LESTARI GEMS

Vol. 10

Banking on Cybersecurity

By Joshua Ng I joshuang@kenanga.com.my

Featured Report

Banking: Fortifying Against Cybersecurity Threats

ESG News Round-up

MITI to launch National Industry ESG framework by September

The Ministry of Investment, Trade and Industry (MITI) targets to launch the National Industry Environmental, Social and Governance framework (i-ESG) framework for the manufacturing sector by September.

Minister Tengku Datuk Seri Zafrul Abdul Aziz said the framework comprises four key components that include standards, financial support and incentives, capacity building and market mechanisms.

"What we are looking to do is also to promote and nurture green manufacturing. Note that green businesses in Southeast Asia present up to an estimated USD200b opportunity by 2030," he said at the Second Malaysian Banking Conference yesterday. ─ *New Straits Times*

ISSB rules aim to clamp down on corporate greenwashing

Companies will face more pressure to disclose how climate change affects their business under a new set of G20-backed global rules aimed at helping regulators crack down on greenwashing.

The International Sustainability Standards Board (ISSB) chair Emmanuel Faber said it would be up to individual countries to decide whether to require listed companies to apply the standards, which were written by the ISSB. ─ *Reuters*

New scheme to digitalise Singapore SMEs' ESG credentials

The Monetary Authority of Singapore (MAS), UN Development Programme (UNDP) and Global Legal Entity Identifier Foundation (GLEIF) are collaborating on an initiative to develop digital ESG credentials for small and medium enterprises (SMEs) globally.

The initiative, known as Project Savannah, targets the lowering of barriers faced by SMEs in building sustainability capabilities by establishing a common framework of ESG metrics. ─ *Regulation Asia*

Talk of no new oil investments 'will only lead to energy chaos'

Talk of no new investments in oil projects "will only lead to energy chaos", at a time when the world needs clarity on how to support growing global energy demand while reducing emissions, said OPEC secretary general Haitham Al Ghais at the Energy Asia 2023 in Kuala Lumpur. ─ *Reuters*

China to build 6,000km hydrogen pipeline network by 2050

Li Guohui, vice president of state-owned China Petroleum Pipeline Engineering Corporation said China will develop a 6,000km hydrogen pipeline network by 2050, which would be accessible to hydrogen asset owners and traders.

He also said that total hydrogen demand is expected to grow to 100m metric tonnes per annum by 2060. Hydrogen production in China reached around 33m tonnes in 2020, which is 30% of the world's total. ─ *Carbon Herald*

ESG CALENDAR

3rd Recyclable Mono Material Packaging Solutions

Organiser: Eco-Business

Date: 4−5 July 2023
Venue: Hilton Rotterdam, the Netherlands
Type: Hybrid, Paid
Register here

Climate Change: Exploring the facts and future with Dr. Knute Nadelhoffer

Organiser: Hessel School House

Date: 6 July 2023
Venue: Hessel School House, Avery Arts & Nature Learning Center, 3206 Cedar Street Hessel, Michigan 49745
Type: In Person, Free
Register here

The Edge ESG Forum: Financing for a Green Future

Organiser: The Edge Malaysia

Date: 10 July 2023, 8am−12.45pm
Venue: Mandarin Oriental, KL
Type: In Person (By Invitation)
Enquiries here

Business GoVirtual Expo & Conference 2023

Organiser: Baobab Tree Event
Date: 12−14 July 2023
Venue: Wan Chai, Hong Kong
Type: In Person, Free
Register here

Climate Finance Summit 2023

Organiser: Perdana Fellows Alumni Association
Date: 13 July 2023
Venue: Sasana Kijang, Bank Negara Malaysia
Type: In Person, Free (RM30 refundable registration
Register here

ESG Rating 4 stars

Company	F4GBM Index	Rating	TP (RM)
ABMB	Yes	OP	4.40
CIMB	Yes	OP	6.55
PBBANK	Yes	OP	4.90
KLK	Yes	OP	24.50
IOI CORP	Yes	MP	3.80
PPB	Yes	OP	19.30
MISC	Yes	MP	7.60
YINSON	Yes	OP	3.65
CTOS	Yes	OP	1.80
SUNCON		OP	2.13
GAMUDA		OP	5.15
SAMAIDEN		OP	1.15

