Brief Ideas No.36

December 2022

Strengthening the Digital Trade Ecosystem: The Next Frontier for Malaysia

Farlina Said | Imran Shamsunahar | Juita Mohamad

IDEAS
INSTITUTE FOR DEMOCRACY AND ECONOMIC AFFAIRS

Authors

Farlina Said is a senior analyst in the Foreign Policy and Security Studies programme. She graduated from S Rajaratnam School of International Studies, Nanyang Technological University with an MSc (Strategic Studies). She was involved in crafting various dialogues and forums on cybersecurity, radicalisation and Malaysia-Korea relations. Her work and comments have appeared in the local and international media, such as New Straits Times and South China Morning Post. She was a part of SEARCCT's Experts on Violent Extremism and Community Engagement (EVOKE) Council (2018-2019).

Imran Shamsunahar is an Executive Researcher at the Economics and Business Unit. He focuses mostly on political economy and international trade. He received his Bachelors in History and Contemporary Asian Studies at the University of Toronto, as well as his Masters in Strategy and International Security from the University of Hull. He is also a freelance writer, having published pieces on the Asia Pacific in Nikkei Asia, the South China Morning Post, and National Interest. He's also been interviewed on Australia's ABC Radio National and quoted in Benar News.

Dr. Juita Mohamad is the Director of the Economics and Business Unit and the Director of Research at IDEAS. She has served as a Fellow in the Economics, Trade and Regional Integration (ETRI) Division of Malaysia's Institute for Strategic and International Studies (ISIS) and as an Economist at the Asia Desk, OECD Development Centre in Paris. Juita earned a PhD in International Studies (Economics Discipline) from Waseda University. Her current research interests include trade, regional integration, protectionism, wage inequality, the informal sector, and digital trade.

Table of Contents

Objective of the Study

The COVID-19 pandemic and the resultant lockdowns and social restriction measures put in place to contain it saw a global shift towards digital services by both consumers and businesses. This was no different for Malaysia, with a recent report by Google and Temasek estimating that Malaysia's Internet economy saw 47% growth between 2020 and 2021 in terms of gross merchandise value, while projecting further growth of 14% between 2021 and 2025.

To boost such growth, the digital trade environment needs to be supported in a timely manner. Investors and consumers alike must also feel secure in investing and using digital services. There needs to be an emphasis on establishing proper cybersecurity, transparent digital taxation frameworks, and data localisation policies. This policy report examines several areas that impact the digital economy, with a particular focus on how they impact the ICT and e-commerce sectors. Among the areas looked into include digital taxation frameworks, cross-border data flows, and data protection and privacy.

This report is one of the deliverables of the project titled, Strengthening the Digital Trade Ecosystem: The Next Frontier for Malaysia'. Funded by the Australian High Commission in Kuala Lumpur, this project aims to:

1. Identify the benefits and challenges in strengthening the digital trade ecosystem in Malaysia and how this can support further trade activities with existing partners like Australia to secure a sustainable economic growth and recovery from Covid-19 in the medium to long term.

2. Explore and examine existing laws and policies related to digital trade activities including regulations on labour movement, digital taxes and data localisation, cyber security among others.

3. Engage with different stakeholders (businesses, international investors, policy makers, government agencies) to gauge the extent of these challenges on the ground and examine international best practices.

4. Present policy recommendations on the factors needed to support the Malaysian digital trade activities within and beyond the country.

5. Conduct an engagement session with relevant stakeholders' from various ministries, agencies and organisations.

Executive Summary

The progress made in the financial sector coupled with advancements made from the 3IR and 4IR waves, subsequently followed by the rapid developments in disruptive technologies like the AI, robotics and blockchain have all played their part in transforming Malaysia's domestic economic landscape. This came soon after the government identified the digital economy and digital trade activities as bringing huge potential for Malaysia's future development.

According to the Department of Statistics Malaysia's (DOSM) Digital Economy 2018 report, Malaysia's digital economy, which includes the e-commerce and ICT sectors was estimated to be valued at about RM270 billion, or about 18.5% of GDP. Due to the rapid growth of the digital trade activities, boosted by the lockdowns and restrictions of movements during the pandemic, some estimates suggested that this share in GDP would have reached more than 20% by the end of 2020 (DOSM, 2018).

With the boom of investments in the ICT and e-commerce sectors, naturally this has led to digital trade transactions within Malaysia and beyond. Digital trade can be defined as "digitally-enabled transactions of goods and services that can be delivered physically or digitally". These transactions can include consumers, firms as well as governments. To be more specific, even though all types of digital trade are made possible by using digital technologies, not all forms of digital trade are delivered digitally. For instance, digital trade can involve a digitally-enabled platform, but the goods or services can be physically delivered or rendered to the consumer. Some examples include purchasing a physical book through an online bookstore or booking a stay on Airbnb for an apartment in the city.

This policy report examines two components of the digital trade ecosystem; namely taxing the digital economy and cybersecurity components. Taxing the digital economy is not an easy feat by any standard. Recognising the tax-related challenges that the digital economy brings as well as the concurrent limitations of contemporary taxation methods, over the last five years the Malaysian government has either introduced or proposed a series of taxes directly or indirectly targeting the digital economy. The immediate justifications for introducing or proposing such taxes have largely centred on i) ensuring Malaysia's taxation framework remains adequate for the digital economy as well as ii) levelling the playing field for local businesses. Recently implemented or proposed taxes targeting the digital economy can be broken down into direct and indirect taxation. These taxes include Sales Tax (Amendment) Bill 2022), Service Tax on Digital Service and Tourism Tax (Amendment) Act 2021 among others. In an engagement session with selected stakeholders in Malaysia, some have raised a variety of concerns about digital taxes either already proposed or introduced in Malaysia over the last few years. These concerns include confusion over definition and double taxation, lack of transparency in implementation plans and increasing cost of doing business.

On the cybersecurity side, in today's interconnected environment, harm from undiscovered vulnerabilities or lax processes in compliance can have terrible consequences. Failures in oversight mechanisms can result in a data breach as exploited vulnerabilities can create opportunities for crime. Further, as governments are exploring methods to secure data such as implementing data localisation measures, the burden of due diligence increases. Thus, cybersecurity becomes more than securing systems. It has become a whole of government and whole of nation endeavour, needing various parties from an informed public to effective enforcement agencies.

Malaysia can be considered as one of the more digitised countries in the world with a culture that is positive for technology adoption. In 2015, approximately 70.1% of Malaysian households were connected to the internet. The trend continued to grow, as a year prior to the pandemic, more than 90.1% of Malaysian households had access to the internet. Internet access in Malaysia can be structured in individual or household access. In 2021, more than 95% of individuals are online while household computer access reached 88.3%. Household mobile access was at 99.6% and individual internet access peaked at 96.8%. Covid-19 has further aided Malaysia's digitalisation process through the lockdowns that forced the public and private sector to utilise cyberspace for economic and social needs. According to surveys conducted by the Malaysia Communications and Multimedia Commission (MCMC), Internet activities in Malaysia remain predominantly focused on social networking purposes, with more than 90% using the internet for messaging (96.5% in 2018 and 98.1% in 2020).

However, Malaysia's maturing digital landscape must contend with several challenges, including overlaps in jurisdiction of regulating and enforcing bodies, challenges to data governance and creating the culture of cybersecurity to match a positive technology-adoption outlook. By 2021, Malaysia typically records approximately 10,000 cyber incidents reported to MyCERT. Incident reporting is practised by operators of the Critical National Information Infrastructure (CNII) with Sector Leads and National Cyber Coordination and Command Centre (NC4), the cyber coordination centre under NACSA.

Malaysia has two data classification regimes where obligations for cybersecurity are in accordance with the data user. For the private and commercial sector, the Personal Data Protection Act (PDPA) 2010 states that data management should be in line with the 7 principles of data protection, which are (i) the General Principles, (ii) the Principles of Notice and Choice, (iii) Disclosure Principle, (iv) Principles of Safety, (v) Retention Principle, (vi) Data Integrity Principles, and (vii) Access Principle. Data classification

for the government differs from those of the commercial sector with the central document for the classification being the OSA 1972. The Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS), articulates information classification for the government which are graded into four classifications: Top-Secret, Secret, Confidential and Restricted (MAMPU, 2002). The classifications are elaborated further in preparation of adopting cloud technology, the goal announced in the Malaysia Digital Economy Blueprint or MyDigital.

Under the PDPA, data localisation requirements are not imposed. The PDPA does state that transfers to third countries should only be possible if the country is approved or whitelisted. However, potential updates to the PDPA proposes a 'blacklist' approach instead, which could address differences in data management. Conversely, data managed by the government takes a data residency approach where the department opting for cloud computing should know the 'source of origin' for the cloud computing services. This is inclusive of understanding the data flows and data residency processes to ensure that the information and strategic data could not be addressed by foreign powers.

As such, Malaysia's cross-border data policies are concerned of weak cybersecurity practices outside of jurisdiction that could allow unwanted access to data centres. Jurisdiction issues will also cause problems for the government to collect evidence for investigations. The emphasis is for storage and processing to be under the control and jurisdiction of the Malaysian Government. Thus, while the guidelines would not prohibit the usage of data centres residing abroad to store data in accordance with the relevant information classification, the departments may store data locally for the convenience of compliance.

