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/

01

SLEEPLESS OVER CYBERTHREATS

CYBERSECURITY BREACHES: A QUESTION OF "WHEN", NOT "IF"

In the face of digital disruption, banks are spurred on to catch the FinTech wave by making substantial investments in their digital transformation journey as a competitive edge to deliver greater customer experience.

Trust has always been a core foundational value for banks in delivering their services, a big part of which includes ensuring the safety and security of customer assets. But the security of financial institutions has now come under immense threat, judging from the many high profile reports of reputable and trusted multinational and local banks falling prey to cybercriminals, both internally and externally.

Operating in a supercharged digital deployment environment and a heightened cyberthreat landscape, it is hardly surprising that most banks rank cyber risk as among their top risks.

As banks embark on their digital transformation initiatives to remain relevant and competitive in this new era of digital disruption, cyber and technology risks are among the top risks in the Board agenda.

Ong Ai Lin

Independent Non-Executive Director, RHB Bank Berhad

Aug 2014
A US investment bank fell victim to one of the largest thefts of customer data in history, resulting in a total estimated loss of **RM4 billion**

Aug 2018
Mexico's central bank announced that hackers siphoned approximately **RM650 million** from five companies through fraudulent transactions

Nov 2016
Customer accounts of UK banks were compromised, resulting in a total loss of approximately **RM10 million**

Oct 2016
Banks in India suffered one of the largest data breaches, resulting in the debit card information of an estimated **3.2 million** individuals being compromised

Mar 2017
A bank in India lost approximately **RM14 million** due to a bug in the Unified Payments Interface (UPI) system, which enabled users to transfer funds illegally

Aug 2018
A bank in India was hacked, resulting in fraudulent bank transfers worth **RM8.2 million**, and unauthorised ATM withdrawals worth **RM47.2 million** from cash machines

Feb 2016
SWIFT, a secure financial messaging service, was compromised when hackers initiated a legitimate instruction to transfer approximately **RM320 million** from Bangladesh

Oct 2017
Hackers took approximately **RM240 million** from a Taiwanese bank in a SWIFT attack

Sept 2014
Malaysian banks' ATM machines were hacked, with total losses amounting to approximately **RM1.2 million**

Jul 2017
Hackers launched multiple DDoS attacks on several Malaysian online brokerages, resulting in the disruption of stock trading for 2 hours

Mar 2018
Malaysia's central bank detected a cybersecurity incident involving unauthorised fund transfers using falsified SWIFT messages

Drivers of cyberthreats and their impact

Factors driving cyberthreats

Technological change

75% attributed it to the speed of technological change

Digitisation

59% say digitisation of the business ecosystem has impacted security spending

Impact of cyberthreats

Stakeholder trust

91% of top CEOs believe stakeholder trust will be negatively impacted by cybersecurity breaches in business information or critical systems within the next 5 years

Business strategy

92% of Board Members in Malaysian banks think that cyberthreats are very likely to modify their business strategy in the next 3 years

BUILDING RESILIENCE: THE WORK CONTINUES

The interconnectedness of digital ecosystems and the threats they pose are driving changes in cybersecurity. Technological advancements are also prompting regulatory changes globally. As a result, more resources and investments are being channelled towards cybersecurity to strengthen banks' security defences.

While banks generally feel there is a significant increase in regulatory focus on cyberthreats, they are very clear that their security response strategy is not driven merely to comply with regulatory demands.

What is interesting, however, is that a majority believe there is still much to be done. Among our respondents, many of their existing efforts have not yet addressed the worries and concerns of the Board as it relates to their organisation's cybersecurity posture.

Survey response from Board Members

17%*

Very comfortable that management has adequately tested resistance towards cyberattacks

8%*

Very comfortable that cyber incident response plans have been adequately tested

75%

Somewhat comfortable with the current reporting metrics on cybersecurity from their management. Of this percentage, 44% are from foreign banks that mainly leverage their global resources

17%

Do not feel comfortable at all with how their current management is reporting to them on cybersecurity risk faced by the organisation

** All respondents from foreign banks*

CYBER RESILIENCE: A BUSINESS ISSUE, NOT "AN IT THING"

The belief that cybersecurity is "an IT thing" is a common misconception that increases an organisation's potential exposure to attacks and widens the gap between those charged with protecting the enterprise and those whose obligations include maintaining strong corporate governance and ensuring good shareholder returns.

While the financial services industry has become more responsive to cyber risks than other industries, financial institutions still have a great deal of work to do to become cyber resilient.

Larger banks have, for some time now, viewed cyber risk as an issue that goes beyond just the IT department. However, many have yet to elevate the status of cyber risk to a major risk category, e.g. credit or market risk, or to actively involve their senior management and Boards in cyber risk management.

>70%

More than **70%** of banks are still relying on their existing IT security or IT operations to perform cybersecurity-related functions and responsibilities

58%

58% of Board Members indicate that reporting of cybersecurity matters are still predominantly performed by the CIO or CTO

Clearly, there's a gap — one that can be filled by a proper cyber risk management approach, designed to build cyber resilience. An organisation's systems and operations need to be designed to detect cyberthreats and respond to cyber events to minimise business disruption and financial losses.

02

TAKING ACTION

BUILDING CYBER RESILIENCE

The case for change

While information-security risks have dramatically evolved over the past few decades, the approach that financial institutions use to manage them has not kept pace. Take, for instance, the traditional information-security model that many banks use – it is typically controls- and compliance-based, perimeter-oriented, and aimed at securing data and the back office, which do not necessarily address the realities of today.

Banks need to view cybersecurity issues from a holistic risk-management perspective. Staying resilient starts with knowing your threats, and it involves the whole organisation staying alert and responding in a concerted manner. Banks need to be agile and adapt quickly as the cyber risk landscape is changing.

Michael Guenther

Head of Risk, Malaysia, Deutsche Bank

Objectives

The ultimate objective of cyber risk management is to build cyber resiliency, where an organisation's systems and operations are designed to detect cyberthreats and respond to cyber events to minimise business disruption and financial losses.

While this doesn't eliminate cyber risks, it allows banks to stay ahead of those risks through an informed decision-making process.

Building it

Building a robust cyber risk management programme is a complex process involving many components of your overall business risk environment. It requires executive management engagement, on-going governance, risk management techniques, threat correlation, collaboration throughout the organisation, and adoption of a new business operating model.

Who it involves

Being cyber resilient is really a question of strategy rather than tactics. It requires those at the highest levels of a company, organisation or government to recognise the importance of avoiding and mitigating risks. While it is everyone's responsibility to cooperate to ensure greater cyber resilience, leaders who set the strategy for an organisation are ultimately responsible, and have increasingly been held accountable for including cyber resilience in the organisational strategy.

