LH AG ADVOCATES AND SOLICITORS

Ransomware: Legal Aspects and Considerations

G Vijay Kumar
Partner (Dispute Resolution)
Technology, Media & Telecommunications
T: +603 6208 5870
E: vkg@lh-ag.com

Teo Wai Sum
Partner (Corporate Advisory)
Technology, Media & Telecommunications
T: +603 6208 5805
E: tws@lh-ag.com

Eunice Chan Wei Lynn
Partner (Corporate Advisory)
Technology, Media & Telecommunications
T: +603 6208 5872
E: cwl@lh-ag.com

CK Lung
Partner (Dispute Resolution)
Technology, Media & Telecommunications
T: +603 6208 5948
E: ckl@lh-ag.com

The rapid advancement of the cyber world has, without a doubt, opened new frontiers to organisations, impacting the key aspects of business operations from processing of information, to data storage, as well as communication methods. The embracing of, and heavy reliance on, technology has increasingly facilitated, streamlined and simplified the digitalisation of commercial activities — even more so during these unprecedented times. However, technology is not without its vulnerabilities.

There has been a surge in cyber fraud cases in recent years,[1] including ransomware, which has been described as "*the most prolific criminal business models in existence today*".[2] Ransomware is generally a type of malware that infects computing platforms or data systems, resulting in the restriction of users' access to the infected platform. A ransom payment, normally by way of cryptocurrency, is demanded in exchange for a decryption key to unlock and regain access to the hacked systems. This, of course, is a cause for grave concern, as the targeted systems would normally include valuable data, trade secrets and confidential information of an organisation. Earlier this year, the single biggest global ransomware attack by the Ransomware Evil, or REvil, group hit approximately 800 to 1,500 organisations and public agencies worldwide, with a ransom demand totalling up to USD70 million.[3] It is clear that cyber fraud attacks pose an enormous threat to businesses everywhere.

Is there any legislation regulating cyber fraud, particularly ransomware?

1. Penal Code

An act of extortion is described under s 383 of the Penal Code as intentionally putting any person in fear of any injury to that person or to any other, thereby dishonestly inducing the person or to put in fear to deliver to any person any property or valuable security. The very nature of ransomware, where valuable property is held at ransom followed by an extorted demand for payment in exchange for recovering such property, would amount to an act of extortion and therefore punishable under the Penal Code. An offence of extortion is punishable by imprisonment for a term which may extend to 10 years or a fine, or even whipping.

---

1 Between January and May 2021, 4,615 cybersecurity incidents were reported to the National Cyber Security Agency: Qishin Tariq, "More Cybercrime Reported During Pandemic", *The Star Online* (3 June 2021) https://www.thestar.com.my/tech/tech-news/2021/06/03/saifuddin-more-cybercrime-reported-during-pandemic

2 NST Business, "Ransomware Still A Huge Cyber Threat in 2021", *New Straits Times* (26 February 2021) https://www.nst.com.my/business/2021/02/669211/ransomware-still-huge-cyber-threat-2021

3 Rachel Lerman and Gerrit de Vynck, "Hackers Demand $70 Million to Unlock Businesses Hit By Sprawling Ransomware Attack", *The Washington Post* (5 July 2021) https://www.washingtonpost.com/technology/2021/07/05/kayesaransomware-70-million-fbi/

2. Computer Crimes Act 1997 (**CCA**)

The CCA created several offences relating to the misuse of computers, which includes unauthorised access to computer material,[4] unauthorised access with intent to commit or facilitate commission of further offence,[5] unauthorised modification of the contents of any computer,[6] and wrongful communication.[7] It is arguable that those deploying cyber fraud attacks, particularly ransomware, would be in contravention of s 5 of the CCA, where it amounts to the unauthorised modification of the contents of any computer, regardless of whether such modification is or is intended to be, permanent or temporary.[8] If such act is found to have been done with the intent to cause injury to any person, which includes injury to property, such offence is punishable by a fine not exceeding RM150,000 or imprisonment for a term not exceeding 10 years, or to both.

3. Communications and Multimedia Act 1998 (**CMA**)

The CMA regulates the communications and multimedia industries, including providers and users of network facilities and network services. Section 233 prohibits the improper use of network facilities or network services, and this includes soliciting or initiating the transmission of any communication which is menacing with the intent to abuse, threaten or harass another person. Additionally, any interception and disclosure of communications without lawful authority is illegal under s 234. Therefore, the deployment of ransomware through a network service would likely fall foul of the aforementioned sections, which are punishable by a fine not exceeding RM50,000 or imprisonment not exceeding one year, or to both, with a liability of a further fine of RM1,000 for every day which the offence is continued after conviction.

4. Copyright Act 1987 (**CA**)

The CA sets out several protections afforded to copyright owners. Generally, an infringement of a copyright (i.e. the use without the consent or licence of the owner of the copyright) amounts to an offence under s 36, and this would include distributing the copyrighted article for a purpose that it prejudicially affects the owner of the copyright. More often than not, the systems or data held at ransom would include copyrighted materials of an organisation, and hence would fall foul of the aforementioned provision. Additionally, s 36A prohibits the circumvention of the technological protection applied to a copy of a work and makes it an offence for any person to offer to the public or provide any

---

4 CCA, s 3
5 CCA, s 4
6 CCA, s 5
7 CCA, s 6
8 CCA, s 5(3)

service in respect of any technology, device or component which is primarily designed or produced for the purpose or enabling or facilitating the circumvention of technological protection measure.