The dual data regimes indicate the expectations for compliance and the levels of security accorded to the data user whether it is government or the private sector. As enforcement of the laws are under different agency jurisdictions, the cybersecurity environment can cause confusion. As such, enforcement for data-related issues for the public sector is under CGSO, MAMPU and PDRM while those for the private sector is under the PDPD, PDRM and MCMC.

Moving forward there are ways to improve both the taxation framework and the cybersecurity components. Firstly there needs to be transparency in the introduction of taxes in the digital economy. Secondly, capacity building is needed in creating a sustainable digital taxation framework. Thirdly, Malaysia needs to develop and standardise efforts for cybersecurity, due to the high cost and investment of cybersecurity, the barriers for consistent cybersecurity updates to the system may burden smaller players like the SMEs. Fourthly, Malaysia's cybersecurity agencies should consider increased transparency in data breach investigations as currently the PDPD does not publicise investigation activities though court cases and compounds have been ongoing. Finally, Malaysia needs to embark on Digital Economic Partnerships in multilateral forms that would stimulate the digital economy and build rules-based environments for cyber as well as the digital taxation framework.

1. Taxing the Digital Economy

1.1 Background on Malaysia's Digital Economy

The progress made in the financial sector coupled with advancements made from the 3IR and 4IR waves, subsequently followed by the rapid developments in disruptive technologies like the AI, robotics and blockchain have all played their part in transforming Malaysia's domestic economic landscape. This came soon after the government identified the digital economy and digital trade activities as bringing huge potential for Malaysia's future development.

According to the Department of Statistics Malaysia's (DOSM) Digital Economy 2018 report, Malaysia's digital economy which includes the E-commerce and Information Technology sectors was estimated to be valued at about RM270 billion, or about 18.5% of GDP. Due to the rapid growth of the digital trade activities boosted by the lockdowns and restrictions of movements during the pandemic, some estimates suggested that this share in GDP would have reached more than 20% by the end of 2020 (DOSM, 2018).

Nevertheless, it is clear that due to the pandemic, the digital economy's share of the whole economy has surpassed that mark. In its latest report in 2020, the Information and Communication Technology Satellite Account recorded that the ICT and E-commerce sectors reached the value of RM320 billion that year. This value represents about 23% of total GDP. To break it down even further, the ICT component contributed to about 14% of GDP while E-commerce activities represented about 8% of the GDP in that specific year (DOSM, 2021).

The report further elaborated that in terms of employment the ICT sector employed 1.2 million workers, and this represents 7.7% of total employment in the formal sector. Compensation to employees stood at 37% of total income from the ICT sector. In 2020, at the onset of the pandemic, it was found that usage of the internet increased not only among the urban population but also among the rural population, reaching 92% and 79% respectively (DOSM, 2021).

The rise of e-commerce activities and the ICT sector coincides with developments of regional and international digital trade. Digital trade can be defined as "digitally-enabled transactions of goods and services that can be delivered physically or digitally". These transactions can include consumers, firms as well as governments. To be more specific, even though all types of digital trade are made possible by using digital technologies, not all forms of digital trade are delivered digitally. For instance, digital trade can involve a digitally-enabled platform, but the goods or services can be physically delivered or rendered to the consumer. Some examples include purchasing a physical book through an online bookstore or booking a stay on Airbnb for an apartment in the city.

1.2 Malaysia's growing data centre market

The boom in the ICT sector within the digital economy ecosystem was long fueled by the rapid expansion of data centers in Malaysia. According to a 2019 report by global real estate services firm Cushman & Wakefield, the Southeast Asia region was projected to be the fastest growing region for coocation data centres over the next five years, with its market size expected to expand by a compounded annual growth rate (CAGR) of 13% between 2019 and 2024. In the Cushman & Wakefield's Data Centre

Competitive Index 2019 rankings for the Asia Pacific region, Malaysia was ranked fourth behind Singapore, Hong Kong, and South Korea. The index determines the competitiveness of a country in the data centre market in terms of factors such as physical, economic and social attributes like connectivity, ease of doing business, political stability, corporate tax rate, natural disaster and energy security. The report projected that Malaysia's data centre market would expand by 12.9% between 2019 and 2024 (Cushman & Wakefield, 2019).

Real estate service firm JLL has noted that there is an increasing pattern of data centre providers choosing to locate their data centre campuses outside of the more advanced developed markets of Hong Kong and Singapore, with Southeast Asian countries being the likely choices. Malaysia in particular has been described as the preferred data centre location in Southeast Asia after Singapore and Indonesia, owing to solid connectivity and high internet penetration. The Malaysian government's MyDigital Framework, which encourages companies and investments to venture into data centres and cloud computing, has also played a part in facilitating Malaysia's data centre market (The Edge, 2022, Arizton Advisory and Intelligence, 2022).

According to data by the Malaysia Digital Economy Corporation (MDEC), Malaysia currently has a total of 17 data centres across the country. Among the companies which have sought to invest in data centres in Malaysia include Microsoft, which in 2021 announced plans to establish its first data centre in the country to deliver cloud services locally. In the second half of 2022, Google also stated it plans to include Malaysia as its new Google Cloud region, an investment that will involve a data centre (MDEC, 2022, The Star, 2022).

1.3 Existing framework for taxing the digital economy

Recognising the tax-related challenges that the digital economy brings as well as the concurrent limitations of contemporary taxation methods, over the last five years the Malaysian government has either introduced or proposed a series of taxes directly or indirectly targeting the digital economy. The immediate justifications for introducing or proposing such taxes have largely centred on i) ensuring Malaysia's taxation framework remains adequate for the digital economy as well as ii) levelling the playing field for local businesses. Recently implemented or proposed taxes targeting the digital economy can be broken down into direct and indirect taxation (see Table 1).

Table 1: Types of Taxation

	Indirect Taxation	Direct Taxation
Implemented	Sales Tax (Amendment) Bill 2022	Updated Guidelines on Taxation of Electronic Commerce Transactions
	Service Tax on Digital Services	
	Tourism Tax (Amendment) Act 2021	
Proposed	Service Tax on Goods Delivery Services	

Source: Parliament of Malaysia, Royal Malaysian Customs Department, Malaysian Inland Revenue Board

1.3.1 Indirect Taxation on the Digital Economy

Sales Tax (Amendment) Bill 2022

In August 2022, the Dewan Rakyat passed the Sales Tax (Amendment) Bill 2022, which seeks to impose a flat 10% sales tax on goods purchased online and delivered to Malaysia by vendors registered with the finance ministry. This flat rate will be imposed on low-value goods (LVG) sold online that are priced below RM500, as under the current sales tax such goods are exempt from taxation. The new tax rate will be implemented in 2023, and the government expects to collect some RM200 million in 2023 from the tax (Parliament of Malaysia, 2022).

According to a piece by news outlet The Edge, Malaysia's then Deputy Finance Minister I Datuk Mohd Shahar Abdullah defended the new tax by pointing out that the expansion of the sales tax was one of the steps under the government's revenue sustainability initiative, which was announced in Budget 2022. He also noted that taxing such goods sold online was in line with economic development and the Organisation for Economic Cooperation and Development's (OECD's) International VAT/GST Guidelines published in 2017, which outlines the proposed indirect tax on transactions involving cross-border transactions in addressing the challenges of taxing the e-commerce economy (The Edge 2022).

The government has also justified the tax by arguing that it would level the playing field between traders both inside and outside Malaysia, therefore empowering local manufacturers and businessmen. Under the current system, low-valued goods priced RM500 and below are not subject to any tax when they are imported to Malaysia in accordance with the de minimis facility. According to the government, this has caused unfair treatment to local traders as locally-produced goods are subject to the sales tax (The Edge 2022).

Service Tax on Digital Service

Effective from 1st January 2020, a foreign registered provider (FRP) that provides a digital service to any consumer in Malaysia will be required to pay service tax at the rate of 6%. This comes after the Malaysian government amended the current service tax legislation under the SST to make foreign service providers (FSP) who provide digital services to Malaysian consumers liable to be registered as an FRP. An FSP will only be subject to registration if their annual revenue from digital services exceeds RM500,000 (RMCD, 2021).

Like the amendments made to the sales tax, the service tax was amended to ensure equal treatment within the industry. Prior to the implementation of the digital service tax, taxable services provided by service providers within Malaysia were subject to service tax under the SST (RMCD, 2021).

Malaysia has been described as one of the pioneer countries in Southeast Asia in extending the scope of its indirect tax to cover the supply of foreign digital services. Prior to the implementation of the Malaysian digital services tax, it was anticipated that the new tax would increase tax revenue by more than RM2.4 billion a year. However, the Malaysian government was only able to collect RM428.07 million from foreign service providers in 2020. Notwithstanding this, such a new taxation trend seems to be the right approach to increasing revenue collection for the government (Kumar and Yap Wen, 2021).

Service tax on goods delivery services

In Malaysia's 2022 Budget, it was proposed to expand the scope of service tax to include goods delivery services regardless of the status of the service providers (whether licensed or not). This new tax would exclude delivery services for food and beverages as well as logistic services. Initially set to take effect 1 July, 2022, on 30 June, 2022, the Royal Malaysian Customs Department announced the postponement of the implementation of service tax on goods delivery services to a later date. To date, it is unknown when the new tax on goods delivery services will take effect instead (KPMG 2022, RMCD, 2022).

