



---

T K M T E C H N O L O G I E S ( U K ) G R O U P

---

tkmtechnologies

*Discovering the whole truth*

t: +44 (0)1773 770 267  
f: +44 (0)1773 770 268  
e: enquiries@tkmnet.co.uk

[www.tkmnet.co.uk](http://www.tkmnet.co.uk)

## Language Information

TKM Technologies is actively involved in work in a number of countries around the world. Our standard business language is English but we can correspond and provide written or oral reports in a number of other languages, including Spanish, Portuguese, German, French, Arabic, Chinese and Japanese.

For more information, or if you require a copy of this brochure in a different language, please contact us.

## Confidentiality and Privacy

Many of our clients - both existing and prospective - trust us to exercise a duty of confidentiality when handling their sensitive business information. We take this responsibility very seriously and information you share with us during the course of our business relationship will never be passed to a third party unless we are obliged to do so by a Court order or other legal instrument issued by an authority of competent jurisdiction.

## Expert Advisors from Complimentary Disciplines

Occasionally, your case may involve issues outside our core area of expertise (for example, clarification of points of national law). We regularly work with legal teams and experts in other disciplines to compliment our own skills and experience and we will make recommendations to you should the need arise. TKM Technologies is an independent corporation and we do not receive benefits for these recommendations.

*TKM Technologies is an independent company. We work with business, law enforcement and government to extract and interpret evidence from computer systems.*

*We provide an effective defence against those who seek to misuse information technology to facilitate or hide criminal activity and civil misdemeanour.*

Table of Contents	1
Who We Are	2
The People	3
Data & Evidence Recovery	4
Computer Security	5
Fraud	6
Intellectual Property	8
Corporate Corruption	9
Parallel Trading	10
Staff Poaching	11
Documentation & Policies	12
Notes	13



International Headquarters  
96a High Road, Beeston  
Nottingham NG9 2LF UK  
t: +44 (0)1773 770 267  
f: +44 (0)1773 770 268  
e: [enquiries@tkmnet.co.uk](mailto:enquiries@tkmnet.co.uk)  
[www.tkmnet.co.uk](http://www.tkmnet.co.uk)

E&OE © TKM Technologies Limited 2005 All rights reserved.

*“...specialists in investigative information technology forensics and legal procedure...”*

TKM Technologies comprises a range of skills in investigation, information technology, forensics and legal procedure. With a combined total of more than 27 years experience in the field of investigations and risk management, TKM's two Executive Directors have been helping corporations and law enforcement agencies to handle business-critical issues both within their own organisations and involving third parties.

Our investigative expertise has helped law firms, administrators and corporations to recover more than US\$110million in cash and assets.

Our services span more than 20 countries including Germany, Japan, Singapore, Australia and the United States and we report to clients in more than 12 languages.

TKM's extensive experience and professional, discrete approach has helped us to build a close relationship with leading companies around the world. When it comes to protecting your business, there is no better partner than TKM Technologies.



## Thomas K Moore



In 1994, Thomas began working in computing as a hardware engineer. Having gained experience of a number of hardware, software and procedural standards, he became, in 1997, an Executive Director of TKM Technologies Limited.

Specialising in business systems, Thomas worked with a number of major corporations including banks, airlines, law firms and accountancy groups. Increasingly, he began to investigate security-related issues and advise companies on ways to prevent, handle and investigate breaches of internal security.

In 1999, Thomas handled the recovery and analysis of electronic evidence in the liquidation of Flowtex Technologie GmbH (Germany). After the successful recovery of material assets in this major insolvency case, Thomas went on to specialise further in the retrieval and analysis of computer-based evidence.

Since 1999 Thomas has recovered and analysed evidence in a variety of civil and criminal cases. He has presented testimony to Courts in England, Germany and France and is recognised as an Expert Witness by Courts across Europe. He has worked in conjunction with regional High-Tech Crime Units of the British police and his corporate clients include some of Europe's largest businesses.

Thomas is an accredited Member of the British Computer Society and a Member of the Expert Witness Institute.

Thomas is TKM Technologies' Director of Forensic and Investigative ICT.



# Data & Evidence Recovery

## What is it all about?

Recovering information from computers and storage media which has been destroyed, damaged or tampered with. This includes the recovery of data from equipment which has been physically damaged.

## Why is it important?

Because of their range of everyday use, computers often hold revealing evidence of a person's actions. This can prove invaluable in civil or criminal investigations and can be pivotal in establishing motive, method and ultimately guilt or innocence.

Data can usually be recovered from computer systems even after extensive attempts to delete or hide it. Even severe physical damage can leave behind sufficient trace elements from which to reconstruct useful evidence.

## The Problem

Because of the ease with which computer-based data can be manipulated, great care must be taken during recovery and analysis to ensure that forensic handling procedures are properly observed. Without such diligence, an accused party might justifiably claim that the evidence is unreliable and inadmissible. These procedures include using the correct methods for seizing computer equipment and the use of approved analytical software tools by properly qualified specialists.