ESG Rating 2 stars

Company	F4GBM Index	Rating	TP (RM)
TENAGA	Yes	OP	10.64
ARMADA	Yes	OP	0.75
TAANN		MP	3.40
KOSSAN		UP	1.28
SUPERMAX		MP	0.96
BAT		MP	10.00
CARLSBERG		MP	23.50
HEINEKEN	Yes	MP	28.60

Banking

Fortifying Against Cybersecurity Threats

OVERWEIGHT
↔

By Clement Chua I clement.chua@kenanga.com.my

We hosted Deloitte Malaysia's Cyber Risk Services Team to provide insights on prevailing cybersecurity threats faced financial institutions. In the sharing session, we came to better understand Bank Negara Malaysia (BNM)'s efforts to prevent and remediate ongoing threats, in which its Risk Management in Technology (RMiT) framework serves as the backbone. As expert in the field, Deloitte also presented solutions and possible enhancements in achieving corporate cybersecurity objectives. From our own channel checks, we also share common practices within the industry and validated the challenges faced by financial institutions. We are OVERWEIGHT on the banking sector and we believe the sector's resilience is under-appreciated amidst looming market-wide concerns. Our preferred picks are AMBANK (OP; TP: RM5.05), CIMB (OP; TP: RM6.55) and PBBANK (OP; TP: RM4.90) as tactical opportunities amidst ongoing share price weakness.

Cybersecurity is an ever-growing concern given our only increasing reliance on digital infrastructure in daily life. Focusing on financial institutions, the move is natural to instil the following value accretion, but not limited to:

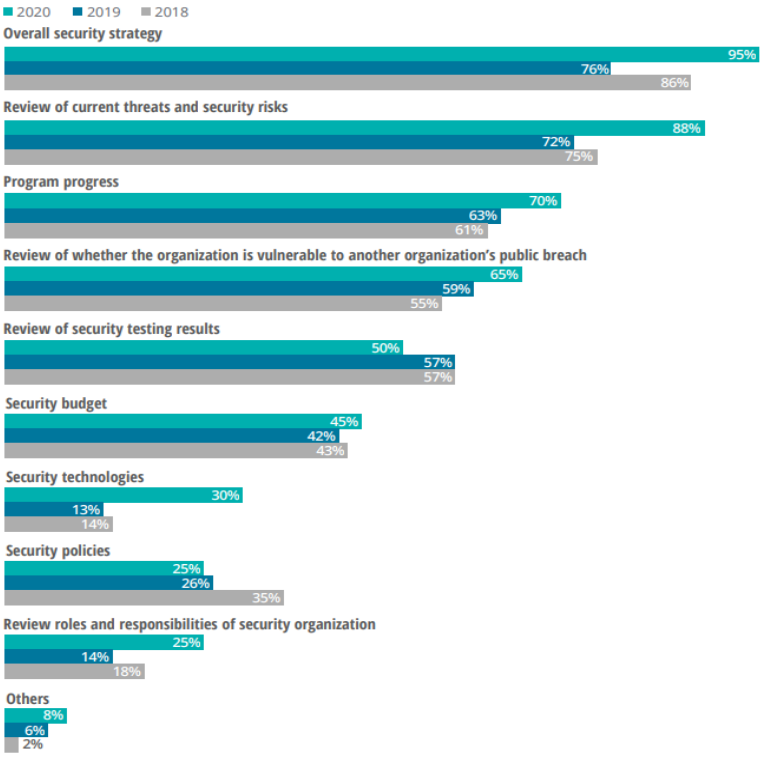
1. enhancing customer experience, engagement and products through websites and mobile applications;
2. automating manual back-end processes to accelerate timeliness and cost efficiency;
3. more holistic data management with significantly smaller physical footprints; while also
4. enabling data analytics to understand customer behaviour and refine marketing strategies

Given the heavy dependency above, the compromise on a financial institution's digital integrity could expose them and their customers to severe ramifications such as: (i) identity theft, (ii) breach of data privacy, (iii) leakage of sensitive information, and (iv) monetary loss through unauthorized transactions.