HAVING A PLAN TO CUSHION THE FALL

Banks are ever more vulnerable to incoming cybersecurity threats from new directions and adversaries. Attacks in the form of “hacktivism”, corporate espionage, insider and nation-state threats, terrorism, and criminal activity can cost an organisation time, resources, and irreparable harm to its reputation.

The information-security environment continues to change, hence the need for banks to ensure that their cyber risk strategies address the following matters:

- **Highly skilled, elusive threat actors — not just external actors, but also among employees**
- **Cyber campaigns that are scalable and easy to customise, and**
- **A complex and evolving digital environment.**

These preparations are crucial to becoming cyber resilient. They can help banks to keep pace with evolving threats, enabling them to avoid financial damage, negative publicity, and loss of customer trust.

THE NEED FOR BOARDS TO BE MORE INVOLVED IN CYBER RISK MANAGEMENT

The executive team should lead the transformation, moving their security programme from one that is reactive and sporadic to one of cyber resiliency. This means taking ownership of cyber risk at the executive level to avoid potential damage to a financial institution's bottom line, reputation, brand, and intellectual property. Specifically, they should collaborate upfront to understand how the institution will defend against and respond to cyber risks, and what it will take to make their organisation cyber resilient.

Leading banks are transforming their organisations from ones that are centred on security and technology, to ones that employ an approach that combines the two with business management, risk disciplines, and cyberthreat expertise. By becoming cyber resilient, banks will be able to plan for, and mitigate cyber risks according to its appetite to withstand disruption and bounce back quickly.

03

BREAKING IT DOWN TO THE **BASICS**

Insights from our study highlight the need for banks to have an effective **risk-driven function** that is situation-aware, intelligence-driven — with timely response to a rapidly changing threat landscape – and agile and quick in recovering from an attack.

This study highlighted several key themes on which banks should focus in building cyber resilience:

STRENGTHENING CYBER RISK GOVERNANCE

The foundation of a strong cyber-resilient organisation is a governance process for managing risk. It starts with the tone from the top.

Among the respondents, the majority of banks believe the "Full Board" has primary responsibility for overseeing cybersecurity risks, and challenging management's assumptions.

Who on the Board is Primarily Responsible for Overseeing Cybersecurity Risks

Full Board
40%

Risk Management Committee
30%

Audit Committee
10%

IT Committee
10%

Other committees
10%

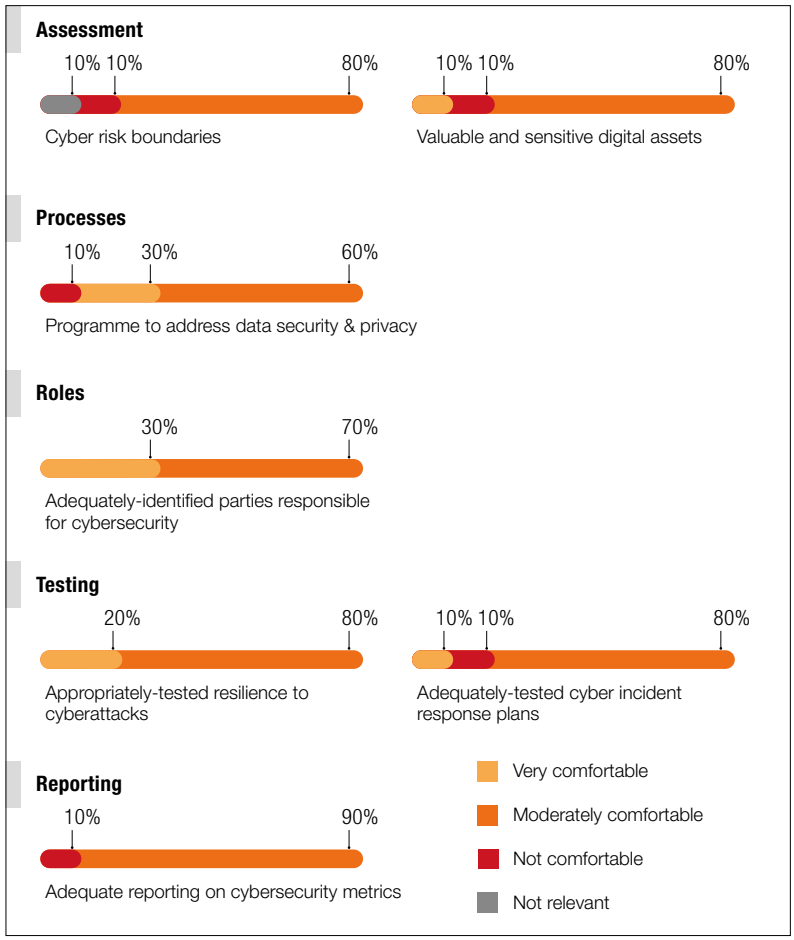
Spending more quality time with the Board

A good governance process is designed to provide visibility to senior management and the Board. In Malaysia, more than 70% of Board respondents rated their management's cybersecurity strategy as fairly effective.

Management also indicated that from their perspective, their Boards actively participate in the areas of overall security strategy, security policies and review of current security and privacy risks. However, many of them indicated that not enough time is spent on deliberating and managing cyber risks.

Board Members want more focused discussions on managing cyber risk before they can feel comfortable that enough is being done in this area.

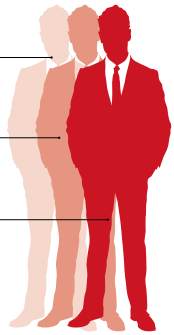
FOCUS AREAS OF CONCERN FOR BOARDS



STRENGTHENING CYBER RISK GOVERNANCE

Board-level capabilities

Boards are expected to assume greater responsibility for ensuring an organisation's cyber resilience. Our study revealed that directors recognise a clear need for more cybersecurity capabilities on their Boards.



10%
say they have it

20%
say they don't have it

70%
believe they have some capabilities, but require more

For some, the answer lies in recruiting a director with technology-related skills. For others, they may look for other ways to close any present gaps, such as implementing continuing education and engaging external advisors to supplement the capabilities gap.

Embedding security and control features into the new products and services being offered and ensuring that all new products developed are subject to rigorous system development, testing and business continuity standards require new skills, both at senior management and Board level.

Ong Ai Lin

Independent Non-Executive Director, RHB Bank Berhad

IMPLEMENTING A THREAT-LED CYBER RISK MANAGEMENT PROGRAMME

In dealing with cybercrime, one must start by understanding threats present in the context of the banking environment. Multinational banks have greater leverage on their global investments in cyberthreat analytics to stay ahead of the game.