Tourism Tax (Amendment) Act 2021

The Tourism Tax (Amendment) Act 2021 was set up in February 2021 and sought to impose a digital tax on accommodation premises reserved through digital platform service providers (in this case RM 10 per room per night). Tourists who are Malaysian nationals or permanent residents of Malaysia are exempt from the tax. Prior to the amendment, tourists who booked their accommodation through online booking platforms were exempt from paying the tourism tax, which would be paid to the operators of accommodation premises through direct booking. Originally scheduled to take effect on 1 July, 2021 the tax was postponed in Budget 2022 until 31 December, 2022 (Parliament of Malaysia, 2021, Ramesh Dipendra Jeremiah Law 2021).

1.3.2 Direct Taxation on the Digital Economy

Updated Guidelines on Taxation of Electronic Commerce Transactions

In May 2019, the Malaysian Inland Revenue Board (IRB) published its updated Guidelines on Taxation of Electronic Commerce Transactions, replacing the earlier guidelines released in January 2013. The IRB decided to update the guidelines in response to the evolvement of the e-commerce sector and the development of new business models (IRB, 2019, Ernst & Young, 2019).

Under the "scope of charge" of income tax, the 2019 Guidelines state that any income in relation to e-commerce is deemed to be derived from Malaysia if it is associated with any activities in Malaysia regardless of whether that income is received in Malaysia or otherwise (IRB, 2019, Ernst & Young, 2019).

Additionally, under the "scope of tax liability for business," the 2019 Guidelines stipulate that for business income, where the business operations are carried on in Malaysia, the income attributable to those business operations is deemed to be derived from Malaysia. According to the guidelines, whether or not a business' income is considered derived from Malaysia is a question of fact and degree. The wider the scope and extent of the business operations in Malaysia, the greater the likelihood that the income of those operations is subject to taxation in Malaysia (IRB 2019, Ernst & Young, 2019).

1.4 Concerns raised about digital taxation

In an engagement with selected stakeholders in Malaysia, some have raised a variety of concerns about digital taxes either already proposed or introduced in Malaysia over the last few years. These concerns include:

- Confusion over definition and double taxation: in the case of the recently amended sales tax, concerns were raised about whether the definition of "seller" may include both sellers on online marketplaces and the online marketplace operators themselves, leading to the possibility of double taxation if both decide to charge the sales tax. Similar concerns were also raised about the digital services tax, especially if a Malaysian business falls within the ambit of 'digital services' and 'imported taxable services' (Deloitte, 2022, Kumar and Yap Wen, 2021).

- Lack of transparency: concerns have been raised by the private sector about how certain taxes have been implemented without adequate details and time to prepare accordingly. In the case of the amended sales tax, businesses have been given less than five months to implement the rules without the relevant rules and regulations being released (Deloitte, 2022).

- Cost of business: stakeholders have noted that the introduction of certain taxes may raise the cost of doing business. Beyond simply paying taxes, the expansion of digital trade will also be upended by the greater requirements for tax reporting. Much of this reporting burden will fall on intermediaries within the digital economy, especially on smaller firms without the resources and capacity to address compliance concerns. Increasingly, firms will be asked to submit, on behalf of customers or clients, a wide and growing range of tax-related information on business sales to tax authorities. This will also challenge the competitiveness of Malaysia, as well as possibly discourage foreign investments (Elms, 2021).

1.5 Twin-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy

In response to these challenges, in 2013 the OECD and G20 initiated the OECD/G20 BEPS Project, whose ultimate goal was the implementation of an international framework to combat tax avoidance by multinational enterprises using BEPS tools. The OECD described BEPS, or base erosion and profit shifting, as tax planning strategies used by multinational enterprises which exploit gaps and mismatches in tax rules to avoid paying tax. In 2015, a 15-point action plan was released, in which 'Digital Economy' was identified as one of the action plans needed to tackle tax avoidance, improve the coherence of the international tax system, and ensure a more transparent tax environment. In 2016, the OECD/G20 Inclusive Framework on BEPS (IF) was established to ensure interested countries and jurisdictions, particularly developing economies, can participate on an equal footing in the development of standards on BEPS related issues, as well as review and monitor the implementation of the OECD/G20 BEPS Project (OECD, 2018).

On 8th October, 2021, 137 countries and jurisdictions joined a landmark agreement on a Twin-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy (often shortened to the Two-Pillar Solution). The Two-Pillar Solution was the outcome of intensive work carried out under the BEPS Action 1 "Addressing the tax challenges arising from the digital economy", and builds upon the

Two-Pillar approach established in January 2019. Among the signatories to the Two-Pillar Solution was Malaysia (OECD, 2022, OECD, 2021).

The Two-Pillar Solution agreed upon in October 2021 is broken down as such:

- Pillar One: This pillar specifically aims to reallocate taxing rights over a portion of the residual profits of MNEs (Amount A) to the market countries and jurisdictions where they have business activities, regardless of whether they have a physical presence there or not (thereby ensuring a fairer distribution of taxing rights). Specifically, multinational enterprises with global revenues above EUR 20 billion and profitability above 10% will be covered by the new rules, with 25% of their consolidated group profit over and above the 10% profit margin to be reallocated to market jurisdictions using a formulaic approach (OECD, 2021).

  Amount B, on the other hand, refers to the profit generated by distribution and marketing activities to be reallocated to market jurisdictions. The OECD proposes that each market jurisdiction could include in its tax base a share of profits generated by such activities. Amount B would be calculated as a baseline percentage of such profits generated in the market jurisdiction.

- Pillar Two: This pillar specifically introduces a 15% global minimum tax that applies to MNE groups with consolidated revenues of at least EUR 750 million. They consist of a coordinated system of rules, under common framework, which ensures in-scope MNE groups pay at least the agreed minimum level of tax on the income arising in each of the jurisdictions in which they operate (OECD, 2021).

In terms of progress made in implementing both pillars, with regards to Pillar 1, the OECD reported that significant progress has been made on the design of the technical rules for the reallocation of taxing rights under Amount A. As such, the implementation timeframe for Pillar 1 has been set to 2024 (OECD 2022).

With regards to Pillar 2, in December 2021 the OECD released the model rules that sets out the structure of Pillar 2 along with additional technical guidance on their operations. An Implementation Framework is due to be completed by the end of 2022 to support domestic implementation and administration of the model rules, with the OECD envisaging Pillar Two to take effect in 2023 (OECD, 2022).

In Malaysia's Budget 2023, it was announced that Malaysia would seek to implement the global minimum tax as recommended under Pillar 2 of the Twin Pillar Solution in order to broaden its tax base while also remaining competitive in terms of attracting foreign direct investment. It had earlier been stated by Malaysia's then Finance Minister Tengku Datuk Seri Zafrul Aziz that Malaysia is expected to start implementing the Twin Pillar Solution in 2024 (The Edge, 2022, Malay Mail, 2022).

Ultimately, the implementation of the Twin Pillar Solution will compliment Malaysia's own goals when it comes to taxing the digital economy, namely of ensuring Malaysia's taxation framework remains adequate for the digital economy (by tackling the issue of how to tax companies with no physical presence in the country) as well as levelling the playing field for local businesses (by preventing a race down to zero between countries when it comes to attracting FDIs). That being said, the global minimum

tax still contains carve outs, meaning not all companies and investments will fall under the Pillar 2 measures. Moving forward, Malaysia will need to take a more holistic approach to its tax incentive structure including both fiscal and non-fiscal incentives.

1.6 The Challenges of Taxing the Digital Economy

It is becoming commonly perceived that the digital economy is less taxed and regulated than other sectors of the economy. While digitalization has allowed businesses to generate revenue from a wider consumer base, including from outside markets, it has also indirectly led to tax leakages as e-commerce businesses generally do not pay taxes in foreign jurisdictions where they do not have a physical presence. This has been identified as a major limitation in the current international tax system, which was designed in the age of the brick and mortar economy and where governments focused on taxing firms with a physical presence in their country (Athanasaki, 2020, Hufbauer and Hogan, 2022).

This has disproportionately affected developing countries, who often have a higher reliance on corporate income tax to fund government. As observed by Athanasaki, the digital economy has created an artificial segregation between the place of value creation and the place of taxation, creating challenges from a taxation perspective (OECD, 2017, Athanasaki, 2020).

A policy brief by the ADB lists several challenges about taxing the digital economy which modern taxation frameworks remain inadequate in addressing. These include (ADB 2017):

- The intangible nature of digital goods and services: traditional tax policies are rooted in clear-cut jurisdictional barriers. This is directly linked to the assumption that brick-and-mortar physical locations where goods and services are produced could signify physical presence (also known as a permanent establishment), and they could be used to determine where tax must be paid. In the digital economy, almost all commerce along the supply chain is done virtually without a significant physical presence in one or any jurisdiction, although a company may still have physical stores, factories, or warehouses.

- Difficulty of collecting value-added tax on digital cross-border trade: this issue stems from challenges to do with anonymity and difficulty of identifying companies in the digital economy, the absence of a paper trail, determining the amount of tax, and the increased ability to conceal incomes and assets offshore using tax havens.

- Difficulty in domestic enforcement of the peer-to-peer or gig economy: determining the tax implications of workers in the gig economy, such as workers of an online taxi, car transportation, or food delivery mobile app who use their own cars, and whether they are considered employees or self-employed independent contractors.

