CYBER HOSTAGE

To pay or not to pay?

With the FBI recently warning that ransomware attacks could be a billion dollar criminal industry by the end of 2016, it is a good time to consider how businesses should respond when their systems have been infiltrated. Ransonware is a form of malware which gets into a computer or server and encrypts the files, ensuring that the computer files cannot be accessed, closing down the operation of that system unless a "fee" or ransom is paid to the individual or group behind the attack. Such attacks are taking place on schools and hospitals but are also hitting businesses. When the attacks happen the victims are left in a position where they either seek to restore their systems from backups or they could choose to pay the ransom. Where restoring the systems could take some time and involve an inevitable interruption of service, paying the ransom is no guarantee that the systems will be restored to the state they were in prior to the attack, whilst also involving possible legal implications and potentially leaving the organisation open to future hacks. Similar issues arise for distributed denial of service (**DDoS**) attacks, where a threat is made that the DDoS attack will continue indefinitely, denying or limiting customer access to the website, until a ransom is paid. Such DDoS attacks can be crippling for internet based retailers.

In certain circumstances, the making of a ransom payment could be illegal, for example, where such a payment is in breach of the Terrorism Act 2000 or would amount to an offence under the various sanctions provisions. Outside of terrorism and sanctions, would the making of a payment amount to a criminal offence? There are good public policy reasons for saying that such payments should not be made as it only funds the hacking organisations and encourages their activity, however, that does not necessarily entail that the making of such a payment would be criminal.

The Bribery Act 2010 (**BA 2010**) creates an offence where an offer, promise or giving of a financial advantage to another person is done in circumstances where it is known or believed that the acceptance of the advantage would constitute improper performance of a relevant function or activity. However, the relevant function should have been performed in good faith, impartially, or where the person performing it is in a position of trust. If a ransom payment were made to the perpetrators of a malware or DDoS attack, then it would be to persons who are performing a function which is, by its very nature, improper and the making of the payment is to stop them from conducting themselves improperly. As such, it is hard to envisage that the making of such a payment would amount to a BA 2010 offence. When considering the money laundering offences, the ransom payment would only become criminal property once it has been acquired through criminal conduct, i.e. once it is in the hands of the hackers. As such, it is difficult to see that a payer of a ransom would commit an offence under the Proceeds of Crime Act 2002. Further, an analysis that paying a ransom does not involve the payer committing a crime within this

jurisdiction sits comfortably with certain shipping insurance cases, where paying a ransom to pirates following the hijacking of a tanker is not considered an illegal payment.

Although there are good grounds for the view that making a ransom payment is not an offence in this jurisdiction, it does not mean that it is not be an offence in the jurisdiction where the payment is being received. Equally, although paying a ransom might be considered as a last resort, it is no substitute for having in place the IT systems and processes to ensure, to the fullest extent possible, that a company is not held hostage by such an attack in the first place.