3 July 2024

THAILAND Newsletter

Thailand's Cybersecurity Snapshot: Current Laws and Emerging Trends

A. Introduction

In recent years, news and headlines have increasingly highlighted the surge in cyber threats and crimes. Organizations and individuals in Thailand have been targeted by a variety of cyber threats, including ransomware attacks, system hacks, spam calls, and phishing scams. These threats are often linked to data leaks or illegal sales of personal information.

To address these issues, the Thai government has developed a comprehensive cybersecurity framework. This framework includes legal measures to enhance technology security and privacy standards. Additionally, the government has established a cybercrime department within the criminal court to handle cybercrimes more effectively.

With numerous parties involved and a wide range of regulations in place, this article provides an overview of the key aspects of Thailand's cybersecurity-related legal regime and aims to help business operators review their understanding of and ensure compliance with current cybersecurity standards.

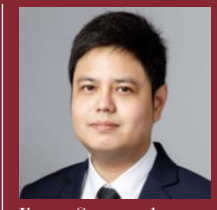
B. Who do "cybersecurity" compliance requirements apply to?

First, "cybersecurity" in this article refers to the broader concept of cybersecurity and is not limited to the Cybersecurity Act, B.E. 2562 (2019) (the "**Cybersecurity Act**"), which is merely one of several Thai laws related to cybersecurity. Business operators must understand that they may still be subject to other cybersecurity compliance requirements, even if they are not subject to the Cybersecurity Act.

Designated "critical information infrastructure operators (collectively referred to as "**CIIOs**", and individually as a "**CIIO**")" are subject to the Cybersecurity Act. CIIOs include both public and private organizations that provide services across various sectors, such as information technology and telecommunications, energy and public utilities, banking and finance, and transportation and logistics, among others. These sectors are vital for the functioning of the country; hence, specific requirements, especially regarding their operating systems, are essential.

Key Contacts

Panupan Udomsuvannakul
+66-2-009-5159
panupan.u@mhm-global.com



Jirayu Sanguankaew
+66-2-009-5186
jirayu.s@mhm-global.com

Koraphot Jirachocksubsin
+66-2-009-5163
koraphot.j@mhm-global.com

Suphakorn Chueabunchai
66-2-009-5168
suphakorn.c@mhm-global.com

Supakan Nimmanterdwong
66-2-009-5173
supakan.n@mhm-global.com

However, not all non-CIIO business operators can assume they are free from legal obligations. These business operators are still subject to other regulatory compliance, such as the Computer Crime Act, B.E. 2550 (2007) (the "Computer Crime Act"), and the Personal Data Protection Act, B.E. 2562 (2019) ("PDPA"). Additionally, the criminal court has established a cybercrime department in order to specifically handle cases related to computer crime, cybersecurity, and privacy.

C. What are the recent legal highlights in relation to cybersecurity?

This section will not discuss specific laws in detail, but will instead highlight notable recent trends and movements:

1. **Reinforcement of Personal Data Protection Measures.** The Personal Data Protection Commission (the "**PDPC**") has become noticeably proactive since early this year, officially establishing the PDPA center to handle complaints and provide advice on data protection and data breaches. In addition, the PDPC Eagle Eye Personal Data Violation Surveillance Center ("**PDPC Eagle Eye**") has been established to actively monitor, inspect, and supervise relevant agencies and data protection officers (the "**DPO**").

2. **Reports of 5,273 data leak cases, and 1,789 cyberattack cases.** According to the PDPC Eagle Eye, the PDPC proactively investigated organizations and identified 5,273 data leak cases during the period from November 2023 to January 2024. In addition, the National Cyber Security Agency reported 1,789 cyberattack cases in 2023. Reports also indicate that the most targeted business sectors in both data leaks and cyberattacks are banking and financial services, telecommunications, and logistics.

3. **Establishment of a cybercrime division in the criminal court.** Recognizing the increasing complexity and volume of cybercrime, the Supreme Court of Thailand has announced the establishment of a specialized technology crime division within the criminal court. This new division will have jurisdiction over crimes under the Computer Crime Act and other offenses involving technology and computer crimes, including fraud and extortion committed using computer systems, as well as offenses related to measures for the prevention and suppression of technological crimes. It will also address offenses related to personal data and handle cases concerning orders issued by government officials under the Cybersecurity Act, the Computer Crime Act, and the PDPA.

D. Keeping up with Cybersecurity compliance and trends

Amidst rapid development, it is crucial to remain informed and compliant at all times. An organization may begin with the following steps:

- Conducting self-assessments and risk assessments to identify potential treats and vulnerabilities within the organization.
- Assessing appropriate technical and organizational measures to protect the data collected by the organization and IT system from potential cyber treats.
- Developing internal documentation, IT systems, and crisis management measures to handle cybersecurity incidents effectively.
- Raising awareness on cybersecurity and privacy among employees to reduce risks arising from employee carelessness, such as phishing and identity theft.
- Ensuring employee understanding of laws and compliance with internal rules when handling data or managing cyber systems by conducting regular cybersecurity awareness training and implementing phishing simulations to test and improve employees' responses to potential cyber-attacks.
- Conducting due diligence on third-party vendors and service providers to ensure they meet the organization's cybersecurity standards.
- Including cybersecurity and data protection clauses in contracts and/or service level agreements with third-party vendors.
- Monitoring and auditing operations regularly to identify and address any potential weaknesses or compliance gaps.

This collaboration will help to ensure that all aspects of cybersecurity are thoroughly understood and addressed. By understanding and implementing the necessary measures, an organization can protect itself against cyber threats, ensure compliance with relevant laws, and maintain customer trust and business integrity.

Organizations are advised to remain vigilant, as preparedness can make a significant difference when incidents occur. They should ensure their teams are equipped with sufficient knowledge and the appropriate documentation needed to handle potential threats effectively.

For comprehensive information and insights, or if you have any questions related to the issues discussed in this article, please feel free to contact the authors listed in the left-hand column.

Contact Us
Chandler MHM Limited
17th and 36th Floors
Sathorn Square Office Tower
98 North Sathorn Road
Silom, Bangrak, Bangkok 10500
Thailand
www.chandlermhm.com