3PB's Cyber Law Series
Ransomware attacks: a practical guide to survival

By Matthew Wyard
3PB Barristers

1. In response to the growing number of instructions regarding cyber incidents, this series of articles aims to address and provide practical advice on dealing with, common scenarios faced by businesses. This first article addresses the risk of a ransomware attack and considers the practical steps that an organisation needs to take to survive such an event.

2. Firstly however, it is worth clarifying what a ransomware attack is and the type of attacks commonly used against organisations.

What is a ransomware attack and what types of attacks are used?

3. The definition of a ransomware attack was neatly summarised in the recent report of the Ransomware Task Force: 'Combating Ransomware: A comprehensive framework for action' ("the RTF Report") as:

> *"[an] evolving form of cybercrime, through which criminals remotely compromise computer systems and demand a ransom in return for restoring and/or not exposing data…"*

4. Typically, the first an organisation knows of a ransomware attack is when they log onto their system to discover a message from the threat actor confirming that the organisation's IT security systems have been breached and that all the data therein has been encrypted; typically, a timeframe is given for the organisation to meet a demand (usually to pay a large sum of money) otherwise risk the loss or publication of their data. A link is typically given to a page on the Darkweb allowing the organisation to access a chat room and timer whereby they can communicate with the threat actor and see how long they have left to pay the money requested.

5. The three most common types of ransomware attacks currently in use are:

   a. **Conti news attack**: the type of attack envisaged above where the victim organisation's data is algorithmically encrypted, and the threat actor requires the organisation to make a payment to it under the twofold threat of having its data published on the Darkweb or to business competitors and the loss of access to its data due to the encryption. Such an attack is usually initiated through the opening of phishing emails or internal organisational sabotage.

   b. **Jigsaw attack**: an attack that relies upon malware to encrypt an organisation's data and progressively delete it until a financial ransom is paid, typically over a 72-hour period at which point all the organisation's data would be deleted.

   c. **A locker attack**: Similar to a conti news attack except, rather than encrypting an organisation's data, it locks the organisation out of its own devices and thereafter demands a ransom to unlock the devices.

Why should we take the risk of a ransomware attack seriously?

6. The 17th annual joint report prepared by IBM and the Ponemon Institute 'Cost of a Data Breach Report 2021' made troubling reading, finding:

   a. That the average costs of a data breach has increased to $4.24million;

   b. The average cost of a data breach was far higher where remote working was a factor in causing the breach.

7. The RTF Report noted that ransomware attacks are unlikely to disappear as:

   "Most ransomware criminals are based in nation-states that are unwilling or unable to prosecute this cybercrime and because ransoms are paid through cryptocurrency they are difficult to trace".

8. Ransomware attacks are not restricted only to large organisations that have deep pockets. Many organisations nowadays have cyber insurance meaning that, if the ransom is to be paid, the costs won't be paid by the organisation. This provides the threat actors have some sense of security when attacking and means that they needn't trouble themselves with only trying to breach the security systems of larger, sophisticated corporations.

Pre attack

9. So, what steps can be taken prior to an attack to prepare an organisation to be able to respond to it as thoroughly and quickly as possible?

10. The first thing to be understood is that it is not possible to completely mitigate against the risk of a cyber-attack. 'Zero Day Attacks' are not defendable as they rely on the threat actor finding a compromise in the victim organisations IT system that the IT system's operator was previously unaware of or, alternatively, cracking the organisation's security systems in ways that were previously not possible, meaning that the organisation will only discover their vulnerability when the attack takes place.

11. That said, the most effective way to increase an organisation's prospects of surviving a ransomware attack (or indeed any other form of cyber-attack) is to prepare thoroughly for such an event. The most prepared organisations will have:

    a. Put in place technical measures to control the risk of unauthorised access to their IT systems;

    b. Commissioned annual penetration testing in a bid to identify any compromises in their IT security systems;

    c. Commissioned internal and external vulnerability scanning;

    d. Provided training to their staff on the risk of cyber-attacks and how to identify potential threats;

    e. Put in place organisational measures that guide the organisation through responding to an attack including, but not limited to, a thorough cybersecurity policy, a cyber defence strategy, a threat engagement policy, a communication protocol;

    f. Secured insurance that provides for coverage against cyber-attacks;

    g. Proper system and data back-ups and recovery processes in place;

    h. Reviewed, upon entering into contracts, the terms of any contracts and noted which (if any) contracts require a cyber-attack to be communicated to the other contracting party (for instance, IT provision of service agreements).

Initial actions

12. If you have a cyber defence strategy in place, then it should cover the immediate actions to be taken upon the identification of an attack.

13. The immediate step that should be taken upon the identification of an attack is that a crisis management team should be put together made up of the following:

    a. A senior member of the organisation who has the delegated authority to make decisions in respect of defending the organisation. This would typically be an Executive Officer or a member of the organisation's C-Suite;

    b. A senior member of the organisation's IT team who understands the technical side of the organisation and is able to undertake initial fact finding as to the cause of the attack;

    c. In house counsel who is able to advise on the legal risks of any potential action;

    d. The Data Protection Officer who can assist identify and take the necessary action should a personal data breach have occurred;

    e. A member of the organisation's communications team who can advise upon and implement the communication strategy in response to the attack.

14. Alongside internal individuals, consideration must be given to external individuals being appointed to the crisis management team including:

    a. Expert solicitors/counsel who are familiar with advising on the legal risks associated with a ransomware attack;

    b. A specialist IT/cyber forensic investigator who is able to work alongside the organisations inhouse IT team to conduct a fact-finding investigation into the attack and identify the technical ramifications;

    c. A cyber-intelligence consultancy or cyber risk consultancy who can offer ransomware negotiation services;

    d. A PR organisation specialising in cyber-attack communication strategies.

