Stopping the leak...

IJA's Electronic Countermeasures (ECM) team are frequently called to conduct regular 'sweeping' programmes on behalf of clients wishing to ensure the integrity of sensitive 'business critical' operations are retained. During one routine visit a device hidden behind an air vent grill in the Board room was discovered, and so began a salutary tale of a disgruntled employee using technology to steal information with the intent to damage his employer's reputation...

This was the start of a fascinating case which lasted for several months and dealt with a technophile senior employee hell-bent on obtaining information about our client's activities. It ended with a court injunction, the delivering-up of stolen information, and the discovery of an array of computer and communications equipment, listening devices and recording media.

Our client was in the midst of some delicate negotiations and had commissioned a physical security review which, in addition to a comprehensive ECM sweep programme, paid particular attention to the safeguarding of proprietary information, its main asset. A major part of the review was a security assessment of the networked information communications technology (ICT) system.

Our report concluded that:

- Even the most fundamental logical security was absent.
- There was no defined policy on centralised IT function and resources.
- There was no security strategy documentation.
- Access controls had been applied equally to all applications.
- There was no tried and tested disaster plan.
- The server system was outdated, with only a small library of attendant security utilities.
- No encryption algorithms or digital signatures were deployed.
- The use of passwords was inadequate and they were seldom changed.
- Software at the firewall needed to be hardened to control access attempts by remote sites.
- The A drives on PCs were not blocked off with software released to users of the network, so as to prevent the introduction of Trojan horses.
- No intrusion detection system (IDS) was installed.
- the relevant parts of the client's database were not securely classified.

'Rogue emails were sent using an unidentifiable account'

These deficiencies were subsequently all acted upon.

It came as a shock when we heard of the 'spamming' of several hundred of our client's customers a few days later. The rogue email was sent using an unidentifiable email account.

The email contained:

- Verbatim extracts from past board meetings.
- Accurate summaries of some key recent internal policy decisions.
- Confidential and accurate financial information.
- Acidic comments aboard members.
- An incitement to lobby against the interests of the client.

Some of the recipients received printed hard copies of the offending email (which warned of further, similar missives to come) by post.

'It is vital in the early stages of an investigation to document the reasons for deciding to launch an enquiry'

INITIAL SUSPICIONS

A provisional profile of our client's potential opponents and adversaries came up with a raft of competitors and former employees and even posed the possibility of foreign government intervention. However analysis of the email revealed a level of knowledge and familiarity with internal procedures indicative of only a few senior employees. Also, the spamming audit trail, partly listing the recipients of the email, was a direct match with an internal email database that was only accessible to the CEO and his secretary. The investigation was homing in.

Detailed background checks using online databases and the Internet, confirmed that a senior employee had an employment history which was at variance with his CV and job application. Only cursory background checks had been conducted prior to his employment. He was an erratic timekeeper, often staying late and regularly working over weekends. He appeared to enjoy challenging authority and was a gifted writer of prose. We had a suspect.

LEGAL ADVICE

It is vital in the early stages of any investigation to document the reasons for deciding to launch, and subsequently to continue with an enquiry. These reasons need to be justifiable, in accordance with data protection and human rights legislation, and must steer a fine path between the rights of the client and the rights of the suspects.

Ian Johnson Associates Limited (IJA) - Linden Place - Seale - Farnham - Surrey - GU10 1HS.
T: (+44) (0)1252 782664 **F:** (+44) (0)1252 782818. **E:** info@ija.co.uk **W:** www.ija.co.uk

Continued from page 1

Our early overview concluded that there had been an unauthorised, and hence illegal attempt to bug a board a meeting, that confidential information had been stolen, and that a database had been downloaded from our client's computer system. While not discounting the potential for a criminal action, our objectives were to identify the miscreants, recover our client's information, get financial restitution and issue injunctions to limit further damaging and publicly humiliating emails. This was to be a civil law case.

Initial investigative options included;

- Reviewing selected personnel files
- Real time electronic audits of boardroom meetings to monitor interceptions
- Covert disk imaging of PC's and laptops
- Reviewing the client's server to monitor outgoing email traffic
- Telephone call log analysis of key employees
- Intercepting the telephone and fax lines of selected employees
- Fingerprint analysis of the envelopes and contents of letters
- DNA matching from the stamp and envelope with selected staff samples
- Handwriting analysis to match the writing on envelopes with control samples
- Indented impression (ESDA) testing on envelopes and contents
- Striation testing to match printed pages with printers and photocopiers
- Covert desk searches of employees
- Physical surveillance of employees
- 'Disputed utterance' analysis of written material
- Lifestyle analysis and background checks on staff
- Creating an 'incident' to elicit a response
- Working with informants or undercover operatives to obtain more intelligence

During the initial phases of an investigation that is likely to develop at speed, it is essential to obtain legal advice from a law firm which is familiar with investigative techniques, has a strong stomach for litigation, and a track record of successfully applying for injunctive relief in the courts. In this case, the lawyers undertook the essential task of collecting employment contracts and associated papers that might be used as the basis for an affidavit and for laying a complaint.