The use of correct handling procedures becomes even more important when evidence has been intentionally modified or deleted. Recovery and reconstruction in such cases is often possible but only with the correct expertise and preparation.

One of the most common barriers to successfully recovering evidence is the inappropriate handling of computer equipment before it reaches a forensic specialist; the key is to involve a TKM data recovery expert at the earliest opportunity.

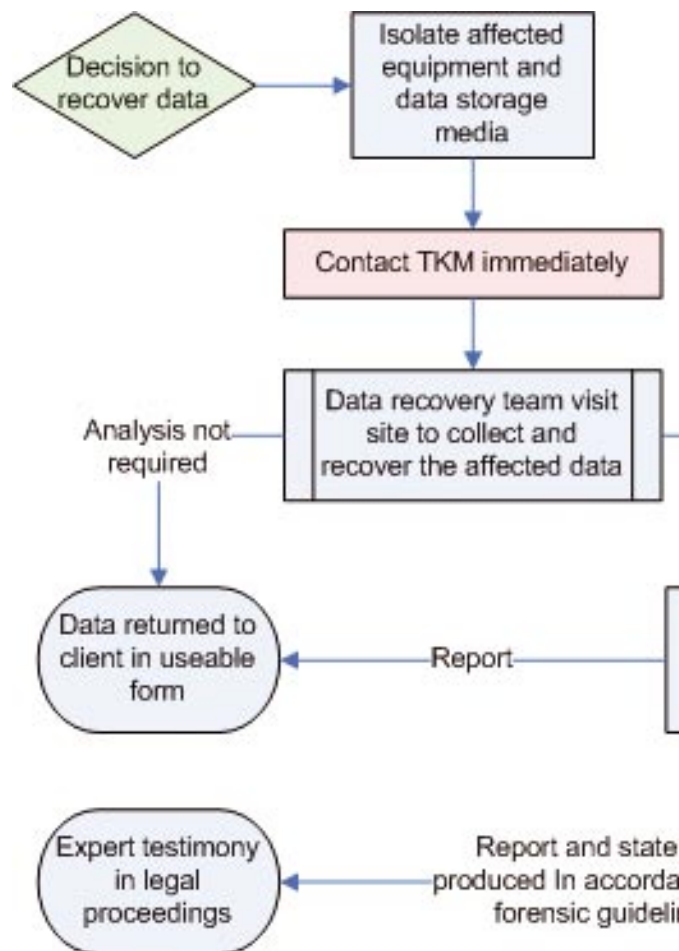
## The Solution

Retrieving electronic evidence in a format which is both usable and forensically sound requires immediate specialist involvement.

Early consultation with a TKM forensic computing expert will provide you with sound advice on what to do straight away to increase the likelihood of successful data recovery.

Usually, this immediate advice is given by telephone and followed-up within 24 hours by a visit from the same recognised TKM forensic specialist, who can secure the evidence and begin detailed analysis using approved forensic tools and procedures. The process concludes in the presentation of a full report, complete with exhibits, which conforms to the highest standards required by law enforcement agencies and Courts around the world.

If you choose to pursue criminal or civil recourse, TKM's reporting standards and expert testimony will provide a reliable basis for your case.



## What is it all about?

Ensuring the security of computer systems and the information they hold. This includes protecting information from unauthorised duplication and deletion and guarding electronic communications (such as e-mail) against eavesdropping.

## Why is it important?

In a modern business, the information held on computers is often far more valuable than the computers themselves. The theft of designs, financial information, client lists and business planning documents would all represent a major threat to long-term business stability. The unauthorised deletion or modification of this same data could have catastrophic consequences for any business which relies on computer-based information for decision-making.

## The Problem

Physical assets such as buildings and equipment can be protected by door locks and security cameras but information is more difficult to safeguard. Perhaps the most significant challenge is to identify when information has been stolen and by whom. Then begins the specialist task of determining how many copies of the stolen data have been made and where they are stored.

Unlike physical assets, data can be duplicated and distributed across the world in moments, so a rapid response is vital if the culprits are to be identified and the propagation of valuable business information is to be halted.

## The Solution

No matter how slight the suspicion, cases of data theft should be investigated as soon as possible. Involving TKM as soon as the first indications of a problem come to light can prevent widespread embarrassment and expense.

Upon receiving your telephone call, a specialist from TKM will discuss your suspicions with you



confidentially and we will use our combined expertise to recommend a course of action. TKM can then discretely investigate the problem and identify the parties involved. By adhering to forensic and investigative procedure, the case that we build during our investigation can be used to support civil or criminal action against those involved if you chose to pursue such a solution.

In any case, a thorough investigation by TKM will protect valuable business information and provide peace of mind for investors, clients and company officers.

