The emergence of technology with borderless access discovers a new spectrum of world to mankind - the virtual world. Thanks to technology, our daily activities and businesses are facilitated, simplified and accelerated. However, with the advancement of technology, dangers and threats through the virtual world are more imminent. As technology evolves and the medium revolves, various new cyber-related criminal offences emerge. With a single click, one could be a victim of cyber-criminal offences without knowing any information about the offender.

Ransomware attack is one of the biggest threats against preservation of information assets or systems. Ransomware can be described as a kind of malware that prevents users from accessing their computing device resources and/or personal data using various methods. The data on the victim's computing device becomes unusable until the device owner pays ransom to remove the restriction[1] and regain access to the hijacked system. In 2018, CyberSecurity Malaysia through Malaysia Computer Emergency Response Team ("**MyCert**") has reported 62 ransomware incidents involving different kinds of variants from Malaysian and non-Malaysian parties[2]. According to Sophos' global survey made on several Malaysian bodies and institutions, "The State of Ransomware 2021", 58% of the respondents stated that ransomware is already so prevalent that it is inevitable they will get hit and 41% of the respondents stated that they are already experiencing an increase in attempted ransomware attacks.

Legislations Relating to Ransomware

In Malaysia, the following legislations are in place to deter cybercrime, including offences related to ransomware attack:

a) Computer Crimes Act 1997 ("CCA 1997")

Being one of the earliest legislations enacted to battle cybercrime in Malaysia, CCA

1997 is a statutory legislation which governs offences relating to misuse of computers. Section 5 of CCA 1997 makes infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses) an offence when the attack is done with knowledge that such act will cause unauthorized modification of contents of any computer. Although ransomware and/or malware attack is an offence under CCA 1997, to date, there is no reported case arising out of this provision.

b) Communications and Multimedia Act 1998 ("CMA 1998")

CMA 1998 regulates the administration and licensing requirements of multimedia operations as well as utilization of network services. Although CMA 1998 makes it an offence when a person by means of any network facilities or network service or applications service annoys, abuses, threatens or harasses any person at any number or electronic address using any applications services, irrespective of whether the communication is ensued and whether the identity of that person is known or unknown, prohibits communication interception and possession of devices or software to commit unauthorized access to network services, applications services or content applications services, CMA 1998 does not address the elements of cyberextortion.

c) Penal Code ("PC")

Section 383 of PC provides the offence of extortion when one intentionally puts the victim in fear of any injury to himself or to any other, and thereby dishonestly induces the victim to deliver any property or valuable security. This provision may be extended to prosecute perpetrator who commits cyberextortion by launching ransomware attacks and thereafter extort for payment from the victim but there is no case reported pursuant to this provision relating to ransomware attack and cyberextortion.

The Need to Step Up the Game

The limelight of the above discussion focuses on the perpetrator of the offence. What about the information technology (IT) users and potential victims of cybercrime? Is there any statutory obligation on the part of IT users, including organizations to implement security measures against any cyber-criminal attacks?

Save for the Personal Data Protection Act 2010 ("**PDPA**"), there is no law enacted to address the prescription of security measures on the part of users, including corporate entities and organizations. Although PDPA addresses the requirement of complying with minimum-security standards prescribed by the Personal Data Protection Standards 2015 (PDPC) to ensure the protection of personal data against any loss, misuse, modification, and unauthorized access, this is only applicable to data users undertaking commercial transactions and those who process personal data.

In 2016, the Securities Commission issued Guidelines on Management of Cyber Risk that is applicable to all capital market entities, imposing the responsibility upon the entities to

develop and implement preventive measures against cyber threats. In 2020, the Central Bank of Malaysia issued a policy on Risk Management in Technology (RMiT) to prevent exploitation of weak networks or systems.

Further, there is also no statutory obligation on the victim to lodge a report regarding a ransomware attack. This makes the combat against ransomware more difficult. With the increasing number of cyber threats, especially ransomware, Malaysia should enact a robust cyber legal framework to impose preventive measures and reporting obligation as a preventative measure against cyber threats.

Does it Pay to Pay?

The main dilemma that would linger around victims of ransomware attack is to decide whether to pay or not to pay the ransom. Foreign jurisdictions such as United States and United Kingdom have a clear stance in relation to legality of ransomware payment. Through an advisory, United States has advised the public on the risks of making ransomware payment and declared ransomware payment illegal if it is made to sanctioned persons listed by Office of Foreign Assets Control (OFAC)[[3]. Meanwhile, in the United Kingdom ransomware payment will be rendered illegal if it is made for the purpose of money laundering, financing terrorists or made to sanctioned designated individual or bodies which appear on lists published by OFSI (the Office of Financial Sanctions Implementation) of United Kingdom.

In Malaysia, there is no law which prohibits or make illegal payment of ransom arising out of ransomware attack. The decision would be a commercial decision that needs to be determined by the victim. Notwithstanding the absence of law prohibiting ransom payment arising out of ransomware attack, a victim of ransomware attack should consider the following risks before deciding whether or not to make ransom payment:

a) No guarantee on recovery of access to system/data

Payment of the ransom will not guarantee that the access to the system/data will be returned to the victim. Further, the perpetrator may also withhold certain key data of the victim. Sophos State of Ransomware 2021 Report found that only 8% of the respondents managed to recover their data despite making ransom payment. From the same survey, 29% could not recover more than half of the encrypted data[4].

b) Exposure to ransomware attack in the future

Making ransom payment would not guarantee that the victim would be safe from future attacks from the same perpetrators. In fact, payment of ransomware may encourage the perpetrator to commit the same attack against the victim particularly where the perpetrator is curtained that the victim would make ransom payment to regain access to its system/data. Cybereason exposed in its report that 80% of organizations experienced a second attack after making ransom payment. Additionally, half of them believe that the subsequent attacks were committed by the same perpetrator[5].

c) Risk of committing offence

Since the perpetrator's identity is unknown, there is a risk that a victim paying ransom to the perpetrator may be indirectly providing financial assistance to any terrorist organization or any organization which carries out any unlawful activity pursuant to the Penal Code and Anti-Money Laundering, Anti-terrorism Financing and Proceeds of Unlawful Activities Act 2001, notwithstanding knowledge or intention on the part of the victim.

Conclusion

What is obvious is the need for enhanced cybersecurity laws to battle cybercrime and as much as integration of technology in daily business is encouraged, safe and secured integration should always be prioritised.

---

[1] Nihad A. Hassan (2019). Ransomware Revealed: A Beginner's Guide to Protecting and Recovering from Ransomware Attacks, page 3.
[2] Muller, J. (2021). Number of Ransomware Incidents Reported to CyberSecurity Malaysia 2018 by Variants. Retrieved from https://www.statista.com/statistics/1043328/malaysia-ransomware-incidents-by-variants/
[3] Department of Treasury (2020), Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments
[4] Winder, D (2021), Ransomware Reality Shock: 92% Who Pay Don't Get Their Data Back
[5] Walman, A (2021), Repeat Ransomware Attacks Hit 80% of Victims Who Paid Ransoms

Written by:

Fozi Addina Mohamad Fozi
Associate
fozi.addina@azmilaw.com

Zhilal Adnan
Legal Executive
zhilal@azmilaw.com

Corporate Communications
Azmi & Associates
7 July 2021