15. The second immediate step would be to notify the organisation's insurers if they wish to rely on their cyber insurance policy to cover the costs of responding to the attack. It may be that the insurance company is able to put the organisation in touch with any external advisers that it has experience of working with in responding to cyber-attacks.

16. Once the crisis management team is put together, it is important that emergency contact details are shared. Cyber-attacks typically occur on a Friday, and it can be frustrating if decision making is slowed down by an inability to get hold of the members of the crisis management team over the weekend.

IT investigation / Fact finding

17. Once the crisis management team has been put together, the first thing that needs to happen is for IT/IT forensics to investigate the threat and determine if the organisation's system has been compromised and, if so, how. Once any compromise is found then it needs to be resolved to prevent future attacks and an investigation must be undertaken as to what data the threat actor has accessed, when it was accessed and, if possible, where from.

18. A thorough and detailed report should be prepared detailing the conclusions reached. This report should be addressed to the legal adviser in a bid to make the report privileged, thereby avoiding any potentially embarrassing or commercially sensitive information being able to be made public after the event.

19. Once the facts have been established, the organisation can then consider and take advice from its lawyers and communication advisers on its statutory notification obligations and its internal and external communication strategies.

Notification requirements

20. The most significant statutory requirement is the notification of the Information Commissioner's Office (ICO) found at Article 33 of the UK GDPR. An organisation must notify the ICO without delay and not later than 72 hours where the cyberattack:

    a. Results in a personal data breach;

    b. The organisation was the controller for the purpose of the breached personal data; and

    c. The organisation cannot rely on the exemption that the breach is "*unlikely to result in a risk to the rights and freedoms of natural persons".*

21. Cyber criminals are typically aware of this notification requirement and, accordingly, will regularly initiate cyber-attacks on Fridays to add additional pressure to the organisation knowing that it will have to notify the ICO on the following working day, Monday.

22. Where the organisation has to notify the ICO then it will also be required (by Article 34 of the UK GDPR) to notify the data subjects.

23. Notifying the ICO and the data subjects gives rise to additional risk to organisations who may have to subsequently deal with regulatory action taken against it by the ICO and/or

claims for damages by data subjects whose data protection rights have potentially been breached.

24. Organisations also need to consider their regulatory obligations and determine whether they need to notify their regulatory bodies of a data breach (or of the act of a cyber-attack).

25. Additionally, many organisations with whom the victim organisation is contracted may, particularly those working in IT, require that they are notified of data breaches or other cyber-attack events.

Communications

26. Alongside the statutory notification obligations, thought needs to be given to a communication strategy more generally. This communication strategy will need to consider, as a minimum, communication with:

    a. Employees;

    b. Shareholders;

    c. The media;

    d. Regulatory bodies;

    e. Contracting parties (where applicable).

27. Consideration may need to be given to a media strategy, particularly if the organisation is particularly large or a particularly large amount of data has been accessed.

Should you pay the ransomware demand?

28. Whilst inevitably a key issue, the question of whether and how to pay any ransom request is one of the last areas of consideration.

29. The first issue in relation to paying a ransom is whether the organisation actually can pay a ransom, in particular:

    a. whether it has the financial means to pay any ransom (including whether any insurance company has approved payment);

    b. whether it has the technical ability to pay if the ransom is in cryptocurrency;

    c. whether it would be committing a criminal offence by making the payment.

30. The first two considerations are fairly self-explanatory. The third issue, the question of criminal liability, requires further thought.

31. Unlike in the United States, there is nothing unlawful in the act of paying a ransom itself in the jurisdiction of England and Wales. However there are, broadly, three risks of criminal liability that must be thoroughly considered before making any payment:

    a. Firstly, organisations must ensure that they are not making payments to countries that are subject to UN or UK financial sanctions. Any payment made to such a country may fall foul of the Sanctions and Anti-Money Laundering Act 2018;

    b. Secondly, organisations need to ensure they are not inadvertently putting themselves in breach of the Terrorism Act 2000, s15 – 17A. It is suggested that particular care must be taken where a payment is paid in cryptocurrency in this respect;

    c. Thirdly, organisations need to ensure they are not breaching the Proceeds of Crime Act 2002, s328 although, generally, as long as the funds being used to pay the ransom are not proceeds of crime themselves, organisations will be safe in this regard.

32. The second issue is whether the organisation wants to pay the ransom, considering issues such as:

    a. Whether it's financially viable to make the payment or, alternatively, whether it would be more cost effective not to do so;

    b. Whether ethically/morally the organisation feels able to make the payment;

    c. Its view on the impact of payment on its risk profile: will paying cause such attackers to attempt future attacks.

33. Once these issues have been considered then your cyber attack negotiators can work on decreasing the amount of the payment, or extending the time within which payment should be made.

Following payment - resulting civil liability

34. Once the immediate threat of the ransomware attack has been resolved, the organisation will need to undertake further technical investigations and put measures in place, if possible, to strengthen its IT security.

35. It also however, needs to consider any resulting civil liability. There are two key issues in this regard:

a. A full contract review should be undertaken to identify any potential contractual liabilities that need to be addressed;

b. The more prevalent risk however is of claims arising out of breaches of the UK GDPR / Data Protection Act 2018. Such claims will be explored in detail in the second instalment of 3PB's Cyber Law Series – Data Protection claims: a guide for defendants.

19 August 2021

Matthew Wyard

Barrister
3PB Barristers

0117 928 1520
matthew.wyard@3pb.co.uk

3pb.co.uk