



Issue 8, June 2005

Risk Advisory

Helping our clients evaluate, manage and mitigate risk

In this issue

2 DIARY

3 Investigating leaks of information

5 What are your rights as an employer?

6 Litigation and remedies

8 Electronic security – firewalls and fake cleaners

9 Security issues in outsourcing

In 2002 we conducted a review of the last 50 fraud investigation cases that we had conducted for corporate clients. As a result of that review we discovered that senior executives commit 72 per cent of all corporate fraud in which sums at risk are more than £1 million – but only one in six face criminal investigation or prosecution. The combined loss to businesses from these cases totalled more than £350 million.

Since then we have conducted many more fraud investigation cases and a review of those cases demonstrated broadly similar results.

Similarly an analysis of the results of the screening undertaken by our employee screening division in 2003 demonstrated that no less than two-thirds (65 per cent) of CVs submitted by job applicants contained lies or inaccuracies. That is misstatement of qualifications, previous roles within organisations, salaries and in extreme cases criminal convictions. In our view employees continue to represent the greatest single threat to corporates.

For corporates which are listed on the U.S. exchanges the secondary consequences of a fraud have become even more acute. The advent of Sarbanes-Oxley, the requirement for CEOs and CFOs to certify as to the adequacy of internal controls and the lack of materiality in relation to the reporting of fraud mean that when a fraud is discovered the regulatory repercussions have the potential to be far greater than the fraud itself.

Regulatory changes in the UK in respect of data protection, human rights and the interception of communications make investigating fraud a potential minefield for the unwary. Similar legislation across Europe creates more bear traps.

To help our clients manage the risks associated with investigating internal fraud, The Risk Advisory Group conducted a joint seminar with Simmons and Simmons on the 26 April. In this edition of **Risk Advisory** we produce the papers given at that seminar. In addition to dealing with the practical and legal issues surrounding an internal investigation we also dealt with the next generation of threat to corporates namely the risks around outsourcing particularly to non UK legal environments and infiltration by service providers.

If you have any questions about any of the papers or would like to arrange a free internal briefing for your organisation please do not hesitate to email me at bill.waite@riskadvisory.net.

Bill Waite
Chief Executive
The Risk Advisory Group



THE RISK
ADVISORY
GROUP LTD



DIARY

To book for any event,
please call Emily
McFadyen on 020
7578 0000 or email at
emily.mcfadyen@riskadvisory.net

2 June 2005

7.45am – 9.15am, London

East-West/Energy Forum: 'What may be the effect of Russia's domestic policy on contracted and future Russian energy supplies to Western Europe?'

BABi Members: £24.50+VAT (£28.79) Non-members: £29.50+VAT (£34.66)

In association with British American Business Inc (BABi)

Speakers:

Oleg Babinov, Head of Emerging Markets, The Risk Advisory Group
Jake Ulrich, Managing Director, The Centrica Energy Management Group
Mark Sullivan, United States Executive Director, EBRD

9 June 2005

2.30pm – 6.00pm, London

Analyse: Operate – Janusian Conference

Free to attend

This year's event will give an insight into the vital but much misunderstood intelligence process and how it underpins both the "war on terror" and security best practice in high risk situations. In particular we will be debating what intelligence can and can't provide to both the good guys and the bad.

Speakers at the conference will include Dr. Paul Cornish - Peter Carrington Chair in International Security Chatham House and Head of the New Security Issues Programme, and Nick Fielding - Senior Investigative Reporter at The Sunday Times.

23 June 2005

8.30am – 9.30am, London

Loss prevention and reputation protection – effective fraud control

Free to attend

A briefing on how organizations can reliably and cost effectively identify their exposure to financial and reputation damage through fraud.

Simon Dawson, Head of Corporate Investigations at The Risk Advisory Group will explain an approach that includes consideration of areas and issues that are not generally considered by audit teams but which are fundamental to effective fraud control. He will consider how the identified risks can be mitigated leading to reduced losses from fraud and a reduced risk of reputation damage.



Investigating leaks of information

//
...investigation
of information
leaks needs to
be considered,
proportionate
and cost
effective.
//

Introduction

Information is power. The uncontrolled dissemination of commercially sensitive information can create the opportunity for fraud and other criminal activity, disrupt business operations, derail corporate strategies and adversely affect stakeholder value.

The investigation of information leaks needs to be considered, proportionate and cost effective. Regard must be paid to obtaining evidence in a legal and ultimately admissible way, especially with regard to the requirements of the relevant jurisdiction. In the United Kingdom, this means that the provisions of data protection, computer misuse and communications monitoring legislation must be considered.

