CYBER SECURITY ACT 2024: A FACELIFT TO THE CYBER SECURITY IN MALAYSIA

Sonny ZULHUDA*

Orcid: 0000-0003-0192-1971

1. Introduction

Digitalization has permeated all aspects of life, with many critical activities now dependent on digital systems. Their disruption could severely impact citizens' well-being and essential services. The G20 recently emphasized the importance of digital connectivity for inclusion and transformation, stressing the need for a secure online environment to build trust in the digital economy (ITU, 2024). However, this vision faces challenges including digital divides, privacy concerns, intellectual property issues, online safety, disinformation, and cybersecurity threats. The World Economic Forum report highlighted technological risks as a key global concern, including widespread cybercrime, critical infrastructure breakdown, digital inequality, and adverse outcomes of new technologies (World Economic Forum, 2024). Weak cybersecurity infrastructure exacerbates these issues, potentially leading to misinformation, social cohesion erosion, supply chain collapse, and even social conflicts. Therefore, strengthening cybersecurity policies is crucial for addressing these challenges and ensuring a resilient digital future.

Cybersecurity is the process of protecting information by preventing, detecting and responding to attacks. It is a 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 organisation and user's assets (ITU, 2008). Such organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems and the totality of transmitted and/or stored information in the cyber environment. The aim of cybersecurity is to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment.

* Assoc. Prof. Dr.Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia. E-mail: sonny@iium.edu.my

Furthermore, we can summarise that the objectives of cybersecurity are to achieve the three components, namely, availability, integrity which may include authenticity and non-repudiation and confidentiality. Pertaining to the cyber system or digital assets of any country, therefore, three components are crucial, namely:

1. The confidentiality of cyber system. This aspect of security focuses on the need to ensure only relevant persons would have access to every type of the digital assets. Measures must be taken to prevent unauthorised hands or eyes from entering the restricted space or accessing confidential information. There are incidents we heard from many parts of the globe where confidentiality of digital assets was compromised, such as leaks of military and official secrets, massive breach of personal data that impacted the public at large or an illegal interception of confidential communications systems.
2. The integrity of the cyber system. This second aspect of the CIA-triangle aims at preventing malicious or negligent disruption to the accuracy, completeness or truth of the system. Threats such as illegal intrusion ("hacking") of digital systems, unauthorised modification to the digital system, data theft as well as disinformation and misinformation are incidents that compromise with the integrity of a cybersecurity system. When threats such as these happen, the owner of the critical information system must be prepared to embrace the worst scenario of cybersecurity attacks. Therefore, access restriction and data preservation mechanisms must take place and must be enforced by law to ensure abuses can be effectively prevented or prosecuted.
3. The availability of system's security. This third objective of cybersecurity perceives that any interruption to the smooth working of digital system of a country or an organisation must be prevented, quickly detected or otherwise responded to. This is because such interruption will not only stop or slow down the system's function, but certainly when it comes to the CII, this may cause disturbance to public service delivery and may therefore create massive disturbance to public safety or economic chaos. Thus, threats such as sabotage and shutting down of the system, malicious downtime and the denial of services (DOS) should be perceived as serious disturbances to national security.

2. Threat to Cybersecurity and Critical Infrastructure in Malaysia

Malaysian cyberspace has never been a quiet zone. The country's National Cyber Security Agency (NACSA) under the National Security Council, Prime Minister's Office, revealed that the cyberattack trend has been increasing between 2016 and 2022. The trend includes

Distributed Denial of Service (DDoS), intrusion malware infection, malware hosting and advance persistent threats. NACSA reported 7192 incidents of cybersecurity in 2022, an increase from 5575 reported a year earlier.[2]

In the beginning of 2024, the Government of Malaysia initiated the Central Database Hub ("PADU") system as a key part of the country's digital transformation. The citizen data repository is an integrated socio-economic database that combines data from various government departments to provide a fair representation of each household's status in Malaysia (Prime Minister's Office Website, 2024). According to the release, PADU aims to ensure government services reach deserving recipients and prevent leakage in aid distribution and would therefore put an end to the issues of subsidy misappropriation, which currently costs the government RM80 billion. Barely three months after the announcement, we were informed that PADU has attracted a huge amount of cyberattacks. The Economic Affairs Minister revealed that there were two million weekly cyberattack attempts were put up against PADU database (*The New Straits Times*, 11 March 2024). Meanwhile, the defense minister warned that there were over 3000 cyberattacks made daily against the Malaysian cyberspace (*The New Straits Times*, 30 March 2024). These are perhaps just a tip of an iceberg we can never be sure of. But we know that the Malaysian cyberspace is never a quiet and peaceful playfield.