To expand our knowledge on the matter, we had invited Deloitte Malaysia's Cyber Risk Team to understand key methodologies exercised on their end. The team was developed during the early phases of internet banking and has observed several key developments in the domestic markets, particularly the establishment of the RMiT framework by BNM.

Assessing Risk Elements

Top cybersecurity areas of interest identified by survey respondents



Source: Deloitte FS-ISAC "Reshaping the cybersecurity landscape"

According to surveys conducted, Deloitte gathered that sources of cybersecurity threats mostly originate from external individuals and organised groups. While motivations may vary, such attacks could stem from monetary objectives or to sell private information for profit or purely for malicious intent. Internal parties do still pose a threat which could involve assailants with deep knowledge of the infrastructure or security systems within the organisation.

The majority of materialised attacks appear in the form of phishing, malware or ransomware. These are a form of cyberattack typically disguised as a deceptive email or link that affects its targets by compromising its system integrity to extract data for unauthorised use or with threats to expose such data unless a ransom is paid. Denial of service is also one of the more common cyberattacks which disrupts access and functionality of a computer system or online service.

The ramifications of a successful attack may vary but it is found that disruption of service is the key concern as it could extend to material financial losses if a company is unable to execute and deliver on its key protocols, primarily those time-sensitive in nature. Greater safety concerns from customers could also undermine a company's reputation and translate to longer term challenges.

Cyber incidents and breaches are resulting in the following negative consequences for organizations

Negative consequences resulting from cyber incidents and breaches	2021 (Rank)	2023 (Rank)	2023 (Percent)
Operational disruption *(including supply chain/or partner ecosystem)*	1	1	58%
Loss of revenue	9	2	56%
Loss of customer trust/negative brand impact	4	3	56%
Reputational loss	5	4	55%
Defunding of a strategic initiative	N/A	5	55%
Loss of confidence in tech integrity	N/A	6	55%
Negative talent recruitment/retention impact	8	7	54%
Intellectual property theft	2	8	54%
Drop in share price	3	9	52%
Regulatory fines	7	10	52%
Change in leadership	5	N/A	N/A

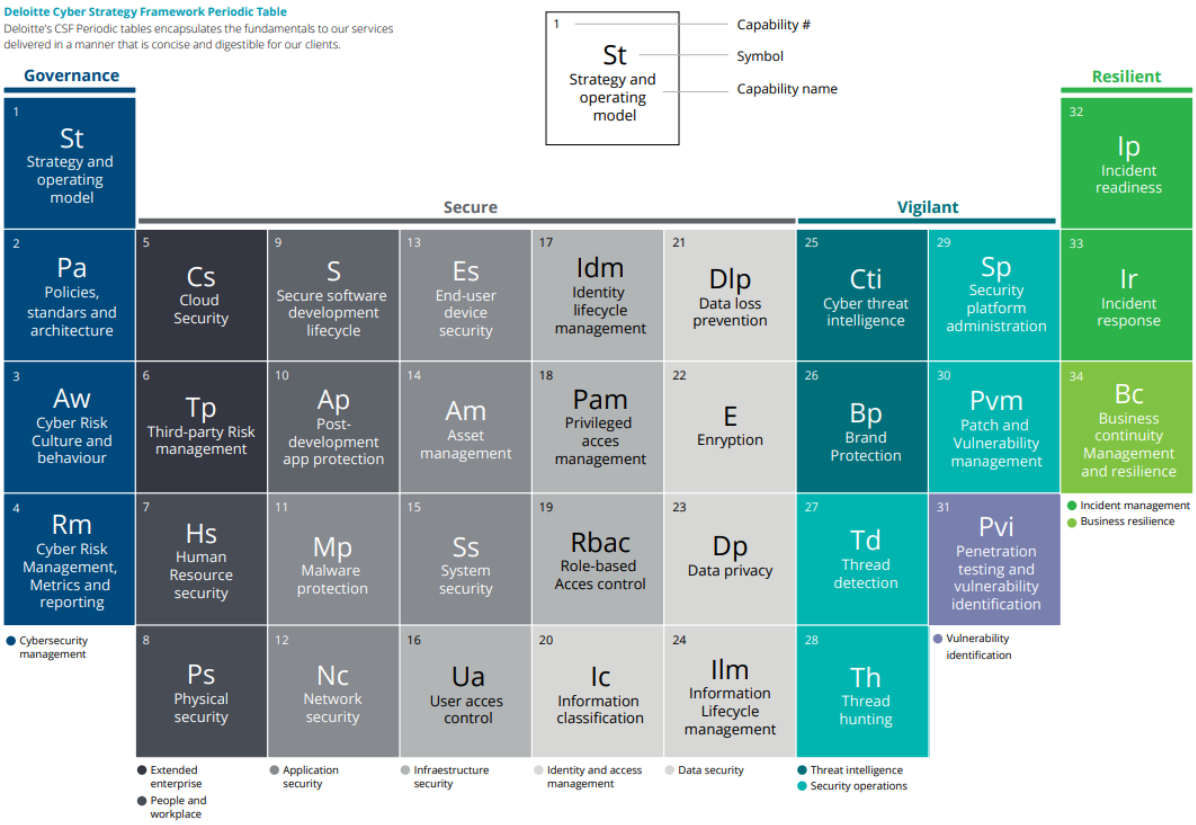
Source: Deloitte 2023 Global Future of Cyber Survey

