THE SALIENT FEATURES OF THE CYBER SECURITY ACT 2024

* Ida Madieha bt. Abdul Ghani Azmi

ABSTRACT

This article uses the 5W1H method to analyse the salient features of the Cyber Security Act 2024. The legal analysis focuses specifically on the extent of the regulatory duties outlined in the Act. As a result, the penalties and enforcement mechanisms will not be discussed. The Act will be framed by comparing its provisions with those in other nations' benchmark laws. The article ends by highlighting areas to be addressed in the future by looking at recent legislative revisions in different countries.

Keywords: cybersecurity, critical information infrastructure, designation, duties of CII entities, cyber incidence notification

* Professor, Civil Law Department, Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia.
E-mail: imadieha@iium.edu.my

INTRODUCTION

The entry into force of the Cyber Security Act 2024 on 26th August 2024 was a momentous occasion. Prior to that, a total of four regulations were released, i.e. the Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024, the Cyber Security (Notification of Cyber Security Incident) Regulations 2024, the Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024 and the Cyber Security (Compounding of Offences) Regulations 2024. Malaysia has a lot to celebrate with this achievement, but there is also a substantial catching up with other countries that have legislated earlier on cybersecurity. In the region, Malaysia rolled out the law later than Singapore and Vietnam, who did that in 2018[1] and China in 2016. Outside Asia, the US promulgated its cybersecurity law in 2015, and the EU in 2019.[2] The lessons learned from these countries is that a strong lead agency at the national level is needed, endowed with the authority to ensure compliance, followed by stiff enforcement measures.

The benchmarking with other countries also demonstrates that achieving optimal protection over cybersecurity is an incremental process and not a one-off attempt, depending on the readiness of the industry players. More so when huge gaps can be found in the level of cyber resilience among the NCII (National Critical Information Infrastructure) sectors, as was found during the successive engagement process with the industry players. Rolling out a platinum-level legal framework would not work as the gap between these sectors has to be bridged first. Experience from other countries has shown that no one model fits all. With the fast-changing technology, the law must inevitably move fast, constantly revised to keep tabs of the trends in cyber-attacks and the sophistication of technology.[3]

---

1 Ngoc Son Bui and Jyh-An Lee, "Comparative Cybersecurity Law in Socialist Asia," *Vand. J. Transnat'l L.* 55 (2022): 631.

2 Liudmyla Balke, "China's New Cybersecurity Law and US-China Cybersecurity Issues," *Santa Clara L. Rev.* 58 (2018): 137, https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2849&context=lawreview.

3 Ching Yuen Luk, "Strengthening Cybersecurity in Singapore: Challenges, Responses, and the Way Forward," in *Security Frameworks in Contemporary Electronic Government* (IGI Global, 2019), 96–128,

The Act explicitly provides for the application of the law to the Federal and State Governments. The provision illustrates the government's position to adopt stringent cybersecurity measures. Whilst such commitments are admirable, the next concern is whether these government agencies would equally be subjected to prosecution for failure to comply with the statutory obligations. On this note, the express provision is that the federal and state governments would not be liable for prosecution for any offenses under the Act. This assertion does not mean that the governments, particularly their officers, are entirely absolved from liability. Government officers are subjected to the highest standards of conduct, honesty, and probity in discharging their public duties as well as in their private lives. Disciplinary action can be taken against them for any misconduct which includes non-compliance with statutory obligations.

This article explores the salient features of the Cyber Security Act 2024 by addressing the 5W1H method with the following queries: (1) The corpus of cybersecurity law: What is cybersecurity law? (2) The rationale for cybersecurity law: Why is there a need for a specific and dedicated cybersecurity law? (3) The subject matter of protection: What is the subject matter of protection? (4) The locus of protection: Where are the locations of the computer/computer systems that are being secured? (5) The manner of protection: How are we securing the computer/computer system? and lastly (6) The time frame of statutory obligations: When do the statutory obligations commence?

By addressing these basic questions, the corpus of law known as 'cyber-security law' would be elucidated. The article will start examining the first question i.e. The corpus of cybersecurity law: What is cybersecurity law?

https://doi.org/doi:10.4018/978 1 5225 5984 9.ch005. Ching was of the view that "The chase for a perfect cybersecurity system or strategy is both impossible and unnecessary. However, it is important and necessary to establish a cybersecurity system or formulate a cybersecurity strategy that can monitor, detect, respond to, recover from, and prevent cyber-attacks promptly, and make the nation stronger, safer, and more secure.