Lee Lung Nien
Chief Executive Officer, Citibank Berhad

Knowing yourself, knowing your enemies

Similar to warfare, having information on an enemy's plans gives you a tactical advantage when developing a defensive/offensive strategy. Similarly, "threat intelligence" provides first-hand knowledge on the Tactics, Techniques and Procedures (TTP) of adversaries, giving banks insights on where to station the "bricks and cannons" when fighting cybercriminals.

Today, most business leaders know that they are responsible for cybersecurity and privacy threats, wherever they occur in disparate enterprise systems. What many do not understand is how to design, implement and manage a real time threat intelligence and information-sharing programme.

Know yourself

Threat intelligence is not just a feed for tactical response — it must be worked into your risk defence strategy

Knowing the tactics of your adversaries is just a start. Banks need to understand how these tactics can be used against them and be able to identify which part of the organisation is at risk.

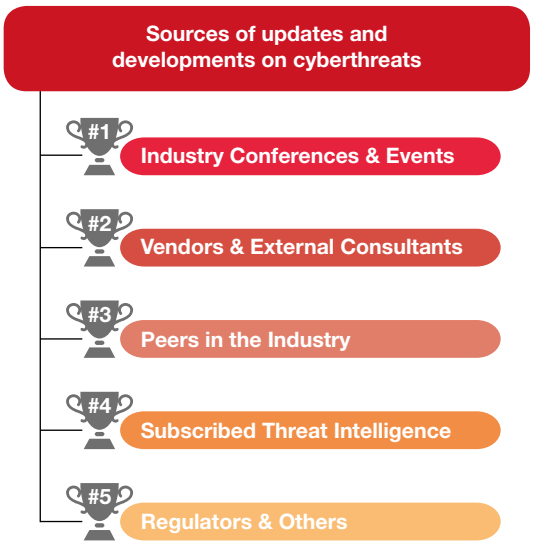
Since cyber resilience is really a matter of risk management, there isn't a single point at which it begins or ends. Instead, it comes from building strategy and working to ensure the risk transfer mechanisms that work for more traditional threats are also leveraged for new cyberthreats.

IMPLEMENTING A THREAT-LED CYBER RISK MANAGEMENT PROGRAMME

Know your enemies

While banks are generally reaching out to keep themselves up-to-date on cyberthreats, they tend to rely on generic industry conferences and their vendors as sources of information, as opposed to sources specific to them, i.e. from other financial institutions as well as their own threat intelligence.

When asked "Where do you normally obtain sources of updates and developments on cyberthreats?", our survey respondents replied:

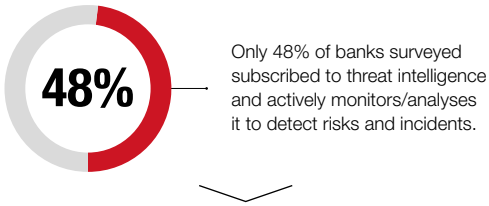


Staying ahead

Banks need to strive for a threat-led cyber risk management programme that covers four key areas:

- The ability to extract and digest meaningful, validated intelligence in real time.
- The ability to assess the organisational impact of that intelligence concurrently.
- The ability to identify specific actions to mitigate threats.
- Capabilities to take prompt technical, legal and operational actions.

Our survey results demonstrate a clear need for banks to focus on building a threat-led cyber risk management programme:



Of that 48%, the majority (60%) come from IT while less than 40% come from Risk and Compliance. There is room for banks' second line of defence to greatly leverage threat intelligence to embed it into overall risk treatment strategies.

Building a cyber risk management programme requires banks to have access to deep cybersecurity expertise as well as a multidisciplinary team that includes stakeholders from IT, legal counsel, risk, privacy and business units. This team can then be responsible for creating customised processes to integrate activities across systems and the bank.

KNOWING YOUR RISK BOUNDARIES

Decades ago, the cyber risk perimeter for banks was limited to the data centre. Such perimeters have since expanded to include third-party service providers that are integrated into the bank's supply chain. Today, banks are also partnering with FinTech players who co-exist within the same banking value chain. This means banks will need to consider the security risk exposure for their extended boundaries. For example, API endpoints that are left unsecured at customer touchpoints by business partners can be a source for data breaches.

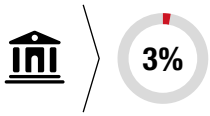
50% of respondents stated that they do share sensitive customer data with outsourced service providers.

Know your partners

Leading international banks already have established risk-based compliance programmes to continuously assess their outsourced service providers. This allows banks to know the security risks to which they are exposed on account of their business partners. Boards should understand how their banks select, vet and monitor third parties, as well as how these parties protect the company's sensitive information.

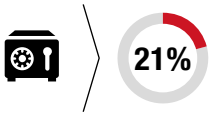
Local banks are lagging behind when dealing with third-party risks

When asked how often banks perform a review of their service providers, the majority of respondents indicated that they do this on an annual basis.



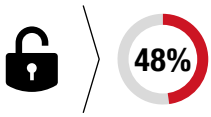
With only 3% of respondents adopting a risk-based approach when deciding on the frequency of the review.

Such practices are driven by lower third-party-related incidences for banks in Malaysia.



Only 21% of respondents quoted third parties as a source of security incidents in the last 12 months. Meanwhile, the survey also revealed that 34% of respondents do not know the root causes of their security incidences.

By contrast, incidents related to compromised third parties were recorded as one of the top security incidents by the financial services respondents in PwC's *Global State of Information Security Survey (GSISS) 2018*.



About half (48%) of the financial services respondents from GSISS 2018 indicated that their security incidents in the last 12 months were attributed to third parties, including service providers, contractors and vendors.

Being unprepared for such risks is a ticking time bomb that banks have to grapple with.

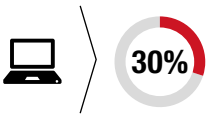
80% of Board respondents indicated being "moderately comfortable", while 10% are "not comfortable", that banks have identified all the parties that may attack a company's digital assets.

KNOWING YOUR RISK BOUNDARIES

Know your employees

The threat within

Banks need to also consider third-party risk in the context of contractors and temporary staff. The threat of crimes such as insider trading, theft, and cyber vandalism being committed by internal sources is real and on the rise.



Current employees remain the top source of security incidents. 30% of respondents from PwC's *Global State of Information Security Survey 2018* attributed the cause of their security incidents to insiders.

The survey also highlighted that the statistics of findings on insiders — third parties that include suppliers, consultants, contractors and employees — have stayed the same or increased over the last 12 months. Interestingly, incidents attributed to hackers, competitors and other outsiders have declined.

