NISHIMURA & ASAHI

西村あさひ法律事務所

Response to Cyber Threats in Thailand

Corporate Crisis Management / Asia Newsletter

April 28, 2022

Author:
E-mail Jun Katsube
E-mail Vira Kammee
E-mail Vullope Techakasin
E-mail Pasayu Israsena Nah Ayudhaya

The COVID-19 pandemic has necessitated social distancing. Consequently, government and private-sector operators have shifted towards internet-based economic endeavours; requesting their employees to work remotely, including communicating and authorising transactions, via the internet. However, internet-based communication also facilitates various cyber-crimes, which continue to increase both in Thailand and around the globe. In this newsletter, we discuss how companies should respond to cyber threats in Thailand.

1. Cyber threats in Thailand

(1) Definition of "Cyber Threats" under Thai law

The Cyber Security Act B.E. 2562 (2019) defines "Cyber Threats" as any action or unlawful undertaking by the use of a computer, computer system or any kind of program, with an intention to cause harm or damage in any way to the computer system, computer data or other relevant data.

(2) Types of cyber threats typically effecting business operations in Thailand

✓ "Ransomware" using "information" as hostage - Ransomware is a type of malware created with the purpose of locking or encrypting various types of files of user data, regardless of whether the file is in document, audio or picture format, causing the user to lose access to the affected files. The cybercriminal hacks into the database of the user and then encrypts the files, thus preventing access by the user, while leaving a ransom note requiring the user to pay a certain amount of money to recover the files; otherwise, the affected files will never be recovered or retrieved.
Cybercriminals have implemented Ransomware attacks with results that range from data encryption to data breach. They steal the information contained in the files to increase their bargaining power. Traditionally, the "ransom" is money, in exchange for which they promise decryption of the data. As such, certain business operators who are not in immediate need of such "hostage" data may be able to negotiate or delay the ransom payment. However, there are risks that the stolen data might be lost or significantly damaged. Therefore, business operators tend to immediately pay the ransom in order to mitigate such risks.

✓ "Phishing" - The cybercriminal typically sends a phishing e-mail to users in order to obtain important information, such as login information (i.e. username and password) related to a financial account. For example, the cybercriminal creates an e-mail pretending to be a financial service provider and attaches a counterfeit file or link with an URL to a scam website displaying a webpage similar to the genuine website

of the financial service provider. Once accessed, the users are prompted to insert their login information. Then, the cybercriminal uses such login information to access the financial information of the users.

(3) Thai laws related to cyber threats

✓ Computer-Related Crime Act

The Computer-Related Crime Act B.E. 2560 (2017) is a law which governs various computer-related crimes, such as illegal access to a computer system or data, and is typically enforced after the crime has been committed.

✓ Electronic Transactions Act

The Electronic Transactions Act B.E. 2544 (2001) is a law which permits the use of "electronic information as permissible evidence in court". As such, information regarding computer-related crime collected and submitted to the court in electronic form by attorneys to initiate a case against cybercriminals shall be permissible evidence against offenders.

✓ Cybersecurity Act

The Cybersecurity Act B.E. 2562 (2019) is a law that prescribes precautionary measures. Section 49 of said Act prescribes that the "Organisation of Critical Information Infrastructure" are the organisations with a mission or services in relation to:

- national security;
- public services;
- banking and finance, such as a bank and the stock exchange;
- information technology and telecommunications;
- transportation and logistics;
- energy and public utilities;
- public health, such as a hospital; and
- others as prescribed by the National Cybersecurity Committee.

Said organisations shall maintain minimum cybersecurity standards for the purpose of "preventing" cyber threats. In this regard, a foreign company who conducts business with a Thai organisation mentioned above, whether directly or through a joint venture, should place emphasis on cybersecurity.

An example of the precautionary measures of such Organisation of Critical Information Infrastructure is to prescribe and prepare a code of practice and standard framework for the maintenance of cybersecurity of each organisation (Section 44); notifying the names of executives, operational staff, owner and person processing the computer and the person monitoring the computer system to the Office of the National Cybersecurity Committee so that it can coordinate the maintenance of cybersecurity (Sections 46 and 52), examine the minimum cybersecurity standard and conduct risk assessment on the maintenance of cybersecurity (Sections 53 and 54). In the event of a cyber threat, the Organisation of Critical Information Infrastructure has the responsibility to inform the Office of the National Cybersecurity Committee and its supervisory or regulatory authority without delay to remedy such threat (Section 57). In order to remedy a cyber threat, the competent official has the authority to issue a letter requesting cooperation from the relevant persons to provide information or documents, including entry into a property or place of business

with consent from the person in possession of such place (Section 62). Nevertheless, such measures are only preliminary measures prescribed by the current law; the Office of the National Cybersecurity Committee has the authority by virtue of Section 9 of the Cybersecurity Act B.E. 2562 (2019) to prescribe additional measures.