THE CORPUS OF CYBERSECURITY LAW: WHAT IS CYBERSECURITY LAW?

As far as a decade ago, the legal solution to problems posed by cyber-attacks is addressed through an amalgam of "century-old privacy norms, torts, and criminal laws that deal with hacking and intrusion into privacy."[4] Whilst these legal norms are useful in addressing the liabilities of these cyber-attacks, they have little to do with the protection of systems, networks, or data targeted by them. Sad to say, many countries do not have in place a set of cohesive cybersecurity laws even though the world is now heavily dependent on the internet. In other words, there was a lack of clear consensus as to the corpus of law known as cybersecurity law.

History has also shown how the vital interest in the safeguarding of personal data led to the promulgation of personal data laws. However, there seems to be a lack of adequate safeguards on the information systems that are vital to national security and economic interests. Breach notification was first created for personal data and not for attacks on national security and economic harms caused by cyber-security incidents.[5] Whilst the harm posed by personal data may transcend human integrity and may encroach into business and economy, the harm posed by a breach of security is even more multifaceted and multidimensional which includes the loss of life.

The ultimate question to address is if we were to develop the legal framework, the focus should be on maintaining confidentiality, integrity, or availability of systems, networks, and data, also known as the CIA triad.[6] Traditional cyber-crimes law resolves the issue of confidentiality of data but does little to address integrity and availability of information which is the effect of ransomware and malware attacks.

On this basis, cybersecurity law cannot be a stand-alone law. The law must be read together with existing provisions on computer crimes, criminal law, and other procedural laws. Moreover, as the need for

---

4 Jeff Kosseff, "Defining Cybersecurity Law," *Iowa L. Rev.* 103 (2017): 985.

5 Jeff Kosseff, "Upgrading Cybersecurity Law," *Hous. L. Rev.* 61 (2023): 51.

6 Kosseff, "Defining Cybersecurity Law."

cybersecurity cuts across all sectors, the relevant legislations from these sectors also form the backbone of the legal corpus understood as cybersecurity laws.

This is the exact spirit adopted by the Cyber Security Act 2024 that defines the term "cybersecurity" as "the state in which a computer or computer system is protected from any attack or unauthorized access, and because of that state— (a) the computer or computer system continues to be available and operational; (b) the integrity of the computer or computer system is maintained; and (c) the integrity and confidentiality of the information stored in, processed by or transmitted through, the computer or computer system are maintained".[7]

---

[7] In comparison see, Section 2 of Singapore's Cybersecurity Act 2018 is as follows–

"cybersecurity" means the state in which a computer or computer system is protected from unauthorized access or attack, and because of that state —

(a) the computer or computer system continues to be available and operational;

(b) the integrity of the computer or computer system is maintained; and

(c) the integrity and confidentiality of information stored in, processed by, or transmitted through the computer or computer system is maintained;

See also Article 2 of the Japan Basic Act on Cybersecurity Act (Act No 14 of 2014):

The necessary measures have been taken to prevent the leakage, loss, or damage of information that is recorded, sent, transmitted, or received in electronic form, magnetic form, or any other form that cannot be perceived by the human senses (hereinafter referred to as "electronic or magnetic form" in this Article) and to securely manage that information in other such ways; that the necessary measures have been taken to ensure the security and reliability of information systems and of information and communications networks (including the necessary measures to prevent damage from unauthorized activities directed at a computer through an information and communications network or through a storage medium associated with a record that has been created in electronic or magnetic form (hereinafter referred to as "electronic or magnetic storage medium")); and that this status is being properly maintained and managed."

The above definition anchors on the state of the computer or computer system involved. As such, "cyber security" in the Act is meant to indicate the preferred status quo of the computer or computer system whereby there exists an absolute protection to the integrity of the system operation and the information stored within such a system.

The type of cyber-attack ranges from a real threat to a potential threat, which are both treated as threat under the Act. This is the distinction drawn between cybersecurity threats and cybersecurity incidents. Under the Act, a cybersecurity threat is defined as "an act or activity carried out on or through a computer or computer system, without lawful authority, that may imminently jeopardize or may adversely affect the cyber security of that computer or computer system or another computer or computer system"[8].