- Logistical issues and administrative capacity: there are also logistical challenges as the digital economy has bolstered the cross-border movement of people, goods, and services as well as the number of economic agents operating in the system. Such an increase in numbers presents a greater workload for tax administrators, making administering tax law effectively more difficult.

Strengthening Malaysia's tax capacity will be more important than ever in the post-pandemic economy. As noted by the ADB in a March 2021 brief, despite consistently strong GDP growth in many Southeast Asian countries in recent years, tax yields have not increased in tandem. Even prior to the pandemic, many countries had failed to achieve the desired tax yield of 15% of GDP, a level seen as the minimum required for sustainable development. In the case of Malaysia, tax revenues as a share of GDP measured at 12.5% in 2018, one of the lowest in the region. This situation has been aggravated by the pandemic, which increased pressure on public expenditure and decreased tax revenue. Indeed, Malaysia's 2023 Budget, which focused on alleviating rising cost of living due to higher interest rates and inflationary pressures, would be the largest ever tabled at RM372.3 billion. As such, implementing wholesale tax reforms to broaden Malaysia's currently narrow tax base will be more crucial than ever (ADB, 2021, The Edge, 2022).

1.7 International Best Practices: ASEAN and Taxing the Digital Economy

As mentioned previously, all across Southeast Asia governments have struggled to raise their tax yields despite consistently strong GDP growth rates, with many countries failing to achieve the minimum required tax yield level of 15% of GDP. Their lack of tax capacity has been aggravated by the COVID-19 pandemic, which forced ASEAN governments to ramp up public expenditure while overseeing a shrinking tax base. With a robust digital economy and booming e-commerce market, many ASEAN governments have targeted the digital sector with new levies (ADB, 2021).

Like Malaysia, these new levies are motivated by a desire to ensure national taxation frameworks remain adequate for the digital economy, as well as to level the playing field for local businesses. Some of the measures recently introduced by ASEAN governments over the last few years can be seen in Table 2.

Table 2: Taxation Policies Introduced

Countries	Taxation policies introduced	Date introduced	Digital economy sector targeted
Cambodia	Cambodia introduced Sub-Decree 65, which requires VAT-registration by non-resident entities with no physical presence in Cambodia but that provide e-commerce services to domestic consumers.	April 2021	E-commerce
Indonesia	The Government of Indonesia will start collecting VAT from e-commerce activities in Indonesia. Under the previous regulation, the VAT only applied to certain intangible goods and services provided online to Indonesian consumers from overseas. The updated VAT covers streaming services, mobile applications and digital games.	June 2020	E-commerce
Singapore	The Goods and Services Tax Act (Chapter 117A of Singapore) ("GST Act") provides for GST to be levied on the provision of web-based digital services by an overseas supplier to local customers	October 2021	E-commerce and digital services
Thailand	The Act Amending the Revenue Code No. 53 (the "Act") introduces VAT on electronic services consumed by non-VAT registered service recipients that are either supplied by overseas service providers or supplied through overseas electronic platforms	February 2021	Digital services

Source: Sheehan, Jack and O'Connell, Clint, 2021, Vertex, 2022, Tilleke & Gibbons, 2021

2. Cross Border Data Flow, Data Protection and Cybersecurity

The second component for digital trade is cybersecurity. In today's interconnected environment, harm from undiscovered vulnerabilities or lax processes in compliance can have terrible consequences. Failures in oversight mechanisms can result in a data breach as exploited vulnerabilities can create opportunities for crime. Further, as governments are exploring methods to secure data such as implementing data localisation measures, the burden of due diligence increases. Thus, cybersecurity becomes more than securing systems. It has become a whole of government and whole of nation endeavour, needing various parties from an informed public to effective enforcement agencies.

2.1 Malaysia's cybersecurity environment in 2022

Malaysia can be considered one of the more digitised country in the world with a culture that is positive for technology adoption. In 2015, approximately 70.1% of Malaysian households are connected to the internet. The trend developed with positive growth as a year prior to the pandemic, in 2019, more than 90.1% of Malaysian households have access to the internet (DOSM, 2021). Internet access in Malaysia can be structured in individual or household access. In 2021, more than 95% of individuals are online while household computer access reached 88.3%. Household mobile access was at 99.6% and individual internet access peaked at 96.8% (DOSM, 2021). Covid-19 has further aided Malaysia's digitalisation process with lockdowns that forced the public and private sector to utilise cyberspace for economic and social needs. However, the Malaysia Communications and Multimedia Commission (MCMC), have surveyed Malaysia's internet activities to remain predominantly for social networking purposes, with more than 90% using the internet for messaging (96.5% in 2018 and 98.1% in 2020).

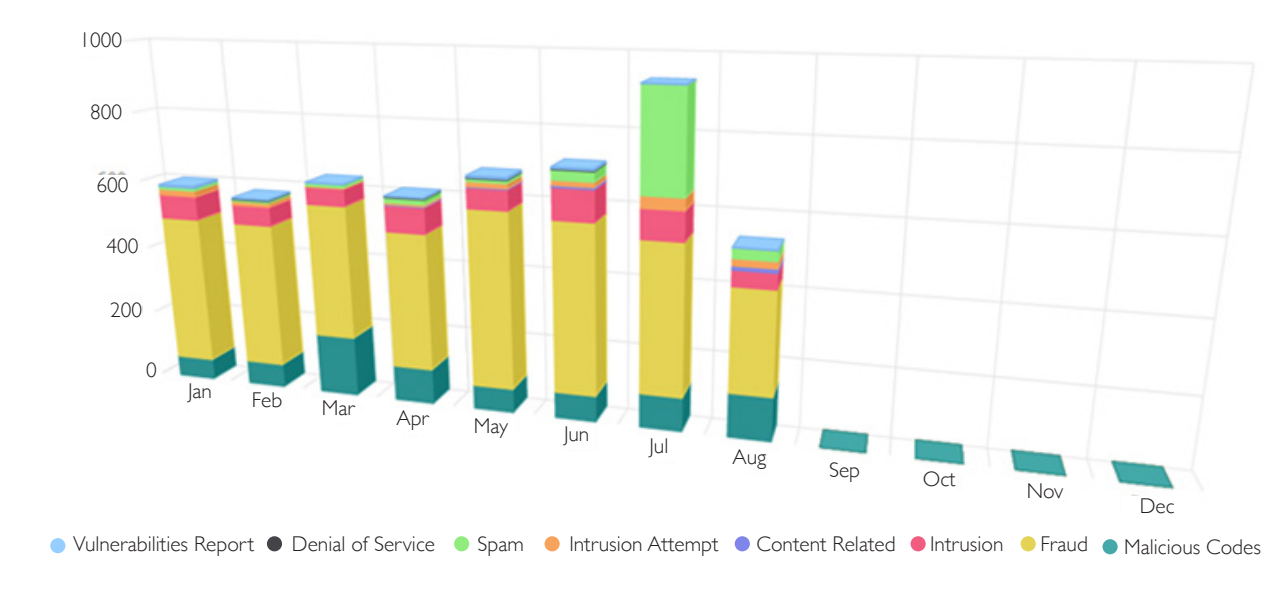
Since the turn of the millennium, Malaysia has placed ICT as a priority. Malaysia was among the first in the region to formulate a National Cyber Security Policy in 2006 and Malaysia's computer-crime related legislations such as the Communications and Multimedia Act 1998 and the Computer Crime Act 1997 accompanied Malaysia's ambitions to build the knowledge economy. Thus the approach for cybersecurity developing in tandem with economic ambitions can be illustrated by the developments of laws and policies alongside development goals such as the 8th Malaysia Plan and the Multimedia Super Corridor (MSC) policies. The MSC status is succeeded by Malaysia Digital though preserving the 10 Bill of Guarantees that includes ensuring no censorship of the Internet (MDEC 2022). As Malaysia develops the knowledge economy alongside cybersecurity policies, Malaysia's traditional approach to digital governance can be considered open to cross border data flows, is technologically-neutral and is oriented towards protection of critical infrastructure and government modernisation.

Malaysia's goals and ambitions are enshrined in policies and documents such as the Malaysia Digital Economy Blueprint, National Cyber Security Strategy 2020-2024, the Defence White Paper, the National Policy on Science, Technology and Innovation 2021-2030 as well as the 10-10 Malaysian Science, Technology, Innovation and Economy (MySTIE) Framework. Malaysia's commitment to the knowledge economy and cybersecurity bears fruit in Malaysia's global positioning in cyber. The World Economic Forum's Global Competitiveness Report in 2019 places Malaysia 33rd out of 141 for ICT adoption (WEF 2019). In addition, the Belfer Center's National Cyber Power Index 2020 places Malaysia 19th out of 30 for Malaysia's cyber capabilities (Voo, Hemani et al, 2020), while in the Cyber Security Index 2020 report by International Telecommunications Union (ITU), placed Malaysia fifth on the list, demonstrating the country's commitment to cybersecurity (Bernama 2022).

