

# To catch a cyber thief: tracing internet crime

Your business's computers represent a route to valuable company data, which makes them a tempting target for competitors, bitter ex-employees and criminal gangs. Although hackers can try to cover their tracks, there are ways to trace them, as **Anthony Riem** explains

**IN MUCH THE SAME WAY AS A BANK trades with money, a company trades upon the value of its know-how, knowing just when to sell a stock or take over a company, or who needs insurance for which product and the type of cover needed.**

Companies go to great lengths to obtain and develop their know-how, whether it be a client list, the financial analysis of a proposed takeover of a company, or the profit margin figures on a particular product. This know-how is often held in a computer system, which makes it an extremely tempting target for competitors, disgruntled employees and, increasingly, criminal gangs.

Although much of this know-how can be obtained legally through undertaking the same research as the company, it is increasingly being obtained illegally.

One of the easiest ways for an unauthorised third party to gain access to a company's know-how is via its computer system, which is often its Achilles' heel.

While there are measures that a company can take to protect its know-how, this article deals with what happens when a third party has already 'broken' into a company's system, and what the company can do to try to locate the third party and stop it from hacking again.

## KNOWING WHAT TO LOOK FOR

Asking an ex-employee to hand back a client list and/or delete it from their



**By Anthony Riem, partner, international fraud and commercial litigation, PCB Litigation**

computer is one thing; tracing a computer hacker is another. The identity of the ex-employee will be known, and it is a relatively straightforward process to obtain a court order ordering them to hand back all unauthorised data. Compliance with the court order can be confirmed (at least in part) by obtaining permission from the court to check their home computer. It is also usually possible to identify which particular piece of data the ex-employee has in their possession, making the search and retrieval easier.

In the case of a hacker or a group of hackers (often the case with criminal gangs), a victim is initially unlikely to have any idea of what data has been stolen and over what period. The unauthorised access could be the first such intrusion or an example of a longstanding hack. This makes a search for the missing or copied know-how somewhat difficult – the company does not necessarily know what to look for. All that may be known is that someone has gained unauthorised access to the computer system.

The location of the hackers is also unlikely to be known. You may be trying to find a computer hacker based in Russia, India, the USA, or the company or house around the corner. In each case, it is necessary to be aware of the steps that can be taken in a particular jurisdiction. If nothing is done, the competitor and/or criminal gang will

simply strike the same company again, potentially damaging it with each attack.

## CYBER FOOTPRINT

To catch a cyber thief, you need to follow their trail. To do this, it is necessary to know what to look for, who to go to for help with your search, and the time frame in which you need to act. This is often difficult, as cyber attacks can be disguised by a false trail. For example, a cyber thief may use 'zombie computers' – computers owned by innocent third parties but controlled by the cyber thief – to carry out the attack.

In much the same way that an old-fashioned bank vault is protected by a large door with a key, access to a company's computer system is through a password or (somewhat rarely) a series of passwords. These should change regularly and should only give access to a limited area of the company's know-how, as opposed to the whole database (although this is not always the case). A hacker may download spyware onto a home computer (or via a joke sent to a work computer), obtain the necessary password and then access the company's network. The company's information is then damaged by the loading up of a virus and/or is stolen by sending it to another computer. Entering and exiting the computer system is done by computer, which leaves a cyber footprint. >

## Cyber crime

'Internet companies do not have the data storage capacity to save all their internet logs. It is vital to act quickly to preserve this data, otherwise it will be overwritten and the trail will be lost.'

To obtain a court order tracing a cyber thief by following their cyber footprint, it is necessary to know (at a basic level) how the internet works. This will enable a company to explain to the court how it can assist in tracking down the person who sent the virus and/or stole confidential information.

It is important to remember that accessing any computer system will modify its electronic records. Further, a company's IT department often does not have an understanding of what a court will require to enable a claim to be established. In dealing with any suspected attack on a computer system, it is therefore essential to use a computer forensic expert to preserve the integrity of the evidence and establish an audit trail.

### HOW IS INFORMATION SENT ON THE INTERNET?

An e-mail sent from one computer to another needs to leave its source, locate its destination and arrive in the correct format and not just as a jumble of text. The data is first digitised into a series of numbers and sent in a standard format, according to uniform transmission rules, from the sender's computer. It is then fragmented or split up into chunks (an IP packet), which are sent along a network device known as a router. The data goes from one router to another (known as a 'hop' – each router choosing the

optimum route to the end destination) until it reaches its destination, the recipient's computer. The data is reassembled and delivered to the internet address, or internet protocol (IP) address, of the recipient's computer. Each IP address uniquely identifies the recipient within the network, in much the same way as a postal address. The routers are controlled by internet service providers (ISPs) and they therefore have the information necessary to enable you to trace the source of an attack.