A cyber security incident is defined as "an act or activity carried out on or through a computer or computer system, without lawful authority, that jeopardizes or adversely affects the cyber security of that

---

[8] Section 4 of the Cyber Security Act 2024. The term 'cyber security incidents' has been defined in both NSC Directive No. 26 as well as the General Circular No. 4 on the Management and Handling of Public Sector Cyber Security Incidents as follows:

a. NSC Directive No. 26

"cyber security incident" is an unwanted cyber incident that results in impairment of information confidentiality, interference with the integrity of the data or system, or interference that fails to obtain information from a computer system and the possibility of a breach of information security regulations, certain policies or security standards practices, as well as incidents involving misuse of cyberspace resulting in financial loss to a party or contribute to terrorism-related activities, as well as the posting of content that is contrary to the laws of the country, touches the sensitivity of society or is capable of influencing the thinking of society and is capable of threatening the stability and security of the country as well as undermining national values and identity.

b. General Circular No. 4

"Cyber security incident" is an unwanted cyber incident when the loss of information confidentiality, interference with the integrity of data, or systems, or interference that causes failure in obtaining information from computer systems and the possibility of violations of information security rules, certain policies, or cyber security standard practices.

computer or computer system or another computer or computer system"[9]. The element of 'imminent' and the possibility of attack could be understood from the definition of 'cyber threat' as opposed to a cyber security incident.

THE RATIONALE FOR CYBERSECURITY LAW: WHY IS THERE A NEED FOR A SPECIFIC AND DEDICATED CYBERSECURITY LAW?

History has shown that laws are regulated to compel individuals to follow certain normative values. Given that many countries have faced regular and consistent cyber-attacks, some form of regulation is needed to mitigate the harms posed by these attacks. In Malaysia, statistics have shown that the highest number of attacks come in the form of malware, followed by intrusion attempts, website intrusion, and denial of service attacks. On that basis, the exact purpose of the specific and dedicated cybersecurity regulation is to achieve that state of 'cybersecurity' as desired.[10]

The most fundamental question is why is a need for cybersecurity regulation. In the EU, the discourse is the notion that the fundamental right to security can be extended to a new right to cybersecurity.[11] Vagelis Papakonstantinou, for example, suggests:

> "It is suggested that this could be achieved through the distinction between cybersecurity as *praxis*, whereby actions and measures undertaken by the cybersecurity addressees are meant, and cybersecurity as a *state*, whereby a conceptual protective sphere is created to the benefit of the cybersecurity recipients within which they are and remain (cyber)secure. This distinction is considered useful in order to create clarity and improve understanding in today's complex global environment that creates confusion. Such confusion becomes evident as early as when trying to provide cybersecurity

---

9 Section 4 of the Cyber Security Act 2024. Both these definitions were a deliberate departure from the NSC Directive No. 26 and the General Circular No. 4.

10 Annegret Bendiek and Eva Pander Maat, "Cybersecurity by Regulation," in *11* (Santa Clara Journal of International Law, 2013), 421–53.

11 Pier Giorgio Chiara, "Towards a Right to Cybersecurity in EU Law? The Challenges Ahead," *Computer Law & Security Review* 53 (2024): 105961, https://doi.org/https://doi.org/10.1016/j.clsr.2024.105961.

> with a commonly accepted definition. The distinction between cybersecurity as *praxis* and as a *state* is also critical while examining the existence of a new right to cybersecurity because it sheds light on its necessary parts: under a *praxis* lens the cybersecurity's addressees, recipients, as well as, its subject matter and protective scope become identifiable; under a *state* lens, the cybersecurity protected sphere for natural and legal persons emerges, that forms the core of the right to cybersecurity."[12]

The easiest way to justify the need for cybersecurity laws can stem from the three types of harms resulting from cyber-attacks i.e. (1) harm to individuals (2) harm to business interests and (3) harm to national security. For individuals, the harm comes in the form of leakages of personal data and identity theft. The harm to business interest comes in the form of the cost in mitigating cyber-attacks and incidents, business reputation, and loss of clientele as well as conducting cyber forensics. The third type of harm is the damage caused to national security. Cyber-attacks on critical infrastructure can bring enormous harm to the country. Attacks on the power grid, for example, do not only cause chaos in the country but can potentially cause human deaths.