2.2 Malaysia's cybersecurity landscape

However, Malaysia's maturing digital landscape can feature conflicts and overlaps in jurisdiction of regulating and enforcing bodies. Further, challenges to data governance and creating the culture of cybersecurity impact cybersecurity that matches Malaysia's positive technology-adoption outlook. By 2021, Malaysia typically records approximately 10,000 cyber incidents, reported to MyCERT (MyCERT nd). Incident reporting is practised by operators of the critical national information infrastructure (CNII) with Sector Leads and National Cyber Coordination and Command Centre (NC4), the cyber coordination centre under NACSA. The practise is in place since the National Cyber Security Policy was introduced and supported by policies such as the National Security Council Directive No. 24 (*Arahan Majlis Keselamatan Negara* No 24) and coordination exercises such as X-MAYA (MKN nd). However, yearly figures can be under-represented as it would not include those unreported or addressed internally by the private sector who are not operators of CNII.

Figure 1: Reported Incidents based on General Incident Classification Statistics 2022



Source: Incident Statistics (2022) CyberSecurity Malaysia MyCERT

Table 3: Reported Incidents based on General Incident Classfication Statistics 2022

	JAN	FEB	MAC	APR	MAY	JUN	JUL	AUG	TOTAL
Vulnerabilities Report	6	3	3	4	5	5	3	2	31
Denial of Service	0	2	1	1	4	2	0	1	11
Spam	8	5	6	15	7	27	286	27	381
Intrusion Attempt	15	12	4	6	15	14	32	21	119
Content Related	2	0	0	2	2	7	1	10	24
Intrusion	68	54	50	74	59	89	82	45	521
Fraud	431	423	388	396	509	486	429	294	3,356
Malicious Codes	62	68	174	103	70	75	98	124	774
Total	592	567	626	601	671	705	931	524	5,217

Source: Incident Statistics (2022) CyberSecurity Malaysia MyCERT

The above figure depicts the incident statistics until the month of August in 2022, where incidences reported reflect the type of activities in Malaysia's cybersphere. Typically, Malaysia records high fraud and intrusion attempts where in 2021 and 2019, there were 7,098 and 7,774 incidences reported for fraud and 1,410 and 1,359 reports of intrusions, respectively. Further, there are reports of an increase in ransomware, with greater alerts for concerns of data leakages and unauthorised data access. For instance, Trend Micro reported a 282% year-over-year increase of ransomware attacks in the first half of 2022 (Murugiah, 2022). Malaysia's cybersecurity concerns would include content-related matters, inclusive of defamation and sedition.

Meanwhile, high profile data leakages in recent months have raised concerns of vulnerabilities in data management. Circa September 2021, the possible data breach of the National Registry Department (JPN) is linked to the availability of a database containing personal information of four million Malaysians online (SERI 2021). Close to a year later, the information of 22 million Malaysians also allegedly linked to JPN is found for sale (Morden 2022). These are interspersed with careless data management such as those occurring to the Public-Private Covid-19 Industrial Immunisation Programme (PIKAS) managed by the Ministry of International Trade and Industry (Boo 2022).

Lastly, Malaysia was featured in reports by the private sector associated with advanced persistent threats (APT) intended for information gathering purposes such as APT30 and APT40 (MyCERT 2022). The APTs may be an extension of conflicts in the South China Sea or to gain information on government-sponsored projects.

2.3 Malaysia and Data Protection

Malaysia has two data classification regimes where obligations for cybersecurity are in accordance with the data user. For the private and commercial sector, the Personal Data Protection Act (PDPA) 2010 states that data management should be in line with the 7 principles of data protection, which are (i) the General Principles, (ii) the Principles of Notice and Choice, (iii) Disclosure Principle, (iv) Principles of Safety, (v) Retention Principle, (vi) Data Integrity Principles, and (vii) Access Principle. Data is classified into "personal data" and "sensitive personal data" where personal data is any information related directly or indirectly to a data subject that could identify or be identifiable in conjunction with other information in the possession of a data user or collector. Meanwhile, "sensitive personal data" means any personal data consisting of information such as physical or mental health or condition of a data subject, political opinions, religious beliefs or other beliefs of a similar nature. The classification bears significance for security and data management practices.

Data classification for the government differs from those of the commercial sector with the central document for the classification being the OSA 1972. The Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS), articulates information classification for the government which are graded into four classifications: Top-Secret, Secret, Confidential and Restricted (MAMPU, 2002). The classifications are elaborated further in preparation of adopting cloud technology, the goal announced in the Malaysia Digital Economy Blueprint or MyDigital. Thus, a fifth classification, 'public' allows data to be placed in the cloud. The introduction of guidelines such as the Guidelines for the Management of Information Security through Cloud Computing in the Public Sector identify the respective security practices and requirements of systems for each classification grade (PMD 2021). Restricted and Confidential official secrets could be facilitated by private clouds developed and

permitted by the government. Meanwhile Secret and Top-Secret require the highest discretion thus departments opting for cloud need to consult with CGSO for practices.

Under the PDPA, data localisation requirements are not imposed. The PDPA does state that transfers to third countries should only be possible if the country is approved or whitelisted. However, potential updates to the PDPA proposes a 'blacklist' approach instead, which could address differences in data management. Conversely, data managed by the government takes a data residency approach where the department opting for cloud computing should know the 'source of origin' for the cloud computing services. This is inclusive of understanding the data flows and data residency processes to ensure that the information and strategic data could not be addressed by foreign powers. Further, government departments are encouraged to anchor approaches with data sovereignty where the departments has to refer to legal requirements and jurisdiction where the data will physically reside. Data sovereignty considerations are to identify (i) the data management and stakeholders in the relevant department (ie appoint a dedicated CIO if needed), (ii) data security, (iii) physical geographical location and residency of the data, (iv) the rules, procedures and laws, (v) security risks, (vi) data classification, (vii) ownership of data, and (viii) data flows.

As such, the Malaysian government's data management practices wary of data flowing across borders are concerned of weak cybersecurity practices that could allow unwanted access to data centres and the inability for the government to collect evidence for investigations. The emphasis is for storage and processing to be under the control and jurisdiction of the Malaysian Government. Thus, while the guidelines would not prohibit the usage of data centres residing abroad to store data in accordance with the relevant information classification, the departments may store data locally for the convenience of compliance.

The dual data regimes indicate the expectations for compliance and the levels of security accorded to the data user whether it is government or the private sector. As enforcement of the laws are under different agency jurisdictions, the cybersecurity environment can cause confusion. As such, enforcement for data-related issues for the public sector is under CGSO, MAMPU and PDRM while those for the private sector is under the PDPD, PDRM and MCMC.

2.4 Government Agencies in Cybersecurity

Malaysia's developing digital landscape evolves with the responsibilities of the government agencies. Thus, producing policy, crafting regulations and enforcing laws do require various bodies interlocked in governance.

1. Financial Sector

- Central Bank Malaysia. Bank Negara Malaysia (the Central Bank of Malaysia), is a statutory body which is governed by the Central Bank of Malaysia Act 2009. The role of Bank Negara Malaysia is to promote monetary and financial stability. Bank Negara Malaysia also oversees the nation's payment systems infrastructure which emphasise on the efficiency and security of the financial systems.

2. Economic Sector

- Ministry of International Trade and Industry (MITI). MITI is the agency responsible for the National Policy on Industry 4.0 (Industry4WRD). The policy highlighted the importance of Cyber Security - insufficient local capabilities and capacities in providing cybersecurity solutions that protect Industry 4.0 applications and the strengthening of cyber security as one of the strategic key enablers, in terms of Regulatory Framework & Industry Adoption. Specifically, to improve data integrity, standards, sharing and security to facilitate seamless integration of manufacturing value chains and to support intra-ministerial coordination for effective Industry 4.0 programmes. MITI is also mandated to (i) to develop and implement policies on industrial development, international trade and investment, (ii) to enhance national productivity and competitiveness, particularly in manufacturing and services sector, (iii) to ensure a conducive business ecosystem to facilitate trade and investment and (iv) to promote and accelerate adoption of digitalisation and innovative technologies, including data-driven policies, towards growing globally competitive industries.

- Malaysia Digital Economy Corporation. MDEC is mandated to ensure Malaysia makes the Digital Leap into the Fourth Industrial Revolution to drive shared prosperity, and firmly establish Malaysia as the Heart of Digital ASEAN. MDEC supports the growth of Malaysia's cybersecurity industry by building collaborations between industry and the government to provide cybersecurity startups with access to technical mentoring, business support and advice. Through the partnership with industry, government agencies and institutes of higher learning, MDEC has launched several cybersecurity programmes covering industry growth, innovation and talent development.

- Ministry of Domestic Trade and Consumer Affairs. MDTCA formulates policies, strategies and reviews matters pertaining to the development of domestic trade. The Ministry regulates companies and businesses based on the related acts, encourages good corporate governance practices, and develops and administers the intellectual property protection system. The Ministry enforces protection of intellectual property rights under the Copyright Act 1987, which is inclusive of literature, film, music and software, the licensing and manufacturing of optical discs under Optical Discs Act 2000 and the Trademark Act 2019.

- MyDIGITAL Corporation. MyDIGITAL Corporation is a special purpose vehicle formed under the Prime Minister's Department's Economic Planning Unit. MyDIGITAL Corporation functions as the Strategic Change Management Office to facilitate Malaysia's MyDIGITAL Initiative. This would be inclusive of building multi-stakeholder approaches to addressing connectivity, digital adoption and data-related issues. MyDIGITAL Corporation also serves as the secretariat for the National Digital Economy and 4IR Council.

