

Strengthening cyber resilience in banking industry

Focus Malaysia 06 Sep 2018 16:39

Leading banking industry leaders, regional regulators and cybersecurity experts gathered today at the Asian Institute of Chartered Bankers' (AICB) Cyber Resilience Conference 2018 themed "Powering the Winds of Change: The Shift to Cyber Resilience", at Sasana Kijang, Bank Negara Malaysia.

As part of AICB's thought leadership initiative towards building a more competent and professional banking workforce, the conference served as a high-level forum to exchange ideas and discuss emerging cybersecurity trends and cyberthreats, as well as create greater awareness on the critical importance of collaboratively building stronger cyber resilience for the banking sector.

The conference attracted over 200 participants from the region and featured a stellar line-up of over 30 eminent local and international speakers from the public and private sectors, including regional regulators, banks, fintechs and cybersecurity organisations. Among the distinguished speakers included James Allman-Talbot, the Global Head of Cyber Incident Response at BAE Systems Applied Intelligence, UK; Mary Jo Schrade, Assistant General Counsel, Microsoft Operations, Singapore; Brian Hansen, Intelligence Officer For Asia-Pacific, Financial Services Information Sharing and Analysis Center (FS-ISAC), Singapore; Thomas Beretti, Member Of Secretariat, Basel Committee on Banking Supervision, Bank For International Settlements, Switzerland; Kevin Lau, Head of International Risk, Ant Financial, China and Rob McMillan, Research Director, Gartner, Australia.

AICB Chief Executive Prasad Padmanaban said: "In an integrated financial sector with rapid technological advancements, it is not unexpected that cyberattacks are on the rise. Based on AICB's cyber resilience survey findings, over 70% of Malaysian banks still rely on their existing IT security or IT operations to perform cybersecurity-related functions and responsibilities. This indicates that cyber risks are still largely seen as an IT risk, not a business one. Therefore, there is a need to create a greater awareness on cyber resilience for the banking sector."

He added that the Cyber Resilience Conference 2018 was a key feature under AICB's Global Banking Discourse Series initiative, which offers AICB members and industry participants an opportunity to engage with international cyber experts and thought leaders to further enhance their professional knowledge, share experiences and learn about various developments taking place in the new cyberthreat landscape.

At the event, AICB also launched a thought leadership and survey publication entitled *Building a Cyber Resilient Financial Institution – Are You Ready for the Imminent Breach?*, developed in collaboration with PwC Malaysia. The publication aims to provide greater insight and awareness on the state-of-play in the domestic and global landscape of cybersecurity, with a strong focus on the shift towards cyber

resilience and what it means for businesses as they reshape their strategies to be fit and ready for the future.

PwC Malaysia Partner and Digital Trust & Security Leader Tan Cheng Yeong said: "Building cyber resilience is about enabling all lines of defence to be ready to withstand cyber threats as they continue to evolve, and to recover from inevitable cyberattacks. Critically, banks need to strengthen their cybersecurity posture by building a threat-led cyber risk management programme and advocating for better reporting of cybersecurity metrics.

But 58% of Board Members from the Malaysian banks surveyed indicated that the reporting of cybersecurity matters is still predominantly done by the CIO or CTO. For any transformation initiative to be successful, the responsibility lies with boards to push for a shift in mindset.

Boards also need to give their full backing to cyber stress testing programmes so that companies have a clearer understanding of their defence capabilities, giving them the opportunity to plug any gaps before an attack occurs. Without the right tone from the top setting the foundation for trust, you'll be hard-pressed to build cyber resilience effectively."

Other substantive areas discussed at the conference included key issues and challenges of cyber risk, global regulatory developments, best practices and international standards of cyber risk management, and how financial institutions can further strengthen collaboration to sustain cyber resilience. Speakers also shared insights into the latest skills and scenarios, particularly on hacking techniques and cyberattack methodologies.