In Malaysia, before the promulgation of the Cyber Security Act 2024, two national policies were framed: (i) the National Cyber Security Policy 2006 (NCSP) followed by the Malaysian Cyber Security Strategy 2020-2024 (MCSS)[13]. The MCSS that replaces NCSP is more inclusive and comprehensive in terms of strategic initiatives rolled out to protect the CII. Five core pillars constitute the bedrock of MCSS i.e. which includes strengthening legislative framework and enforcement.[14]

All these strategies rolled out by the national policies are short of the actual legislative support, which means that there was no legislative power to instil compliance. It is clear thus, that a specific

---

[12] Vagelis Papakonstantinou, "Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?," *Computer Law & Security Review* 44 (2022): 105653, https://doi.org/https://doi.org/10.1016/j.clsr.2022.105653.

[13] Among the key recommendations of the NCSP is to implement ISMS certification for the CII entities.

[14] Both the National Cyber Security Policy 2006 and Cyber Security Strategy 2020-2024 are available at https://www.nacsa.gov.my/.

and dedicated law is needed to bolster cybersecurity governance in Malaysia.

THE SUBJECT MATTER OF PROTECTION: WHAT IS THE SUBJECT MATTER OF PROTECTION?

Cybersecurity is not only concerned with information but also the hardware, devices, control system, and network as the 'cybersecurity' targets involve more than just data, but also system and network security. This is transparent from the definition given by The International Telecommunications Union (ITU) which 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" within the cybersecurity foci of CIA triad and objectives.

It must be reiterated here that cyber-attacks such as trojan horses, malware, denial of service (DDoS), ransomware, or botnet attacks compromise the ability of the system to operate. Thus, the impact posed on the computer and computer system could be more than the availability of the system, as it compromises the fundamental ability of the system to operate as normal.

Core to the cybersecurity laws is the protection of critical information infrastructure and not personal computers belonging to individuals not connected to the CII. The impression of the members of the public is that the new law is supposed to resolve the issue of cyber-crimes as at the time of the drafting of the law, that is the main problem faced by the public. Instead, cybersecurity law is set to address the security of a 'protected system' i.e. computer systems managed under large corporations, entities, and government offices. As such the Act targets 'a critical system' called the "national critical information infrastructure" (NCII) that refers to a computer or computer system, the disruption to or destruction of which would have a detrimental impact on the delivery of any service essential to the security, defence, foreign relations, economy, public health, public safety or public order

of Malaysia, or on the ability of the Federal Government or any of the State Governments to carry out its functions effectively.[15]

What constitutes the object of protection is the computer and computer system which forms part of the NCII. On this point, the scope of the definition of 'computer system' covers not only the IT system but also the operational technology system in the following manner:

> "Computer system" means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes— (a) an information technology system; and (b) an operational technology system such as an industrial control system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system.[16]

It becomes clear that the object of protection is beyond the computer and data, but also encompasses the control system. In an Internet of Things, where hardware, devices, and systems are all connected, the control system is equally a point of attack.

This definition is adopted from the Singapore Cybersecurity Act 2018, along with the definition of the term 'computer' itself.[17] The term 'computer' in the Cyber Security Act 2024 is a refined and revised version of the same term in the Computer Crimes Act 1997 and

---

15 Section 4 of the Cyber Security Act 2024. The stand taken by under the Act displays a deliberate departure from the existing practice under the NSC Directive No.26 and General Circular N.4/2022 that has already determined the meaning of CNII to be as follows:
"Critical systems that include information (electronic) assets, networks, functions, processes, facilities, and services in an information and communications technology environment that are important to the country where any disruption or destruction to them can have an impact on national defense and security, national economic stability, national image, the Government's ability to function, public health and safety and individual privacy."

16 Section 4 of the Cyber Security Act 2024.

17 For literature on Singapore, see Benjamin Ang, "Cybersecurity and Legislation: The Case Study of Singapore," in *Cybersecurity and Legal-Regulatory Aspects*, ed. Gabi Siboni and Limor Ezioni (World Scientific, 2021), 89–102, https://doi.org/https://doi.org/10.1142/9789811219160_0004.

Evidence Act 1950.[18] Under both Acts, a computer must carry out both the processing and displaying functions at the same time. However, in the world of the Internet of Things many devices no longer perform display functions and with cloud computing, even storage is not done in the computer system itself, but instead on the cloud. Due to this, it is submitted that the definition of a 'computer' contained in Malaysian statutes is outdated. Ideally, the notion of 'computer' must not be fixated with the requirement of a specified feature. In contrast, the UK and Australian legislation chose not to statutorily define the term 'computer' for fear that it would have been overtaken by technological changes.[19]. The Australian Security of Critical Infrastructure Act 2018 also does not specifically define the word 'computer'.

