Ransomware Aftermath: Between a (Virtual) Rock and a Hard Place

Hin Han SHUM

Être confronté à une demande de rançon est un cauchemar pour les entreprises. La décision de payer ou de ne pas payer n'est peut-être pas aussi simple qu'il y paraît. Cet article examine les conséquences d'une cyberattaque, certains des principaux problèmes en jeu lors de la décision de payer ou non et les mesures préventives que les entreprises peuvent prendre.

Estar confrontada a una demande de rescate es una pesadilla para las empresas. La decisión de pagar o no pagar puede no ser tan simple como parece. Este artículo considera las secuelas de un ciberataque, algunas de las cuestiones clave que están en juego al tomar la decisión de pagar y qué medidas preventivas pueden tomar las empresas.

Picture this: Just another workday. You settle in your chair, coffee at hand, and turn on your computer. Suddenly, an unfamiliar ominous screen flashes onto the monitor and informs you that you are now the victim of ransomware. It is like a (virtual) rock came crashing down and abruptly blocked all pathways. A timer pops up on the screen indicating you have less than 24 hours to make one of two choices: (1) pay the ransom to decrypt and regain access to your files, or (2) risk permanent deletion or dissemination of all your files. You are warned not to report the matter to any authorities.

Will you pay the ransom? Or risk losing all the files in your system? Or worse – having all your data exposed? What key matters should be considered before making this decision?

Aftermath of a Cyberattack

Before making the decision to pay or not, it is important to examine what is at stake and whether there are any mitigation actions that can be taken.

Financial Loss

According to the Cost of a Data Breach Report 2020, with research conducted by the Ponemon Institute and published by IBM Security (2020 Report),[1] the global average cost[2] of a data breach occurring between August 2019 and April 2020 was US$3.86 million. This cost represents the average across three root causes (being malicious attack, system glitches and human error), with the average cost of malicious attack breaches amounting to US$4.27 million. The 2020 Report also found that ransomware attacks cost an average of US$4.44 million.

Unauthorised Data Access

There is no guarantee that the cybercriminals have not made a copy of the data and/or that they will not disseminate it for profit or other purposes. These include trade secrets and sensitive information, which may affect the operation of a business.

Personal Data Disclosure

The 2020 Report found that 80% of organisations suffering a breach had seen their customer personally identifiable information compromised.

Increasingly stringent regulatory reporting obligations are in place where personal data is disclosed.

For example, if a business deals with persons in the European Union, a cyberattack that causes personal data to be disclosed without authorisation of the data subject (i.e. the one whose data is collected/handled by the business) may trigger obligations pursuant to the General Data Protection Regulation, which imposes a 72-hour breach report obligation (unless the breach is unlikely to result in a risk to the rights and freedoms of data subjects) and penalties of up to 4% of global annual turnover or €20 million, whichever is higher.

With such a tight deadline, investigations must be conducted immediately upon discovery of a cyberattack incident. Thorough steps for reporting and notification need to be readily available for compliance actions. Failure to deal adequately once a breach has been discovered may exacerbate the problem and may result in higher penalties.

Cybersecurity Experts

The cyberattack can spread to other devices, as well as overseas offices in a multijurisdictional organisation.

It is important to seek the immediate assistance of cybersecurity experts for forensic data breach analysis (to assess what and how much data has been lost, to see where the vulnerabilities exist, and to prevent further spread of the disaster within the organisation). The 2020 Report shows that for breaches of less than 100,000 records, the average cost is US$3.86 million, breaches of 1 million to 10 million records cost an average of US$50 million, and breaches of more than 50 million records cost an average of US$392 million.

If you have an Incident Response Team (IRT) in place (discussed below), cybersecurity consultants with expertise in handling cyber breaches may be on call to assist.

Attorney-Client Privilege

To facilitate the most thorough investigations throughout the organisation, it may be best to have attorney-client privilege intact when data mapping, interviewing

1. Ponemon Institute LLC and IBM Corporation (July 2020), *"Cost of a Data Breach Report 2020"*, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
2. The costs include expenses such as detection and escalation, ex-post response, notification and loss of business.

employees, preparing reports on the system assessment and/or conducting post-breach investigations.

Therefore, engaging lawyers with knowledge of the processes and capabilities to assist in defending cyberattack-related litigation is a key component of an IRT.