✓ Personal Data Protection Act

Section 4, last paragraph of the Personal Data Protection Act B.E. 2562 (2019) states that data controllers who are exempted from the application of the personal data protection law shall have the duty to maintain the security of personal data as per the prescribed standards. Under such standards, the data controllers shall maintain the security and confidentiality of the data. They shall not illegitimately disclose such data to others, nor allow modification of the data and shall prevent access to the data by persons who are not related to the data.

2. Recent example of cyber threats in Thailand

Even though business operators typically have their own cybersecurity measures, including the arrangement of seminars to raise cybersecurity awareness, employee cybersecurity health checks, phishing simulations or creation and monitoring of the organisation's overall cybersecurity health rating, the business operator may still face various forms of cyber attacks or cyber threats. A recent example of this occurred on 18 February 2022, when a telecommunications company that provides mobile services in Thailand was hacked. This caused the information of approximately 100,000 users to be leaked onto the Dark Web (i.e. an online community of hackers). The company informed the National Cyber Security Committee and the National Broadcasting and Telecommunications Commission, which are the governing authorities, as well as the affected users. After the attack, the company conducted assessments and ordered relevant employees to modify the software and security system so it is up to date. Additionally, the company informed the public that its services are not affected by such attacks, and that it is in the process of investigating the wrongdoer and the person who disclosed such information to initiate legal proceedings (there are no legal requirements for the company to inform the public).

3. What are the rights of a business or business operator under the law who has suffered a cyber-attack or cyber threat?

In a case where the business operator suffers losses or damages, it may initiate criminal proceedings or file a claim with a police officer (under Thai law, the police officer who is responsible for accepting a claim is called the inquiry official) to prosecute the offenders, in accordance with the following procedures:

✓ Collection of evidence against the offenders, such as a computer inspection report or the printed screen of the computer that was attacked or threatened in every step since the offence was found in order for it to be submitted to the court as evidence or to the police officer to initiate the case against the offender. It is noteworthy that an employee of the injured business operator who possesses knowledge of the facts surrounding the attacks or threats must testify before the court or the police. Presently, the Thai police provide a service for injured persons who have suffered a cyber-attack to file their claim online.

✓ The court which has jurisdiction in this case, as well as the police station with the authority to accept the claim, is the court and police station which has territorial jurisdiction over the location where the offence was committed. Alternatively, the claim may be submitted to the Technology Crime Suppression Division, located on the 4th Floor of Building B of the Government Complex Commemorating His Majesty the

King's 80th Birthday Anniversary, Chaeng Wattana Road, Thungsong-Hong Sub-district, Laksi District, Bangkok, which is the agency that specialises in cybercrime.

✓ The court and the police officer accepting the claims may not be able to immediately remedy the act of the offender, such as immediately decrypting the encrypted data, because information over the internet is under the care of each service provider, which would require further legal proceedings.

4. Reporting requirement in the case of cyber threats

Under Section 58 of the Cybersecurity Act B.E. 2562 (2019), only the "Organisation of Critical Information Infrastructure" has the duty to inform the governing authority in the case of cyber threats or potential cyber threats toward the telecommunications system. As such, if any other operator aside from the "Organisation of Critical Information Infrastructure" under the Cybersecurity Act B.E. 2562 (2019) is faced with a cyber-attack, there is no duty for such operators to inform the governing authority. Nevertheless, after a cyber-attack which affects others, such as customers or users, the operators should inform their customers and users of the attack and should increase their security in further transactions. Furthermore, the operators should also inform the Office of the National Cybersecurity Committee for acknowledgment and information.

5. Conclusion and recommendations

For those business operators who have faced cyber-attacks or cyber threats and desire to prosecute the offender under the law, it is advisable that such business operators seek advice from an attorney who specialises in cybercrime; for the collection of evidence of the offence to initiate the claim against the offender and to file the case with the court or the inquiry official of the relevant jurisdiction as soon as possible. Any delay may cause the offender to delete or destroy evidence related to the offence.

Public Relations Section, Nishimura & Asahi E-mail✉