It is fair to expect that the corporate strength in dealing with cybersecurity issues stem from the tone set by leaders, reliant on the focus and resources allocated. Corporates that do not view these concerns as serious are more likely to under-invest in cyber safety and hence rendering their organisation more vulnerable. There could also be the nuance that the corporates themselves, though keen in reinforcing their cybersecurity framework, may lack an in-depth understanding or knowledge on the thoroughness of the matter.

During their sharing, Deloitte presented its Cyber Capabilities Model in which it identified key considerations for financial institution in addressing its cybersecurity risks and framework. These are dubbed into four categories by Deloitte, being:

1. Strategies to manage cyberthreat risks (**Governance**) to ensure that the organisation has a clear direction of travel with respect to cyber security, and that the necessary structures and rules are in place to maintain and enhance the organisation's cyber security capabilities.
2. Building preventative capabilities and processes (**Secure**) such as proactive protection against cyber-attacks before they occur by identifying, implementing and enhancing the controls that safeguard the organisation's resources.
3. Pro-active measures against transpiring cyberthreats (**Vigilant**) or the ability to discover internal and external threats by leveraging on threat intelligence and working pro-actively to mitigate and minimise any adverse impact to the organisation.
4. Responsive, recovery and resolutive measures (**Resilient**) to minimise any adverse impact of occurred cyberthreats. This also extends to accepting that it is a question of when, not whether, organisations will be attacked.

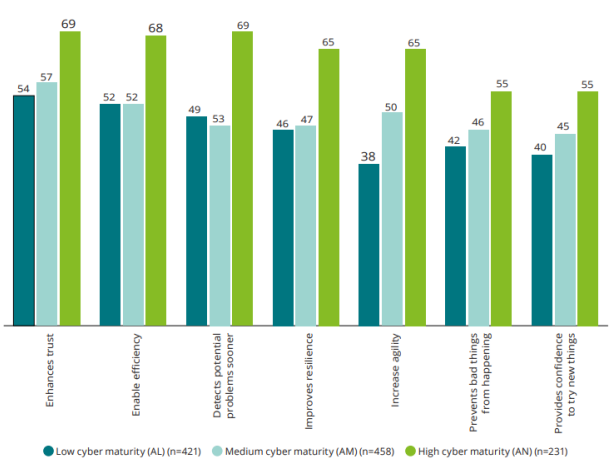
Deloitte's Cyber Capabilities Model



Source: Deloitte Cyber Strategy Framework – A unique platform for managing your Cyber Strategy
https://www2.deloitte.com/content/dam/Deloitte/th/Documents/risk/risk-advisory-publication/Cyber%20Strategy%20Framework%20Brochure.pdf