Preliminary considerations

When starting an investigation into a leak of information there are some important preliminary considerations.

The first of these is the formation of an incident management team, normally comprising:

- Senior executive – who should provide strategic direction but not lead the investigation;
- General counsel – to provide legal advice;
- Human resources – to advise on employment issues;
- IT director – in the event that computer forensics is necessary;
- Internal or external investigator.

The functions of the team are usually to:

- Define the investigation objectives;
- Consider what techniques will be used and in particular to consider their legality, cost and benefit;
- Handle adverse publicity;
- Ensure business continuity;
- Approve disciplinary action and litigation after the investigation;
- Implement any control improvements necessary as a result of the investigation.

Scenario – The Board level leak

Let us examine the investigation techniques around a board level leak to a national newspaper – a not uncommon situation faced by companies.

A national newspaper runs a series of articles about a proposed merger. The articles are highly critical of the proposal and contain detailed references to discussions that are known to have taken place at monthly board meetings. There is no obvious pattern in the timing of the articles, however, and no obvious link to any company executive.

Initial response

It is clearly important to define the objectives of the investigation. These would inevitably include the identification of the person responsible for the leaks, disciplinary action against that person and consideration of litigation for an injunction or damages. Having decided on these aims, the next step is to develop a factual matrix on which to base the investigation.

Developing a factual matrix

Identification of the people in the company who could possibly have had access to the information, e.g. through attendance at board meetings or via the minutes of meetings. This may include executive directors, non-executive directors, personal assistants and secretaries.

Identification of the journalist/s who wrote the articles.

Development of a timeline. An invaluable investigative tool, this may show previously hidden links or connections between people, events and times. It may also firmly exclude some potential suspects who might, for example, have been on leave immediately before publication.

Background investigation

Research should next be undertaken into the possible suspects and the journalist/s. This research will be public record and source based and may show hidden relationships or motivation for leaking information: for example, a particular board member may have a relationship with a certain journalist or a non executive director may have a strong objection to the merger.



//
...review the
security of board
meetings.
//

An important part of this stage of the investigation is to review the arrangements for the security of board papers, i.e. their distribution, security, collection and destruction, which may reveal security weaknesses that could have been exploited. It may show that documents have been distributed to unauthorised people (for example by sending a document to an email group without thinking about who is part of that group) or may demonstrate that security is good, thereby limiting the suspect pool.

Another part of this phase of the investigation is to review the security of the board meetings. This review should include a sweep for electronic eavesdropping devices planted in the boardroom, consideration of physical security arrangements (access control, adjacent rooms, human eavesdropping, presence of contractors in the building and so on) as well as how the minutes are recorded, secured and distributed.

Preliminary analysis

At this stage there should be enough information to carry out two analytical steps.

The first is to compare the text of the minutes and what was said at the meeting (these are often different) and the articles for any obvious correspondence. It may be that there are certain unique phrases that have been minuted which also appear in the articles. This can indicate that the person responsible for the leak saw the minutes but did not necessarily attend the meeting.

Conversely, it may emerge that the articles contain unique phrases that were only said at the meeting and were not minuted. This would give a clear lead that the person responsible for the leak must have attended the meeting.

The second step is to compare publication dates with movements of possible suspects. This can show that some may have been on holiday or away on business. While these factors would not necessarily exclude possible suspects, it may be possible to reduce the target population.

Further investigation

Having reduced the list of possible suspects one can now consider further investigative steps, always remembering considerations of legality, necessity and their cost and likely benefit. There are many legal restrictions on investigation in the UK at present and legal advice should be obtained before using any particular technique.

Investigation would normally include:

- Corporate fixed and mobile phone record analysis – known telephone numbers can be analysed and relevant calls can be compared with publication dates, office hours and board meetings;
- Forensic examination of e-mail. It is possible that deleted emails could provide useful evidence;
- Communications monitoring. This can be valuable if it is suspected that the leak is continuing but must be done strictly in accordance with applicable legislation;
- Examination of suspect's computers. This can reveal deleted documents and emails which may provide leads.
- Intelligence-led surveillance. This can be very valuable if it is suspected that the target of the investigation continues to have contact with the journalists.

Conclusion

As with all investigative activity, results cannot be guaranteed but a properly considered and structured approach to the investigation of information leaks has the best chance of yielding results.

Simon Dawson is Head of Corporate Investigations at The Risk Advisory Group. If you would like to know more about corporate investigations, please contact him at simon.dawson@riskadvisory.net



What are your rights as an employer?

