June 11, 2021

Ransomware – How Should Organisations Respond?

Attorneys
Amanda N. Raad
Rohan Massey
Judith Seddon
Paige Berges
Clare Sellars

It seems that, in recent months, not a day goes by without reports appearing in the media of another significant ransomware attack, with such incidents posing an ever-increasing threat to both private sector businesses and public services alike (including hospitals and health services, schools and local government organisations, among others). It has been reported that ransomware attacks increased threefold last year and are not showing any signs of abating.

Recent high-profile ransomware incidents include, for example, an event that led to eighty UK schools and higher education establishments being delayed in returning to classrooms in March 2021; in the U.S. in May 2021, a major fuel pipeline, Colonial Pipeline, becoming the victim of a significant ransomware cyberattack, allegedly perpetrated by a cyber-criminal gang known as DarkSide, which disrupted its service for several days; and recently the Irish health service computer systems were also targeted in a ransomware attack reported by one minister as "*possibly the most significant cybercrime attack on the Irish state*."

What Is Ransomware?

Put simply, ransomware is malicious computer code that encrypts the servers of an organisation meaning that data cannot be accessed until it is unencrypted and this will usually only be once a ransom has been paid. Ransom payments are usually demanded in some form of cryptocurrency, making them difficult to trace and/or recover once paid (this can also make it harder to identify the perpetrators of attacks).

The problem of ransomware is regarded as an increasing and serious threat worldwide, with both economic and financial consequences and potentially also public health and safety and national security implications. Alarmingly, there is also evidence to suggest that monies generated by ransomware attacks are often used to underwrite terrorism, sanctions evasion, and other types of organised crime.

Ransomware attacks are definitely on the rise and the situation seems to have been exacerbated by the global COVID-19 pandemic. The ransomware business model is so sophisticated and lucrative that third parties are now also able to purchase ransomware-as-a-service from cyber-criminals to deploy on their own accounts.

Possible Consequences of Ransomware Attacks

So what are the likely consequences of a ransomware attack?

Business Disruption

Perhaps the most immediate risk is the potential business disruption that can result from such incidents. The consequences for organisations of being unable to operate their businesses, sometimes for even relatively short periods of time, can be considerable. The recent ransomware attack on Colonial Pipeline demonstrates how the disruption of critical infrastructure as a result of such incidents can have an even greater impact (according to Sophos, infrastructure organisations who are targeted with ransomware are more likely than organisations in any other industry to pay the demanded ransom).

Financial Consequences

The financial consequences of ransomware attacks can also be significant. Whether organisations decide to pay the ransoms demanded or not, the financial impact of being unable to continue with their businesses as usual before they can restore their IT systems and retrieve their data should not be underestimated. According to recent estimates by Emsisoft, a cybersecurity company, the real worldwide cost of ransomware in 2020 (taking into account ransom payments and business interruption costs) amounted to between $42 billion and $170 billion.

The financial consequences of ransomware attacks could be set to become even more serious for victims, as some insurers have announced that they will not write cyber-insurance policies that reimburse for ransom payments. For example, in May 2021 the European insurance company AXA announced that it was planning to adopt this position in France. The insurance industry has come under criticism for supporting criminal activity by reimbursing ransom payments; however, such payments remain legal in major insurance markets, including in the U.S. and UK, and there have not been major legislative proposals to prohibit them.

Loss of Data

Another risk of ransomware attacks is the potential loss of data, both business confidential information and personal data, which can seriously impact upon organisations in a variety of ways. Loss of confidential business information can lead to potential breaches of confidence where third-party confidential information is involved and the loss of an organisation's business confidential information could also impact upon the intellectual property rights and trade secrets used in the relevant business.

Reputational Damage

Reputational damage is another potentially significant risk in the context of ransomware attacks. It is currently difficult to estimate the actual level of ransomware incidents and the full extent of the financial losses involved due to organisations' understandable reluctance to admit that their security has been compromised and that they have been the victims of an attack.

Regulatory Notification Obligations

Under the European General Data Protection Regulation 2016/679 (GDPR), the UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018 (DPA), any ransomware attack involving the personal information of living individuals potentially can constitute a personal data breach and may, in some instances, need to be reported to the relevant supervisory authority.

A ransomware attack that impacts the confidentiality, integrity or, most importantly, the availability of personal data, will constitute a notifiable personal data breach if the lack of access has a significant detrimental effect on the relevant data subjects whose personal data is impacted by the attack. Where notification is required both the GDPR and the UK GDPR and DPA require organisations to act within 72 hours of becoming aware of the relevant breach. This timeline may have an important impact regarding the assessment of payment of any ransom, as notification may lead to the breach becoming public. This risk is increased if the nature of the breach presents a serious enough risk to individuals that they too need to be notified.

Operators of essential services (e.g. providers of services involving health, transport, energy, drinking water supply and distribution and digital infrastructure) and relevant digital service providers (e.g. providers of cloud computing services, online market places and online search engines) have additional reporting obligations regarding security incidents placed on them by the Cybersecurity Directive ((EU) 2016/1148), which was implemented in the UK by the Network and Information Security Regulations 2018 (SI 2018/506). For operators of essential services, this includes reporting incidents with a "significant" impact upon the provision of relevant services and, for relevant digital services providers, all incidents with a "substantial" impact on the provision of their relevant services must be reported. In each case, reports must be made to the relevant supervisory authority within 72 hours.

Responding to Ransomware Attacks – to Pay or Not to Pay?

