Telecommunication

OVERWEIGHT

New Cybersecurity Act Champions ESG Goals

↔

By Kylie Chan Sze Zan I kyliechan@kenanga.com.my

Data protection has long been a core ESG priority for telcos, but the introduction of Cybersecurity Act 2024 (CBSA), effective August this year, was a watershed moment as it addresses long standing gaps in industry best practices. Following a meeting with Cybersecurity Malaysia (CSM), an agency under the Ministry of Communications and Multimedia Malaysia, we concur that while a grace period may ease the transition for telcos, the wheels of self-regulation is now set in motion.

Despite commendable efforts by telcos to-date, much room exists for greater accountability and transparency. As the 2010 Personal Data Protection Act (PDPA) did not explicitly address cybersecurity, telcos have largely adopted measures voluntarily. This is guided by ESG principles and the UN's sustainable development goals focused on data protection and service continuity. Therefore, the CBSA ushers in a significant shift as compliance is now mandatory. Additionally, beyond fines and imprisonment, sector leaders may impose public disclosure requirements on cybersecurity incidents. Hence, this may compel greater adherence by telcos to avoid the risk of reputational damage, erosion of consumer confidence, and long-term customer churn.

CBSA is just the first step, as potential future regulations (eg. Cybersecurity Resilience Act, or amendments to the PDPA Act) may further enhance cybersecurity compliance and standards. We would welcome these developments, as they could help future-proof telcos by counteracting rising cybersecurity threats amid emerging technologies (5G, Generative AI, IoT, cloud).

- **How vital is cybersecurity for telco ESG?**

Cybersecurity is a key ESG pillar for telcos. Cybersecurity has emerged as a critical component within the Environmental, Social, and Governance (ESG) framework, particularly in the social and governance dimensions. Telcos manage a vast repository of data, which include personal and sensitive information for a large segment of the population, billing details, coupled with call and internet usage history. As at 2QCY24, mobile players CDB and MAXIS collectively served 32.7m mobile subscribers, accounting for an estimated 66% of total market share. According to Deputy Home Minister Datuk Seri Dr Shamsul Anuar, telco-related scams (e.g. SMS contests, online impersonation, and phone calls) ranked among the highest in 2023, with 10,348 reported cases resulting in losses totalling RM352.9m. Thus, enhanced cybersecurity measures are crucial to protect telcos' extensive database from breaches, theft and unauthorized access.

Surge in fraud cases linked to cyberbreaches. Data from the Malaysia Computer Emergency Response Team (MyCERT) revealed a 14% YTD rise in cybersecurity incidents, with 4,359 cases reported as of August 2024. Fraud is the most prevalent cybersecurity incident, accounting for 64% of all cases as of 8MCY24. Malicious codes and content-related incidents follow at a considerable distance, comprising just 9% and 8% of total cases, respectively. Additionally, according to Digital Minister, Gobind Singh Deo, RM3.18b was lost to online scams affecting more than 95,800 victims between 2021 and April 2024. Against this alarming backdrop, robust safeguards are essential to protect users from fraud, scams and identity theft, which could result in financial loss and legal repercussions. Failure to address this could undermine United Nations (UN) SDG 16: *Promote peaceful and inclusive societies, provide access to justice for all, and build effective, accountable, and inclusive institutions at all levels.*