One possible option is to adopt newer terms such as 'ICT device' which includes any communication device or application encompassing mobile phones, computers, network hardware, software, the Internet, satellite systems, and so on. The current ongoing negotiation of the UN cybercrime treaty, for example, uses the term 'misuse of ICT device'. However, as the Cyber Security Act 2024 would have to be read together with the existing laws such as the Computer Crimes Act 1997, and Evidence Act 1950 that deal with cybercrimes, the term 'computer' had to be retained so as not to confuse judges, lawyers, and the public.

Other relevant terminologies used are 'network security' under the Communications and Multimedia Act 1998 and 'data security' under the Personal Data Protection Act 2010. Cyber security instead deals with the whole ecosystem from the transmission of signals to the receiving of signals and whatever process in between. It covers the hardware, software, devices, switches, and controls that are necessary

---

[18] See also Money Services Business Act 2011, Rules of Court 2021, Development Financial Institutions Act 2002, Sarawak Syariah Evidence Ordinance, 2001, State Sales Tax Enactment 1998, Cyber Centre & Cyber Café (Federal Territory of Kuala Lumpur) Rules 2012.

[19] The UK Computer Misuse Act 1990 does not define a computer because rapid changes in technology would mean any definition would soon become out of date. The task of defining what constitutes a 'computer,' in the UK, is thus left to the Courts, who are most likely to opt for the most recent definition. In *DPP v McKeown, DPP v Jones* ([1997] 2 Cr. App. R. 155, HL, at page 163), a computer was defined by Lord Hoffman as *"a device for storing, processing and retrieving information."*

for the process to take place. The nearest provision to cybersecurity is s 52A of the Electricity Supply Act 1990 which deals with supply infrastructure information security. This provision mandates licensees under the Act to take measures to ensure a quality electricity supply that is continuous and reliable.[20]

The next issue is to identify the sectors that form part of the critical information infrastructure. Different countries adopt different thresholds as to what sectors are essential to that country. For example, under the Australian Security of Critical Infrastructure Act 2018, there are no specific definitions of Critical Information Infrastructure. The Act, instead, provides a comprehensive list of what would be considered as "critical infrastructure." A total of 11 sectors have been listed as the critical infrastructure sector; i.e. communications, financial services and markets, data storage and processing, defence, higher education and research, energy, food and grocery, healthcare and medical, space technology, transport, and water and sewerage.

The delineation of sectors falling within the CII concept not only varies from one country to another but is also tied down to the sector that faced the most risk in the form of cyber-attacks due to the

---

[20] Supply infrastructure information security 52A. (1) Any licensee as directed by the Commission supplying electricity to consumers shall be responsible for the preservation of confidentiality, integrity, and availability of its information, information systems, and supporting network infrastructure about its duties and other matters as provided under this Act. (2) The licensee shall— (a) take the necessary measures, establish and implement standards and employ the relevant information security controls to prevent, avoid, remedy, recover or restore its information, document, instrument or records stored in its computers and for its operational system by its computers from any risk of— (i) threat or unauthorized access; and (ii) intrusion or removal; (b) take necessary measures to ensure the resiliency of its supporting network infrastructure to minimize business impact against various threats to its activities under the licence; and (c) ensure that the reliability, continuity and quality of electricity supply, its performance of duties and conformity to the provisions of this Act and any regulations made thereunder shall not be jeopardized thereby and shall report to the Commission within the time specified by the Commission, and in the event of any incident which interferes or affects the performance of the activities under the licence, report such incident immediately to the Commission and other relevant authorities.

significance of data systems retained in a particular organisation/sector. Sectors that are not currently perceived as critical to a country at present might be crucial to be protected in the future. One example is research data, currently hosted in research institutes and tertiary institutions may one day be 'prime data and systems' to be intruded for assorted reasons.

The sectors identified in Australia are skewed towards energy and essential facilities that support the country and economy. In Malaysia, using a risk-based analysis, the 11 National Critical Information Infrastructure Sectors identified are: Government Sector, Banking and Finance Sector, Transportation Sector, Defence and National Security Sector, Information, Communication, and Digital Sector, Healthcare Services Sector, Water, Sewerage, and Waste Management Sector, Energy Sector, Agriculture and Plantation Sector, Trade, Industry, and Economy Sector, Science, Technology, and Innovation Sector.