When banks bring onboard contractors and temporary workers, they may be handing over more than just a security badge. There is a need for banks to emphasise internal risk analysis, both to protect against nefarious behaviour and identify workers who may have been unknowingly compromised. Some leading global banks have already invested in advanced risk-based data analytics to look into employee behavioural patterns as a precaution and defence mechanism.

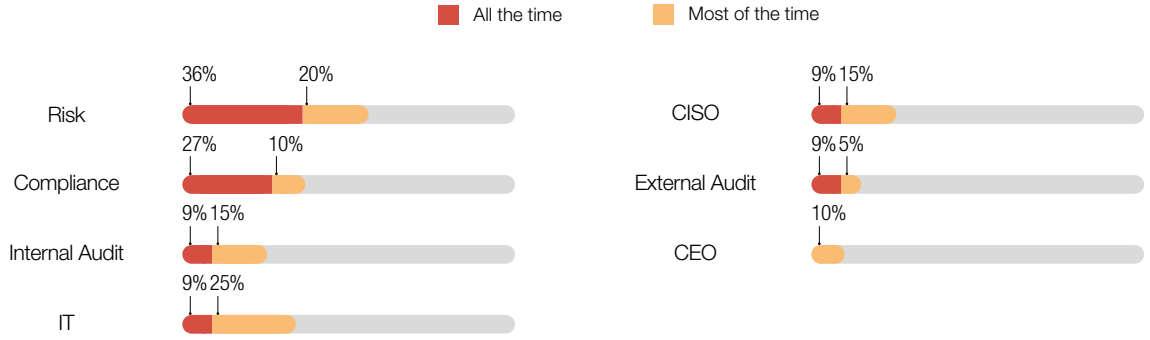
STRENGTHENING YOUR SECOND LINE OF DEFENCE

Technology has always been the go-to function for the first line of defence when it comes to cybersecurity issues. To more effectively manage cyber risk and be cyber resilient, leading banks have been strengthening their governance and management of this top strategic risk by beefing up their second line of defence.

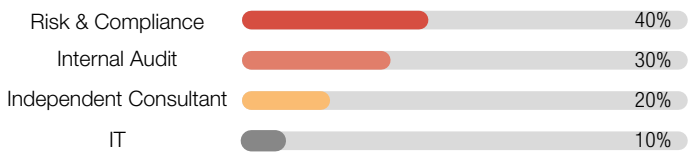
Banks are generally aware of the importance of building an effective second line of defence for cyber risk management.

- **Most of the time, Board Directors look to their second line of defence to keep them abreast of cybersecurity matters**

Reports to the Board on matters relating to cybersecurity



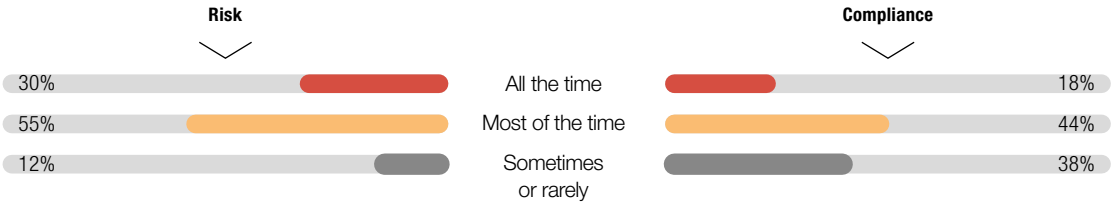
How do Boards know whether the bank's controls and processes are working?



Many risk and compliance functions are expected to provide effective oversight and credible challenge amid the lack of skills and resources necessary to understand cybersecurity practices and techniques, which is a common issue in banks.

- **The role of the second line in strengthening cybersecurity**

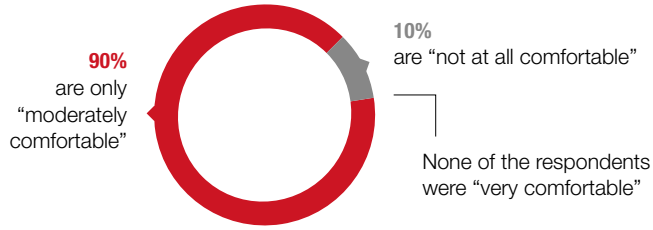
The majority of C-Suite respondents believe their second line of defence can play a greater role in helping to strengthen cybersecurity.



STRENGTHENING YOUR SECOND LINE OF DEFENCE

- **Boards expect better reporting on cybersecurity metrics**

  The majority of Board respondents believe there is room for improvement in reports received on cybersecurity metrics.



Managing cyber risk — a holistic approach

A cyber risk management function is a key component of an enterprise risk management programme. It enables cyber risks to be managed through an informed decision-making process.

Step 1 — Explicitly embed cyber risk management considerations into existing core risk management processes

- Embed cyber risk policies and standards into existing risk governance and oversight framework
- Identify sources of threats and determine risk tolerance
- Embed risk processes to assess cyberthreats when establishing strategic business objectives and approving new products
- Develop risk control mitigation strategies
- Assess risk and monitor risk exposure continuously
- Report to executive management and the Board regularly and frequently
- Design and communicate training and awareness programmes

Step 2 — Enhance ongoing monitoring and reporting

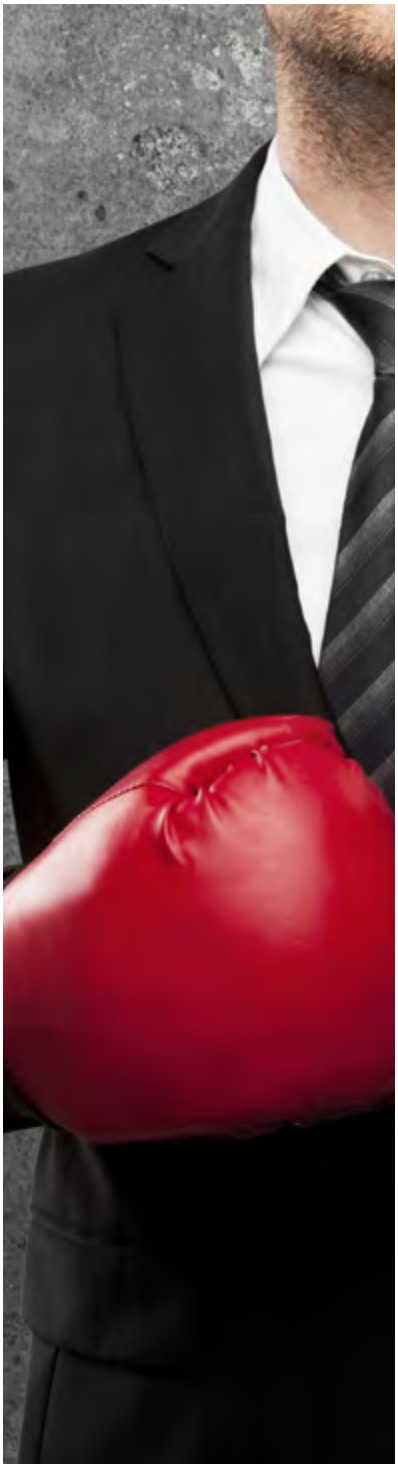
- Establish cyberthreat intelligence capabilities that are managed and overseen by the cyber risk operations team
- Continually gather and analyse cyberthreat data, focusing on internal and external insights on threats, vulnerabilities and control posture
- Communicate threat insights and risk exposure to the cyber risk management committee, which in turn ensures that the necessary risk control decisions are made
- Ensure that decisions on adjustments to the risk and control posture are implemented in line with specific threat information and risk control thresholds