THE INVESTIGATION

Having confirmed that it was owned and paid for by the client, we covertly took an image of the PC on the desk used by the suspect. The machine had a large hard disk and imaging went on into the small hours. Forensic computer imaging is where a digital or optical image of a computer's hard drive is taken for subsequent analysis. A mirror image copy of the data, applications and operating system is garnered so that it can be replicated off-site, and a control copy kept for evidential purposes, while investigators interrogate a duplicate copy.

When a user deletes a computer file it is not lost forever, unless it is overwritten. By using a derivation of basic virus scanning software, it is possible to create a string of key text search words to run against the copy disk until you find instances of the use of the words you have flagged.

'Deleted computer files are not lost unless they are overwritten'

On this occasion, we found in the slack space of the computer (the swap file) an extract of extreme importance to our case. It was a part of a verbatim transcript of the recording of an earlier board meeting, using the exact words that appeared on the emails. We also discovered a mailing list with email addresses attached, which matched those who had received the illicit emails.

During the course of the imaging, we searched the suspect's desk and found diary entries, contact details and background material which would later assist our case.

These and other investigative initiatives revealed that the suspect:

- Kept some sophisticated recording equipment in his desk
- Had encrypted part of the hard drive on his computer at work
- Kept a work's laptop computer at home
- Had handwriting which was a near match ot that found on the posted letters
- Had fabricated part of his job application
- Had not sent the email from an office
- Had copied the posted enclosures using the office photocopier
- Had regular meetings in internet cafes with third parties
- Had many journalistic contacts with whom he maintained close liaison
- Had previously flouted internal rules by accessing secure files and databases

'Our client had taken insufficient measures to protect against loss of information'

RISK MITIGATION

We were by now about two months down the line and had been hit with more detailed email and postal campaigns. The pressure was palpable. Clients, customers, and associates were demanding action to limit the haemorrhage of information.

Legal counsel's advice confirmed that the time was right to proceed with a case. We considered the legal defence and the allegations that might arise:

- The case had not been brought in sufficient time without undue delay or procrastination

Ian Johnson Associates Limited (IJA) - Linden Place - Seale - Farnham - Surrey - GU10 1HS.
T: (+44) (0)1252 782664 **F:** (+44) (0)1252 782818. **E:** info@ija.co.uk **W:** www.ija.co.uk

Continued from page 2

- The demands made of the defendant via the courts were not commensurate with the damage
- It was not illegal to intercept the boardroom conversations by virtue of the frequency on which the device operated.
- The defendant had a claim over ownership of the computers we had imaged.
- Our client had taken insufficient measures to protect against the loss of information.
- This was a fishing expedition to get at other people.
- The defendant was not formally reprimanded when previously caught availing himself of sensitive information, establishing a precedent.
- Surveillance was against the defendants right to privacy
- The defendant should be free to write about his experiences.
- The information that the defendant was publishing was in the public interest
- Some of the information had already been substantially published and he was simply adding to it

'The defendant was not formerly reprimanded when previously caught availing himself to sensitive information, establishing a precedent'

BUG-BUSTING OUTCOME

Our team addressed these issues in the affidavit, which succeeded in supporting an ex-parte delivery-up and gagging order. MDR accompanied a solicitor to the home address of the defendant to retrieve items to help prove our case. This was followed, when the court agreed the case to be proven, with undertakings by the defendant to provide financial restitution, and not to discuss the case.

Our suspect, as defendant, admitted that he had sent the offending email and letters and that he had bugged the boardroom. He had encrypted his hard drive to hide the fact that he had downloaded pornography, and had gained access to the database by obtaining the CEO's password. He had sent the emails from an Internet cafe, and by using his WAP-enabled mobile phone with in-built PDA.

LESSONS

- **Bugs happen. They can be discovered by regular communications security audits.**
- **If you do not take reasonable steps to safeguard your assets, the inevitable will happen. Worse still, it will not be too enamoured by your application for injunctive relief.**
- **Conduct comprehensive pre-employment and contractor screening – and continue with it on promotion or change of reasonable role. The person you hired five years ago is now different.**
- **Hardly any business operate without recourse to ICT, but few bother with ICT security.**
- **Forensic science should be used as a standard operating procedure during an investigation.**
- **Business intelligence takes many forms. It is amazing what is available on the internet.**
- **Laws and regulations are there to help protect the rights of individuals and organisations. They must be respected and not ignored. They are also there to defend those who have been wronged, so do not be afraid to use them.**
- **Policies to combat fraud and malpractice work. They should include conflict of interest statements and be cascaded down the organisation from the top. Review the contracts of your senior employees using a specialist employment or fraud lawyer.**

This account includes some changes in chronology and omits some material facts.

If you would like further advice on dealing with a suspected fraud or internal investigation or would like further information regarding our electronic counter measures and communications security audits, call our consultants on +44 (0) 1252 782664 or alternatively email: info@ija.co.uk

An abridged version of this article appeared in Strategic Risk magazine.

Ian Johnson Associates Limited (IJA) - Linden Place - Seale - Farnham - Surrey - GU10 1HS.
T: (+44) (0)1252 782664 **F:** (+44) (0)1252 782818. **E:** info@ija.co.uk **W:** www.ija.co.uk