Organisations which fall victim to ransomware attacks are faced with a difficult decision—to pay or not to pay the ransom. Many organisations do decide to concede to ransom demands and pay at least part of the requested ransom, rather than trying to restore their data without assistance from the perpetrators of attacks, in order to allow their businesses to resume operations as soon as possible. For example, it has been reported that following days of rising fuel prices, the constriction of fuel supplies across the U.S. and various U.S. states announcing an emergency, Colonial

Pipeline paid DarkSide (the cyber-criminal organisation thought to be behind its recent ransomware attack) nearly $5 million in ransom following the attack on its systems. Although on June 8 the U.S. Department of Justice announced that it had recovered most of the ransom paid by Colonial Pipeline (63.7 of the 75 bitcoins (worth roughly $4.4 million at the time paid)) by obtaining the private key to the cybercriminals' digital wallet, it is not clear how U.S. authorities obtained the key in this case, and given the nature of cryptocurrency payments, those who pay ransoms should not expect to be able to recover their funds.

However, organisations confronting this dilemma will need to take a number of considerations into account. At the UK's National Cyber Security Centre (NCSC) recent CYBERUK 2021 conference, UK Home Secretary, Priti Patel, made clear to sufferers of ransomware attacks that, notwithstanding how disruptive such attacks can be, the UK government does not support the payment of ransoms on the basis that acquiescing to the demands of cyber-criminals in this way may not, in fact, lead to the timely restoration of data. Payment of ransom demands also shows cyber-criminals that ransomware attacks are an effective way to extort money and may also encourage them to revisit the relevant organisation in future, or publish the stolen data in any event.

The Biden administration has not only echoed this position, but President Biden has also signed an executive order to enhance U.S. cyber-defences in view of a significant increase in cyber-attacks during the COVID-19 pandemic.

Civil and Criminal Implications of Paying Ransomware Demands

There are also a number of other considerations to take into account when considering whether to pay ransom demands—in particular, violations of sanctions and anti-money laundering/counterterrorist financing laws. These areas are garnering significant regulatory attention.

For example, on October 1, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) published an advisory to alert companies to potential sanctions risks related to ransomware payments. In recent years ransomware has been used by criminal organizations or sanctioned individuals and entities (for example, the WannaCry 2.0 attacks, associated with a North Korean cybercriminal organization) to raise funds for their illicit activities. Payment of ransomware demands by U.S. persons and companies can present sanctions risks where the attack involves a sanctioned jurisdiction or sanctioned party. The OFAC advisory confirms that ransomware payments to sanctioned parties or jurisdictions, where the transaction involves a U.S. jurisdictional nexus, may violate U.S. sanctions, and subject the payer—as well as any parties who facilitate the payment—to civil penalties. See our separate Alert here.

The U.S. Financial Crimes Enforcement Network (FinCEN) also issued an advisory on October 1 regarding money laundering risks of facilitating ransomware payments. Financial institutions (FIs) have an obligation to seek to identify and report suspicious activity—ransomware payments by definition are payments made to criminals and therefore FIs may be liable where they fail to identify and report ransomware and associated payments.

According to FinCEN, many ransomware schemes involve convertible virtual currency (CVC), which it describes as the preferred payment method for cybercriminals. A few days later, on October 8, 2020, the Department of Justice released an "Enforcement Framework" for Cryptocurrency, setting out broader risks and enforcement initiatives related to cryptocurrency-related crime. See our separate Alert here.

Although the UK regulators have not issued similar specific guidance, inadequate controls and due diligence to identify suspicious activity or the involvement of sanctioned persons in a ransomware payment could similarly subject UK persons, in particular, regulated financial institutions, to civil or criminal liability.

Tackling the Ransomware Phenomenon

The escalating risks of ransomware have led to a number of recent initiatives to try to tackle the issue. For example, the UK has created a new National Cyber Force, which is carrying out a variety of cyber-operations to disrupt antagonistic state activities, bad actors and terrorists which jeopardise the UK's national security, while a worldwide group of technology companies, governments, academic institutions and law enforcement organisations, among others (including

the UK's National Crime Agency and NCSC), have joined the recently created Ransomware Task Force (RTF) to address the global ransomware threat and deter cyber-criminals on an urgent basis.

The RTF has made a large number of recommendations to governments to try to tackle ransomware attacks. These include, for example, defining ransomware attacks as a national security threat, making it compulsory for ransomware attack targets to confirm the fact that they have paid ransoms and strengthening regulation of cryptocurrency services, among other things.

Other commentators, would like to go further. For example, Ciaran Martin, the founder of the UK's NCSC, has called for payments in response to ransom demands to be prohibited by law (subject to certain exceptions where human life is threatened), to help make ransomware attacks less attractive to cyber-criminals. Mr Martin recently observed to The Times: "*At the moment you can pay to make it quietly go away. There's no legal obligations involved.*" Mr Martin also noted the absence of obligations on organisations to report to anyone and the fact that the payment of cryptocurrency is not traceable. As mentioned above, some insurance companies are now also beginning to resist writing cyber-insurance policies that reimburse for ransom payments.

Conclusion

There is no doubt that ransomware incidents are a significant problem for both private and public sector organisations and that the question of whether or not to pay ransom demands is a serious dilemma for victims of attacks. Financial institutions which process such payments are at risk of regulatory enforcement as a result of anti-money laundering and counterterrorist financing requirements. However, currently, apart from the obvious financial consequences, there are usually few ramifications for companies that do decide to cooperate with cyber-criminals in this way—unless the ransomware involves sanctioned countries or persons. As noted above, regulatory changes may be introduced to try to address this growing and potentially highly disruptive and harmful threat.