### TRACING AN ISP

To find the IP address that was the source of the attack, it is necessary to reverse 'hop' from router to router, following the cyber footprint. It should be possible to identify the last ISP that sent the malicious e-mail/virus to the victim's computer system.

The first task is to obtain the records of that last ISP. However, it is unlikely that the ISP will provide that information voluntarily, owing to data protection issues. The victim will therefore need to obtain a court order.

Depending upon the jurisdiction in which the ISP is based, it may be possible to obtain (amongst other data) the identification/telephone number of the previous user terminal, the address of the previous user and the type of terminal, the numbers called, the date of the calls and the total number of units to be charged and, in the case of mobile usage, the location of the caller. The logs will not show the content of the e-mails.

### THIRD-PARTY DISCLOSURE ORDERS

Rule 31.18 of the Civil Procedure Rules enables a victim to obtain disclosure of documents against a person who is not a party to proceedings before those proceedings have started.

As stated in *Mitsui & Co Ltd v Nexen Petroleum UK Ltd*, to obtain this type of disclosure order (often referred to as a *Norwich Pharmacal* order):

'... (i) a wrong must have been carried out, or arguably carried out, by an ultimate wrongdoer; (ii) there must be the need for an order to enable action to be brought against the ultimate wrongdoer; and (iii) the person against whom the order is sought must: (a) be

mixed up in so as to have facilitated the wrongdoing; and (b) be able or likely to be able to provide the information necessary to enable the ultimate wrongdoer to be sued.'

Rule 31.4.1 of the Civil Procedure Rules makes it clear that the meaning of 'documents' is 'not restricted to paper writings but extends to anything upon which evidence or information is recorded in a manner intelligible to the senses or capable of being made intelligible by the use of equipment'.

Given that the whole purpose of obtaining the records from the ISP is to enable a victim to trace the wrongdoer, and that the ISP is only involved because it acted as a means of transmission, Rule 31.18 can be used to obtain an order requiring it to disclose this information. The victim will need to pay the ISP's costs for providing the information, which can then be claimed from the hacker.

The application will need to specify the nature of the breach into the computer system, why access is needed to the ISP's computer log data, and why it is considered that the ISP will still be holding the information. Even if the ISP does not object to the disclosure application, the court will still need to be convinced of its merits and it is for this reason an understanding of the internet is necessary.

It is more than likely that the disclosure order against the first ISP will lead the victim to the contact details of another ISP, rather than the source of the attack. It may therefore be necessary to carry out the same exercise with one or more ISPs, which may be in a foreign jurisdiction, before the trail leads to the hacker's computer.

Depending upon the laws of the country in which the foreign ISP is based, the ISP can be made to disclose its records either on the basis of an order made by a court in that country, or an order made by an English court which is enforceable in that country.

A key aspect of successfully tracing the source of an attack on your computer system is therefore the instruction of computer forensic experts and solicitors with the relevant expertise in obtaining international disclosure orders.

*Mitsui & Co Ltd v Nexen Petroleum UK Ltd [2005]*  
EWHC 625 (Ch)

*Takenaka (UK) Ltd and Brian Corfe v David Frankl (unrep, High Court, 11 October 2000)*

*Ashton Investments Ltd and another v OJSC Russian Aluminium and others [2006]*  
EWHC 2545 (Comm)

### IMAGING

Where a 'hop' leads to a computer, an expert will need to gain access to that computer to see if any further information can be gleaned to show that the computer user is in fact the guilty party, or whether their computer was being used as a zombie computer by the guilty party.

The expert will invariably wish to take an 'image' of the computer to preserve the integrity of the evidence stored on it. The process of 'imaging' is one that enables an exact copy to be obtained of the data in a computer, including deleted and fragments of files. This enables the expert to reconstruct the history of the creation of a particular file, including any deleted versions of it.

The process of imaging should therefore be provided for in the court order by which the computer is inspected. It should also include an obligation on the respondent to the application to disclose details of any password so that access can be obtained.

Consideration may also have to be given as how to deal with any privacy issues. For example, the computer may contain records of third parties that should not be inspected. Depending upon the jurisdiction, there may also be an obligation to notify the owner of the data that an image or copy of their data is being taken.

