PolicyBrief | DECEMBER 2020

SERI SOCIAL & ECONOMIC RESEARCH INITIATIVE

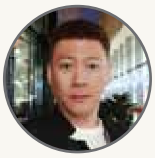
Cybersecurity: Protecting Privacy, Identity & Property

This paper summarises key findings from a panel discussion hosted by the Social & Economic Research Initiative, on 3rd December 2020. Panelists were as follows:

YBhg. Dato' Ts. Dr. Haji Amirudin Abdul Wahab
Chief Executive Officer, CyberSecurity Malaysia

Albert Chai
Managing Director CISCO Systems Malaysia

ACP Puan Siti Kamsiah Hassan
Principal Asst Director, Sexual, Women & Child Investigations Division Royal Malaysian Police



Danry Chin
Head of Public Safety & Social Infrastructure, NEC Corporation of Malaysia

Moderated by
Ahmad Arif Astaman
Research Fellow, Social & Economic Research Initiative

Report compiled by Caitlin Alexandra, Associate, Public Policy and Nabila Hussain, Policy Communications Lead, Social & Economic Research Initiative

For access to the session recording, please visit: https://bit.ly/seridds3

Summary

The world is witnessing the exponential growth of technology. Growth of digital technology illustrates how much humanity has achieved in terms of improvement and innovation which allows us to work seamlessly and virtually in real time. The digital age has made technology a critical tool for Malaysia's economic, social, and political development. However, utilisation of technology pervades the lives of individuals, businesses, and governments in both positive and negative manners. Hence, the steady increase in reliance on internet connectivity parallels the increased need for cybersecurity.

The most vulnerable in our society are the most prone to breaches of privacy, identity theft, and loss of property through fraud, unauthorized use and abuse of personal data. Sufficiently disseminating knowledge and practices on cybersecurity has never been more important today, as more people are introduced to connected devices and services. Without adequate safeguards, the social and economic costs of such breaches are staggering, not to mention the loss of productivity and revenue. We seek to understand and discuss the varying considerations in advancing cybersecurity, and its importance as we embrace present and emerging technologies.

Current Landscape

The Covid-19 pandemic forced us to adapt and assimilate to an increased dependence on the internet and digital infrastructure. In Malaysia, due to the increase in online activities, we have observed the upward surge of internet traffic since the beginning of the Movement Control Order (MCO). The rapid growth of e-commerce, subsequent to the pandemic has reshaped consumer behaviour. For example, meetings, conferences, and seminars have shifted to various virtual platforms.

CyberSecurity Malaysia (CSM) reported that the top 5 highest incidents were fraud, intrusion attempts, malicious code, content related cybercrime and cyber harassment[1]. CSM recorded a total of 6459 incidents as of October 2020, and the Royal Malaysian Police (PDRM) reported that internet fraud was the most prevalent cyber threat in Malaysia in 2018 and 2019.

Malaysia's recognition of cybersecurity as a national priority led to the formulation of the National Cyber Security Policy (NCSP) in 2006 to address potential risks to Critical National Information Infrastructure (CNII).

In October 2020, Malaysia launched the Malaysia Cyber Security Strategy (MCSS) to bolster trust in society, the cyber environment and to support the government's agenda in the digital economy, Industry 4.0 and the adoption of emerging technologies for Malaysia's enhancement.
MCSS outlined 5 strategic pillars:[2]

1. Effective Governance and Management
2. Strengthening Legislative Framework and Enforcement
3. Catalysing World Class Innovation, Technology, Research & Development, and Industry
4. Enhancing Capacity & Capability Building, Awareness and Education
5. Strengthening Global Collaboration

This paper summarises the challenges and opportunities presented by cybersecurity developments in Malaysia.

Key Issues and Challenges

Awareness & Education

Data is swiftly becoming the most fundamental commodity on the planet and the use of Internet of Things (IoT) hardware is on a steady incline. Cybersecurity measures are equally important across multinationals, SMEs, microenterprises, and local businesses.

While many individuals have often fallen victim to data theft, awareness regarding the misuse of personal data is also increasing. The introduction of the Personal Data Protection Act (PDPA) 2010 clarified the framework for the protection of personal data. However, as technology evolves and pervades every sphere of life from communication to the conduct of online transactions, the risk of cyberthreats also increases. Consequently, in the recently launched Malaysia Digital Economy Blueprint, the Government has committed to enhance data protection and review existing laws including the PDPA by 2025.

As working from home has become the new norm, new avenues of potential intrusion into a company have opened. Companies strive to protect their employee's personal devices and reinforce cybersecurity protocols via employee awareness and education.[3] Cybersecurity practices should be anchored on three basic principles, i.e., people, process and technology.

According to a survey conducted by CSM and the Ministry of Education (MOE), there is a severe lack of awareness of cyber safety amongst primary and secondary school students, especially where sexual exploitation is concerned. Cases including rape, child grooming and dissemination of child pornography images and videos have increased. A contributing factor is the increased exposure to social media platforms like Facebook, Instagram, TikTok, and Twitter, and parents' lack of knowledge and/or ability to monitor usage of these channels.

Cybercrime Evidence Collection

PDRM encounters many hurdles, especially in the collection of evidence when computers and the internet are used as a medium to commit crimes. The challenges to evidence collection and analysis include :

i. Offenders are more advanced and possess greater technological skills and knowledge than the investigating officers.
ii. Society is quick to make something viral on social media instead of making a police report. This alerts the offender to remove all evidence of the alleged crime.
iii. The cross-border nature of cybercrime increases the difficulty in detecting offenders who are abroad and anonymous.