//
Employers
should consider
the relevant
employment
contracts and
statutory rights...

//

What does the contract say?

An employer will generally want provisions dealing with:

- confidentiality;
- intellectual property;
- garden leave;
- non-competition for a limited period after termination of employment.

Monitoring of employee communications

An employer should think about various things when considering monitoring:

- Human rights – although this is unlikely to be an issue;
- It will be helpful if there is something in the contract that permits monitoring;
- Data protection means looking at the Monitoring at Work part of the Information Commissioner's Employment Data Protection Code of Practice – an impact assessment is likely to be required which will consider, amongst other things, benefits gained against adverse impact;
- If there is interception of e-mails or calls then the Regulation of Investigatory Powers Act may be relevant – it is still likely to be possible to monitor on the basis of the Lawful Business Practices Regulations.

Investigation

When planning an investigation an employer should look at the Employment Records part of the Employment Data Protection Code. An assessment considering level of intrusion and justification will be helpful.

Dealing with employees who offend (and their accomplices)

Employers should consider the relevant employment contracts (making no assumptions about what these say) and statutory rights (in particular the right not to be unfairly dismissed).

Suspension will generally be permitted and create less exposure than immediate termination. On investigation, from the point of view of 'fairness' the employer will generally want to have the matter investigated (by someone other than the person who is going to make the decision). The employer should follow its procedures before dismissing, most likely the disciplinary procedure.

Philip Bartlett is a Partner at Simmons and Simmons. If you would like to know more about employment law, please contact him at philip.bartlett@simmons-simmons.com.



// ...it may be necessary to take urgent legal action... //

Litigation and remedies

Subject-matter

When considering materials such as software, confidential documents, formulae, designs and so on, the relevant intellectual property rights will normally be copyright and related rights such as design rights/database rights, as well as the protection given by law to confidential information.

The first point to consider is the need to own the relevant rights. Copyright normally belongs to the employer, but remember the position of independent contractors where an express transfer is needed. Such contracts may also seek to preserve certain rights on the contractors' part to use materials independently, and this can cause difficulties. Where contractor documentation is lacking, it may be possible to rely on implied rights, or to negotiate a transfer of copyright later, but this is not ideal.

Copyright generally only protects specific materials and identifiable 'works', as opposed to mere ideas. However, the dividing line between non-protected ideas and protected works is not always easy to determine.

Ideas can be protected if confidential. In relation to confidential information, it is necessary to show that the material has been treated as confidential. Further, once an employee leaves his job, it is difficult to prevent him from using his general skills and knowledge (as opposed to trade secrets of the former employer).

Of course, where an employee or contractor walks off with your materials, or misuses them, there will usually also be a breach of expressly written contract terms – provided the contract has been properly drafted.

The watchword for any action to protect materials against misuse is *urgency*. Any delay in taking action may well be an obstacle to remedying the situation.

Obtaining/preserving Evidence

Where suspicions have been raised, it is often important to preserve evidence, and it may be necessary to take urgent legal action to achieve this. Private investigators or in-house IT specialists (where appropriate) should be used initially. Based on their findings, the options for action include a Search Order or some lesser action such as an application for urgent disclosure. These actions are taken without notice to the defendants, based on affidavit evidence, and there must be full and frank disclosure by the applicant of all potentially material issues (good or bad).

Search Orders (for example, in relation to the Defendant's home, office or vehicles) are drastic remedies and will only be ordered where there is a strong risk of destruction of evidence. Even then, the intrusive nature of the Order may make it difficult to obtain. The purpose of the Order is to search for named items of evidence and copy them/take them into custody. The Order has many restrictions and safeguards in terms of its execution and must be served by an independent Supervising Solicitor.

Defendants in Search Order cases cannot rely on privilege against self-incrimination in relation to intellectual property offences as a ground for withholding material. However, in the recent important case of *O Ltd v Z Ltd*, it was decided that they may rely on that privilege in respect of other categories of offence, even in intellectual property cases.

Next steps

After any preliminary steps as outlined above, there will be another Court hearing – this time with the Defendants present. In the meantime materials obtained must be urgently reviewed. If appropriate, the next step may be an application for an interim injunction pending a full trial, or possibly summary judgment. These would be based on written evidence only.



“Companies should be cautious in taking on employees or contractors who have a history with a similar project for a previous employer.”