The identification of the 11 risk sectors meant that cybersecurity traverses public and private infrastructure. On this basis, the framework of cybersecurity law must strive to protect both private companies and government computers.

The remaining question is what is not covered within the framework of the cybersecurity law? One big vacuum is with regard to cyber-attacks by state actors. The consequences of cyber warfare have been well addressed in many literatures. The problem with cyberwarfare is the difficulty of attributing the attacks to any nation or state agents as it implies accountability as well as sovereignty of a nation.[21] This is unfortunate as the consequences of cyberterrorism are far more serious than cyber-attacks on businesses and corporations. The anatomy and impact of cyber-crime, cyber-warfare, and cyber-attack warrant these attacks to be treated differently.[22] On this point,

---

21 Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility," *Melbourne Journal of International Law*, 2013, https://law.unimelb.edu.au/__data/assets/pdf_file/0006/1687488/05Margulies-Depaginated.pdf.

22 Yuchong Li and Qinghui Liu, "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments," *Energy Reports* 7 (2021): 8176–8186.

Gervais views the lack of consensus on legal norms on cyberwarfare reflects the problem of standard setting on state's conduct in cyberspace at the international level.[23] This reluctance has led to a power vacuum, lending credence that international law fails to address modern challenges in the rapid development of information and communication technologies. Worse still, the existing international instruments do not help determine how cyber-attacks ought to be understood under the existing jus ad bellum (use of war) and jus in bello (wartime conduct) frameworks.[24] This leads to uncertainty and difficulty in going after the perpetrators using international law instruments.[25]

THE LOCUS OF PROTECTION: WHERE ARE THE LOCATIONS OF THE COMPUTER/COMPUTER SYSTEMS THAT ARE BEING SECURED?

The locus or place of protection of the computer/computer system is not something that forms the main criteria under the cybersecurity law. If the computer/computer system were to be located within certain buildings, then securing them is easy as it is a matter of designating the building under the Protected Areas and Protected Places Act 1959. However, an intrusion into computer systems can occur regardless of where the physical computer/computer systems are. The nature of networking means the range of computer/computer systems in need of protection surpasses those devices physically located in one location.

Locus is however still important in determining legal jurisdiction. With many companies choosing to use cloud services, the question of data sovereignty and data residence becomes an issue. On this basis, Malaysia chose to adopt the position in Singapore that states,

---

23 Kubo Mačák, "Is the International Law of Cyber Security in Crisis?," in *2016 8th International Conference on Cyber Conflict (CyCon)* (Tallinn, Estonia: IEEE, 2016), 127–139, https://ccdcoe.org/uploads/2018/10/Art-09-Is-the-International-Law-of-Cyber-Security-in-Crisis.pdf.

24 Michael Gervais, "Cyber Attacks and the Laws of War," *Journal of Law & Cyber Warfare* 1, no. 1 (2012): 8–98.

25 Samuli Haataja, "Cyber Operations against Critical Infrastructure under Norms of Responsible State Behaviour and International Law," *International Journal of Law and Information Technology* 30, no. 4 (2022): 423–43, https://doi.org/https://doi.org/10.1093/ijlit/eaad006.

if 'part' of the NCII is in Malaysia, that will be sufficient to establish Malaysian jurisdiction over the system.[26] Though the issue of 'partly' can be difficult to establish with precision, the thinking is that if the attack is made to a computer system that is connected to the ones in Malaysia, e.g. belonging to a branch of a Malaysian NCII entity then it is subjected to Malaysian law. The same principles apply to employee's own devices. As soon as the device is connected to a computer system in Malaysia, it is subjected to Malaysian law. The 'partly' criteria avoid the insistence that the device must be physically present in Malaysia all the time.

THE MANNER OF PROTECTION: HOW ARE WE SECURING THE COMPUTER/COMPUTER SYSTEM?

The question as to how we secure the cybersecurity of the nation depends on the regulatory model to be adopted. As with many other countries, Malaysia chose a system that is based on both coercive and cooperative laws i.e. a mixture of carrots and sticks. As such the main mode of identifying the essential assets is through designation or mapping of the primary assets to be protected.

In this context, there are potentially two ways to do this:

1. To designate the organizations identified as 'NCII' first. By doing this, all the computer systems hosted by the NCII organizations would be deemed to be falling within the essential computer systems.

2. To identify 'essential services' that form the backbone of the 'NCII." By doing this, only the computer systems that serve the 'essential services' would be considered as falling within the boundary of the NCII.

