CLIFFORD
CHANCE

Briefing note November 2015

Cyber Crime: using criminal investigators to pursue perpetrators

The latest victims of cyber crime have chosen the route of reporting incidents to the criminal authorities and supporting the resulting criminal investigations, rather than using civil proceedings. This has advantages and can leave open the option of civil proceedings at a later date but work still needs to be done and care does need to be taken to protect work product.

Figures from the 2015 Crime Survey for England and Wales show that cyber crime is one of the most prevalent crimes committed against victims in England and Wales, which can result in serious reputational and financial damage. The importance of companies preparing commercially and legally robust litigation strategies is of key importance.

According to media reports, recent cyber crime incidents have been followed within days by arrests and interviews of suspects. The process of working with criminal investigators to pursue perpetrators is a useful one which organisations should always consider.

The Data Protection Act 1998 ("**DPA**") places obligations on organisations which process information, while giving rights to those who are the subject of that data. It requires that companies take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of it.

The Information Commissioner's Office ("**ICO**") explains that taking "reasonable care" of customer data requires companies to "*be ready to respond to any breach of security swiftly and effectively*". Some form of positive action is often necessary. If a reasonable step or precaution has not been taken, organisations are less likely to be able to establish that they have taken appropriate measures. Whilst each hacking incident will have differing circumstances, the ICO has indicated recently that it expects companies to act swiftly in response.

Swiftly advising police of cyber crime incidents may be indicative of an effective response to security breaches. It is therefore prudent for organisations to establish what precautionary or reactive steps and/or security measures they have taken. These steps could go to supporting an organisation's position that it was not in negligent breach of its legal and/or statutory obligations.

Cyber Crime – The UK enforcement landscape

There may have been a perception that criminal enforcement of cyber incidents in the UK is less effective than in other jurisdictions. The reaction to recent UK cyber crime incidents suggests that UK authorities are taking a more aggressive approach to the criminal enforcement of cyber crime. Recent incidents have demonstrated that cyber crime agencies are willing to collaborate with companies to pursue criminals.

Specific UK bodies can investigate incidents relating to data breaches and/or have jurisdiction to investigate the most serious cyber crime incidents:

(a) The Metropolitan Police Cyber Crime Unit ("**MCPPU**"): The MCPPU has responsibility for the investigation of cyber crime and cyber-enabled crime – for example, computer and network intrusions and the online trade in financial, personal and other data obtained through cyber crime or cyber-enabled crime.

(b) The National Cyber Crime Unit (part of the National Crime Agency) ("**NCCU**"): The NCCU provides specialist cyber support and expertise across law enforcement. The NCCU's primary responsibility is the co-ordination of the overall response to cyber incidents across a range of domestic and international bodies.

(c) The Information Commissioner's Office: The ICO has extensive powers to enforce the DPA. The Information Commissioner may take various actions, including the issuing of enforcement notices and/or information notices.[1]

Criminal investigations or civil proceedings?

The Criteria

In 2015, the MCPPU published criteria indicating the circumstances in which it will investigate suspected cyber incidents. The MCPPU is clear that routine reporting of cyber crime will not fall within its jurisdiction. As an initial step, companies should therefore consider the following questions:

(a) Is there a significant international dimension to the breach?
(b) Is the data particularly sensitive? If so, why?
(c) Is the cyber incident likely to cause (significant) public concern?
(d) Is there an arguable case that the specialist powers of the MCCPU, NCCU and ICO are appropriate in the circumstances of the data breach?
(e) Is the evidence available so damning that it is likely to stand up to the "*beyond all reasonable doubt*" criminal test?

