ASIAN INSTITUTE OF CHARTERED BANKERS

pwc

BUILDING A CYBER RESILIENT FINANCIAL INSTITUTION

Are you ready for the **imminent breach?**

KEY FINDINGS

The concerns

As businesses operate in an increasingly digital world, technology underlies many innovative activities and, by extension, opens the door to greater cyber risks.

92%
Local

82%
Global

- 92% of Board Members of Malaysian banks believe cyberthreats are very likely to modify their business strategy in the next 3 years. Globally, 82% of Board Members interviewed shared similar views.*

Ranked #1 concern

- Based on PwC's *21st CEO Survey 2018*, cyberthreats are ranked as the #1 concern by CEOs of banks, where 89% believe that cyberthreats will impact the organisation's growth prospects.

89%

The problem: Security, not resilience

While information security risks have dramatically evolved over the past few decades, the approach used by financial institutions to manage them has not kept pace. Cyber risks are still largely seen as an IT risk and not a business risk:

>70%

- More than 70% of Malaysian banks still rely on their existing IT security or IT operations to perform cybersecurity-related functions and responsibilities.

58%

- 58% of Board Members from Malaysian banks indicate that the reporting of cybersecurity matters is still predominantly performed by the CIO or CTO.

What needs to be done

More emphasis on the following areas is required for banks to strengthen their organisations' resilience towards the imminent breach. This includes:

- Building a threat-led cyber risk management programme
- Cultivating a culture of sharing and collaboration
- Stress testing your cybersecurity defence
- Getting the basics right

** PwC's 2017 Annual Corporate Directors Survey*

CONTENTS

FOREWORD

The Asian Institute of Chartered Bankers (AICB) is the professional body for the banking industry and has been championing the vision of professionalising bankers by upholding the standards of excellence for the banking sector and empowering its workforce through the systematic transfer of knowledge and qualifications. AICB continuously promotes thought leadership through various platforms and collaborative initiatives to ensure members are kept abreast of current issues affecting the banking industry.

In line with this, AICB — in collaboration with PwC Malaysia — has jointly developed this thought leadership publication ***Building a Cyber Resilient Financial Institution: Are you ready for the imminent breach?***, to provide greater insight and awareness into the state-of-play in the domestic banking industry vis-à-vis the multi-faceted nature of cybersecurity, the shift towards cyber resilience and what it means for businesses as they reshape their strategies to be fit and ready for the future.

As cyberattacks become the "new normal", it has become imperative that financial institutions strengthen their vigilance and diligence in the area of cyber risk management and explore new approaches to build greater cyber resilience within their organisations.

Not just another cybersecurity publication

Undoubtedly, there is no shortage of literature on cybersecurity in the public domain. However, the proliferation of cybersecurity-related events in recent times has revealed that traditional defence approaches are no longer sufficient. It is evident that organisations need to fill the gaps in awareness and education pertaining to cybersecurity. To effect a positive change, organisations must assess their digital risks and focus on strengthening their cyber resilience to face the inevitable: A digital landscape replete with the constant threat of cyberattacks.

As cyberattacks become the 'new normal', it has become imperative that financial institutions strengthen their vigilance and diligence in the area of cyber risk management and explore new approaches to build greater cyber resilience within their organisations.

FOREWORD

Presently, there is much information to assimilate and many proven strategies that can be adopted by organisations to ensure data security. But the danger of taking a mere information-security approach to addressing cybersecurity risks lies in the fact that organisations tend to neglect reviewing their risk profiles upon full implementation of a technology and more often than not, are likely to employ extemporary safeguard measures. This approach to technology adoption is both reactive and ineffective.

By promoting an inclusive cyber resilience approach and a long-term cyber strategy, this enables a continuous collaboration between the technology and strategy leaders within an organisation. A cyber resilience approach will ensure greater preparedness and less repetition, which will ultimately lead to a more efficient and effective strategy overall.

Prasad Padmanaban
AICB Chief Executive

Why "resilience" and not "security"?

Security, in contrast to resilience, can be seen as binary. Either something is secure or it isn't. It is often relegated to a single, limited technical function, keeping unauthorised users out of a networked system.[1]

While there are many broader definitions of cybersecurity, there is a difference between the access control of cybersecurity and the more strategic, long-term thinking cyber resilience should evoke.[2] Building resilience is about enabling your organisation to withstand and quickly recover from cyber attacks that disrupt usual business operations.

This publication presents insights to assist the Malaysian banking sector in building cyber resilience, drawing from global industry best practices and supplemented by our Survey results and interviews with C-Suites and other top management figures. As disruption continues to reshape this sector, the ability to address vulnerabilities head-on in combating cybersecurity threats will be increasingly valued.

We hope this publication provides you with an informative read and is instrumental in helping your organisation stay resilient against rising cybersecurity threats.

Tan Cheng Yeong
Partner and Digital Trust & Security Leader, PwC Malaysia

[1, 2] World Economic Forum (2016), "Cyber resilience: everything you (really) need to know", accessed 28 August 2018, https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know/