Ransomware Attacks

To pay or not to pay?

Ransomware attacks are increasingly targeting companies and their executives may be tempted to pay the requested ransom quickly to bring operations back to normal. This is not a decision any company should take lightly.

The number of ransomware incidents has more than doubled between 2018 and 2019, according to Polsinelli, Am Law 100 firm specialist and recognised cyber-security leader. The UK was particularly badly hit during the first six months of 2019, with ransomware volume jumping 195%.

Interestingly, the targets of these attacks have changed over the past months: whereas previously individuals were often targeted, the focus is now more likely to be businesses, partly due to their greater familiarity with Bitcoin.

Ransomware can be deployed in various ways including email phishing campaigns, Remote Desktop Protocol (RDP) vulnerabilities, software vulnerabilities or via MSPs and IT vendors. Whatever the method, the impact is immediate and far-reaching. A ransomware attack usually brings business operations to an abrupt halt, causing costs and stress levels to rise in tandem with the amount of time it takes to resolve the issue.

Experts suggest that targeted companies should not categorically rule out payment, but they should consider a number of factors related to technical, ethical, legal, safety and financial aspects before making a decision.

Arguments against ransom payment

In the US, the FBI's official stance is that paying ransoms emboldens criminals and 'provides an alluring and lucrative enterprise to other criminals.'

From a moral perspective, the decision is straightforward and reflects the law enforcement authority's approach; paying the ransom treats criminals as business partners and arguably promotes criminal activity of this type as well as pushing up ransom demand figures. In the second quarter of 2019, the average ransom payment increased by 184% to $36,295, compared to the previous quarter ($12,762), according to cyber support provider Coveware.

(It's worth mentioning here, that some ransomware demands reach into the tens of millions, often depending upon the sensitivity of data which is being threatened to be destroyed or released into the market place, should such payment not be made).

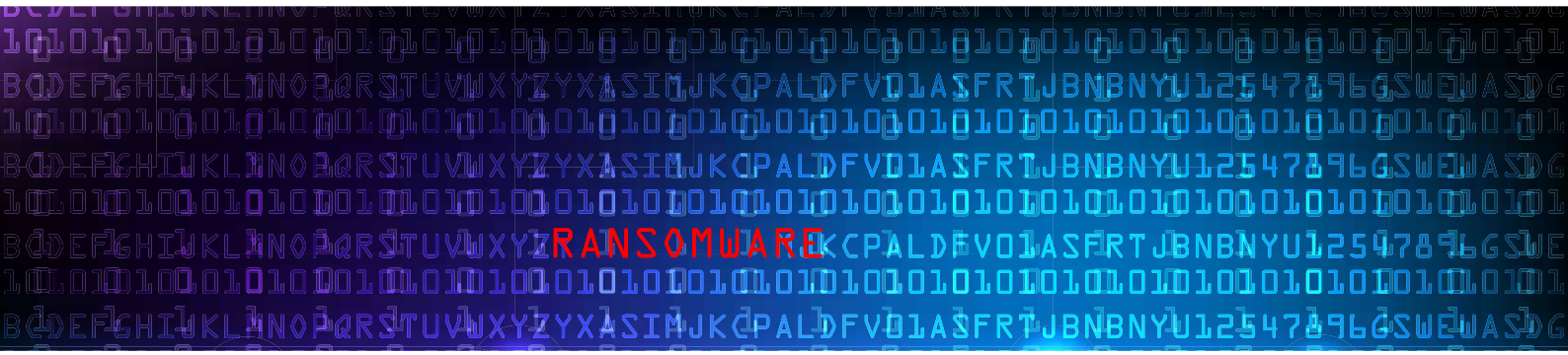
Paying the ransom may not only promote this type of criminal exploit but may also encourage cyber criminals to target the same entity again. If it worked the first time, chances are that it will work a second time.

Furthermore, businesses risk being accused of funding criminal or terrorist organisations by paying the ransom. There is evidence that ransomware groups are involved in other criminal activities such as drug manufacturing or human trafficking and in many ransomware attacks, the ransom is a 'distraction' for other nefarious actions. Against this background, it would be difficult to justify payment that might be applied in furtherance of such crimes.

Moreover, payment does not guarantee that decryption keys will be provided or, if they are provided, that they will actually work due to certain peculiarities of encryption algorithms. Generally, it is in the cyber criminals' interest to deliver a working decryption key to ensure the longevity of this type of criminal action.

However, there is no guarantee that hackers will deliver a decryption key or that any key will work as expected. Indeed, a study by marketing firm CyberEdge Group suggests that there is a significant risk that the decryptor may not work. According to the 2019 Cyberthreat Defense Report, 61.2% of ransom payers successfully recovered their data, which suggests that 38.8% of ransom payers did not.

In a now well-publicised case, Norwegian aluminium producer Norsk Hydro was targeted in March 2019 and decided against paying the ransom. Instead, production lines shaping molten metal were switched to manual functions, and the company reverted to 'the old-fashioned way' of doing business.



Arguments in favour of paying the ransom

The main cost of ransomware attacks is the associated downtime. According to cyber-security firm Datto, downtime costs due to ransomware attacks were up by 200% year-over-year in the first half of 2019.

If the targeted company does not have a secure and separate backup, recovery without a decryption key may be complicated or impossible. Reaching this decision may require the help and assessment of specialised consultants – it may be that the ransom payment is significantly lower than the costs and business interruption losses associated with the system's downtime. In fact, Datto suggests that the average cost of downtime was 23 times greater than the average requested ransom.

Fees of data recovery consultants depend largely on the size of your company and the scale and complexity of the attack, but can reach six-digit figures. Not all insurance policies cover such incidental expenses nor the ransom payment itself, so it is worth checking the exact wording of any cyber policy before making any decision.

Advice for affected companies

After a ransomware attack, companies should run two strategies in parallel. In order to assess the situation fully, the company ought to hire a cyber-security incident response team to run the forensics, assess the extent to which the systems are affected and the viability of recovering systems and processes from backups. At the same time, the company should hire a ransomware specialist to negotiate with the bad actors. This may involve asking for a reduction of the payment on the basis that not all systems need to be decrypted. The expert may also seek confirmation that the decryption key works, perhaps by requesting a decrypted file as proof. Again, a good cyber insurance policy will cover these costs and the underwriter's breach response team will assist in the practical implementation of these measures.

In general, it goes without saying that companies should keep good security hygiene and system health practices so that the consequences of an attack are limited and remediation is straightforward. Maintaining offline backups of any critical data can reduce the impact.

Further, businesses should update their operating system to the latest version and shorten patch cycles, use multi-factor authentication and complex unique passwords for each login, and disable any unnecessary network services.

Before making any decisions, any business on the end of a ransomware attack should consult with its broker or cyber insurer, legal counsel and where appropriate, law enforcement authorities.

For further details please contact:

Vanessa Cathie | Account Executive,
Global Professional & Financial Risks

E vanessa.cathie@uk.lockton.com
T +44 (0) 20 7933 2478