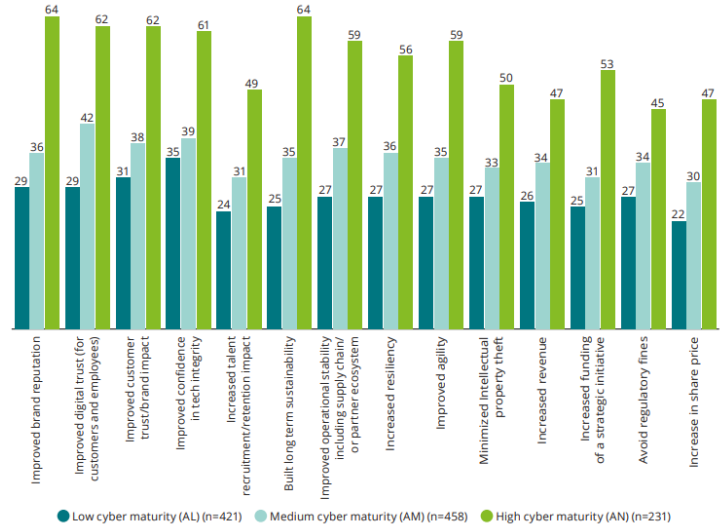
On the other hand, there is the additional equity offered by having a matured foundation for cybersecurity. We opine that the value acquired could be more to do with instilling a stronger culture as merely investing into heavy capabilities does not guarantee an impenetrable framework. Greater confidence here is thought to also trickle to other aspects of a business as well, as what Deloitte's recent survey has shown below.

Impact to business initiatives



Source: Deloitte 2023 Global Future of Cyber Survey

Other direct/Indirect positive impact



Source: Deloitte 2023 Global Future of Cyber Survey

Industry solutions

Given that cybersecurity is not a new issue, corporates have been able to progressively identify gaps in their operating framework as well as to allocate resources in tackling these issues. On that matter, we do understand that there could always be need to do more but a balance should be sought as to not "over-invest" into capabilities with fewer additional benefits.

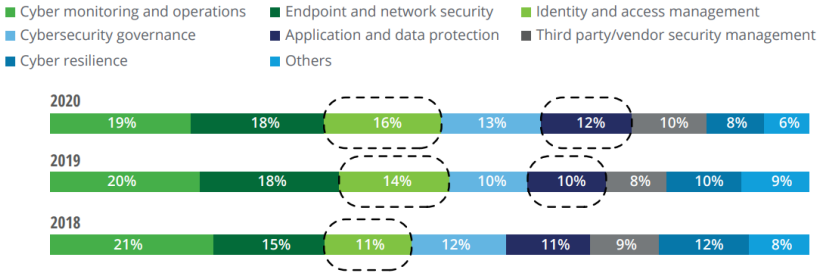
Cybersecurity spending across sectors

Percentage of revenue | Percentage of IT spending | Per FTE

	2019	2020
Retail/corporate banking	0.3% 10.1% US$2,074	0.6% 9.4% US$2,688
Consumer/financial services (nonbanking)	0.3% 9.7% US$2,817	0.4% 10.5% US$2,348
Insurance	0.3% 9.3% US$2,245	0.4% 11.9% US$1,984
Service provider	0.6% 8.9% US$1,956	0.6% 7.2% US$3,226
Financial utility	0.8% 15.2% US$3,630	0.8% 8.2% US$4,375
Aggregated total	0.3% 10.1% US$2,337	0.5% 10.9% US$2,691

Source: Deloitte FS-ISAC "Reshaping the cybersecurity landscape"

Budget allocation across cybersecurity domains by respondents



Note: Percentage totals may not equal 100% due to rounding.

Source: Deloitte FS-ISAC "Reshaping the cybersecurity landscape"

Deloitte as a service provider in cyber risks mitigation shared several services which we see as crucial in the development of an effective cyber security framework. We see these to be value-adding to the banks as certain service providers have stronger competencies given their specialised experience in dedicated fields. We opine that these would assist institutions which may face time constraints in implementation.