If this phenomenon is allowed to proceed, we may certainly end up losing. Public trust erodes, businesses slow down, privacy loses its meaning and our global competitiveness suffers. The most tangible impact will be felt by our national critical information infrastructure (CII). CII are those computer or information systems that are so critical that their disruption may cause detrimental impact on the security, defence, foreign relations, economy, public health, public safety or public order of Malaysia, or on the government functions.

Take for example two incidents affecting the system of public transport. In Malaysia, Kuala Lumpur International Airport ("KLIA")'s Total Airport Management System (TAMS) was disrupted by a technical glitch that caused system network failure on August 21, 2019. The system failure lasted for several days, affecting multiple systems including flight information display, check-in counters, WiFi availability, baggage-handling system and immigration process. This had in turn created dozens of flight delays and long passenger queues in both international terminals. Malaysia's Transport Minister reportedly refuted any elements of sabotage and told the members of parliament that the outage was because the 21-year-old core network switches (CNS) system that was never changed since KLIA began operations in 1998

[2] This is what was reported by the Government in the Parliament back in March 2024 (Hansard Dewan Rakyat, DR 27/3/2024, p. 37).

(Malay Mail, 2019). In a separate and a more recent incident, a series of disruptions occurred to Prasarana Malaysia's LRT signalling system for more than a week in November 2022. In one of the incidents, the operator company revealed that some trains "disappeared" intermittently from the monitoring screen of the LRT operation and control centre, posing a huge hazard (The Star, 2022).

The incidents mentioned highlight the vulnerability of Critical Information Infrastructure (CII) to a wide range of cybersecurity threats, stemming from both intentional attacks and unintentional system failures. Essential sectors including government operations, telecommunications, utilities, public transport, financial systems, and healthcare facilities have all faced significant cybersecurity challenges. Malaysia, like many other countries, has experienced a series of incidents affecting the cybersecurity of its CII in recent times. To address these challenges, a multi-faceted approach incorporating tools, measures, policies, and laws is necessary to prevent, detect, and respond to cybersecurity threats effectively. Particularly crucial are well-crafted policies and robust legal frameworks, which are essential for equipping the nation to navigate the complex and evolving cyber landscape. These elements form the foundation of a comprehensive strategy to safeguard critical infrastructure against cyber threats.

3. Cyber Security Act 2024: An Attempt to Upgrade

With so many stories of cyber threats and cyberattacks incidents, the Malaysian lawmakers brought this issue to the primary stage of policy-making by introducing Cyber Security Act 2024 [Act 854]. The Act was first passed by the House of Representatives on 27th March 2024 and was finally gazetted on 26th June 2024. The Act is meant to enhance the national cyber security by providing for the establishment of the National Cyber Security Committee, duties and powers of the Chief Executive of the National Cyber Security Agency, functions and duties of the national critical information infrastructure sector leads and national critical information infrastructure entities and the management of cyber security threats and cyber security incidents to national critical information infrastructures, to regulate the cyber security service providers through licensing, and to provide for related matters.

There are a number of critical provisions under this Act, i.e.:

- The establishment of the National Cyber Security Committee whose functions include to plan, formulate and decide on policies relating to national cyber security; to decide on approaches and strategies in addressing matters relating to national cyber security; and to monitor the implementation of policies and strategies relating to national cyber

security. Besides, the Committee will be able to advise and make recommendations to the Federal Government on policies and strategic measures to strengthen national cyber security; to give directions on matters relating to national cyber security; and to basically oversee the effective implementation of the Act (Cyber Security Act 2024, 2024).

- The classification of the National Critical Information Infrastructure (NCII) sectors to include eleven sectors, namely government; banking and finance; transportation; defence and national security; information; communication and digital; healthcare services; water, sewerage and waste management; energy; agriculture and plantation; trade, industry and economy; and science, technology and innovation (Cyber Security Act 2024, 2024).

- Designation of NCII sector lead and NCII entity. The Act empowers the Minister, upon the recommendation of the Chief Executive, to appoint any Government Entity or person to be the NCII sector lead (Cyber Security Act 2024, 2024: Section 15). Subsequently, the NCII sector lead may designate any Government Entity or person who owns or operates a national critical information infrastructure as a NCII entity (Cyber Security Act 2024, 2024: Section 17).

- The Act requires cyber security service provider who provides a cyber security service to NCII entity to obtain a special license (Cyber Security Act 2024, 2024: Section 27).

4. Statutory Duties of the NCII Entity

The legislation sets some statutory duties for the entities (government or non-government alike) designated as National Critical Information Infrastructure (NCII) entity. Those duties are quite comprehensive, consisting of both preventive and responsive actions that seek to ensure the objectives of cybersecurity for the primary players in Malaysia. Those duties include the following:

1. Duty to provide information relating to national critical information infrastructure (Cyber Security Act 2024, 2024, Section 20). This necessarily means that NCII entity are, when required, bound to disclose information about their critical computer or computer system which covers both information technology and operational technology system.