3. Cybersecurity

- Cybersecurity Malaysia. Cybersecurity Malaysia is an agency under K-KOM. This agency is committed to provide a broad range of cybersecurity innovation-led services, programmes, and initiatives to reduce vulnerability of digital systems, and at the same time strengthen Malaysia's self-reliance in cyberspace. The agency provides specialised cybersecurity services inclusive

responses for cyber security incidents, outreach and capacity building as well as research and development.

- Royal Malaysia Police. The Royal Malaysian Police (Abbreviation: RMP; Malay: Polis Diraja Malaysia, PDRM;) belong to the security forces structure in Malaysia. RMP's Commercial Crimes Investigation Department functions to investigate, arrest, and prosecute offenders committing white-collar crimes such as fraud, breach of trust, cyber-crimes, forgery, counterfeiting etc. The Commercial Crimes Investigation Department is headed by a Commissioner of Police (CP).

- NACSA. National Cyber Security Agency (NACSA), an agency under the National Security Council, that oversees the cybersecurity strategies in Malaysia. he National Cyber Security Agency (NACSA) was officially established in February 2017 as the national lead agency for cyber security matters, with the objectives of securing and strengthening Malaysia's resilience in facing the threats of cyber attacks, by coordinating and consolidating the nation's best experts and resources in the field of cyber security. NACSA is also committed to developing and implementing national-level cyber security policies and strategies, protecting Critical National Information Infrastructures (CNII), undertaking strategic measures in countering cyber threats, spearheading cyber security awareness, acculturation and capacity-building programmes, formulating strategic approach towards combating cyber crimes, advising on organisational cyber risk management, developing and optimising shared resources among agencies, and fostering constructive regional and global networks among entities with shared interests in cyber security.

- NC4. National Cyber Coordination & Command Centre (NC4) was developed in accordance with the requirements of the National Cyber Security Policy (NCSP) and Directive No. 24 which aims to ensure that the Government can assess the current cyber security level of preparedness in the face of threats and cyber attacks at the national level. NC4 also serves as Malaysia's CERT and primary coordinator for incidents in the CNII sectors.

4. International Engagements

- The Ministry of Foreign Affairs. The Ministry of Foreign Affairs bears the mandate and responsibility to conduct Malaysia's foreign relations with other countries. This includes matters related to political relations, economic affairs, social and cultural promotion as well as security matters.

5. Telecommunications Sector and Online Harms

- Ministry of Communications and Multimedia (K-KOM). Ministry of Communications and Multimedia is a ministry of the Government of Malaysia that is responsible for communications, multimedia, broadcasting, information, personal data protection, special affairs, media industry, film industry, domain name, postal, courier, mobile service, fixed service, broadband, digital signature, universal service, international broadcasting, content. K-KOM also houses the Personal Data Protection Department (PDPD), Malaysia Digital Economy Corporation, Malaysia Communications and Multimedia Commission and Cybersecurity Malaysia.

- Malaysia Communications and Multimedia Commission (MCMC). MCMC is the regulator of the Communications and Multimedia industry based on the powers provided for in the Malaysian Communications and Multimedia Commission Act 1998 (MCMC 98) and the Communications and Multimedia Act 1998 (CMA98). Pursuant to these Acts, MCMC's role is also to implement and promote the Government's national policy objectives for the communications and multimedia sector. The Commission is also charged with overseeing the new regulatory framework for the converging telecommunications and broadcasting industries, and on-line activities. In 2001, the Commission's role was expanded to include overseeing the postal service sector pursuant to the Postal Services Act 1991 and licensing of the Certification Authorities under the Digital Signature Act 1997.

2.5 Digital Economy and Existing laws

Malaysia has approximately 40 laws governing the digital environment in sectors such as e-commerce, cybersecurity and intellectual property. Further, are the guidelines and frameworks such as the Guidelines for Foreign Participation in Distributive Trade Services in Malaysia (Amendment) 2020, the Guidelines on Taxation of Electronic Commerce Transactions (E-commerce Taxation Guidelines) and the Guidelines for the Management of Information Security through Cloud Computing in the Public Sector expected to raise cybersecurity standards and practices while shaping processes for the digital economy.

The following table include several laws in Malaysia that touches on data and data transmissions:

Table 4: Malaysian Laws on Data and Data Transmissions

Related laws	Elaboration on the law
Communications and Multimedia Act 1998 (CMA 1998)	CMA 1998 regulates the communications and multimedia industries, inclusive of cloud service providers. It sets out the offences and penalties for the misuse of network facilities. Regulation of data transmitted is inclusive of offensive content stated in S.211 and S.233.
Personal Data Protection Act 2010 (PDPA 2010)	The Act is applicable for persons established in Malaysia or if the person or institution is not established in Malaysia but uses equipment in Malaysia for data processing. The Act is not applicable for data in transit. The PDPA is not applicable to the government and associated bodies.
Official Secrets Act 1972	OSA 1972 categorises official information collected into Top-Secret, Secret, Confidential and Restricted. The security practices and requirements of systems would differ for each classification grade, inclusive of practices in cloud computing adoption.
Sector-specific code of practice	Alongside Malaysia's PDPA 2010 are the sector-specific code of practice. Existing code of practice include for Licenses under the Communications and Multimedia Act 1998, private hospitals in the healthcare industry, utilities sector (water), utilities sector (electricity), banking and financial institutions, aviation sector and the insurance and takaful industry.
Penal Code	Data is covered in the Penal Code and its usage or expression is permissible within the laws of Malaysia. Thus, data in the context of the Penal Code

Source: Collated by author from various sources

2.6 Laws Related to E-Commerce

Malaysia's digital economy is set to be worth USD 35 billion by 2025 in Global Merchandise Value (Bernama 2022). Realising the targets may require international collaborations, investments from abroad or participation from multinational corporations. Thus, the appeal in competitiveness is dependent on a digital ecosystem that is secure and is anchored by trust. Malaysia has a number of laws relevant in e-commerce transactions. These are inclusive of the Electronic Commerce Act 2006, Consumer Protection Act 1999 and Sale of Goods Act 1957. E-commerce is also subject to other legislations such as the Computer Crime Act 1997, Digital Signature Act, Personal Data Protection Act 2010, Trade Description Act 2011, Price Control and Anti-Profiteering Act 2011 as well as Weight and Measures Act 1972. Other legislations indirectly relevant are inclusive of Registration of Business Act 1956, Direct Sales and Anti-Pyramid Scheme Act 1993 and Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001.

The table below illustrates a few of the laws relevant to e-commerce:

Table 5: Malaysian Laws Relevant to E-Commerce

Related laws	Elaboration on the law
Electronic Commerce Act 2006	Section 7 of the ECA 2006 states that a contract formed through electronic communication is valid, binding and enforceable by and on the contracting parties.
Consumer Protection (Electronic Trade Transactions) Regulations 2012 (CP Regulations 2012)	CP Regulations 2012 is applicable for e-commerce traders such as those utilising personal websites for commerce and to e-commerce market operators such as Mudah.my, Lazada and Shopee. CP The Act states requirements that must be adhered to and complied with, inclusive of information that must be displayed on a website by online sellers.
Anti-Money Laundering Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001	The Act includes supplementary documents that sets out the minimum requirements and standards for remittance service providers to observe, such as implementing electronic Know Your Customer (e-KYC) for establishing business relationships and conducting consumer due diligence in carrying on remittance business through online or mobile channels.

Source: Collated by author from various sources

2.7 Laws Related to Intellectual Property Rights

Malaysia's primary government body responsible for developing and managing IP-related matters is the Intellectual Property Corporation of Malaysia (MyIPO), an agency under the Ministry of Domestic Trade and Consumer Affairs (MDTCA) with jurisdiction also shared by Customs, the Malaysian Communications and Multimedia Commission, Royal Malaysian Police and local councils. Awareness and patents-in-force have increased in the past few years, from 20,917 in 2011 to 31,975 in 2020. Further, trademarks have increased by 234,000 and industrial designs by 12,774 from 2011 to 2020. Malaysia's IP-related concerns can be skewed towards fraud, piracy and counterfeit goods. Thus, activities by MDTCA could be focused on awareness campaigns in shopping malls or seizing counterfeit goods, inclusive of electrical goods, computer and communication equipment. Enforcements have included blocking or taking down web contents as in 2020, 601 websites were blocked and 622 web contents taken down.

2.8 Data Flows, Cybersecurity, and its Challenges

1. Harmonising approaches to data governance

Cyber can be a multi-jurisdiction issue with enforcement of data controls subjected to national policies. This can mean that there are inconsistencies in policies on data governance where a data user has to comply with various standards of adequacy determined by other countries. The differences range from laws applied such as the General Data Protection Regulation (GDPR) to standards for cybersecurity, such as ISO compliance. Countries in ASEAN and APEC are attempting to raise adequacy levels to encourage while securing cross-border data flows such as the ASEAN Data Management Framework and APEC Cross-border Privacy Enforcement Arrangement. Currently there are only a handful of ISOs that address Cybersecurity and Ethical AI, such as ISO 27001. In the prospective landscape of developing cyber threats, more standards need to be developed that could be enforced by bodies such as SIRIM.

