DREWTECH SERIES
CHAPTER 7

My Kingdom for a Horse
– When your Systems are Held to Ransom

22 January 2021

LEGAL UPDATE
In the epoch of information, the threat of malicious actors holding you to ransom by encrypting and denying access to your data is an ever-present one.

This article discusses the immediate steps to be taken in the event of a ransomware attack, as well as possible implications under the Personal Data Protection Act.

03 INTRODUCTION

03 WHAT IS A RANSOMWARE ATTACK?

04 THE DANGERS OF INCIDENT REPORTS – THE ROLE OF LAWYERS

05 TO PAY OR NOT TO PAY

06 TO NOTIFY OR NOT TO NOTIFY – (SOON TO BE) MANDATORY NOTIFICATION

07 CONCLUSION
INTRODUCTION

ATTENTION: All Your Files Are Belong to Us!!

All files on your hard drive are encrypted by WinWord64.

Your documents, photos, and other important files have been encrypted with the strongest encryption and unique key generated for this computer.

A private decryption key is required to decrypt your files, and no one else can decrypt your files unless you pay for the private key.

You must send $500 worth of bitcoin to this address to purchase the decryption key: ABCDEF123456789.

Look familiar? This is quickly becoming a sign of our times – the chances of your organisation’s systems being hit by a cyber-attack are higher than ever. And while commendable steps have been taken by organisations (public and private entities alike) to beef up both their online and offline defences to prevent such attacks, it would be presumptuous for one to assume that one’s (digital) kingdom is entirely safe from attack.

So, what happens when an attack occurs? Many organisations have prepared steps to isolate the affected servers and restore their systems. It is often too little too late. Ransomware attacks work quickly and widely and would likely have already affected many aspects of the IT infrastructure leading to data and service loss.

When ransomware strikes, the question that will naturally be asked is: “How did such an attack occur?” It is instinctive to engage computer forensic experts to investigate and determine how the attack happened. While this is an important step, it is also critical to keep in mind other priorities. In this article, we discuss several issues an organisation should consider when faced with a ransomware attack.

WHAT IS A RANSOMWARE ATTACK?

A ransomware attack is a cyber-incident whereby a malicious actor successfully encrypts the data on the victim’s systems, rendering it inaccessible. These malicious actors will then typically make a ransom demand, often in the form of cryptocurrency, in exchange for the decryption key which they claim will be able to unlock the data.

A ransomware attack can occur by different means and take different forms. For instance, an employee may receive an email from “ITadmin@microsoft.com”, requesting that he or she install an urgent
update from an attached file. A user may not notice that the “M” in “Microsoft” has been substituted with “RN” (did you?), the malicious payload is inserted into the system, and it all goes downhill from there.

Of course, not all ransomware attacks are caused by phishing emails. It may also take the form of internal sabotage from a disgruntled employee, or an unsecured vulnerability on your systems that is exposed to the internet, allowing an attacker from anywhere in the world to drop a malicious payload into your network.

Beyond the initial penetration of IT infrastructure, the specific bug contained in the inserted payload may also vary. Different variants of ransomware selectively target different types of files, and more sophisticated ones may also seek out backups and delete them, or burrow into the system and stay dormant, only to spring up at a later date. Certain strains are even capable of sending data back to their masters, presenting serious confidentiality and personal data protection issues. It is therefore vital that experts be called in to determine the type of ransomware that one is dealing with, as well as if the infection has been torn out, root and branch. However, this course of action is not without its own pitfalls.

THE DANGERS OF INCIDENT REPORTS – THE ROLE OF LAWYERS

After the initial shock of an attack, the instinctive response (immediately after disconnecting all computers from the internet and each other) would often be to call in the experts to identify what has happened and how. This often involves the preparation of an incident report, setting out the causes of the incident. While prompt action is desirable, the unfortunate truth is that haste makes waste. Two points arise – the first is a question of unwanted exposure, the second the scope of the anticipated incident report.

Legal privilege

A key concern in the preparation of incident reports is that in the event of litigation arising out of the attack, relevant documents are disclosable to the other party, including drafts of incident reports. This may not just be embarrassing if they reveal any lapses in cybersecurity but potentially prejudicial in litigation proceedings.

A key step that a victim can take is to instruct legal counsel, who will then act as intermediaries between the forensic experts and the victim, including by giving instructions to forensic experts on the scope of the investigative report which could then be used to provide legal advice. This could possibly establish legal privilege over the preparatory
materials or the reports, and will assist in providing the grounds to claim that the documents are privileged, and therefore not disclosable.

Scope of the report

Forensic experts are unquestionably the best persons to understand the technical and technological details of any cyber-incident, including ransomware attacks. However, it may sometimes be the case that these reports may not be appropriate for consumption by a non-technical reader, for the simple reason that the experts preparing the reports have the necessary training and experience that others do not. The role of appropriate legal counsel is therefore to work closely with these experts to prepare a document that appropriately reflects the truth of the matter while explaining the facts in a clear, concise and simple way.