1. **Development of Cybersecurity Strategy:** Building a comprehensive and efficient strategy to manage cyber threats and risks within an organization. It encompasses identifying and evaluating potential vulnerabilities, setting goals and objectives for cybersecurity, and establishing a plan for implementing protective measures.
2. **Evaluation of Cyber Vulnerabilities:** This includes the identification and assessment of vulnerabilities present in an organization's information systems, networks and infrastructure. This could help to identify and minimise weak points which may naturally arise during a bank's operations which may be open for exploitation. The objective is to pinpoint weaknesses that could be exploited by cyber attackers. Typically, vulnerability assessments include conducting scans and tests to identify vulnerabilities, analyzing the results, and providing recommendations for addressing them. This process enables organizations to understand their security weaknesses and take appropriate actions to mitigate risks.
3. **Intelligence-led Penetration Testing** (also known as Red Teaming): This form of testing involves simulating real-world cyber attacks to evaluate an organization's security readiness and its ability to detect and respond to threats. The "red team" acts as an external attacker, utilizing advanced techniques to identify potential vulnerabilities and exploit them. This type of testing goes beyond vulnerability assessments by actively attempting to breach the organization's defenses. It offers valuable insights into the effectiveness of security controls and assists organizations in enhancing their security measures based on the findings.
4. **Cyber Exercise:** A cyber exercise is a simulated activity designed to assess an organization's response capabilities in the event of a cyber incident or breach. It entails conducting scenario-based simulations to evaluate the efficiency of incident response plans, communication protocols, and coordination among different cybersecurity teams. The purpose of cyber drills is to identify gaps, assess response times, and enhance the organization's preparedness for real-world cyber incidents. These drills provide an opportunity to train personnel, validate response strategies, and improve incident management processes. By participating in cyber drills, organizations can strengthen their ability to respond promptly and effectively to cyber threats.

Legislation and BNM's Risk Management in Technology (RMiT)

Currently, Malaysia has several laws on cybercrimes i.e. the Computer Crimes Act 1997, Communications and Multimedia Act 1998, the Malaysian Penal Code and Personal Data Protection Act 2010. There are also two agencies dedicated to strengthening Malaysia's cybersecurity via various initiatives and research & development i.e. the National Cyber Security Agency (NACSA) and CyberSecurity Malaysia. In October 2022, the National Scam Response Centre (NSRC) was set up to enable swift and integrated action to tackle cyber fraud cases. Under a joint effort among the National Anti-Financial Crime Centre (NFCC), the Royal Malaysia Police, BNM, the Malaysian Communications and Multimedia Commission (MCMC), as well as financial institutions and the telecommunications industry, its 997 hotline has received over 30,000 complaints as of April 2023. Recognising the importance of tackling cybersecurity issues in a concerted and coordinated manner, the government is drafting the Cyber Security Bill to bolster the country's resilience and response to cyber threats. At the same time, the country is also streamlining the roles of NACSA and CyberSecurity Malaysia to avoid overlapping functions, and amend the Personal Data Protection Act to make it more robust.

To establish a stronger line of defense, BNM first issued the RMiT on 1 June 2020 as an active call for all financial institutions. The RMiT serves as the leading point of reference as it also take points from other global regulators with BNM benefitting from its participation in global associations. Briefly, we condense the key requirements and objectives of the RMiT into the following:

1. **Enhanced governance and oversight:** Banks must establish a strong framework for governance that clearly defines roles, responsibilities, and accountability in managing technology risks. This framework should include more rigorous internal technology audits and be overseen by the board of directors / cyber risk committee and senior management.
2. **Establishing a risk management framework:** Banks need to have a comprehensive framework for managing technology risks across the organization. This framework should identify, assess, and mitigate risks in areas such as cybersecurity, data protection, outsourcing, and business continuity. This should extend to measures to safeguard their systems, networks, and customer information from cyber threats. This involves conducting regular risk assessments, implementing suitable controls, and having a plan in place to respond to incidents.
3. **Policies on data protection and data privacy:** Banks must have policies and procedures in place to ensure the confidentiality, integrity, and availability of customer data. This includes complying with relevant laws and regulations pertaining to data protection and privacy.
4. **Business continuity management:** Banks should have robust plans in place to ensure the timely recovery of critical systems and operations in the event of disruptions. This includes regular testing, updating plans, and maintaining alternative infrastructure and facilities.
5. **Incident reporting and response:** Banks are required to establish efficient processes for reporting and responding to technology-related incidents. This includes promptly identifying, reporting, and investigating incidents, as well as implementing measures to prevent their recurrence.