2. Malaysia's SME-heavy environment shapes data governance and approaches

Malaysia's PDPA has to regulate the activities of various data users. These could be small and medium enterprises (SME) to larger multinational corporations (MNC). While MNCs are able to invest in security based on ISO or international standards, SMEs are impacted by limited resources. Thus, smaller players may not be able to afford heavy cybersecurity costs. Therefore, PDPD has to consider the capacity and capability of smaller players to meet the minimum of compliance for data management and cybersecurity.

3. Malaysia's PDPA update may face implementation challenges

Malaysia is currently amending the PDPA to include new elements such as the appointment of data protection officers (DPO), mandatory data breach notification, the ease of data portability, heavier obligations for major data processors to safeguard data and to pursue a blacklist approach to cross-border data management. Mechanisms for implementation of an updated PDPA can vary. For instance the appointment of a DPO will require training, especially if a company would appoint the DPO from the existing pool of human resources. Data portability would require an open data ecosystem, which can be challenged by technology compatibility, jurisdiction, capability of data users to share information and compliance with data retention mechanisms.

4. The absence of data breach notification requirements shape Malaysia's awareness on good data hygiene

Malaysia does not require mandatory data breach notifications, whether it is to the government or for data users to data subjects. This means that investigations are triggered by complaints or information available on social media. This also means that the Malaysian government's approach aims to preserve existing trust and reputation between the data user and data subjects. The challenge in this approach is the deterrent effect that could be created with greater transparency of data breach notifications and investigations if justice for negligence is demonstrated. Publicising data breach investigations should create more awareness on data management hygiene as data breaches could occur from human weaknesses such as through phishing and social engineering exercises. Further, companies managing personal information would be encouraged to comply if prosecutions are conducted.

2.9 Malaysia's Cybersecurity Practices and International Standards

Malaysia's commitment to cybersecurity is consistent through the years. However, future approaches are impacted by a technological landscape that is vastly changing. Yet, unlocking the USD 35 billion by 2025 requires Malaysia to engage with partners either to (i) harmonise data governance laws, computer systems and cybersecurity practices or (ii) to collectively develop future standards with the purpose of aligning digital rules and standards.

Take for instance Singapore's approach to Digital Economy Agreements (DEA) that aim to (a.) align digital rules and standards and facilitate interoperability between digital systems (b.) support cross border data flows and safeguard personal data and consumer rights; and (c.) encourage cooperation between Singapore's economic partners in nascent areas such as digital identities, artificial intelligence and data innovation (MITI 2020).

Thus, key modules and articles for digital economic partnership agreements and digital economy agreement may contain the following:

Table 6: Key Modules and Articles for Digital Economic Partnership Agreements

Modules and articles	Elaborations
Artificial Intelligence	Looks into ethical AI governance frameworks and developing principles to harness AI responsibly with the purpose of allowing Singapore businesses to adopt and use AI technologies responsibly across jurisdictions.
Cross-border data flow	To allow data to flow freely across borders and prohibit the localisation of data, except for legitimate purposes such as personal data protection
Personal data protection	To promote compatibility and interoperability in respective legal approaches with development of safeguards for the transfer of personal data
Data innovation	To promote data-driven innovation domestically and across borders. Needed are regulatory sandboxes in consultation with government policy makers.
Digital IDs	To provide data from government-verified sources to form a digital user profile where Singapore aims to promote compatibility between different digital ID regimes
E-invoicing	For the purpose of achieving shorter invoice processing time, faster payment and saving costs related to physical invoices, interoperability of e-invoicing systems would allow for e-invoice generated in Singapore to be accepted directly by another country's e-invoice system.
Fintech and e-payments	To seek compatibility with Singaporean regulations in e-payments, For faster payments, reduced transaction costs and enhanced trade, agreements and partnerships with fintech and e-payment components would make it easier to navigate the payment regulations of foreign markets.

Source: MITI Singapore paraphrased by author.

It can be noted that the partnerships and agreements can differ in terms of requirements. For instance, the Digital Economy Agreement (DEA) between Australia and Singapore has obligations for expeditious and efficient installation, maintenance and repair of submarine telecommunications cable systems. Meanwhile, the digital agreement obligations under the CPTPP would include online consumer protection, personal information protection, compliance with requests of source codes for investigation, enforcement or judicial purposes; and adopting measures to reduce or prevent unsolicited commercial electronic messages.

Malaysia does have compatible agencies with the jurisdiction to engage in DEA spaces. For instance, MCMC for telecommunications, internet services, as well as online content problems. The Personal Data Protection Department under the Ministry of Communications and Multimedia Malaysia whose mandate is to regulate the processing of personal data of individual users. Further is the Royal Malaysia Police whose jurisdiction include fraud, finance and trade issues identity theft and hacking and the Ministry of Domestic Trade, Co-operatives and Consumerism who would look into Intellectual Property and Copyright matters.

There are points of convergence as there are gaps in harmonisation for cross-border data governance. For instance, Australia highlights 13 privacy principles while Malaysia has 7 principles for personal data protection. Among Australia's privacy principles is the open and transparent management of personal information, principles on anonymity and pseudonymity, dealing with unsolicited personal information and principles for direct marketing. As principles would determine data management practices and cybersecurity standards, harmonising approaches to meet domestic and international thresholds should strengthen cybersecurity levels. Malaysia's preparedness to engage in digital economic partnerships would be dependent on Malaysia's intended outcome, and should seek to develop cybersecurity and the digital economy.

3. Policy Recommendations

Moving forward there are ways to improve both the taxation framework and the cybersecurity components. Below are a few recommendations that may be taken into account in strengthening the digital trade ecosystem in Malaysia.

Transparency in Introduction of Taxes in the Digital Economy

As one of the biggest concerns in Malaysia is the planning and introduction of new forms of taxes for the digital economy and digital trade activities, it is important that impact assessments of such measures take into account feedback and input from the stakeholders affected. Such policies and clear guidelines of implementation provide ease of doing business for both local and international firms.

Capacity Building in Creating a Sustainable Digital Taxation Framework

Due to the difficulty and complex nature of taxing the digital economy with the boom in of digital trade activities, building local capacity and know-how is key. Capacity building exercises and training sessions can take place with collaborations with neighbouring countries like Singapore or Australia, who have developed a somewhat robust framework in the wake of their own digital economies domestically or via Digital Free Trade Zones.

Develop and Standardise Efforts for Cybersecurity

Due to the high cost and investment of cybersecurity, the barriers for consistent cybersecurity updates to systems may burden smaller players. Further, varying international standards for compliance impact cybersecurity approaches where companies may not know which to prioritise or adopt. Thus, further conversations could be held to develop and standardise efforts for cybersecurity, which could adopt some forms of ISO standards. This would ease compliance should higher standards of cybersecurity be mandatory for SME practitioners. Such conversations on the development of diluted versions of ISO standards can be pursued by government bodies such as Cybersecurity Malaysia and SIRIM.

Malaysia's Cybersecurity Agencies to Consider Increased Transparency in Data Breach Investigations

Currently the PDPD does not publicise investigation activities though court cases and compounds have been ongoing. The course of the investigation and its outcome is not made public, which impacts the possibility of other errors occurring in other parts of the digital ecosystem. While publicising investigations could impact the reputation of a company, the future landscape of cyber incidents and data breaches require increased vigilance in the whole-of-society.

Embark on Digital Economic Partnerships Stimulates the Digital Economy and Build a Rules-based Environment for Cyber and Digital Taxation Framework

Competing and conflicting standards would impact the modernisation of Malaysia's industries with further implications for Malaysia's digital economy ambitions. As conflicting standards in emerging technologies would impact digital developments, this could include impacting developments in AI or production of future technologies. Thus, while DEAs are intended to open Malaysia for digital economic activity, such partnerships can also be seen as platforms to build conversations on rules and standards. Thus, engagements should ensure Malaysia's national interests are protected and industries promoted.

References

Arizton Advisory and Intelligence. "Malaysia Data Center Market to Reach Over $2 Billion by 2027. Hyperscale Providers to Ramp up their Investments". August 2022

Asia Business Trade Association. "FTA Digital Trade Regulations Comparisons". *Asia Business Trade Association*, June 2019

Asian Development Bank. "ADB Briefs: Strengthening Domestic Resource Mobilization in Southeast Asia". March 2021

Athanasaki, Vasiliki. "Contemporary aspects of the taxation of digital economy: A unified approach for a fairer allocation of taxing rights and the Global Anti-Base Erosion Proposal ("GloBE")". *European Law Observatory on New Technologies*, September 2020

Aurat, Varapa. "Thailand Enacts Law Imposing VAT on Foreign e-Services and e-Platforms". Tilleke & Gibbons, February 2021

Bernama. "MSCC Malaysia to be enhanced, renamed as Malaysia Digital". *The Malaysian Reserve*, January 2022

Bernama. "Saifuddin: Malaysia Ranked Among Top 10 Countries with Highest Commitment to Cybersecurity". *Ministry of Communications and Multimedia Malaysia*, July 2022

Chai Yee Hoong. "Malaysia's data centre market remains strong, says JLL". The Edge, August 2022

"Data Centres Directory". MDEC, Data Centre Directory - MDEC. Accessed 22/11/22

Department of Statistics Malaysia's (DOSM) Digital Economy 2018

– (DOSM, 2021). latest report in 2020,

– (DOSM, 2021). report further elaborated

Elms, Deborah. "Trade and Tax in a Digital World". *Asian Digital Economy Series*, as published by the Asian Trade Centre, July 2021

EY. "Malaysia publishes updated Guidelines on Taxation of e-Commerce Transactions". July 2019

Hufbauer, Gary Clyde and Hogan, Megan. "How do digital services taxes work?". *Peterson Institute for International Economics,* March 2022

Juswanto, Wawan and Simms, Rebecca. "Policy Brief: Fair Taxation in the Digital Economy". *Asian Development Bank Institute*, December 2017

KPMG. "Malaysia: Implementation of service tax on goods delivery services postponed". July 2022

Kumar, S Saravana and Yap Wen Hui. "The evolving world of Malaysia's digital services tax". *International Tax Review*, December 2021

Lee, Esther. "Budget 2023: A caring budget, but major reforms lacking". *The Edge*, October 2022

Majlis Keselamatan Negara. "Arahan MKN No 24: Dasar & Mekanisme Pengurusan Krisis Siber Negara". (presentation), MKN, n.d.