Step 3 — Implement threat playbooks and scenario rehearsals

- Identify cyberthreat scenarios
- Document incident response plans
- Conduct ongoing simulation and rehearsals

PwC, Enhancing business resilience: Transforming cyber risk management through the role of the Chief Risk Officer (CRO), 2015

PERFORMING STRESS TESTING



It pays to be prepared

Banks — through their risk management functions — have set a firm foundation to robustly stress test their credit risk, market risk and liquidity risk. Similarly, the idea behind cyber stress testing as part of operational risk is to determine the critical systems, people and locations needed to continue serving customers, and identify how best to protect and recover them.

This requires banks to:

- Understand the threats relevant to them
- Translate the threats into risks
- Formulate scenarios to "stress test" their risk mitigation measures
- Quantify the value at risk
- Focus and channel their security spending

This scenario-based analysis and testing can help provide banks with the information it needs to adjust risk profiles and response plans to create a more resilient organisation.

A growing priority for banks

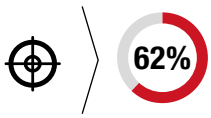
With regulators placing more emphasis on being cyber resilient, cyber crisis simulations have made it into banks' business continuity plans.

94% of respondents indicated having included cyberattack scenarios into their business continuity programme and performed a "table-top" exercise.

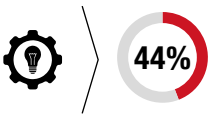
PERFORMING STRESS TESTING

Build a Red Team exercise into your cyber stress testing programme

Penetration testing has also become the norm in local banks' security functions. Globally, many multinational banks already have more sophisticated threat-led scenario-based cyber stress testing programmes built into their risk management plans. Among the many benefits of stress testing programmes include the ability to simulate a realistic threat, linking it to the risks, and identifying the gaps in their mitigation measures to formulate a more targeted cyber resilience plan.



62% of respondents ranked penetration testing and vulnerability assessment among the top 3 in terms of security spending.



44% of respondents indicated that they have not considered any "stress testing" using the Red Team exercise, or ranked such an exercise among the lowest 3 in terms of security spending.

WHAT IS A "RED TEAM"?

Red Team is a military term akin to a friendly war game between two countries to simulate "attack" and "defend" scenarios. The aim is to play out the "attacker" scenario to identify weaknesses within and across the organisation, and learn from it. The concept has made its way into the corporate world.

When used in cybersecurity, Red Team is a process designed to detect network and system vulnerabilities and test security strength by taking an attacker-like approach to system/network/data access. Their role is to emulate the behaviours and techniques of likely attackers to make it as realistic as possible.

The benefit is that the organisation will obtain a more realistic idea of their true defence capabilities by seeing how their security teams react to the simulation without preparation. The ultimate aim of such a test is to assess an organisation's security maturity as well as its ability to detect and respond to an attack.

It is believed that playing the role of an attacker can make your team better at defence.

PERFORMING STRESS TESTING

Security spending is not risk-based

Security spending is still primarily driven by compliance and regulatory requirements. There is an opportunity for banks to have a longer-term strategic risk-based investment in security as they will then be better positioned to handle threats.

$

40% 40% of respondents indicated that their security spending is driven by compliance and regulatory requirements.

59% 59% indicated that their cybersecurity spending is not exclusively risk-based. (For those that agree that their spending is based exclusively on risk, 60% are foreign banks and 40% are local banks.)

43% Additionally, 43% of respondents (out of which 38% are foreign banks and 62% are local banks) indicated that most of their security budget is used for security infrastructure.

PERFORMING STRESS TESTING

Let's not forget that it all starts with good basic cyber hygiene

When cyber forensics experts are engaged to investigate cyber breach incidents, the findings often revolve around the need for better basic cyber hygiene, which includes good password practices, timely patch managements and updated software.

Cyber hygiene issues such as traditional software vulnerabilities were ranked #2 in the list of contributors of security incidents occurring in the last 12 months. By contrast, it was ranked the lowest contributor by the respondents of PwC's *Global State of Information Security Survey 2018*.

Banks need to put in place a robust risk-based cyber compliance programme that provides regular assurance reports on the state of their cyber health.

A lot of attacks would not have been successful if organisations had paid more attention to cyber hygiene. Cyber hygiene provides a solid foundation upon which organisations can anchor their cybersecurity programme. Banks should run up-to-state systems and maintain them current in terms of patches and cyber defence measures.

Yuen Ka Wei

CISO APAC Manager, Deutsche Bank

ENCOURAGING INDUSTRY SHARING AND COLLABORATION

New attacks, new ways of working

One thing seems certain: Cybercriminals do a very good job of networking to share technical knowledge, tools and methodologies. As cyberthreats become increasingly sophisticated, many organisations are taking a cue from their adversaries: They are sharing critical threat intelligence with business peers, industry groups and government agencies to collectively advance cybersecurity capabilities.

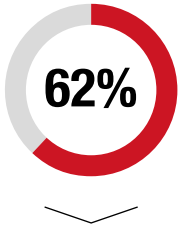
Leaders in the industry establish open communication channels between corporate security, information security, threat management and analysis, law enforcement coordination, intelligence agencies, fraud, and operational risk to facilitate timely sharing of threat information with the right people to help mitigate the impact of cyberattacks.

For example, in the UK, several large banks have formed the Cyber Defence Alliance to work with the UK National Cyber Crime Unit. This industry-government group aims to enable banks to swap timely information on cyberthreat intelligence and response techniques. One of the banks[3] has also dispatched an analyst to Interpol's cybersecurity investigations unit in Singapore.