On an application for an interim injunction, the Applicant must offer a cross-undertaking to pay damages if the injunction turns out to have been wrongly granted. The Court must decide whether either side would be adequately compensated by damages following trial or whether their position needs to be protected in the interim – this will affect whether or not to injunct the Defendant. The Court will also look at the relative strengths of the parties' cases.

Ultimately, the Applicant/Claimant will be seeking a final injunction, damages and costs. A 'springboard' injunction may be granted in appropriate cases to restrain the Defendant from taking unfair advantage of misuse of confidential information – even after information has entered the public domain.

The position of third party recipients of the material may also have to be taken into account. Once they are on notice, they can normally also be restrained by injunction from misusing the materials, whether on the basis of copyright or breach of confidence. However, the position of 'bona fide purchasers without notice', in relation to remedies for breach of confidence, can be complex, and such recipients may have a defence to an action for injunctive relief.

Practical implications

It is important to consider these issues from the other side of the fence. Companies should be cautious in taking on employees or contractors who have a history with a similar project for a previous employer. If there is any danger of an accusation of copying or misuse of confidential information, full enquiries should be made and 'clean room' procedures and record-keeping rigorously undertaken.

Jeremy Morton is a Partner at Simmons & Simmons. If you would like to know more about intellectual property, please contact him at Jeremy.morton@simmons-simmons.com



// ...all of us,
remain as easy
to dupe as ever

//

Electronic security – firewalls and fake cleaners

You need technology to keep your secrets safe but don't trust it too much – a broad and layered range of security measures gives better protection when things go wrong. Remember that all technologies are flawed in some way and all people can be duped.

Take the German Second World War coding machines – Enigma. The basic version looked like a heavy duty typewriter but its keys and rotors could be configured in 159 million, million, million ways – and the more sophisticated versions for sending orders to U Boats at sea and for Hitler's personal traffic were even more complex. But the allies broke them all through a combination of a single technical shortcoming – no letter could be encoded as itself – and the accumulated mistakes of thousands of operators who failed to follow their very strict instructions properly – sloppinesses like starting every report with "Heil Hitler" or "we have nothing to report" allowing the mathematics dons and crossword enthusiasts at Bletchley Park a priceless crib.

Modern computer security systems are much the same – clever criminals can normally bypass some of their securest features. And people, all of us, remain as easy to dupe as ever.

The Sumitomo Bank heist of March 2005 makes the point nicely. The national hi tech crime unit pulled off its biggest coup to date when it foiled what would have been the biggest bank robbery ever on the UK mainland. A group of criminals managed physically to install spyware on a number of computers in the London branch of Sumitomo bank. Anti-virus programmes usually pick up its presence but it is more difficult to detect if it is not active – in other words if it simply records what is going on but makes no effort to transmit that data elsewhere. The spyware used in this case was probably some sort of key logging software which records all the key strokes made on a computer – thus giving away passwords and protocols. This gave the bad guys

access to key confidential passwords and details that allowed them to access the bank's mainframe and instruct it to pay out large sums of money to selected accounts across the world. Luckily police in both the UK and Israel became aware of a major breach in the bank's computer security last October and were lying electronically in wait for the criminals to make their move.

The criminals' plan was very simple. Infiltrate the office disguised as office cleaners. Attach key logging devices to the relevant computers, garner the secret information on the computers – probably again through the use of office cleaners – not just passwords and security but the step by step process for ordering and then authenticating large scale money transfers. No need for any high tech hacking – just a passive device on a computer. The first criminal made his move in Israel earlier this year and was quickly picked up by the Israeli police.

The fitting of devices onto computers by bogus cleaners hardly merits the term high tech. The lesson of this celebrated case is that no security is ever perfect. But a spectrum of measures can give reasonable protection in depth. Yes you do need expensive software to protect your system from ever more sophisticated hackers – but you also need the humble locked door or suitably vetted cleaning company.

Crispin Black is a Director of Janusian Security Risk Management Ltd. If you would like to know more about security risk management, please contact him at black@janusian.com



Security issues in outsourcing

// ...offshoring greater volumes and more complex functions will affect a company's risk profile... //

One of the most important factors to consider prior to outsourcing a service or business process is whether the supplier can be trusted to keep data and confidential information secure. Recent security scares involving information brokers and outsourcing vendors have highlighted the risks of trusting a third party with sensitive data. Late last year, Choicepoint, a company that collects information on most US households and is a leading provider of identification verification services, allowed criminals posing as legitimate businesses access to the personal data of approximately 145,000 individuals.