*(Refer to the **appended link** for the updated issue of the RMiT dated 1st June 2023)*

It is understood that due to the comprehensiveness demanded by the RMiT, banks have been given a more lenient timeline to comply with the framework during its inception. However, there could be a stricter enforcement on the matter going forward, with a new deadline.

In addition to the RMiT, BNM in Sep 2022 announced five additional measures for financial institutions to take urgently to further strengthen safeguards against financial scams. The measures are migrating from the SMS one-time passwords (OTP), tightening fraud detection rules and triggers for suspicious transactions, a cooling-off period for the first-time request of online services or secure devices, restricting customers to one device for the authentication process, and setting up of dedicated hotlines for customers to report financial scam incidents. In response, banks have also more recently implemented a "kill switch" function which blocks all outgoing transactions and deactivates access to internet banking services.

Kenanga's Take

While digitalisation in financial institutions has greatly benefitted consumers, the rise of digital banking, the growing adoption of remote work, and the increasing use of multiple devices and apps by customers and other third parties, are pushing the boundaries of the financial sector's cyber capabilities. These areas are also exposing new security areas which need specific measures at each level.

Statistics by the Royal Malaysia Police's Commercial Crime Investigation Department showed that Malaysians lost over RM850m in more than 25,000 online fraud cases in 2022. In March 2023, the Malaysian Anti-Corruption Commission (MACC) said that it was investigating an investment scam syndicate, including looking into the role of five major banks implicated in the case. There were no details on the banks implicated. The syndicate has reportedly earned about AUD60m (RM200m) by defrauding victims locally since 2019 and up to RM1b worldwide through their international operations.

On one hand, financial institutions are not solely responsible for financial losses due to online frauds and scams. On the other hand, they are the "gatekeepers" of wealth entrusted to keep consumers' monies safe and secure. The rising prevalence of online frauds, data breaches and the increasing sophistication and complexity of cybercrimes are forcing financial institutions to stay ahead in cybersecurity and ensure stealth-like protection for consumers without sacrificing accessibility and convenience.

Looking ahead, financial institutions can expect a more challenging operating environment as innovations such as cloud services and AI become more common thus heightening cybersecurity risks amidst rising customers' expectations of better security and safety. Adding to the gravity is the shortage of talent in the field of cybersecurity and the legal challenges involved when dealing with different jurisdictions. Hence, cross-organisational and cross-border cooperation is essential to address the seamless world of cyberspace. Coordinated surveillance and assessment are crucial not only for effective risk mitigation but also for the successful arrest and prosecution of perpetrators.

One key issue for customers is the return of monies lost in fraudulent transactions. There needs to be better and stronger regulations and laws that compel quicker refunds. While customers themselves are the best defence in the battle against scammers, it is imperative that banks play a bigger role in keeping customers informed and aware of potential private data breaches and scam tactics.

Due to the limitations of disclosures, it is a challenge to establish a benchmark between the listed financial institutions. The current industry practice includes reporting on data privacy and cybersecurity efforts within the “Sustainability Statements” in their respective annual reports, although consistency between them could be further enhanced. It is still appreciated that information provided offers a sense of effort taken by the respective banks, such as:

1. Materiality matrix and risk management frameworks
2. Referenced legislations and guidelines
3. Staff education and training on cybersecurity and awareness

However, to enable a more comprehensive perception to be established, we propose for disclosures to include more transparency and with more numerical emphasis; albeit we gather that these information could be sensitive towards the reputational risks to the banks. These items could include:

1. Frequency of cyber risk incidences and timeliness of resolution
2. Financial losses incurred from incidences
3. Total investment into security system upgrades and maintenances

We believe such information could enable investors to better exercise their own objective views as to how the banks manage cyber risks in day-to-day operations. While this may also lead to varying perceptions owing to a higher/lower gravity in comparing (i.e. larger banks may invest more into security systems but smaller banks have a higher proportion of spending to develop security capabilities), this could also provide opportunities for the banks to educate its investors and highlight on its specific strengths to build equity.