Malay Mail. "Tengku Zafrul: Malaysia expects to implement two-pillar taxation approach in 2024". October 2022

Malaysian Inland Revenue Board. "Guidelines on Taxation of Electronic Commerce Transactions". May 2019

MITI. "All You Need to Know about Singapore's Free Trade Agreements and Digital Economy Agreements". *MITI Singapore*, October 2020.

Mohd Uzir Mahidin. "Contribution of Digital Economy was 18.5 per cent to National Economy". *Department of Statistics Malaysia*, October 2019

Mohd Uzir Mahidin. "Malaysia e-commerce income soared 17.1 per cent to RM279.0 billion in the third quarter 2021". November 2021

Morden, Zarrah. "Report: New NRD database leaked online, offered for just US$10,000". *Malay Mail*, May 2022

Murugiah, Surin. "Malaysia saw 282% y-o-y jump in ransomware attacks in 1H22 — Trend Micro". *The Edge,* September 2022

MyCERT. "MA-892.112022: MyCERT Alert - IOCs and TTPs Associated with APT40". *MyCERT,* Nov 2022.

MyCERT. "Reported Incidents based on General Incident Classification Statistics 2021". *MyCERT*, n.d.

Nair, Kirennesh. "Data centre investments – good or bad for Malaysia?". *The Star*, September 2022

Li, Christine and Wong Xian Yang. "Data Centres in Southeast Asia Poised for Rapid Growth". Cushman & Wakefield, August 2019

OECD Secretariat. "OECD/G20 Inclusive Framework on BEPS". Based on the *5th meeting of the Inclusive Framework in Lima, Peru*, June 2018

OECD Secretariat. "OECD/G20 Inclusive Framework on BEPS: Progress Report September 2021-September 2022". September 2022

OECD Secretariat. "OECD/G20 Base Erosion and Profit Shifting Project: Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy". October 2021

Ong, Shazni. "Dewan Rakyat approves Bill to tax imported low-value goods sold online". *The Edge*, August 2022

Pak Wei Lee, Nicholas and Yi Ning Suah. "Bill to introduce sales tax on low-value goods approved by parliament". *Deloitte*, August 2022

Parliament of Malaysia. "Act A1633: Tourism Tax (Amendment) Act 2021". As found on the website of the *Royal Malaysian Customs Department*, February 2021

Parliament of Malaysia. "Sales Tax (Amendment) Bill 2022". As found on online legal database *CLJ Law*, August 2022

Prime Minister's Department. "Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) dalam Perkhidmatan Awam". *Prime Minister's Department*, August 2021

Ramesh Dipendra Jeremiah Law. "Tourism Tax on Online Digital Accommodation Booking Platforms". April 2021

Royal Malaysian Customs Department. "Guide On: Digital Services By Foreign Service Provider (FRP)". February 2021

Royal Malaysian Customs Department. "Penangguhan Tarikh Kuatkuasa Pelaksanaan Pengenaan CP ke atas Perkhidmatan Penghantaran Barang". June 2022

Schwab, Klaus. "The Global Competitiveness Report 2019". *World Economic Forum*, 2019

SERI. "Alleged govt data breaches must be addressed". *The Star*, October 2021

Sheehan, Jack and O'Connell, Clint. "Taxation of E-Commerce in Southeast Asia". *DFDL*, May 2021

Su-Lyn, Boo. "MITI Site Allegedly Exposed Personal Data of Workers Registered for Covid-19 Jabs". *Code Blue*, May 2022

The Edge. "Full Budget 2023 speech". October 2022

Vertex. "Singapore GST set for 2023 extension to low value goods". 2022

Voo, Hemani et al. "National Cyber Power Index 2020". *Harvard Kennedy School Belfer Center for Science and International Affairs*, September 2020

IDEAS

INSTITUTE FOR DEMOCRACY AND ECONOMIC AFFAIRS

The Institute for Democracy and Economic Affairs (IDEAS) is a nonprofit research institute based in Malaysia dedicated to promoting solutions to public policy challenges. Our vision is :

"A Malaysia that upholds the principles of liberty and justice"

Our mission at IDEAS is to improve the level of understanding and acceptance of public policies based on the principles of rule of law, limited government, competitive markets and free individuals. Our work is independent of vested interests and partisan influences. We have also expanded our work into new areas focussing on our three overarching missions – advancing a competitive economy, ensuring trust in institutions and promoting an inclusive Malaysia. We act as an intellectual centre creating space for cross partisan principles-centric and results-oriented dialogue.

We achieve this by:

- Publishing cutting-edge research
- Initiating dialogues with government, lawmakers, businesses and civil society
- Providing thought leadership
- Facilitating networking between like-minded individuals
- Organising educational programmes

Please support us by making a donation. You can make a contribution by cheque payable to "IDEAS Policy Research Berhad" or by transfer to our account CIMB 8008852042. We can only survive with your support.

IDEAS Policy Research Berhad
The Lower Penthouse
Wisma Hang Sam, 1, Jalan Hang Lekir 50000 Kuala Lumpur

www.ideas.org.my
Reg №: 1219187-V

Selection of IDEAS' Publications (2021-2022)

Policy Ideas

Policy Paper No 75 –The New Economic Policy and Contesting Bumiputera Identity Among Orang Asli and the Indigenous Peoples of Sabah and Sarawak by Wan Zawawi Ibrahim (November 2021)

Policy Paper No 74 – Fifty Years of The New Economic Policy: Revisiting Its Impact on Social Cohesion, National Unity and Creation of Bangsa Malaysia by Abdul Rahman Embong (November 2021)

Policy Paper No 73 – The New Economic Policy Beyond Fifty: Assessing its Strengths and Weaknesses to Chart a Cohesive Malaysian Society by Lee Hwok Aun (November 2021)

Brief Ideas

Brief IDEAS No. 35 – Budget Transparency in Malaysian States: Key Findings of Malaysia's Open Budget Index (MyOBI) 2022 by Sri Murniati Yusuf, Alissa Marianne Rode, and Muhammad Arieff Najmuddin Mohd Mohtar (July 2022)

Brief IDEAS No. 34 – Political financing in Malaysia: Aligning reforms with voters' expectations by Aira Azhar (October 2021)

Brief IDEAS No. 33 – Political financing in Malaysia: Recent developments and plugging potential gaps by Aira Azhari and Tricia Yeoh (October 2021)

Brief IDEAS No. 32 – Falling Through the Cracks: Identifying Children with Learning Difficulties in Malaysian Schools by Sharmini Xavier (September 2021)

Brief IDEAS No. 31 –The government's policy commitments on State-owned enterprises (SOEs) in the National Anti-Corruption Plan (NACP) and the Shared Prosperity Vision (SPV) 2030 by Nur Zulaikha Azmi (August 2021)

Report

API Report No.07 – ASEAN Integration Report 2022 by Dr. Evelyn S. Devadason, Dr. Lurong Chen, Ms Yuanita Suhud, Dr. Aya Ono, Dr. Anh Tuan Nguyen, Dr. Poppy S. Winanti, Dr. Katrina Navallo, Dr. Upalat Korwatanasakul, Dr. Adiasri Putri Purbantina, Mr Imran Shamsunahar, Dr. Juita Mohamad, Ms Julia Merican, Ms Kirjane Ngu and Mr Jazreen Harith (November 2022)

Left Far Behind: The Impact of COVID-19 on Access to Education and Healthcare for Refugee and Asylum-Seeking Children in Peninsular Malaysia by Diode Consultancy and Wan Ya Shin (September 2022)

Contextualising education policy to empower Orang Asli children by Wan Ya Shin and Rusaslina Idrus (December 2021)

ASEAN Integration Report 2021 by Yeo Bee Yin, Felippa Ann Amanta, Nisrina Nuraini Nafisah, Jayant Menon and Jukhee Hong (December 2021)

Public Procurement and Bumiputera Company Development in the Construction Industry: Reviewing Policies, Exploring Possibilities by Lee Hwok Aun (September 2021)

Policy IDEAS are IDEAS' regular publications that introduce and propose ideas for policy reforms based on analysis of existing policies or best practices.

IDEAS
INSTITUTE FOR DEMOCRACY AND ECONOMIC AFFAIRS

Institute for Democracy and Economic Affairs (IDEAS)
The Lower Penthouse. Wisma Hang Sam, 1, Jalan Hang Lekir 50000 Kuala Lumpur

Website: ideas.org.my Tel: +603 2070 8881 / 8882 Fax: +603 2070 8883