KSI
STRATEGIC INSTITUTE
FOR ASIA PACIFIC

POLICY BRIEF ON
CYBERSECURITY AND DIGITAL TRUST

BACKGROUND

Digital Economic Powerhouse of Southeast Asia

The digital future is now. The digital economy of Southeast Asia is poised to reach USD$1 trillion in Gross Merchandise Value (GMV) by 2030 (Bain, 2021). The region has more than 440 million internet users and more than 80% of them are digital consumers (i.e. purchased at least one service). The digital economy is expected to contribute to 22.6% of Malaysia's GDP and create over 500,000 jobs by 2025 (EPU, 2021).

Malaysia's Vulnerability to Cyberattacks

However, the rise of digitalisation has been accompanied by increased cyberattacks.[1] Despite being ranked top 10 in the United Nations International Telecommunication Union (ITU)'s Global Cybersecurity Index (2020), Malaysia is very vulnerable to cyberattacks. Some of the recent cases illustrate this point:

- Malaysians suffered RM2.23 billion in loses from cyber-crime frauds between 2017 and mid-2021 according to the Royal Malaysian Police (NST, 2021);
- 57.8 million virus attacks and 57.2 botnet detection Malaysia in the first quarter (Q1) of 2022 alone (Cybersecurity ASEAN, 2022);
- 84% of SMEs have been compromised by cyber threat incidents (Chubb, 2019) and;
- From January to December 2021, 10,016 cases of cyber incidents with 71% being fraud-related (MyCERT, 2021).

Malaysia's aspiration to become a leader in the digital economy within the region can be derailed by the spectre of cyberattacks. According to a 2018 study by Frost Sullivan and Microsoft (2018), Malaysia could potentially lose up to RM51 billion or more than 4% of our GDP due to cybersecurity incidents.

[1] Cyberattack has a broad definition. A working definition by NIST Computer Security Resource Center: "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."

Techlash and The Need for Digital Trust

The public backlash against technology or ‘techlash’ poses challenges for governments and businesses alike. The public is increasingly suspicious of technology including misinformation, privacy and 5G networks (WEF, 2021). Cybersecurity[2] is important to set the foundation for governments and businesses to operate in a safe and secure digital environment. A 2018 PwC survey on digital trust succinctly put it: “If the lifeblood of the digital economy is data, its heart is digital trust”.

ISSUES AND RECOMMENDATIONS

KSI Strategic Institute for Asia Pacific and Huawei Malaysia collaborated on a webinar to discuss the issues pertaining to cybersecurity on 7th April 2022. Based on the webinar, the brief outlines the specific issues and recommendations.

1. No specific cybersecurity laws

Apart from the Personal Data Protection Act (PDPA), Malaysia does not have a specific law addressing cybersecurity-related offences. Enforcement agencies including National Cyber Security Agency (NACSA) have to rely on existing legislation (e.g. Communications and Multimedia Act 1998, Computer Crimes Act 1997 and Defamation Act 1957) to address cyberthreats (NACSA, 2021). These laws are inadequate due to the evolving nature of cyberspace.

Recommendation: Introduce cybersecurity law to specifically deal with cybersecurity-related matters. Review the PDPA based on personal data legislation from other countries (e.g. EU’s General Data Protection Regulation (GDPR), China’s Personal Information Protection Law, New Zealand’s Privacy Act 2020).

2. Low digital literacy

Malaysia’s internet penetration is close to 90% (Statista, 2022) and access to smartphones is extremely high. However, according to ITU (2021), only 60% of Malaysians have standard ICT skills (e.g. using emails). This explains the vulnerability of individuals and businesses to cyberattacks, particularly fraud. Digital literacy must address the quality of digital education, urban-rural divide and stay apace with the evolving nature of technology.

Recommendation: Review existing digital literacy initiatives (e.g. MDEC’s #SayaDigital, PDRM’s #TakNakScam) to include and emphasise on cybersecurity.

[2] ITU defines cybersecurity as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.”

3. Lack of multilateral and regional technical cooperation

The ASEAN Digital Ministers' Meeting (ADGMIN) launched the ASEAN Cybersecurity Cooperation Strategy 2021-2025 in January 2022 as an update to the previous strategy in enhancing cooperation in cybersecurity (ASEAN, 2022). Capacity-building programmes under the strategy include ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) and ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE). However, these physical centres are confined to Bangkok, Thailand and Singapore respectively, limiting their impact to Malaysia.

Recommendation: Enhance existing initiatives, specifically Malaysia's 5G Cyber Security Test Lab into a centre of excellence with support from regional partners (e.g. ASEAN, China). Consider a Memorandum of Understanding between Malaysia, ASEAN and China on cybersecurity cooperation, specifically on cybersecurity skills, sharing of best practices, capacity building and industry-academic collaboration.

REFERENCES

1. ASEAN (2022), *ASEAN Cybersecurity Cooperation Strategy 2021-2025*, https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

2. Bain (2021), *e-Conomy SEA 2021*, Aadarsh Baijal, Alessandro Cannarsi, Florian Hoppe, Willy Chang, Stephanie Davis & Rohit Sipahimalani, https://www.bain.com/globalassets/noindex/2021/e_conomy_sea_2021_report.pdf.

3. Chubb (2019), *Asia Pacific SME Cyber Preparedness Report 2019*, https://www.chubb.com/hk-en/articles/asia-pacific-sme-cyber-preparedness-report-2019.html.

4. Cybersecurity ASEAN (2022), 'Fortinet Sheds Light on the Top Three Threat Categories in Malaysia and the Resourcefulness of Cybercriminals,' Muhammad Zulhusni, https://cybersecurityasean.com/daily-news/fortinet-sheds-light-top-three-threat-categories-malaysia-and-resourcefulness.

5. Economic Planning Unit (EPU) (2021), *Malaysia Digital Economy Blueprint*, https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf.

6. International Telecommunication Union (ITU) (2020), *Global Cybersecurity Index 2020*, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

7. – (2021), *ICT Skills - Facts and Figures 2021,* https://www.itu.int/itu-d/reports/statistics/2021/11/15/ict-skills/.

8. Microsoft (2018), 'Cybersecurity threats to cost organizations in Asia Pacific US$1.75 trillion in economic losses,' https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/.

9. MyCERT (2021), MyCERT: Incident Statistics, https://www.mycert.org.my/portal/statistics?id=b75e037d-6ee3-4d11-8169-66677d694932.

10. PwC (2018), *The Journey to Digital Trust*, https://www.pwc.com/us/en/services/consulting/assets/journey-to-digital-trust.pdf.

11. National Cyber Security Agency (NACSA) (2021), *Malaysian Cyber Laws*, https://www.nacsa.gov.my/legal.php.

12. NST (2021), 'Malaysians suffered RM2.23 billion losses from cyber-crime frauds', Mohamed Basyir, https://www.nst.com.my/news/crime-courts/2021/07/708911/malaysians-suffered-rm223-billion-losses-cyber-crime-frauds.

13. Statista (2022), *Share of population using the internet in Malaysia from 2010 to 2020 and a forecast up to 2025*, https://www.statista.com/statistics/975058/internet-penetration-rate-in-malaysia/.

14. World Economic Forum (WEF) (2021), 'Why we must rebuild digital trust for a cyber-inclusive future', https://www.weforum.org/agenda/2021/11/rebuilding-digital-trust-for-a-cyber-inclusive-future/.