MAYER·BROWN

Legal Update
August 2017

Cyber attacks: legal and regulatory considerations arising in their wake

Introduction

Cybercrime has been an ever-present threat facing businesses over the past two decades. However, the profile of such threats has been significantly heightened in recent months, since the May 2017 "WannaCry" ransomware attack and June 2017 "NotPetya" cyber attack. The serious implications of these attacks have put a renewed spotlight on the issue of cyber security and caused global organisations to further consider, as a matter of priority, whether they would be prepared for such an attack.

This legal update highlights some of the key legal and regulatory issues facing financial institutions in the context of the current landscape of ransomware attacks.

How do ransomware attacks work?

Ransomware attackers deceive users into running a software containing a virus on their computers. In the WannaCry attack, hackers took advantage of a software vulnerability in the Microsoft Windows operating system known as "EternalBlue", which allows viruses to quickly spread to other computers on the same network. This software vulnerability also affects equipment containing embedded software such as MRI scanners, as the UK National Health Service experienced in the WannaCry attack. If one user opens the virus, all of the computers/equipment on the same network may be rendered inoperative. Data on an infected machine will be encrypted, and users will be presented with a ransom request to transfer money to a Bitcoin address in exchange for decrypting their files within a certain time frame, after which the data will be lost.

WannaCry targeted banks and ATM networks. It is well known that banks and financial institutions' computer systems contain highly sensitive data, making them prime targets for cyber attacks and associated ransom demands. The payment of ransoms and potential data leaks raise both legal and regulatory issues that should be considered carefully.

Key legal issues

Under English law, the payment of ransoms is not prohibited.[1] However, if an institution were to pay a ransom knowing (or having reasonable cause to suspect) that the funds were to be used for terrorist financing, this would be an offence under section 17 of the Terrorism Act 2000. Such an offence could be avoided by seeking consent to the arrangement from an authorised officer of the National Crime Agency.[2]

Banks and financial institutions should also be aware that it is an offence under sections 44-46 of the Serious Crime Act 2007 to intentionally encourage or assist crime. However, an institution may have a defence if it can show that it was reasonable for it to act as it did.

Institutions must ensure that any personal data they control is protected against unauthorised disclosure, destruction or loss. A security breach of personal data may trigger claims for an organisation's failure to implement satisfactory risk management procedures to protect clients' personal data or breach of a privacy policy, as well as risk reputational damage.

1 See *Masefield AG v Amlin Corporate Member Ltd, The Bunga Melati Dua* [2011] EWCA Civ 24, paragraph 71.
2 In accordance with section 21ZA of the Terrorism Act 2000.

Key regulatory issues

The UK Financial Conduct Authority ("FCA") must be notified by regulated entities of "material cyber incidents". The FCA considers an attack to be material if it:

- results in significant loss of data, or the availability or control of IT systems;
- affects a large number of customers; or
- results in authorised access to, or malicious software present on, information and communication systems.

There is no current statutory obligation to inform the Information Commissioner of security breaches, but it is advisable to notify serious breaches voluntarily. This position is set to change when the General Data Protection Regulation ("GDPR") enters into force in all EU Member States on 25 May 2018. The commencement of the GDPR is not expected to be affected by Brexit.

The GDPR is intended to introduce tighter controls on the handling of personal data. Once the GDPR is in force, companies controlling or processing personal data of subjects located within the EU will be obligated to notify the Information Commissioner's Office of any data breach that risks people's rights and freedoms within 72 hours of becoming aware of it. This new regulation will require organisations to put in place adequate response and risk procedures, as failure to notify within the short time limit may result in fines of up to €20m or 4% of global turnover. The factors that will be taken into account when deciding whether or not to impose a fine include the nature, gravity and duration of the infringement, the intentional character of the infringement and actions taken to mitigate the damage suffered.

Conclusions

Cyber attacks represent a risk to all financial services businesses, so it is important to be aware of the threat and implement appropriate technical and organisational risk management procedures. This might include ensuring that software patches are up to date and any critical data is backed up securely. Small steps can also be taken to prevent ransomware from entering a computer network in the first place, for example by training employees to identify cyber risks such as phishing emails. A response strategy will also help to swiftly address the unique challenges presented by a ransomware situation. This might outline guidance for notifying regulators and criteria for paying or refusing to pay a ransom.

The importance of having a practiced emergency plan in place will only increase in the lead up to the implementation of the GDPR in May 2018. It is recommended that institutions begin to consider the impact of the GDPR on their businesses, and put in place rapid response procedures to avoid being caught by the hefty fines it will impose for failure to notify relevant data breaches.

If you have any questions or comments in relation to the above, please contact the authors or your usual Mayer Brown contact.

Mark Stefanini
Partner, London
+44 20 3130 3704
mstefanini@mayerbrown.com

Zahra-Rose Khawaja
Associate, London
+44 20 3130 3914
zahra-rose.khawaja@mayerbrown.com