"Rukun Tetangga" — joining forces to fight cybercrime

Like how most Malaysian households form neighbourhood associations to deal with domestic security issues, the concept of "Rukun Tetangga" can be applied to corporates in joining forces to fight cybercrime.

Such collaborations require banks, authorities and relevant agencies to work together in unity and solidarity, both at the national and international level. The key here is to share intelligence and knowledge gained from past attacks encountered.



In fact, **62%** of respondents stated that collaborations have significantly improved their security positions, whereas 81% believe that collaborations at the Government-to-Government (G2G) level will help improve an organisation's cyber resilience.

[3] *[Bloomberg, Nothing Brings Banks Together Like a Good Hack, 18 October 2016] [Financial Times, Banks join forces to crack down on fraudsters, 9 August 2017]*

ENCOURAGING INDUSTRY SHARING AND COLLABORATION

Strength in numbers

More importantly, when intelligence is shared, it is akin to forming an alliance among those who participate, thereby strengthening the cyber defence of the ecosystem. There is a need to embed such threat intelligence into cyber risk management programmes to give it a "scientific" and tactical element in addressing cyber risk.

Building cyber intelligence and collaboration, to me, is key. This has to happen both at national and international levels. Cybersecurity is not about 'us' anymore, it's the sum of us.

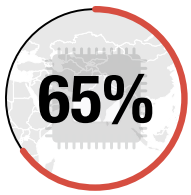
Mohd Suhail Amar Suresh Abdullah
Group Chief Technology Officer, Maybank Group

100% of respondents agreed that it is important to collaborate with others in the industry, including competitors, to improve security and reduce potential future risks.

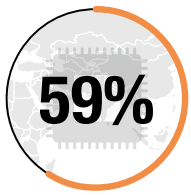
However, only **43%** of respondents indicated that current sharing and collaboration methods practiced within their organisation are sufficient to manage cyber risks.

The Achilles' heel of collaboration

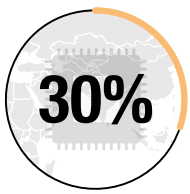
While industry practitioners understand the importance of sharing knowledge on threats and incidents across the industry, many are treading with caution, especially in sharing information on threats and lessons learned, fearing that if such information ends up in the wrong hands, it could expose their vulnerabilities and/or open them up to regulatory scrutiny.



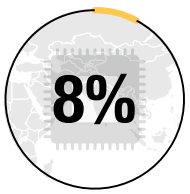
65% of respondents cited fear of disclosing system infrastructure vulnerabilities as one of the top challenges with regards to collaboration.



Meanwhile, 59% of respondents cited limited information-sharing platforms available as one of the main challenges.



30% stated that there is no commercial or business advantage from doing so, which may sometimes create a "free rider" problem.



8% cited other reasons, including banking secrecy rules, parent company policies and sensitivity of information.

Among those who share and collaborate, many have done so through industry networking sessions and chat group messages or informal forums. Not all banks participate in these informal forums.

BUILDING CAPABILITIES

A need to build stronger internal capabilities

Accurate intelligence helps build the right strategy for war. Well trained soldiers help you win a war.

It goes without saying that security capabilities are equally important when it comes to defending the organisation from cyberthreats. Banks realise that it is imperative to gather intelligence input from various functional teams to correlate external cyberthreats faced to the effectiveness of the internal controls, as well as simulate cyberwar games and threat scenarios to measure readiness.

- **A lack of security capabilities across all levels**
  Security capabilities are "rare gems" across all levels. Most banks have established an IT security function, which looks into the day-to-day security operations as required by the regulator, but that is insufficient.

  Today's cybercriminals are as savvy and professional as the businesses they attack. This maturity calls for a review of the bank's current security capabilities and training programmes.

  Based on the survey and interviews we conducted, cybersecurity talent is one of the key constraints in building cyber resilience. In fact, this issue is not specific to Malaysia as the industry faces a shortage of talent at a global level.

More than 56% of respondents agree that upskilling by pursuing advanced-level security certifications, e.g. CREST, OSCP, etc. is essential in building security capabilities, and they would encourage existing staff to do so.

Our neighbour, Singapore[4], also experiences similar challenges. Across all industries, a shortage of experienced professionals is especially acute in the following areas:

- Threat and vulnerability assessment
- Incident and crisis management
- Security management.

- **Automation — doing more with less**
  A cybersecurity talent shortage has arrived and is here to stay. Banks can either confront it or be left behind.

  In addition to implementing talent building and retention strategies, a cyber talent shortage is likely to spur financial institutions on to secure efficiency by focusing on the most important tasks and automating the manual ones, such as log reviews.

  Leading banks have invested in tools such as AI, machine learning and robotic process automation to complete manual repetitive tasks. Skilled team members can then be deployed to focus on high-value activities. Many organisations have reviewed their security job functions to identify what needs to be retained, instead of sourcing for specialists from vendors.

[4] *PwC, Unlocking The Cybersecurity Growth Potential: Singapore's Cybersecurity Industry Outlook, 2016*

CULTIVATING A CYBER RISK-AWARE CULTURE

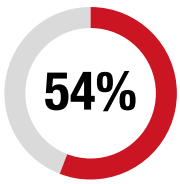
A relentless pursuit needed

The days of relying solely on the implementation of new security technologies as a cyber defence measure have passed. For any cyber strategy to be effective, it must be aligned with an organisation's business objectives, and sustained and enhanced by the right talent, leadership, culture, processes and technologies.

Without the right training, governance and tone from the top, even the most cutting-edge security technologies will be rendered ineffective.

- **Creating a cyber risk-aware culture**
  Cyberattacks can gain entry via any node on an organisation's network — it can start with a seemingly harmless email successfully grabbing the attention of one staff. Such attacks may even spread throughout the enterprise, affecting third-party suppliers, customers or business partners. This means that everyone involved in the organisation's cyber-linked activities has a role to play in ensuring the organisation's security, and that awareness of cyber risks must be an integral part of every decision and action taken.

Cyberattacks can gain entry via any node on an organisation's network — it can start with a seemingly harmless email successfully grabbing the attention of one staff.



54% of respondents attributed security incidents detected in the last 12 months to phishing.

- **Emplacing a targeted risk-based training programme**
  Businesses must ensure that they have a proper cybersecurity awareness programme in place to help employees identify common threats such as phishing, malware and ransomware.

Training and awareness programmes should be tailored to the organisation, as a one-size-fits-all approach is generally ineffective. A cybersecurity training programme that is fit-for-purpose and developed for a specific audience will drive risk-awareness deep into the organisational culture and create a strong defence mechanism capable of responding competently to security risks.