More recently, 16 employees of Indian BPO vendor Mphasis were arrested in connection with bank fraud. The suspects have been charged with stealing money from customers of Citigroup, a major client of Mphasis. This has been the first high profile Indian BPO security scare and coincided with a report from the Financial Services Authority on the risks of offshore outsourcing.

While the FSA concluded that offshoring is not inherently more risky than outsourcing domestically, provided that there is suitable risk monitoring, it did issue a warning to those considering sending work offshore: '[The main risk of offshoring is] the complexity of achieving suitable management oversight and control from a distance.' It said UK companies using offshore strategies have formal oversight structures, but offshoring greater volumes and more complex functions will affect a company's risk profile, particularly in relation to operational risks. Similarly, research company Gartner has said that by the end of this year, security and privacy concerns would replace human capital issues, such as job losses, as the most important offshore-related issue.

What can a customer do to mitigate the effects of such risks? Contractually, it is essential that security be factored into the drafting of the contract to ensure that there is an appropriate risk apportionment between the parties; and commercially, the customer

should have a clear understanding of the vendor's strategy for handling security breaches and ensuring business continuity.

In particular, there are four key areas of the contract that require attention:

- Ownership and protection of personal data
- Audit
- Service levels
- Exit management

Ownership and protection of personal data

It is vital for a customer to ensure that control is maintained over confidential data provided to a vendor. This can be achieved contractually through well drafted confidentiality provisions with appropriate restrictions on how the vendor may use or distribute such information. For example, the vendor should not be allowed to store the customer's data on any system or system media that may be shared by any third party. And upon expiry or termination of the contract, the customer must make sure that they have appropriate rights to have information or data returned or destroyed.

In addition, the seventh principle of the UK Data Protection Act should also be reflected in the contract. This principle, which requires that appropriate technical and organisational measures be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, is extremely wide-ranging. It requires organisations to take measures to prevent unlawful, as well as unauthorised, processing of personal data – with another strand being the need to protect against accidental mishaps involving personal data. The easiest way of achieving this contractually is to devolve the legal obligation on the customer – who will generally be the data controller – to the outsourcing vendor and ensure in addition that the vendor is required to act on all instructions of the customer. It is also vital that the customer retain the



“...there may be an increased risk of a breach if the vendor drops their guard...”

flexibility to change the operational procedures concerning the data if required.

Audit Rights

It is essential to have rights of audit set out clearly within the contract – the right should include both electronic audits, if appropriate, and physical audits of the premises. Such rights should allow the right for the client, and their representatives, to access at any time and without restriction the facilities used by the supplier, their personnel and relevant data and records relating to the services. A customer may also want the right to conduct random ‘spot checks’ of the vendor’s compliance with security requirements under the contract.

It is also important that the right of audit extend to the vendor’s sub-contractors or agents, and a customer should have the contractual right to seek the vendor’s assistance not only in audits of their own systems and staff, but also in obtaining audits of sub-contractor’s systems and staff.

Service Levels

Service levels provide an important tool for customers to maintain oversight of the performance of their services, but also provide an early-warning device for potentially serious security problems. Accordingly, it is important that service levels measure both large and small problems so that the cumulative effect of many small outages can be measured and dealt with – doing so may well lessen the chance of a problem becoming more serious.

It is also useful to have detailed service-level agreements that focus on specific outsourcing security issues (for example, identity and access management controls, time frames for closing dead accounts and access to sensitive data).

Exit Management

During the latter stages of a contract, a vendor may begin ‘winding down’ the services and, from a security perspective, there may be an increased risk of a breach if the vendor drops their guard. Careful management of the exit process is therefore crucial and this should be started prior to the contract’s signing, with discussion and planning of the exit process for the contract. Developing in the contract a procedure whereby the parties will jointly draft an exit plan within a short time of the contract starting can be a way of ensuring the issue gets early attention and is not forgotten once the contract gets under way. Negotiate clauses that ensure the vendor provides assistance not only to the customer, but also to any replacement supplier, to minimise the chances of data getting lost in the transition. A customer should also give careful consideration to what aspects of the supplier’s technology and systems may be needed in continuing the service provision after the end of the contract.

Being proactive about the security provisions of the outsourcing deal is essential to retaining an appropriate level of control over the vendor. Vendors must be kept to a high standard of performance through the use of service levels and monitoring and audit rights, with the customer retaining the flexibility to introduce additional controls if required.

Peter Brudenhall is a Partner at Simmons & Simmons. If you would like to find out more about information technology law, please contact him at peter.brudenhall@simmons-simmons.com