Example:

In 2019, PDRM received information from the Macau police regarding a youth from Macau who lodged a report citing blackmail by a Facebook user. The offender was a Malaysian who possessed child pornography of children aged 10 to 15 years.

Extraction of digital evidence in cyberspace is difficult due to the offender's ability to remove it quickly. Proving the evidence is challenging as it is usually deemed "intangible". Technologies like cryptocurrency and blockchain require deeper technical knowledge to understand the intricacies of its infrastructure. Legality may also be a further concern as difficulties arise in child victims' testimonies due to their maturity of age. In cases like child grooming, children often do not realise that they are being exploited.

Entrenched data silos

Between the relevant government organisations responsible for law enforcement, technology, and child welfare, there exists great potential for fragmentation in decision-making. Coordination issues led to the development of MCSS which shed light on each eyntity's respective roles and to ensure that they complement each other.

Given data's role as an important tool for prevention as well as detection of crime, there must be efforts to enable coordination, collaboration, and data sharing between government agencies and private institutions.

Legislation

Given the fast-evolving nature of societal and technological developments, existing cybersecurity laws are insufficient. This is in large part due to the pace of legislative proceedings compared to the speed of technological development. While amendments, reform, or creation of new laws may take years, technology can advance within days. By the time legal reform is achieved, technology is likely to have progressed, requiring further amendment. **Example:** *Cyberbullying*

No statutory definition of bullying has been provided in Malaysia. *The Communications and Multimedia Act 1998 (CMA 1998)* and the Penal Code are insufficient. *Section 233(3) of the CMA 1998* stipulate that those convicted shall face a maximum fine of RM50,000 or a maximum of one year jail or both, as well as a further fine of RM1,000 for every day the offence continues after conviction. Cyberbullying has brought ramifications as severe as suicide.

Robust legislation and policy frameworks must be developed, while also recognising the fact that cybersecurity is a shared responsibility which requires holistic efforts across the digital ecosystem.

Trust

As cloud is the underlying infrastructure of emerging technologies such as artificial intelligence, and the Internet of Things (IoT), the trustworthiness of cloud providers is fundamental. As government and business organisations seek to select trusted cloud service providers (CSPs) for storing and processing data, they may want to ask the following questions:

1. Have CSPs obtained global certification?
2. How does the CSP protect customer data?
3. How does the data owner have control over the data?
4. Where is the data stored? (Which country, region, data center?)
5. What does the CSP do with customer data?
6. Does the CSP publish/make publicly accessible law enforcement access requests for data stored in its cloud?

Holistic Approach to Cyber Resilience

Malaysia, ranked second in ASEAN, spends about 0.08% of our GDP on cybersecurity while Singapore, ranked first in ASEAN, spends about 0.22% on cybersecurity.[4] Globally, Malaysia is almost 4 to 5 times below the best practice amount for cybersecurity expenditure.[5] Funding, education, and awareness are crucial issues that need to be tackled. When it comes to cyber resiliency, a holistic approach needs to be employed. We cannot merely focus on a single component but rather, we have to look at how they are interdependent and interrelated, encompassing people, process, and technology.

Policy Recommendations

Societal and technological advancements have accelerated the need for regulatory and policy reform. New policies and regulations are required to better fit the challenges and opportunities presented by the digital world. Below are some recommendations :

Elimination of data silos

- There must be collaboration and coordination between all relevant organisations.
- Shared intelligence across organizations, government entities and private institutions would enable data to be converted into actionable insights.
- A public-private partnership is vital for sharing information securely and confidently. Industry players should collaborate with public sector on best practices for sharing intelligence.
- Regulations must be in place to give stakeholders the confidence to share information.

Review education, training and compliance systems

- Security policies, networks and applications must be constantly reviewed and governed.
- Children must be educated and equipped with tools to ensure their own safety especially in relation to risks involving sexual exploitation.
- Parents and educators must have access to training and tools to improve and nurture positive and healthy relationships.

An anti-cyberbullying law should be drafted

- A balanced approach should be employed, to ensure children are protected without over-regulating or stifling children's ability to learn, innovate, and develop new skills.

Awareness

- Cybersecurity is a team sport requiring multi-stakeholder collaboration. Awareness must be increased, in partnership with public sector and private sector stakeholders, in order to ensure the implementation of online safety and cybersecurity best practices.

There is no national security without cybersecurity. With the ever-growing digital economy, Malaysia's cyber resiliency needs to be constantly improved. Malaysia must adopt clear and unambiguous legislation and enabling policies that steer us towards robust security and protection standards.

[1] *https://www.kkmm.gov.my/index.php?option=com_content&view=article&id=15043:bernama-14-may-2019-data-sanitisation-of-electronic-devices-helps-maintain-user-privacy&catid=233&lang=ms&Itemid=589*

[2] *National Cybersecurity Agency, 2020, "Malaysia Cyber Security Strategy 2020-2024"*

[3] *CISCO, 2020, "Future of Secure Remote Work Report"*

[4] *CISCO, AT Kearney, 2018, "Cybersecurity in ASEAN: An Urgent Call to Action"*

[5] *Ibid*