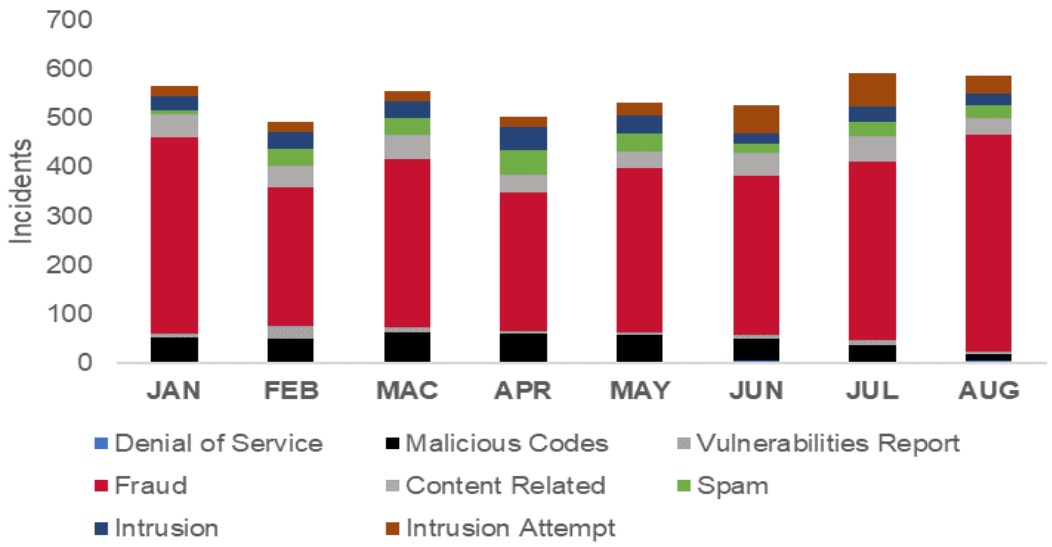
Telcos have the second highest number of cybersecurity incidents. According to CSM, fraudsters and hackers typically target industries that present opportunities for financial theft, focusing on sectors "where the money is". Despite being a primary target, the financial and banking sector merely ranks fourth in the frequency of cybersecurity incidents. In comparison, the education sector ranks third, followed by the telco sector at second place, with government agencies experiencing the highest number of incidents. The relatively lower incidence of cyber breaches in the banking sector is attributed to the successful implementation of the Risk Management in Technology (RMiT) framework. To recap, RMiT was issued by BNM in 2020 to strengthen technology risk management in the financial sector, particularly in cybersecurity, IT governance, and operational resilience. Inspired by this success, the government aims to achieve similar outcomes through CBSA 2024, which empowers sector leaders to enhance cybersecurity risk management within their respective industries.

Personal data for almost all age groups are being targeted. CSM reiterated that fraudsters and scammers target every age group, exploiting their unique vulnerabilities. For example, fresh graduates aged 20-29 may be susceptible to job offer scams, while those in the 30-39 age range might be targeted with fraudulent offers of affordable maid services, which appeals to working parents with young families. On the back of this, telco companies must safeguard their comprehensive database of

personal information, which covers nearly all age groups, including children registered as supplemental line accounts.

Hard to apprehend credential thieves. According to CSM, hackers typically sell stolen personal information on the dark web to scammers, fraudsters, phishers or smishers. Newer information typically commands higher prices, while older data is less valuable. Given that fraudsters operate discretely in underground environments that are challenging for authorities to detect and prosecute, it is vital for telco companies to protect their customer databases from cyber breaches. This embodies the adage 'prevention is better than cure,' as recourse for victims of cybercrimes is often limited and, in many cases, unavailable.

Reported Cybersecurity Incidents based on General Incident Classification Statistics 2024



Source: MyCERT, Kenanga Research

Recent AT&T breaches serve as a reminder to be vigilant. As a case study to highlight the damage caused by cybersecurity breaches, we refer to a recent incident that impacted AT&T, one of the top three wireless providers in the US. In July, AT&T disclosed that c. 109m customer accounts were compromised as hackers stole mobile customers' data via a cybersecurity breach at the company's cloud storage provider, Snowflake. The stolen data primarily covered the period from May-Oct 2022 and included call and text records that reveal phone numbers contacted by AT&T customers, including those with landline services. The US Department of Justice stated that this breach would "pose a substantial risk to national security and public safety." This incident occurred just months after AT&T notified its customers in March about a separate discovery of a stolen dataset found on the dark web. This earlier data set included sensitive information, such as social security numbers for c. 7.6m current AT&T account holders and 65.4m former account holders.

- **Key takeaways from Cybersecurity Malaysia**

New Cybersecurity Act is but the first step. We hosted CSM, which was represented by: (i) Ts. Mohd Zabri Adil Bin Talib, Head of Division, Responsive and Technology Services, and (ii) Mohammad Fahdzli Bin Abdul Rauf, Acting Head, Cyber Solutions. CSM is the national cybersecurity specialist agency, operating under the Ministry of Communications and Multimedia Malaysia. Its main functions include: (i) Incident Response: Provides 24x7 computer security incident response services through MyCERT, (ii) Consulting and Support: Offers cybersecurity consulting, support services, and information security certification, (iii) Awareness and Training: Conducts programs to increase cybersecurity awareness and professional development, (iv) Research and Development: Engages in cybersecurity R&D and collaborates on international initiatives. The key takeaways are as follows:

Telcos are seen to be a NCII sector. Under CBSA 2024, the information, communication and digital sector is classified as one of the National Critical Information Infrastructure (NCII) sectors, encompassing the telco industry. Based on our interpretation, the telco industry qualifies as an NCII sector given that service disruptions will have a detrimental impact on the ability of the government to: (i) carry out its functions effectively, and (ii) deliver services that are essential to Malaysia's security, defence, foreign relations, economy, and public health, safety or order. We believe that cyberattacks on telco infrastructure leading to network failures can disrupt critical services (e.g. healthcare, transportation, and financial systems). Reliable telco services are thus crucial and align with UN SDGs such as: (i) SDG 9: *Build resilient infrastructure, promote sustainable industrialization and foster innovation*, and (ii) SDG 8: *Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all*. While SDG 9 aims to build resilient communication networks, SDG 8 emphasizes economic

growth which is reliant on resilient telco services for business continuity.