Is there a requirement to notify or report to the authorities in the event of a ransomware attack?

The demand for a ransom could amount to an extortion which is an offence under the Penal Code as explained above. Any person aware of the commission of, or the intention of any other person to commit an offence punishable under the Penal Code, is required to immediately give information to the nearest police station of such commission, or intention to commit, of such offence.[9] Therefore, in the event of a ransomware attack, organisations should make a police report.

Apart from the above, there are no obligations to make a notification to any other authorities. However, organisations are encouraged to report any cybersecurity-related incidents to the National Cyber Security Agency (**NACSA**),[10] a dedicated agency overseeing national cyber security functions under the purview of the National Security Council.

Additionally, organisations are also encouraged to make a report to the Malaysia Computer Emergency Response Team (**MyCERT**)[11] of CyberSecurity Malaysia, a national cyber security specialist agency under the Ministry of Communications and Multimedia. MyCERT provides emergency response assistance on computer security-related matters such as malware. MyCERT also provides guidance for organisations on preventive and mitigation steps to be taken when dealing with ransomware (**MyCERT Advisory**).[12]

What are the legal consequences of paying the ransom?

The payment of ransom in response to a ransomware demand is not a criminal offence under Malaysian law, unless in specific scenarios such as where the payment is made to a "specified entity" under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (**AMLA**).[13]

Aside from the above, organisations should be mindful of their obligations under the Personal Data Protection Act 2010 (**PDPA**) as a data user, especially if the ransomware attack results in the

---

9 Criminal Procedure Code, s 13

10 https://www.nacsa.gov.my/index.php

11 https://www.mycert.org.my/portal/index

12 "MyCERT Alert – Increase of NetWalker Ransomware Attacks" (18 September 2020) https://www.mycert.org.my/portal/advisory?id=MA-792.092020

13 Sections 66B(3)(a), 66B(3)(b)(iv) and 66C of AMLA provide that no citizen of Malaysia and no body corporate incorporated in Malaysia shall, knowingly: (1) provide by any means, directly or indirectly, any property with the intention that the property be used, or in the knowledge that the property is to be used by a specified entity; and (2) make available any property or any financial or other related service, directly or indirectly, for the benefit of a specified entity, including doing anything to cause, assist or promote such offence. A "specified entity" means individuals or entities which are determined and declared by the Ministry of Home Affairs in accordance with the provisions under AMLA to be persons involved in terrorist acts.

modification, unauthorised disclosure or access, misuse or destruction of personal data. Section 9 of the PDPA requires data users to comply with the Security Principle, which imposes an obligation on data users to take practical steps to ensure security when processing personal data. This may include, among others, implementing technical security measures within an organisation, monitoring employee use of personal data and safeguarding its systems from malware threats.[14] Therefore, if a ransomware attack is the result of an organisation failing to adhere to the security standards prescribed under the PDPA and the Personal Data Protection Standards 2015, this may amount to a contravention of s 9 which is punishable by a fine not exceeding RM100,000 or to imprisonment for a term not exceeding two years, or to both.

Does it pay to pay?

There is limited guidance provided by the government in dealing with ransomware. However, MyCERT has advised that *"individuals and organisations are discouraged from paying the ransom, as this does not guarantee access will be restored*".[15] Global surveys have also shown that a significant percentage of victims of ransomware that paid the ransom did not successfully recover the data.[16]

Further, an organisation may have received a decryption key to regain access to its systems upon payment of ransom, but its data may have already been copied, disclosed, distributed or sold. More importantly, organisations that have paid or are willing to pay ransom cannot rule themselves out from being earmarked or made a recurring target by hackers in the future.

Therefore, although payment of ransom may be the most expedient method in recovering data, the considerations mentioned above should not be taken lightly.

Points to ponder

It is estimated that 59% of Malaysian organisations will be hit by ransomware in the near future.[17] Thus, it is high time that serious consideration and comprehensive internal technical and organisational security measures be taken to implement a robust cybersecurity protection system to avoid falling victim to cyber fraud and cyber security attacks. Organisations should proactively engage with cybersecurity technical experts to evaluate, assess and test their IT security systems as well as ensure that personnel

---

14 Part II of the Personal Data Protection Standard 2015 sets out the security standards that must be taken into account by a data user in processing personal data.

15 "MyCERT Alert – Increase of NetWalker Ransomware Attacks" (18 September 2020) https://www.mycert.org.my/portal/advisory?id=MA-792.092020

16 Based on a study conducted by Kaspersky, a global cybersecurity company, on 15,000 consumers published on 30 March 2021 https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned

17 "59% of Local Organisations Expect to be Hit by Ransomware", *The Malaysian Reserve* (7 May 2021) https://themalaysianreserve.com/2021/05/07/59-of-local-organisations-expect-to-be-hit-by-ransomware/

are given adequate awareness training to mitigate and prevent cyber fraud attacks. In the event of a ransomware attack, organisations should lodge a police report and also notify and consult NACSA and MyCERT for further guidance prior to commencing negotiations with the hackers, making any payment of ransom or taking any other action.

Eleena Abd Wahab

Eleena Abd Wahab
Senior Associate
Technology, Media & Telecommunications
T: +603 6208 5815
E: eaw@lh-ag.com