Peer Table Comparison

Name	Rating	Last Price (RM)	Target Price (RM)	Upside	Market Cap (RM m)	Shariah Compliant	Current FYE	Core EPS (sen)		Core EPS Growth		PER (x) - Core Earnings		PBV (x)	ROE	Net. Div. (sen)	Net Div Yld
								1-Yr. Fwd.	2-Yr. Fwd.	1-Yr. Fwd.	2-Yr. Fwd.	1-Yr. Fwd.	2-Yr. Fwd.	1-Yr. Fwd.	1-Yr. Fwd.	1-Yr. Fwd.	1-Yr. Fwd.
Stocks Under Coverage																	
AFFIN BANK BHD	OP	1.85	2.25	21.6%	4,207	N	12/2023	23.2	25.9	-62.3%	11.5%	8.0	7.2	0.4	4.5%	11.0	5.9%
ALLIANCE BANK MALAYSIA BHD	OP	3.34	4.40	31.7%	5,171	N	03/2024	48.8	52.9	11.3%	8.4%	6.9	6.3	0.7	10.9%	24.5	7.3%
AMMB HOLDINGS BHD	OP	3.61	5.05	39.9%	11,937	N	03/2024	56.3	62.0	7.4%	10.2%	6.4	5.8	0.6	9.9%	19.5	5.4%
BANK ISLAM MALAYSIA BHD	MP	1.94	2.25	16.0%	4,397	Y	12/2023	24.0	25.0	5.1%	4.1%	8.1	7.8	0.6	7.5%	15.5	8.0%
CIMB GROUP HOLDINGS BHD	OP	5.15	6.55	27.2%	54,925	N	12/2023	61.1	68.2	17.2%	11.5%	8.4	7.6	0.8	9.9%	30.0	5.8%
HONG LEONG BANK BHD	OP	18.94	25.00	32.0%	41,057	N	06/2023	193.0	201.5	20.2%	4.4%	9.8	9.4	1.2	12.3%	70.0	3.7%
MALAYAN BANKING BHD	OP	8.71	10.10	16.0%	104,991	N	12/2023	80.3	80.0	16.8%	-0.5%	10.8	10.9	1.2	11.1%	68.0	7.8%
PUBLIC BANK BHD	OP	3.85	4.90	27.3%	74,731	N	12/2023	36.0	37.2	14.1%	3.3%	10.7	10.4	1.4	13.5%	18.0	4.7%
RHB BANK BHD	OP	5.44	7.10	30.5%	23,318	N	12/2023	77.5	77.7	15.9%	0.3%	7.0	7.0	0.7	10.7%	43.0	7.9%
Sector Aggregate					**324,733**					**12.3%**	**2.6%**	**9.6**	**9.4**	**1.0**	**10.7%**		**6.3%**

Source: Kenanga Research

This section is intentionally left blank

Stock Ratings are defined as follows:

Stock Recommendations

OUTPERFORM	: A particular stock's Expected Total Return is MORE than 10%
MARKET PERFORM	: A particular stock's Expected Total Return is WITHIN the range of -5% to 10%
UNDERPERFORM	: A particular stock's Expected Total Return is LESS than -5%

Sector Recommendations***

OVERWEIGHT	: A particular sector's Expected Total Return is MORE than 10%
NEUTRAL	: A particular sector's Expected Total Return is WITHIN the range of -5% to 10%
UNDERWEIGHT	: A particular sector's Expected Total Return is LESS than -5%

******Sector recommendations are defined based on market capitalisation weighted average expected total return for stocks under our coverage.***

Published by:

KENANGA INVESTMENT BANK BERHAD (15678-H)
Level 17, Kenanga Tower, 237, JalanTunRazak, 50400 Kuala Lumpur, Malaysia
Telephone: (603) 2172 0880 Website: www.kenanga.com.my E-mail: research@kenanga.com.my