In Singapore, the designation is done by mapping the computer and computer systems connected to essential services in the country.[27]

---

26 Section 3 of the Cyber Security Act 2024.

27 See Kah Leng Ter, "Singapore's Cybersecurity Strategy," *Computer Law & Security Review* 34, no. 4 (2018): 924–927.

The process is meticulous, but it would give an accurate account of the assets to be protected.

On the other hand, designating the organizations that serve essential services is much easier as the focus is on the organization, rather than the computer or computer systems that they host. Malaysia chose the latter to continue with the existing practice prevalent in the banking and telecommunication industry that focuses on the organization for easy governance.[28].

Mapping the NCII should be the first task as once the computer/computer systems falling under NCII are identified, then targeted organizations will be the ones to execute the duties and responsibilities of ensuring their cyber resilience.

In Malaysia, with the wide range of sectors involved, the task of designation is given to the sector lead. For that, the Act provides for the appointment of the sector lead for the eleven NCII sectors.[29] To conserve the sensitivities of the government sector agencies, it is further provided that no government NCII entity shall be designated under a sector lead who is non-government entity. The placement of the major responsibility of designation to the sector lead is a major departure from the practice in Singapore. This is deliberately done as these sector leads have a better knowledge of the agencies in their sector and have a stronger rapport with them. Moreover, following the former practice under the NSC Directive No 26, the lead sectors have been tasked with the designation, so naturally, these obligations were carried forward into the Act.

THE TIME FRAME OF STATUTORY OBLIGATIONS: WHEN DO THE STATUTORY OBLIGATIONS COMMENCE?

Today's vulnerabilities will be tomorrow's point of attack. It is thus important for the law to be forward-looking and consider imminent threats to prevent cybersecurity incidents from ever occurring. The progressive nature of the cybersecurity law constitutes the main distinguishing criteria from cybercrime. The latter, like many other criminal laws, aims to punish the culprit after the act has been

[28] Section 17 of the Cyber Security Act 2024.
[29] Section 16 of the Cyber Security Act 2024

committed. Relying on cybercrime to deter cyberattacks is no longer a sufficient deterrent in a world of diverging, diversifying, and evolving forms and intensity of cyber-attacks. In addition, the frequent audit that has been mandated under the law means that agencies should be able to identify vulnerabilities that may be points of attack in the future much earlier. On this basis, the approach adopted in the cybersecurity law is both reactive and defensive.

One important reactive measure is the obligation to notify National Cyber Security Agency (NACSA) of any cyber security incident.[30] With the insistence on incident notification, organizations commence their mitigation process immediately after the incident, including rolling out measures to avoid future attacks. The ambit of the law is thus not focusing only on events already occurring but also imminent threats in the future. The whole basis of cybersecurity is to prevent, detect, respond to, or recover from incidents, served through a mixture of proactive and reactive measures.

The ensuing issue is the exact form and manner of the notification. In the US, the timeline given for the reporting of cybersecurity incidents is 72 hours.[31] The time for reporting is shorter in Australia which is no later than 24 hours for cyber incidents. The Cyber Security Act 2024 is silent on the form, manner, and time of cyber incidents and threats. The Cyber Security (Notification of Cyber Security Incident) Regulations 2014 prescribed this to be the initial notice within 6 hours after the cyber incidents. The detailed report on the affected system is expected later i.e. within 14 days of the incident.[32]

The breach notification for cyber incidents is the same breach notification obligation as set under the personal data protection law.[33]

---

30 Section 23 of the Cyber Security Act 2024. See also s 23 of the Australian Security of Critical Infrastructure Act 2018

31 Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, Proposed Rule, 89 Fed. Reg. 23644 (April 4, 2024)

32 Rule 3(3) of the Cyber Security (Notification of Cyber Security Incident) Regulations 2024.

33 Privacy interests and cybersecurity interests overlap to a certain extent. See literature like Brandon W Jackson, "Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues

In the US, this is made possible through the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) which sets uniform cybersecurity incident reporting requirements for operators of critical infrastructure.

