROLL HONGKONG



Quan Heng Lim
Regional Head, Asia
PRIVASEC



Daisy Sinclair
CEO
CYBER8LAB



Theo Nassiokas
Head Business Controls
WESPAC GROUP



Chris Cubbage
Executive Director
MYSECURITY MEDIA



Darrent Ng
Business Solutions Director
GROUP-IB



Dr. Carrine Teoh
Chief Strategy Officer
BOND HOLDINGS



Allan Cabanlong
Founder & CEO
CYBER GUARDIANS

OVERVIEW >

Cybersecurity is not a separate technology, but rather a priority of the systems spanning technology, people and processes in the Fourth Industrial Revolution. The ongoing shift from cybersecurity to cyber resilience is an important step towards a more trustworthy and sustainable future.

In 2022, companies can expect to face sophisticated attacks that target every part of their IT infrastructure, especially where they are weakest. Defending against modern cyber threat campaigns requires the ability to respond quickly and correctly to rapidly-evolving attacks that can strike anywhere within an organization's IT infrastructure. Organizations need comprehensive security visibility, access to real-time threat intelligence, and an integrated security architecture that can support automated and coordinated threat prevention and response across the entire corporate IT infrastructure.

The below statistics portray how critical it is for companies to adapt to the ever-evolving threat landscape. Whether concerned about botnets, supply-chain attacks, or data breaches, organizations need to review their security strategies in order to survive and thrive in 2022.



Register before 20 May 2022 & receive a complimentary Amazon's best-selling book **Cyber Mayday and the Day After** authored by Shamane Tan & Dan Lohrmann



DID YOU KNOW?

There will be one ransomware attack every **11 SECONDS** by 2022, this is an increase of about 20% compared to the prediction made in 2019 of 14 attacks per second.

By 2025, cryptocurrency crime is predicted to surpass **\$30 BILLION**, up from \$17.5 billion in 2021

2021, organizations experienced the highest average cost of a data breach in 17 years at **\$4.24 MILLION**, rising from \$3.86 million the previous year.

The healthcare industry has seen a **51%** increase in breaches and leaks since 2019

The most malicious file type is still the infamous EXE, making up **52%** of all files

Cyber-attacks are up **50%** in 2021 in comparison to 2020, peaking in December, largely due to Log4j exploitations, treat actors targeting Africa, Asia Pacific & Latin America the most.

83% of small and medium-sized businesses are not financially prepared to recover from a cyber-attack.

WHY ATTEND



Everything You Need To Learn and Everyone You Need to Meet in The Cyber Security Sphere



Discover the Security Use Cases, Business Models and Roadblocks that Can Support Your Digital Transformation



Learn From International Thought-Provoking Cyber Security and Cyber Risk Experts



Connect with Global technologist and Early Adopters to Expand your Network

WHO SHOULD ATTEND >

- Chief Executive Officers
- Chief Operating Officers
- Chief Information Security Officers
- Chief Information Officers
- Chief Risk Officers
- Chief Technology Officers
- Cyber Security Professionals
- Heads of Digital Transformation
- Heads of Insights and Analytics
- Operation Risk Heads and Managers
- Technology Risk Heads and Managers
- Cyber Security Experts