These questions considered, why might an organisation elect to report the cyber crime and thereafter support a criminal investigation rather than pursue civil proceedings? There are a number of contributing factors:

Enforcement and information powers

Criminal enforcement bodies have wide powers to compel or obtain information. Agencies have the power to enter premises to execute search warrants and arrest suspects. For organisations, an arrest, publicly announced, may assist with the immediate implementation of a press strategy designed to protect against reputational losses. Civil litigation may then remain an option with the benefit of the authorities' criminal investigations. Further:

(a) Recent incidents have highlighted that cyber criminals do not necessarily work in concentrated cells and may use proxies or proxy groups. The potential criminals may be located in multiple jurisdictions. Bodies with criminal jurisdiction can utilise wide powers and cross border intelligence-sharing to locate potential defendants.
(b) Once located, the defendant(s) may be held in custody. This, in itself, can publicly evidence an organisation's proactive response to resolving the cyber incident.
(c) Criminal investigative bodies may also access information available from other governmental and public bodies through statutory gateways.[2] Parties to a civil litigation will not necessarily have equivalent powers or tools of the same informational and geographical scope with which to keep track of perpetrators / defendants.

Cost and commitment

Civil litigation is expensive. The claimant bears all the costs of investigating the claim. And civil proceedings, once started, are difficult to end, without loss of face and payment of the other side's costs. If the claimant is ultimately successful at trial, the Court may order the unsuccessful party's costs but these are at the Court's discretion and the defendants may have no available funds.

Organisations should, nonetheless, be conscious that either supporting criminal investigations (or indeed bringing their own private prosecutions) is not a "cost-free" alternative. Organisations will need to ensure that a forensic team of litigators and experts is able to collect evidence and information for any criminal investigation and subsequent prosecution; organisations will need to comply with law enforcement requests for evidence to assist the

[1] Enforcement notices require data controllers to take steps to comply with the law. Information notices require companies to furnish the regulator with the information he requires to assess compliance. The Information Commissioner also has the power to apply for a warrant to seize information and search premises.

[2] For example, see section 115 of the Crime and Disorder Act 1998. Section 115 provides that "*any person who, apart from the [CDA 1998], would not have power to disclose information to a relevant authority shall have power to do so in any case where the disclosure is necessary or expedient for the purposes of any provision of the Act.*"

investigation and any eventual prosecution, and be conscious of the more extensive disclosure obligations which exist in criminal prosecutions. Investigations and prosecutions often have indefinite timelines.

Publicity

Civil proceedings are conducted in open court to which journalists and reporters have access as of right. Any discussions about the nature and extent of any alleged hacking will therefore be a matter of public record. Criminal investigations are generally not publicised, although they may be announced or there may be leaks; and whilst criminal proceedings are conducted in open court, pre-trial hearings are subject to reporting restrictions until the actual trial, which may not take place for some time.

Access to information

Cyber crime victims may often not have enough information to bring a civil claim immediately following a cyber incident. There are often difficulties in identifying the perpetrators. Criminal investigative bodies have access to a wider pool of information on potential defendants. As such, organisations may wish to utilise evidence obtained through criminal investigations to assist a civil case, if they decide to pursue parallel civil proceedings.

Under English law, criminal convictions can be used as evidence in subsequent civil proceedings.[3] A successful prosecution may therefore be influential to the overall outcome of a subsequent civil action.

Investigative bodies may be subject to legal obligations as to the use of information (some information they receive may be subject to conditions that it be used solely for the purposes of the criminal investigation). Moreover, the information provided may be subject to duties of confidentiality between the investigative body and potential defendant(s). Organisations will therefore need to ensure that information is not obtained improperly. At the same time information can become public or can indicate where other useful information can be obtained through civil proceedings. Organisations may also wish to agree a mutual information sharing process with the police as to the use of information provided by them to the police and vice versa.

Sharing information

We know also that the criminal authorities in both the UK and abroad are keen to receive information, even if not for the purpose of prosecution, but rather as intelligence to assist the authorities more generally in their battle against cyber crime. This is a trend also in other jurisdictions. For example, the Hong Kong Monetary Authority recently issued guidance encouraging companies to share information on cyber threats with itself, the police, and each other.

It would be prudent for organisations to ensure that any information sharing process safeguards their commercial interests and privileged information. The recent trend is for organisations to instruct forensic experts to audit, analyse and review information for sensitivity and privilege. This may afford organisations the opportunity to vet their documentation prior to its provision to the authorities.