It starts from educating our employees and providing continuous training so they are more aware of the threats. We can't eliminate cyber risk, but we can at least try to minimise it.

Lee Lung Nien
Chief Executive Officer, Citibank Berhad

A strong cybersecurity culture, where employees are trained to act as the first line of defence, is an organisation's greatest asset and cybersecurity safeguard.

04

THE WAY FORWARD

A major takeaway from the report is the notion that improved cyber risk resilience can lead to stronger economic performance.

Banks of all sizes across all sectors and locations need to look inward, evaluate their approach to managing cyber risks and start focusing on becoming more cyber resilient.

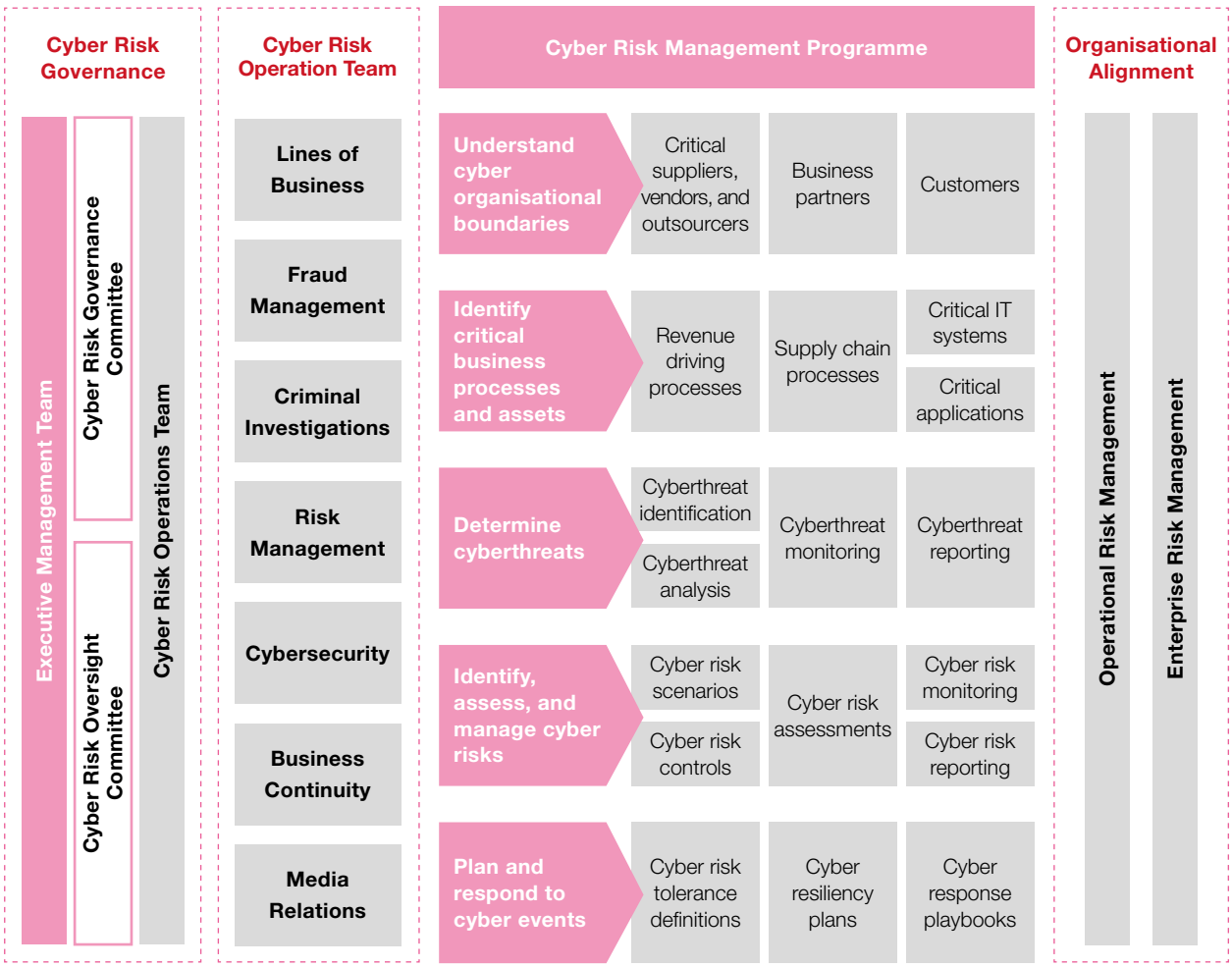
The need to foster a cyber risk culture and perceive cyber resilience as being a part of business operations has never been greater.

NO TIME TO WASTE

For those leading the charge to strengthen cyber resilience in their organisations, the task entails expanding their understanding of the business and sphere of influence and communicating clearly the existing and potential cyber risks in terms of business impact.

For CEOs and board directors, particularly, it means being fully engaged in the process, asking the tough questions and taking a closer look at the organisation's cyber risk management strategy and risk mitigation programme.

ROADMAP FOR BUILDING CYBER RESILIENCE



1. Define cyber risk management roles and responsibilities for your 1st, 2nd and 3rd line of defence.
2. Build capabilities across the organisation to strengthen your cyber risk governance.
3. Know your critical assets that need to be protected.
4. Ensure your cyber risk management programme addresses risks that extend beyond the organisation's physical boundaries.
5. Adopt a threat-led approach to improving your cyber risk management programme.
6. Introduce scenario-based simulated attacks to "stress test" your cyber defences and security controls.
7. Take the lead in collaborations and form alliances.
8. Cultivate a cyber risk-aware culture.

