CLIFFORD
CHANCE

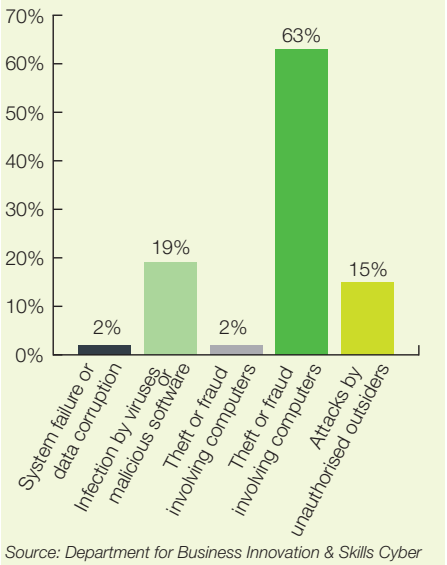
Briefing note October 2015

Cyber-Attack: Seeking refuge in the English Courts

Cyber attacks expose companies to many risks, including reputational damage and claims from employees and third parties. Companies need to plan how they will respond to an attack, and the possibility of court action must be part of any plan. Courts do not offer all the answers but, in appropriate circumstances, courts can restrict dissemination of confidential information or, if that is not possible, turning to the courts displays publicly that the victim is determined to respond seriously and openly to the attack.

Cyber attacks come in innumerable forms and are conducted for innumerable reasons. The risks that cyber attacks pose are, however, easier to quantify. Depending on the nature of the attack, these risks may include the loss of business secrets, reputational damage and claims from customers and employees. When faced with these risks, a business must respond and, sometimes as importantly, be seen to respond. For these purposes, courts can play an important role (though not, of course, an exclusive role), both because of the orders they can make and because resort to the courts demonstrates to the world, including to regulators, that the victim is taking the attack seriously and is doing all it can to respond.

Types of breaches



Source: Department for Business Innovation & Skills Cyber Security Breaches Survey 2014; respondents with 250+ staff

> "Cyber attacks are seldom from sovereigns or Bond villains lurking in extra-territorial bunkers"

If the attack is, say, from a foreign government, whether by way of industrial espionage or to obtain and publish embarrassing internal materials, there may ultimately be little that can be done in response other than to tighten security measures to try to ensure that it cannot happen again. But cyber attacks are seldom from sovereigns or Bond villains lurking in extra-territorial bunkers. For example, recent surveys suggest that more than half of all cyber attacks originate from employees or ex-employees, who are likely to be easier to engage through the courts.

Courts are well aware of the potential consequences of cyber attacks, and the law provides them with the means to respond and to do so quickly. For example, a cyber attack may involve not only breach of the civil law (for e.g. breach of confidence or breach of contract) but it may also involve criminal offences under the Computer Misuse Act 1990. Examples of cases where court action has been effective as part of a damage limitation exercise include the following:

Barclays Bank Plc v Guardian News and Media Limited [2009] EWHC 591 (QB)

An employee of a financial institution leaked tax-related documents, including privileged documents, to an MP, who passed them to a newspaper, which published an article based on them. Another newspaper then obtained the documents, and published them in full on its website. The financial institution was able to obtain by telephone an injunction on the basis of breach of confidence requiring the newspaper to remove the documents from its website and, subsequently, to retain that injunction when challenged by the newspaper. This was despite the fact that the documents had been on the internet for some time, generating "internet chatter", and that the newspaper argued that its publication was protected by its right to freedom of expression under the Human Rights Act 1998.

British Pregnancy Advisory Service v the person using the alias 'Pablo Escobar' [2012] EWHC 572 (QB)

A charity from which sensitive private information was stolen through a cyber attack by a person using an assumed name was able to secure an interim injunction to prevent publication of the information in order to allow the police to conduct investigations and to allow the charity to contact those whose details had been taken. The police found and arrested the perpetrator, who pleaded guilty to two offences under the Compute Misuse Act 1990.

Ashton Investments Limited, Ansol Limited v OJSC Russian Aluminium (Rusal) [2006] EWHC 2545 (Comm)

A company alleged that a Russian group had planted spyware on its servers in London, and sued on various grounds, including breach of confidence and conspiracy. The Russians challenged the jurisdiction of the English court but the court decided that it had jurisdiction because the servers were in London and the damage occurred in London. The court rejected the argument that the company should have sued in Russia.

The business disruption risk suffered as a consequence of a cyber attack can of course be mitigated to a certain degree by cyber insurance. The courts can be useful here for the swift resolution of coverage disputes for a particular event. Equally, they may have an involvement in claims seeking compensatory damages from third party suppliers and subcontractors, which are often not clear cut as to where responsibility may lie. Whilst recognising there is that traditional more reactive role for the court, and each situation will depend upon its facts and the contractual framework, a board faced with a cyber breach should also consider using the courts offensively and not only for damage limitation purposes.

What steps can be taken in such situations? Identifying those responsible for the cyber attack is key. The internet service providers which provided access to the computer systems can be asked and if necessary ordered by the court, to provide details of those behind the accounts used. Often where employees or ex-employees are involved there are alternative sources of information within the companies' own records and systems that can be accessed. Once those responsible are identified, they can be engaged via correspondence and, if they fail to respond in an open and cooperative manner, via court proceedings, in which orders can be obtained at short notice and even, in cases of real urgency, by telephone applications.

The courts are available and are prepared to help. Indeed, the courts have expanded their jurisdiction in order to be able to do so: for example the courts have concluded that the recently developed civil claim for misuse of private information is a tort, which gives a wider jurisdictional reach than if it had been treated as retaining its equitable foundations. If damage has been suffered in England and Wales – even if the attack emanated from across the seas – the English court has shown a willingness to assert jurisdiction. However, as with the cyber world itself, speed of action will usually be essential.

"Courts are well aware of the potential consequences of cyber attacks, and the law provides them with the means to respond and to do so quickly"

Authors

Iain Roxborough
Partner, London
T: +44 20 7006 8418
E: iain.roxborough@cliffordchance.com

Christopher Yates
Senior Associate, London
T: +44 20 7006 2453
E: christopher.yates@cliffordchance.com