On the defensive side, cyber hygiene practices and standards are important in ensuring the cybersecurity posture of the whole country. The monitoring of such cyber hygiene practices is through the setting of cyber hygiene baselines through a code of practices which can be based on internationally recognised standards.[34] Second, the Act sets the obligation for the entities to conduct an annual cyber security assessment and biennial compliance audit.[35]As some sectors such as the telecommunication and banking sectors have put in place stringent cybersecurity standards, their full observance would be considered as compliance with the Cyber Security Act 2024. The disparities in cybersecurity standards can provide weak points for cyberattacks. NACSA as the lead agency's main role is to 'mentor' sectors with weaker cybersecurity resilience through continuous monitoring and upgrading of security cybersecurity baselines and standards.

The remaining vacuum in the loop is individuals who use and connect to the information resources. The human aspect of the whole ecosystem is one of the neglected aspects of cybersecurity laws. Cains et al, in their seminal article, posit that most laws focus on software,

---

Surrounding the European Union General Data Protection Regulation and Autonomous Network Defense," *Minn. JL Sci. & Tech.* 21 (2019): 169, https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1476&context=mjlst; Read also Maria Grazia Porcedda, "Cybersecurity, Privacy and Data Protection in EU Law.," 2023.

34 Section 21 of the Cyber Security Act 2024

35 Section 22 of the Cyber Security Act 2024. Regulation 3 of Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024.
"A comprehensive risk assessment enterprise risk management strategy, which includes a careful risk definition, crafting of policies and procedures aligned with the organisation's approach to risk management, and a comprehensive corporate compliance programme that ensures the policies and procedures are being followed, can change the outcome and impact of major security incidents". Briget MEAD, Joseph Goepel, Jared Paul MILLER, 'Defensibility: Changing the Way Organisations Approach Cybersecurity and Data Privacy' (2021) 33 SAcLJ 127.

hardware, and devices but do not touch much on the individuals involved.[36] NCII entities, thus must train their personnel on cybersecurity as the main weakness in the loop is the humans themselves.[37] In the Internet of Things, machinery and equipment can be controlled remotely, rendering it more crucial than ever to train human resources.[38] The increasing volume and sophistication of cyberattacks mean that continuous training needs to be conducted to ensure that the humans behind the essential computer and computer systems are well-equipped to address them. To that extent, the provision under the Cyber Security Act 2024 on mandatory participation in cyber exercises could achieve this to a certain measure. What the NCII sector requires is close assistance from the lead agency in terms of resources, expertise, and training to face the non-ending cyber onslaught.

CONCLUSION

The nation's move to ensure the attainment of cybersecurity through strict legal obligations under the Cyber Security Act 2024 highlights the importance of protecting our information resources. Frequent and continuous cyber-attacks could lead to massive loss of government resources, business losses as well as harm to the economy, society, and country.[39] Due to rapid changes in technology, diversity, and intensity of cyberattacks since the beginning of the drafting of the Cyber Security Act 2024, three countries that were benchmarked i.e. the EU, Australia, and Singapore have introduced new revisions. Among areas

---

36 Mariana G Cains et al., "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context Using Expert Elicitation," *Risk Analysis* 42, no. 8 (2022): 1643–1669, https://doi.org/https://doi.org/10.1111/risa.13687.

37 Li and Liu, "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments."

38 Rolf H Weber and Evelyne Studer, "Cybersecurity in the Internet of Things: Legal Aspects," *Computer Law & Security Review* 32, no. 5 (2016): 715–28.

39 Xiang Liu et al., "Cyber Security Threats: A Never-Ending Challenge for e-Commerce," *Frontiers in Psychology* 13 (2022): 927398, https://doi.org/https://doi.org/10.3389/fpsyg.2022.927398.

of revision is the express extension to the Internet of Things, cloud computing, smart devices, and artificial intelligence. The EU through the proposed Cyber Solidarity Act (2023/0109 (COD), set up a regional-based cybersecurity alert system. Australia's Cyber Security Act 2024, meanwhile expands the list of the essential services as systems of national significance. Singapore's revisions in the Cybersecurity (Amendment) Act 2024, focus on the extension of the measures beyond the CII to include the supply chain as well. At the same time, the provision was strengthened to explicitly cover cloud computing services.

Whilst this article highlights the salient features of the Cyber Security Act 2024, the journey to attain the optimal state of cybersecurity is ongoing. Continuous updating of the technical baselines and standards can be done through the introduction of a new code of practices as well as directions from the NACSA's Chief Executive as the lead agency. On top of that the Act also requires continuous revision to take stock of global trends, to achieve global and harmonised standards as well as respond to new forms of cyber-attacks and technological changes. True to the phrase, both the journey and the destination is important to Malaysia.