Reputation and Client Management

Loss of confidence may be the tipping point between the survival and death of a business reeling from a publicised cyberattack.

Public relations experts may need to be engaged to work with lawyers in the IRT, to manage the reputation of the business, as well as its customer communications, and respond to the grievances of affected customers while complying with the law.

Industry Requirements

The cyberattack can spread to other devices, as well as overseas offices in a multijurisdictional organisation.

Depending on the jurisdiction and the relevant contracts, industries holding confidential and sensitive data (e.g. law firms, banks, hospitals and schools) may be subject to industry-specific rules, codes and guidelines, and failure to comply may result in disciplinary actions.

These may include obligations to notify the relevant regulator and/or the data subjects about the potential breach/unauthorised disclosure of data. Analysis of the obligations and any reporting deadlines should be included in an Incident Response Plan (discussed below) to be prepared by the IRT.

Contractual Requirements

Contracts with clients and customers may call for reporting and mitigation actions pertaining to cyber-breach incidences. Failure to act pursuant to a contract may result in additional civil liabilities.

Such obligations would normally be included in the Incident Response Plan.

Insurance

The terms of the insurance policy should be complied with to keep the coverage in effect. Generally speaking, an insurer should be notified at the earliest possible opportunity. Preparation should be made to ensure timely performance of these obligations, to protect the interests of the organisation, and avoid further liability.

Should You Pay the Ransom?

Where the only way to resume business operations is to pay the ransom, what are the risks in making payment?

Sanctions for Payment

The act of paying the ransom may itself be subject to sanctions in some jurisdictions.

On 1 October 2020, the US Department of Treasury issued an Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, reminding the public that its Office of Foreign Assets Control (OFAC) will impose sanctions not only on cybercriminals, but also on those who "materially assist, sponsor, or provide financial, material, or technology support for these activities". This means that those who pay the ransom may be subject to sanctions by the OFAC.[3]

Furthermore, there is a general prohibition on US persons from engaging in transactions, directly or indirectly, with:

(a) individuals or entities (persons) on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List);

(b) other blocked persons; and

(c) persons covered by comprehensive country or region embargoes (such as Cuba, the Crimea region of Ukraine, Iran, North Korea and Syria).

Where there are sanction violations, civil penalties may be imposed based on strict liability. In other words, one could be held liable even if the offender did not know, or have reason to know, it was transacting with a person prohibited under related sanctions laws and regulations. The identity of a cybercriminal is usually unknown, so a victim paying the ransom has a significant risk of making payments to persons on the SDN List, or other prohibited persons mentioned above.

3. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

Anti-Money Laundering Obligations

In Hong Kong, various ordinances cover money laundering offences [e.g. Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405), Organized and Serious Crimes Ordinance (Cap. 455) (OSCO) and United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)].

These ordinances set out a duty to report knowledge or suspicion that any property (including money), in whole or in part, directly or indirectly, represents any person's proceeds of, was used in connection with, or is intended to be used in connection with, an indictable offence.

A ransomware attack would, *inter alia*, be an indictable criminal offence of blackmail (under section 23 of the Theft Ordinance (Cap. 210)). Ransom payments may be property given in connection with the commission of the criminal activity. Where payment is intended to be paid in satisfaction of a ransomware attack, the reporting obligation may apply. Failure to report could amount to a fine of HK$50,000 and a three-month imprisonment term.

There is also an obligation not to tip off the cybercriminal about the reporting made, so as not to prejudice any investigation of the crime. Contravention of this obligation may lead to a summary conviction with a fine of HK$100,000 and a one-year imprisonment term, and conviction upon indictment with a fine of HK$500,000 and a three-year imprisonment term.

Principles

Certain clientele may abhor the thought of funding criminal activity. Paying a ransom may raise issues of ethics and morality. Depending on the industry of the organisation, the reputation backlash may need to be considered.

Easy Target

An organisation succumbing to ransom demands may be labelled an easy target. An unwanted reputation may be built and may make way for other (or the same) cybercriminals to attack that organisation.

No Guarantees

There are concerns that even if the ransom payment is made, a decryption key to unlock the system might not be provided. According to a study by Kaspersky, of the 56% of victims who paid the ransom to re-access their files, 17% of those did not see their full data returned.[4]

Since a cyberattack is illegal and the initial infiltration is likely based on dishonest methods, it is not inconceivable that the cybercriminals will make off with the payment without performing their side of the bargain. Furthermore, some believe that cybercriminals have more incentive to write ransomware (which generates profit) rather than to create a decryption key (which is an expenditure).