MCMC could play the role of a sector lead. CBSA 2024, which came into effect on 26 August, is expected to promote self-regulation regarding cybersecurity threats and incidents, and improve incident reporting by telco companies and other entities. CBSA 2024 outlines the duties and powers of the Chief Executive of NACSA (National Cyber Security Agency), the key executive agency responsible for imposing penalties for offenses and violations under this act. CBSA 2024 also defines the functions and duties of the NCII sector leads. The latter are government entities or persons who own or operate NCIIs, and are responsible for formulating practice codes on cyber security management for their respective sectors. For example, Bank Negara Malaysia (BNM) may serve as the sector lead for the banking and finance industry. According to CSM, the identity of the sector leads will be revealed by September. In addition, CSM does not discount the possibility that the Malaysian Communications & Multimedia Commission (MCMC) could potentially be sector lead for the telco industry.

Improved accountability for telcos on a "stick" approach. Given the crucial nature of the infrastructure operated by NCII entities, they must conduct a cyber security risk assessment at least once a year and carry out audits every two years. Under CBSA 2024, failure to submit the audit report will result in: (i) a fine up to RM200K, or (ii) imprisonment for a term up to 3 years, or both. Meanwhile, failure to comply with the Chief Executive's direction will result in a fine up to RM100k. In addition, authorized individuals (eg. Chief Security Officer or Chief Information Officer) of an NCII entity must report cyber security incidents electronically and submit initial details within six hours of awareness, followed by additional information within 14 days. Failure to do so may attract a fine of up to RM500k or imprisonment up to 10 years, or both. Meanwhile, the decision on whether to disclose each cyber incident to the public via mass media (or other means) will likely be determined by the NCII sector leads.

Propelling cybersecurity and hence ESG. We are positive on CBSA 2024 as prior to this, incidents of data breaches and telco network service disruptions caused by cyberattacks were likely under-reported by telcos. However, going forward, CSM expects telcos to increase their reporting efforts, as failure to notify authorities about cybersecurity incidents now constitutes a legal violation with material penalties. As reporting improves, telcos are expected to adopt stronger measures to protect their databases and network against future cyberattacks, thus reducing the risk of recurring failures. Furthermore, If telcos are required by their sector lead to reveal cybersecurity failures, we believe this would result in reputational damage. Erosion of confidence in the telco's ability to safeguard personal data could result in customer churn, leading to long-term financial losses.

Grace period for gradual transition. Nevertheless, according to CSM, there will be a transitional "grace period" of 2-3 years before full enforcement of CBSA 2024. This provides NCII entities with adequate time to adjust their cybersecurity practices and comply with the act's requirements. During this period, CBSA will focus on collecting data to assess the act's effectiveness, rather than imposing major penalties. This approach aligns with the government's intention to prioritize the prevention of cybersecurity incidents over penalizing offenses after they occur. In addition, we understand that NACSA may issue warning letters to NCII entities found in violation of CBSA 2024. This is to encourage voluntary compliance and rectification of cybersecurity issues to avoid legal consequences.

PDPA needs a refresh to adapt to new landscape. Building upon the success of CBSA 2024, the government plans also to improvise and modernize the PDPA, which governs the processing of personal data in commercial transactions. In CSM's view, the PDPA was gazetted over a decade ago in 2010, and remains a valuable and functional framework. However, updates are required to align it with current data protection standards. Hence, rather than effecting a complete overhaul, the amendments will focus on enhancing the act's effectiveness and relevance.

More legislation still ahead to protect telco user records. The government plans to potentially introduce legislation to protect consumers and non-NCII sectors from cybersecurity threats that could compromise personal data. This may include the 'Cybersecurity Resilience Act (CRA)' which will mandate cybersecurity certification for communication devices, including mobile handsets. This is expected to be similar to SIRIM certification, but focused on cybersecurity standards. In our view, it bears resemblance to the EU Cybersecurity Act (EUCA), which requires cybersecurity certification for ICT products, services, and processes. EUCA aims to enhance the resilience of devices and systems across the EU by establishing a certification framework to ensure products meet security standards. If CRA is implemented, we believe it would provide an additional layer of security to protect telco users' personal data. In addition, according to CSM, there are plans to potentially introduce an 'Omnibus Act' to regulate the sharing of personal data between public agencies to enable execution of their functions.