ABOUT THIS SURVEY

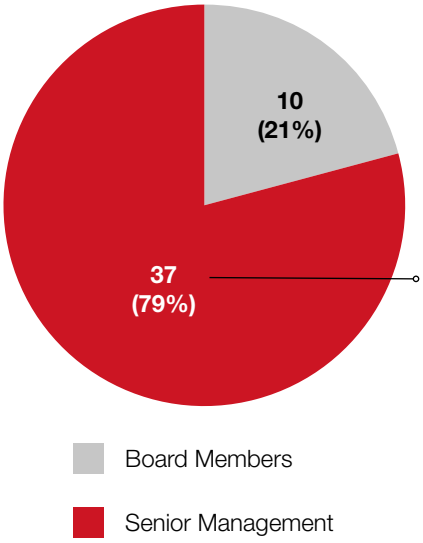
Survey methodology

We draw our insights from the following sources:

- Online survey conducted from July - August 2018
- Face-to-face and written interviews
- *Global State of Information Security Survey (GSISS) 2018*

Respondents' statistics

Online Survey



Foreign Banks

3 Board Members

18 Senior Management

Local Banks

5 Board Members

12 Senior Management

Local DFIs

2 Board Members

7 Senior Management

Senior Management Respondents

2 Chief Executive Officer (CEO)

15 Chief Risk Officer (CRO)

2 Chief Operating Officer (COO)

3 Chief Information Officer (CIO)

9 Chief Compliance Officer (CCO)

6 Chief Information Security Officer (CISO)

Interview participants:

Participants	Names	Designation	Bank
Board Director	**Ong Ai Lin**	Independent Non-Executive Director	RHB Bank Berhad
Senior Management	**Mohd Suhail Amar Suresh Abdullah**	Group Chief Technology Officer	Maybank Group
	Lee Lung Nien	Chief Executive Officer	Citibank Berhad
	Michael Guenther	Head of Risk, Malaysia	Deutsche Bank
	Yuen Ka Wei	CISO APAC Manager	Deutsche Bank
	Achim-Ingo Ringel	Non-Financial Risk Management APAC	Deutsche Bank

ACKNOWLEDGEMENTS

AICB and PwC would like to thank the following individuals and organisations for their invaluable contributions to the development of this publication:

- **Ong Ai Lin,** RHB Bank Berhad
- **Lee Lung Nien,** Citibank Berhad
- **Mohd Suhail Amar Suresh Abdullah,** Maybank Group
- **Michael Guenther,** Deutsche Bank
- **Yuen Ka Wei,** Deutsche Bank
- **Shireen Kandiah,** AICB
- **Felicia Song,** AICB
- **Tan Cheng Yeong,** PwC Malaysia
- **Clarence Chan,** PwC Malaysia
- **Caere Chin,** PwC Malaysia
- **Alex Cheng,** PwC Malaysia
- **Chealsea Tan,** PwC Malaysia
- **Woon Tian Yi,** PwC Malaysia
- **Ong Khar Keong,** PwC Malaysia
- **Sarah Lee,** PwC Malaysia

PUBLICATIONS AICB

Banking Insight
First Quarter 2017

Banking Insight
Second Quarter 2017

Banking Insight
December 2017

Banking Insight
June 2018

Recovery &
Resolution Planning

Catching the
FinTech Wave

Law & Regulations
in Malaysian Banking

PUBLICATIONS PwC

The Global State of Information Security Survey 2018

How Your Board Can Be Effective in Overseeing Cyber Risk

Governing Cybersecurity Risk: It's Time To Take It Seriously

Converging Cyber Risks in A Digital World

Know the Game, Not Just the Rules – The Changing Face of Cybersecurity

Cyber Risk – Enlightenment Through Information Risk Management

21st CEO Survey – The Anxious Optimist in the Corner Office

ABOUT AICB

The Asian Institute of Chartered Bankers (AICB) is the professional body for the banking industry in Malaysia governed by a Council with representatives from Bank Negara Malaysia, The Association of Banks in Malaysia, and the Malaysian Investment Banking Association. Guided by the transformation blueprint for the Malaysian banking education landscape, AICB aims to elevate the professional and ethical standards of banking practitioners by creating a banking workforce that subscribes to high standards of professional conduct, knowledge and competence.

Upholding trust in the banking profession is the cornerstone of the Institute and together with its exclusive training partner, the Asian Banking School (ABS), AICB continues to ensure that its suite of professional qualifications for banking services remain relevant to equip banking talent with the requisite skill sets and values to meet the evolving banking landscape and contribute to strengthening public trust. Among the professional qualifications offered are Bank Risk Management, Professional Credit Certification, Pasaran Kewangan Malaysia Certificate, Regulatory Compliance, Certificate in Internal Auditing for Financial Institutions, Certification for Bank Auditors, Certified Anti-Money Laundering and Counter Financing of Terrorism (CAMCO), Investor Protection Professional Certification, Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT), and the Chartered Banker programme. The Chartered Banker programme, which is the gold standard in global banking, is AICB's flagship programme awarded together with the Chartered Banker Institute, UK.

AICB also supports members through various learning and thought leadership initiatives and promotes continuing professional development (CPD) for members to keep abreast of the latest industry developments.

CONTACTS

PRASAD PADMANABAN
Chief Executive

Asian Institute of Chartered Bankers
(Formerly known as Institut Bank-Bank Malaysia)

Tel: +603 2095 6833
prasad@aicb.org.my

SHIREEN KANDIAH
Director,
Strategy, Partnerships & Communications

Asian Institute of Chartered Bankers
(Formerly known as Institut Bank-Bank Malaysia)

Tel: +603 2095 6833
shireen@aicb.org.my

SOO HOO KHOON YEAN
Assurance Leader

PricewaterhouseCoopers PLT

Tel: +603 2173 0762
khoon.yean.soo.hoo@pwc.com

ONG CHING CHUAN
Financial Services Leader

PricewaterhouseCoopers PLT

Tel: +603 2173 0550
ching.chuan.ong@pwc.com

TAN CHENG YEONG
Partner and Digital Trust & Security Leader

PricewaterhouseCoopers Risk Services Sdn Bhd

Tel: +603 2173 0539
cheng.yeong.tan@pwc.com

G DEVAN NAIR
Partner and Technology Practice Leader

PwC Consulting Associates (M) Sdn Bhd

Tel: +603 2173 1512
g.devan.nair@pwc.com

CLARENCE CHAN
Associate Director,
Digital Trust & Security

PricewaterhouseCoopers Risk Services Sdn Bhd

Tel: +603 2173 0344
clarence.ck.chan@pwc.com

WILLIAM PHUAH
Senior Manager,
Technology Consulting

PwC Consulting Services (M) Sdn Bhd

Tel: +603 2173 1051
william.aw.phuah@pwc.com

This page has been intentionally left blank.

Asian Institute of Chartered Bankers (35880-P)
(formerly known as Institut Bank-Bank Malaysia)
Wisma IBI 5 Jalan Semantan
Damansara Heights
50490 Kuala Lumpur, Malaysia

Tel: +603 2095 6833
Fax: +603 2095 2322

www.aicb.org.my

PricewaterhouseCoopers Risk Services Sdn Bhd (1154008-H)
(formerly known as PricewaterhouseCoopers Services Sdn Bhd)
Level 10, 1 Sentral, Jalan Rakyat
Kuala Lumpur Sentral
50706 Kuala Lumpur, Malaysia

Tel: +603 2173 1188
Fax: +603 2173 1288

www.pwc.com/my

www.aicb.org.my
www.pwc.com/my