Exclusive Interview with Chartered Banker, Fad'l Mohamed, CEO of Maybank Investment Bank Berhad
'Future-Proofing the Next Normal'

BANKING INSIGHT

IDEAS FOR LEADERS | **DECEMBER 2021**

PP 17327/05/2013(032407)

Move Along, Goldilocks

Forget about the economic sweet spot. Fundamentals are what we want.

Quantum Computing: Finance's Next Frontier

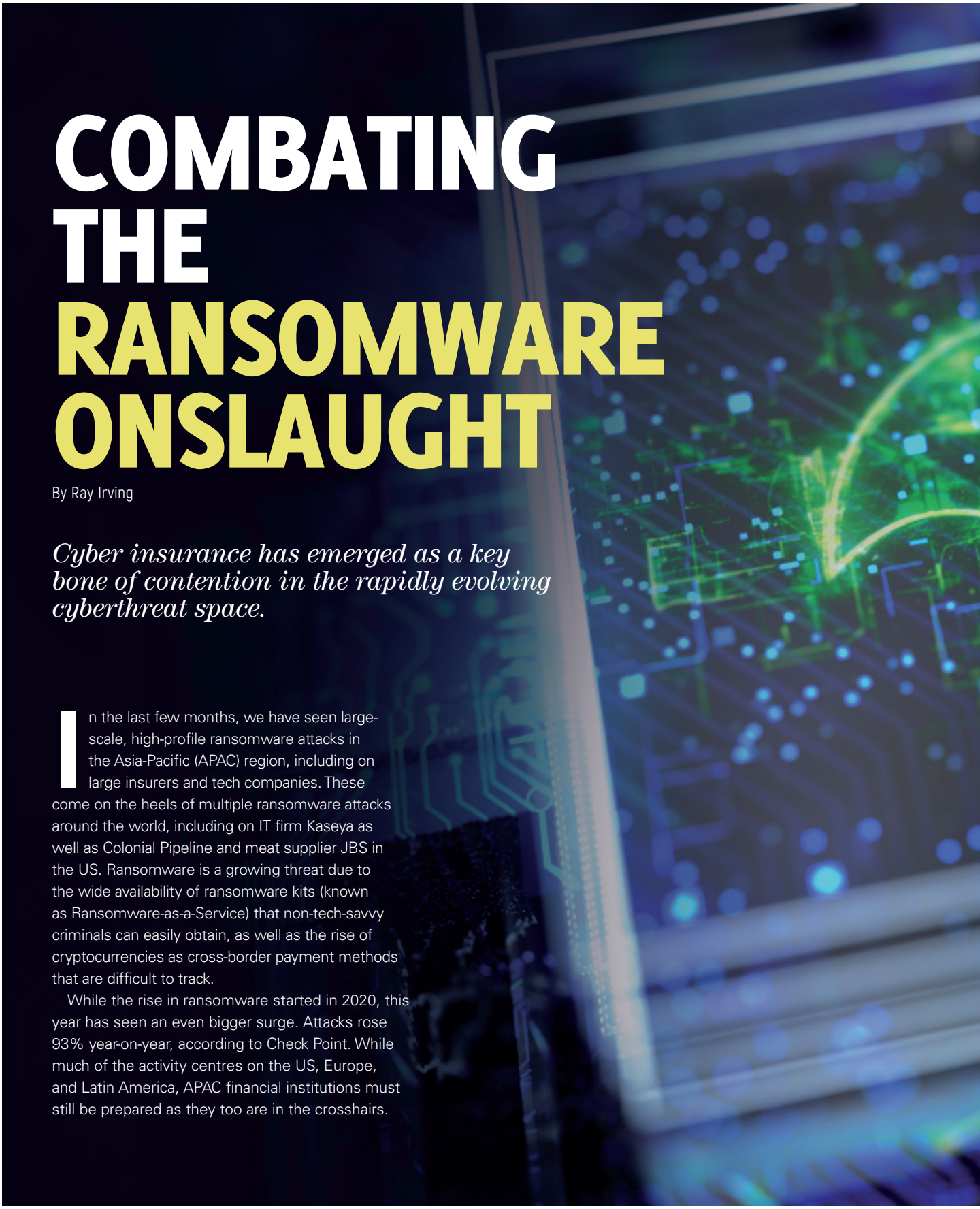
SUCCESSFUL TEAMS MUST BANISH SELF-DOUBT

AGILE MUST EVOLVE OR DIE

A PUBLICATION OF

AICB
ASIAN INSTITUTE OF CHARTERED BANKERS

ISSN 2231-6264



COMBATING THE RANSOMWARE ONSLAUGHT

By Ray Irving

Cyber insurance has emerged as a key bone of contention in the rapidly evolving cyberthreat space.

In the last few months, we have seen large-scale, high-profile ransomware attacks in the Asia-Pacific (APAC) region, including on large insurers and tech companies. These come on the heels of multiple ransomware attacks around the world, including on IT firm Kaseya as well as Colonial Pipeline and meat supplier JBS in the US. Ransomware is a growing threat due to the wide availability of ransomware kits (known as Ransomware-as-a-Service) that non-tech-savvy criminals can easily obtain, as well as the rise of cryptocurrencies as cross-border payment methods that are difficult to track.

While the rise in ransomware started in 2020, this year has seen an even bigger surge. Attacks rose 93% year-on-year, according to Check Point. While much of the activity centres on the US, Europe, and Latin America, APAC financial institutions must still be prepared as they too are in the crosshairs.

Ransomware criminals, knowing that many firms would rather their **INSURERS PAY QUICKLY AND QUIETLY TO AVOID OPERATIONAL DISRUPTION AND REPUTATIONAL DAMAGE**, have increased their demands substantially. Ransomware gangs such as Ryuk have publicly stated that they specifically target firms with cyber insurance.

According to Kaspersky, 635 (35%) out of 1,764 companies and individuals attacked in 2020 by REvil – a major Russian-based ransomware group – were from the APAC region.

CYBER INSURANCE: IN THE EYE OF THE STORM

Insurers are especially juicy targets for cybercriminals because of the possibility of also accessing customer data, including around limits for cyber insurance policies. Cyber insurance has been on the rise over the last several years, but the explosion of ransomware has meant that many firms turn to their policies to pay out ransoms rather than look for alternative methods of dealing with an attack. Ransomware criminals, knowing that many firms would rather their insurers pay quickly and quietly to avoid operational disruption and reputational damage, have increased their demands substantially. Ransomware gangs such as Ryuk have publicly stated that they specifically target firms with cyber insurance.

As more firms and institutions rely on cyber insurance to insulate themselves from cyber risk, opportunistic cybercriminals have quickly realised that cyber insurers are now attractive targets themselves. By hacking and accessing an insurance company's policy data, cybercriminals can curate a list of ransom demands according to each victim's policy and business profile. They can therefore multiply their return on investment for one attack by targeting both the insurer and their customers.

The Banking Insight publication is exclusive to AICB members.

Kindly log in to AICB's Member Portal to read the full publication, or send us an email at enquiries@aicb.org.my to request for a copy.