2. Duty to implement code of practice (Cyber Security Act 2024, 2024: Section 21). Under this provision, a NCII entity shall implement the measures, standards and processes as specified in the code of practice to ensure the cyber security of the national critical information infrastructure owned or operated by the national critical information infrastructure entity.

3. Duty to conduct cyber security risk assessment and audit. A NCII entity are obliged undet the new law to conduct a cyber security risk assessment in respect of the NCII owned or operated by such entity in accordance with the code of practice and directive. Apart from that, NCII entity shall ensure audit is carried out by an auditor approved by the Chief Executive to determine the compliance of the NCII entity with this requirement of the Act (Cyber Security Act 2024, 2024: Section 22).[3] The risk assessment and audit shall be held in a manner and time to be prescribed by the Authority.

4. Duty to give notification on cyber security incident. If it comes to the knowledge of a NCII entity that a cyber security incident has or might have occurred in respect of the NCII owned or operated by the NCII entity, the entity shall notify the Chief Executive and its NCII sector lead of such information within the period and in such manner as may be prescribed (Cyber Security Act 2024, 2024: Section 23).[4]

5. Participation in cyber security exercise held by the Chief Executive is necessary for the purpose of assessing the readiness of any NCII entity in responding to any cyber security threat or cyber security incident (Cyber Security Act 2024, 2024: Section 24).

5. Conclusion

Cyber Security Act 2024 is meant to provide a coordinated national mechanism to defend Malaysia's NCII by outlining various preventive, detective and responsive measures to protect our cyberspace. Among those preventive and detective measures are the obligations for the

[3] Cyber Security Act 2024, section 22. The corresponding Regulations 2024 prescribed that the cyber security risk assessment has to be conducted at least once in a year, while the compliance audit at least once in two years.

[4] Cyber Security Act 2024, section 23. The corresponding Regulations 2024 stated that the cyber security incident notification must be made immediately, and within six hours some initial information need to be reported to NACSA. Subsequently, more thorough report needs to be submitted within fourteen days after the first initial report.

NCII entity to conduct cyber security risk assessment and audit as well as undertaking cyber security hygiene and exercises. Furthermore, as part of responsive measures, the duty to notify cyber security incident is crucial. Failure to do those obligations constitutes an offence under the Act.

All these mechanisms introduce new norms of cyber security in Malaysia. Most, if not all, of data breaches in the past came to our attention only long after they happened, and often through third party channels. This would hamper any effort to prevent the harm or losses to the Malaysian NCII sectors as well as individuals. The Act is hoped to bring a loud and clear message about Malaysia's aim to achieve a national cyber resilience and cyber sovereignty as outlined by the Government's Malaysia Cyber Security Strategy 2020-2024. For this end, we hope the new Cyber Security Act 2024 paves the way for a better security in Malaysian digital economy.

Cybersecurity is more than just a policy product; it is a national journey worth travelling. It requires a long-term plan that visions the whole aspects of the national objective, economic growth and sustainability and social wellbeing. To achieve this, cybersecurity law and policy shall be firmly rooted in our commonly shared values and tradition as well as being driven by civility and innovation.

References

ITU. (2008). ITU-T X.1205: Overview of Cybersecurity. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items (Accessed on December 20, 2024).

ITU. (2024). G20: Digital connectivity to advance sustainable development, ITU News Magazine, 1/10/2024, https://www.itu.int/hub/2024/10/g20-digital-connectivity-to-advance-sustainable-development/ (Accessed on December 20, 2024).

Malay Mail. (2019). No Sabotage in KLIA Systems Disruption, Transport Minister Insists. (October 29, 2019), https://www.malaymail.com/news/malaysia/2019/10/29/no-sabotage-in-klia-systems-disruption-transport-minister-insists/1804770 (Accessed on December 20, 2024).

NACSA. (2024). Cyber Security Act 2024. https://www.nacsa.gov.my/act854.php, (Accessed on December 20,2024).

Prime Minister's Office Website. (2024). PADU ensures Government services will be enjoyed by deserving recipients – PM Anwar. 2 January 2024, https://www.pmo.gov.my/2024/01/padu-ensures-government-services-will-be-enjoyed-by-deserving-recipients-pm-anwar/ (Accessed on December 20, 2024).

The Star. (2022). Trains 'disappeared' from Our Control Screens on Nov 8, Says Prasarana. (November 10, 2022), https://www.thestar.com.my/news/nation/2022/11/10/trains-039disappeared039-from-our-control-screens-on-nov-8-says-prasarana (Accessed on December 20, 2024)

World Economic Forum. (2024). Global Cybersecurity Outlook 2024. 11/1/2024, https://www.weforum.org/publications/global-cybersecurity-outlook-2024/ (Accessed on December 20, 2024).