- **How have telcos been navigating cybersecurity for ESG compliance?**

Notable cybersecurity efforts signify commitment to ESG. Telcos' current cybersecurity efforts are commendable, aligning with their commitment to ESG principles and UN SDGs. In summary, these measures emphasize information security governance, endpoint control, and incident response. Key practices include data encryption, identity and access management, as well as ongoing security awareness training. Most telcos have established strategic programmes on cybersecurity and security operations centres to monitor threats and enhance cyber resilience. They also collaborate with partners to adopt new technologies and improve compliance with standards such as ISO 27001 and the PDPA. In addition, proactive threat hunting and phishing simulations are common among telcos to mitigate risks and protect customer data.

Proactive measures in cybersecurity education. Notably, CDB's comprehensive National Scam Awareness Survey 2024, released in July 2024, has been instrumental in raising public awareness about scams and frauds. It also highlights the proactive role taken by telcos to educate society on cybersecurity. The survey was conducted with communities from c.307 National Information Dissemination Centres (NADI), which provide internet access to underserved communities, particularly in rural areas. The findings revealed that 73% of respondents had either experienced scams, or were victims of scammers. For various reasons, respondents with higher education and income levels encountered greater incidence of attempted scams. The most common channels used by scammers were voice calls (76%) and text messages (51%). Despite the availability of the National Scam Response Centre hotline number (997), awareness remains low, with only 36% of respondents recognizing the hotline number.

But public disclosure on incidents need to ramp up. On the other hand, we believe telcos need to have greater transparency in public disclosures regarding data breaches and network disruptions. Accountability across the sector appears limited with the exception of TM, which reports data breaches for Unifi customers, and also issues updates on service and installation faults. Enhanced accountability could foster greater trust with customers, while motivating telcos to strengthen security measures to prevent future incidents that require public disclosure.

ESG boost from regulations. Full enforcement of CBSA 2024 is expected to enhance cybersecurity and reporting standards among telcos to ensure regulatory compliance. In particular, if CBSA sector leads require public disclosures of cybersecurity incidents, this would elevate accountability and enable telcos to meet their ESG goals. In the longer term, CBSA and potential future regulations will likely drive continuous advancements in data protection and cybersecurity. Thus, this will bolster the resilience of Malaysian telcos' databases and networks against evolving threats, bringing them closer to global ESG standards. We maintain our **OVERWEIGHT** recommendation on the sector with our top picks being TM and CDB. All our telco companies are currently rated 3 stars by Kenanga in terms of ESG ratings.

Peer Comparison

Name	Rating	Last Price (14/06/24) (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																	
AXIATA GROUP BHD	OP	2.50	2.75	10.0%	22,954.8	Y	12/2024	7.5	7.9	27.7%	4.4%	33.1	31.7	1.3	3.2%	10.0	4.0%
CELCOMDIGI BHD	OP	3.70	5.59	51.1%	43,406.6	Y	12/2024	15.3	16.3	-5.4%	6.4%	24.1	22.7	2.6	10.1%	12.0	3.2%
MAXIS BHD	MP	3.84	3.74	-2.6%	30,079.2	Y	12/2024	16.6	17.8	5.8%	7.4%	23.1	21.5	5.2	22.7%	20.0	5.2%
OCK GROUP BHD	MP	0.480	0.599	24.8%	512.8	Y	12/2024	3.3	3.8	-17.0%	13.9%	14.5	12.7	0.8	5.3%	1.0	2.1%
TELEKOM MALAYSIA BHD	OP	6.70	7.53	12.4%	25,712.6	Y	12/2024	45.7	46.3	-13.0%	1.2%	14.7	14.5	2.5	18.0%	23.5	3.5%
SECTOR AGGREGATE					**122,666.0**					**-2.6%**	**4.8%**	**22.1**	**21.1**	**2.5**	**11.8%**		**3.6%**

Source: Bloomberg, Kenanga Research **** (as of 14/06/2024)***

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, Jalan Tun Razak, 50400 Kuala Lumpur, Malaysia
Telephone: (603) 2172 0880 Website: www.kenanga.com.my E-mail: research@kenanga.com.my