Not only is there no guarantee that the system will be restored, there is also a risk that the reinstated files may be corrupted.

Be Prepared

When faced with these crises, most people wish they could turn back time. However, turning back time is not the solution – preparation is.

According to the 2020 Report, it takes an average of 280 days to identify and contain a breach, with an average of 315 days when it comes to malicious attacks. While one continues their day-to-day operations, malware may have already infiltrated the systems for months, waiting for the perfect opportunity to strike (i.e. right before the deadline for a big project). Complete prevention is ideal, but even if there is a breach, the chances of containing the breach are better the sooner it is identified. Therefore, at any moment in time, we should take steps to prepare for, and manage, those risks.

Incident Response Team

Building an IRT is one of the most important preparatory works to be done. The 2020 Report showed that while the average cost for companies without an IRT and tabletop exercises was US$5.29 million, organisations with this preparation spent around US$2 million less (i.e. US$3.29 million).

The IRT will likely consist of persons within the organisation, as well as external experts, such as cybersecurity experts.

4. AO Kaspersky Lab (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

An IRT will usually prepare an Incident Response Plan and conduct the necessary system assessments, run cyber tabletop preparation exercises (including simulated phishing expeditions) to evaluate weaknesses within the system, and lead the development of training and IT system upgrades. Many of the prevention methods discussed below may be covered by the work of an IRT team.

Incident Response Plan

To best prepare for such incidents, companies are encouraged to have in place an Incident Response Plan in relation to cybersecurity events. This will be a didactic playbook to allow any personnel to follow structured steps to contain a breach and to facilitate recovery works. Typically, this will include step-by-step guidelines listing who to contact in terms of forensic teams, lawyers and public relations and strategic communications companies to facilitate speedy actions.

Backup of files should be done frequently and securely stored, to allow business continuity in the event the current systems are locked.

Such an Incident Response Plan will need to be regularly updated to keep abreast of new forms of cyberattacks.

A hardcopy of this Incident Response Plan should be readily accessible, in the event all systems are locked.

Training

Employees are key assets to a business. They are also usually the gatekeepers and the first to identify and respond to suspicious incidents. Proactive training of employees may help to reduce the chances of a cyberattack.

The training should be regularly delivered, usually by an IRT well versed in the latest cyberattack methods and technologies, to keep employees abreast of developments.

Alternative Secure Communication Channels

One of the most frightening effects of ransomware is that all systems are down, including communication. Failure to immediately inform other colleagues may enable the spread of the cyberattack, and hinder coordination of mitigation actions. Forming alternative secure communication channels to facilitate an investigation and to continue business operations becomes a fundamental aspect to counter the effects of the cyberattack.

Specialised Insurance

Specialised insurances, such as business disruption or cyber insurance, may assist to mitigate potential losses.

It may be necessary to engage external consultants and experts (such as the IRT) to consider the suitability of the policies.

Where the policies call for certain steps to be taken (e.g. notification obligations and settlement restrictions), such steps should be highlighted (e.g. in the Incident Response Plan) to ensure compliance.

Technology and Processes

The need for stronger technological support and well-thought-out processes will help with prevention of a cyberattack. Impact assessments can be conducted to discover weaknesses, for easier reinforcement of the systems.

Data categorisation systems and data mapping may also be helpful for quick identification of the information lost, and to facilitate regulatory reporting.

Backup of files should be done frequently and securely stored, to allow business continuity in the event the current systems are locked.

Concluding Thoughts

Whether or not to pay a ransom is ultimately up to the organisation, having regard to the commercial, legal and financial risks.

The best way to streamline the crunchtime decisions is to ensure that proper preparation has been done. This could either completely prevent a cyberattack, or at least reduce the time needed to conduct investigations, quickly quell the spread of the attack, and facilitate better recovery. ■

Hin Han SHUM
Associate, Squire, Patton, Boggs
Hong Kong (SAR), China
hinhan.shum@squirepb.com

The thoughts expressed are those of the author and do not necessarily reflect the views of the Firm, its clients, or any of its or their respective affiliates. This article is for general information purposes only as to the position of related information as at May 1, 2021 and does not exhaustively discuss the topic. This article is not intended to be and should not be taken as legal advice.