There are a number of additional protections that may be considered to protect commercial interests and limit the information made available for the purposes of the investigation. The concept of limited or restricted waiver of privilege allows one party to disclose privileged communications to another without losing privilege against others. So long as organisations provide information (i) for a limited purpose, and (ii) on a confidential basis, privilege remains intact (and can therefore be claimed) against the rest of the world.

Any form of waiver of privilege is not without risk. Organisations should therefore be live to the issues arising out of a waiver of privilege and carefully consider the scope of any waiver provided. Organisations should have in mind the following considerations which are often relevant in this area:

(a) The extent of the waiver must be clear in order to avoid interpretation issues at a later date.

(b) Organisations and their legal advisers should ensure that the privileged material satisfies the scope/limited purpose of the waiver provided.

(c) Organisations should obtain confirmation from the recipient of the waiver that they acknowledge that the waiver is being made for a limited purpose (and that they also agree to make no claim that there has been a general waiver).

A prosecuting authority could not agree to fetter its discretion to use that information, should proceedings follow, given its disclosure obligations. The limited nature of the waiver could nevertheless continue if the onward

[3] Section 11 of the Civil Evidence Act 1968.

disclosure were suitably restricted in the hands of defendants – of course, if documents are ever referred to in open court, privilege would be lost.

Private prosecution

Despite the growth in cyber crime, and despite the increasingly aggressive approach being taken by criminal authorities as well as the increase in resources given to fighting cyber security, it is still the case that relatively few cyber criminals are brought to justice, in part because the scale of the threat is not yet matched by the resources devoted to it and, as we mentioned in an earlier briefing on the growing threat of cyber crime, "*the pace of technological change and the adaptability of the cyber criminal means that law enforcement will always be playing catch-up.*" [4]

For those reasons, businesses affected by cyber crime may in the future decide to pursue perpetrators by bringing their own private prosecutions. In England and Wales, any individual has the right (although no duty) to bring a private criminal prosecution.[5] Whilst private prosecutors are likely to need to involve the criminal authorities in order for example to effect an arrest or obtain a search warrant, nevertheless, once sufficient evidence is gathered, an individual or company can pursue a prosecution through the criminal courts in the same way as a prosecuting authority – albeit they will be subject to disclosure and other obligations, in the same way as prosecutors are.

Disadvantages to criminal investigations/prosecutions

There are potential disadvantages to supporting criminal investigations rather than pursuing civil litigation. There will be continued public scrutiny once an investigation is announced and organisations will need to consider whether the breach is so significant that it was bound to become public knowledge in any event.

Whilst compensation for any loss or damage resulting from the offence can be awarded as part of any sentence following conviction, traditionally this has only been done in straightforward cases where the amount at stake is not great. In complex cases or where substantial amounts of money are involved, recovery has usually been by way of civil proceedings - although that position is changing, given the increasing expertise of criminal courts in dealing with complex financial matters arising from their involvement in confiscation proceedings. In any event, in many cases the perpetrators can be hard to locate and may not have assets out of which to recover any damages awarded.

Organisations will never have control of a criminal investigation. One may not be started. Another may continue long after they would prefer it ended. Once an investigation is started, the victim company will have little or no control over it and any subsequent proceedings. Of course, if a private prosecution were to be brought, then control would be much greater over decisions taken and the process followed. And in civil proceedings the organisation is the claimant so it can have more control and oversight as to the timetable and scope of the claim.

Losing control of the process or of information provided in the ensuing process will always be a consideration and needs to be weighed against the perceived benefit at the earliest possible stage in the development of a strategy.

[4] National Strategic Assessment of Serious and Organised Crime 2015 at page 4.
[5] Prosecution of Offences Act 1985, s.6.

Authors

Iain Roxborough
Partner

E: iain.roxborough
@cliffordchance.com

Judith Seddon
Partner

E: judith.seddon
@cliffordchance.com

Christopher Yates
Senior Associate

E: christopher.yates
@cliffordchance.com