Legal counsel can also provide direction to the report. One of the roles of the expert report will be to establish the explanations for the cyber-incident, so as to be able to deal with external parties such as regulators and counterparties in the event that this is necessary. Experienced legal counsel will know what these external parties are concerned about, and how best to address these concerns. They will therefore be well placed to provide suggestions on particular areas where more extensive investigation is necessary, or further elaboration is appropriate.

TO PAY OR NOT TO PAY

It may also sometimes be tempting for a victim to pay the ransom sum demanded, in the hopes that the attackers will just go away. This is not recommended for several reasons.

The first is obvious – one is negotiating with criminals, plain and simple. There is no assurance that even if the ransom is paid, these criminals will hold up their end of this extortionate “bargain” and provide the decryption key. These criminals are anonymous and often located outside of jurisdiction. The fact that they often ask for payment in cryptocurrency is intended to further obfuscate their identity. It is well possible that a victim will simply be poorer, while their data remains locked away.

The second is that the encryption process used is not always a perfect one. As the typical ransomware attack involves dropping a payload into the victim's systems which will then autonomously wreak havoc, it is occasionally the case that the data is not only encrypted, but corrupted beyond recovery. Even counting on honour from thieves, payment of
the ransom may not be able to restore the victim’s systems to its previous state.

Third, payment of the ransom often serves as a signal to the attackers that a victim is willing to pay. With the scent of blood in the water, the ransom sum may be increased – resulting in an impossible situation where the victim is faced with the possibility of ever-escalating extortion.

TO NOTIFY OR NOT TO NOTIFY – (SOON TO BE) MANDATORY NOTIFICATION

Where there is a ransomware attack, it is often the case that amongst the data that has been encrypted is personal data as defined in the Personal Data Protection Act (“PDPA”), such as NRIC numbers, names, birthdates, addresses, etc. This can be the personal data of customers, employees, or counterparties. There is therefore a concern that the victim of the ransomware attack may additionally be found in breach of the PDPA, in particular the obligation to protect personal data.

In the face of this, victims must consider if they wish to proactively notify the Personal Data Protection Commission (“Commission”) of the incident. While there is no obligation to do so at present, the Commission has published guidelines stating that voluntarily notifying the Commission of the personal data breach as soon as it is discovered and co-operating with the Commission is a mitigating factor to be taken into consideration.

An additional point is that the present position will certainly change soon, though how the cards will eventually fall is still unclear.

Parliament has passed the Personal Data Protection (Amendment) Bill on 2 November 2020, which will come into force by a notification in the Government Gazette. Amongst the changes is a new mandatory notification obligation. This obligation applies where there has been, amongst other things, “unauthorized access, collection, use, disclosure, copying, modification or disposal of personal data” which results or is likely to result in significant harm to affected individuals, or affects a prescribed number of individuals.

While this obligation appears to clearly require notification in the event of a ransomware attack, the answer is not obvious. A ransomware attack does not, strictly speaking, modify personal data itself, but the expression of the data in an electronic medium. There is likely and often no change in the data itself – for instance, accurate NRIC numbers still are paired to the correct individual without transposition, it
is simply that it is no longer readable, akin to having the information printed in black ink on black paper.

It therefore remains to be seen whether notification is appropriate in every circumstance, and how the amendments to the PDPA will affect this decision-making process.

CONCLUSION

Ransomware attacks are increasing in frequency and sophistication. While it would certainly be ideal to not be affected at all, this is becoming an increasingly unlikely proposition. It is therefore essential that potential victims, which are unfortunately all persons with valuable data, take great care in dealing with the aftermath of an attack to deal with the multifarious issues that will certainly arise.

UPDATES IN DREWTECH SERIES

1. Chapter 1: The Importance of an Exit Strategy in Technology Contracts <6 March 2019>
2. Chapter 2: Employees, Technology and A Legal Hangover – Bring Your Own Problems? <4 June 2019>
4. Chapter 4: Diabolus ex machina <18 February 2020>
5. Chapter 5: Bringing hygiene online – the MAS notice on cyber hygiene <28 April 2020>
6. Chapter 6: Signing without signing – contactless contracts <16 July 2020>
7. Chapter 7: My Kingdom for a Horse – When your Systems are Held to Ransom <22 January 2021>

The content of this article does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances. Copyright in this publication is owned by Drew & Napier LLC. This publication may not be reproduced or transmitted in any form or by any means, in whole or in part, without prior written approval.
If you have any questions or comments on this article, please contact:

Rakesh Kirpalani
Director, Dispute Resolution & Information Technology
Chief Technology Officer
T: +65 6531 2521
E: rakesh.kirpalani@drewnapier.com