The imaging process is relatively quick and the expert should make back-up copies of the imaged data. When dealing with a computer network, the court is unlikely to order that an image of the whole system be taken. Instead, it is usually necessary to perform a targeted search, looking for encrypted/deleted files, or specific words or phrases in documents. Clearly, the choice of search terms is vital and is a matter upon which both the computer forensic expert and solicitor will provide advice.

Once the computer image has been reviewed, it should be possible to confirm whether the computer was used to gain unauthorised access to the victim's computer network and/or steal the company's know-how.

### A CASE STUDY

The case of *Takenaka (UK) Ltd and Brian Corfe v David Frankl* shows how

the use of disclosure orders, experts and imaging can lead to the identification of a wrongdoer.

Takenaka (the claimant) had been receiving malicious e-mails that had been sent from Microsoft Hotmail accounts. Hallett J granted the claimant an order requiring Microsoft to disclose the sender's registration details which, given the ease of setting up a Hotmail account, were unsurprisingly fictitious. However, the IP numbers on the e-mail header were owned by a US company. The US company was then ordered by Hallett J to disclose information contained in its records that linked the IP numbers to a CompuServe account through which they were sent. A further disclosure order against CompuServe revealed that the account was held by Thames Water Utilities, installed on a laptop computer in Turkey.

Only two people had access to the account on that laptop. Forensic evidence, including details of when the laptop was accessed, established which of them was responsible for sending the malicious e-mails.

This process, as the expert said in his report to the Court, consisted:

'... of matching the dates and times between the ISP's billing information, the hotmail access logs and the computer traces (from the file structure, the file content, unallocated space, cluster analysis and cache indices.'

Takenaka not only succeeded in recovering damages and its legal costs but also the costs of the investigation.

### POTENTIAL PITFALLS

Owing to the amount of internet traffic, internet companies simply do not have the data storage capacity, or the money to pay for such capacity, to save all their internet logs. It is vital to act quickly to preserve the internet log data, otherwise it will simply be overwritten and the trail will be lost.

In the USA, for example, an application can be made for a court order that requires the internet provider to retain its logs for up to 180 days (see 18 USC s2703(d) (Electronic Communications Act)). In the European Union, member states currently offer

their own time periods for the retention of data (in some cases one year, in others three years). However the EU Data Retention Directive, which came into force in May 2006, requires member states to enact legislation allowing the retention of data from six months to two years (see Article 6 of the EU Data Retention Directive 2006/24/EC).

A hacker will usually use as many 'hops' as possible to make the tracing task all the harder. They will use programs that distort the IP packet size (or footprint), so it is not as easy to track a similar-sized IP packet (or footprint) across the web, all in a bid to throw you off the trail. The hacker may also seek to hide their identity through the use of anonymous websites, such as 'anonymiser.com', and the IP address that sent the e-mail may even be a 'pay-as-you go' address. This does not mean that the hacker cannot be identified, but it may mean that further disclosure orders need to be obtained, for example, to trace the method of payment used by the hacker to disguise their identity.

### TRACING WITHOUT DISCLOSURE ORDERS

It is possible to trace the source of a cyber attack without having to obtain disclosure orders.

In *IHL146* (p51), I referred to the case of *Ashton Investments Ltd and another v OJSC Russian Aluminium and others*, in which it was alleged that spyware had been installed on the claimant's computer system.

The defendant was able to trace the source of the spyware by examining the internet traffic it received and then tracing the IP address to an internet address in Russia registered in the name of the defendant.

In a current case, PCB Litigation has instructed a computer forensic expert who has traced the source of an attack to an address in Russia using IP addresses.

### CONCLUSION

It is possible to obtain disclosure of computer logs from third parties and therefore identify the party responsible for accessing a company's know-how without authorisation.

To do so, it is necessary to have a plan in place: you need a contact with the relevant experience in tracing cyber

## Cyber crime

attacks, from both a technical and a legal point of view. It is necessary to act quickly and to ensure that the evidence on your own computer system is not inadvertently compromised by an internal investigation.

Not having a plan in place to deal with a cyber attack is akin to driving without insurance – if your business is hit

by cyber criminals it may end up as a total write-off. **IHL**

*By Anthony Riem, partner,  
international fraud and commercial  
litigation, PCB Litigation.*

*E-mail: [ajr@pcb litigation.com](mailto:ajr@pcb litigation.com).  
Tel: +44 (0)20 7831 2691.  
[www.pbc litigation.com](http://www.pbc litigation.com).*

'In a current case, PCB Litigation has instructed a forensic expert who has traced the source of an attack to an address in Russia using IP addresses.'