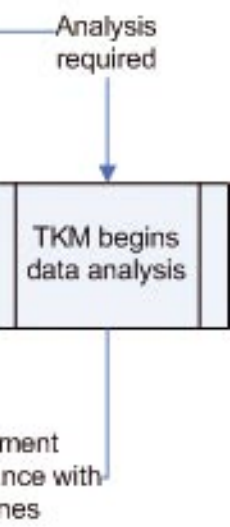
## Data Recovery - Your First Actions

Data recovery is heavily reliant upon ensuring that the equipment or storage media concerned is isolated at the earliest opportunity.

Contact us as soon as you have a need for data recovery services by calling +44 (0)115 9253060. Follow the advice you are given during the call.

In the meantime, the following steps will increase the likelihood of successful data recovery:

- If the data recovery involves equipment such as computers or handheld PDAs, do not allow anyone to use this equipment. Do not move it unless absolutely necessary and try to isolate both the equipment and the surrounding area.
- In the case of removable media such as floppy disks, CD-ROMs and external storage devices, place these in a secure location away from heat and magnetic fields. Do not attempt to use them.



## What is it all about?

Investigating instances where the dishonest activities of an employee, Board member or third party may be adversely affecting company finances, reputation or legal compliance.

## Why is it important?

Fraud directly affects the profitability of a business and jeopardises its continued existence. Fraud can damage the reputation of a company, destroy investor and client confidence and leave an organisation open to criminal charges.

Reported fraud in the United Kingdom increased by 116% in the first six months of 2004 to GBP£435 million, compared with the same period in the previous year and this trend is echoed around the world. This growth is fuelled in part by the reduced physical danger and less severe penalties which fraud attracts compared with other forms of crime.

The proceeds of fraud are rarely recovered in their entirety and even a successful conviction against the perpetrator can leave the victim financially ruined. Criminal prosecutions can take in excess of two years and the complexity of fraud over such a long period of time can be difficult to communicate in a courtroom.

## The Problem

Part of the problem is that there is no strict definition of what constitutes fraud. Broadly, it is any situation where deception is used to gain an advantage to which the perpetrator is not entitled. More specifically, fraud usually falls into one or more of the following categories:

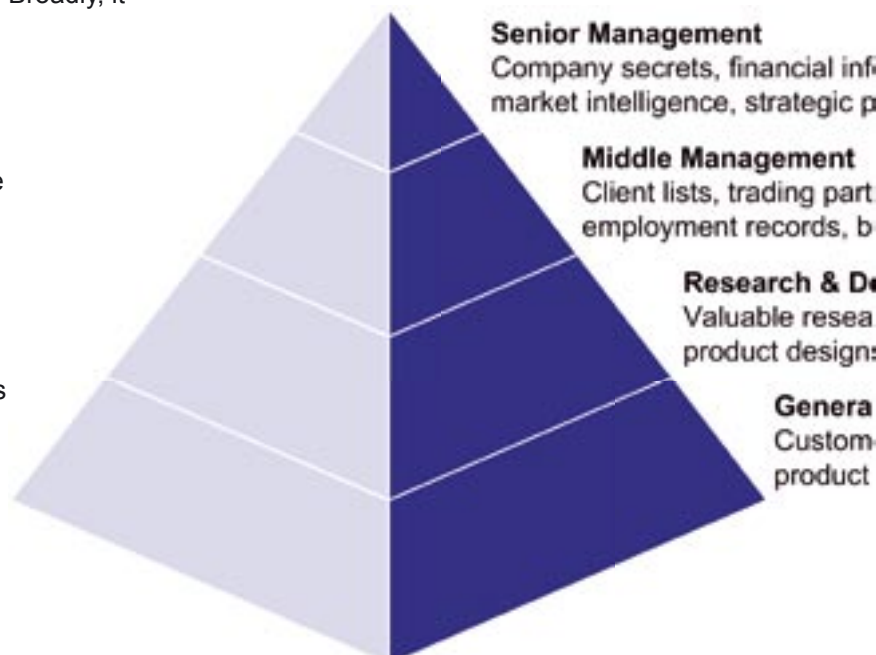
**False accounting** involves dressing up company figures to hide losses, exaggerate or hide profits and thereby attract investors and win contracts. The recent Enron and Parmalat scandals are examples of false accounting.

**Asset misappropriation** occurs when company employees, management and Directors - possibly in collusion with third parties - conspire to steal assets from a business. This could mean the theft of stock, intellectual property, client lists, price lists or money through payroll fraud or inflated expenses claims. Kickbacks or bribes which lead an employee to act against the best interests of a business and the preferential award of contracts to third parties where there is an inside interest are other examples of this type of fraud.

**Trade fraud** involves the fraudulent use of import / export documentation and letters of credit such as happened in the case of the trader Milton Kounnou, who defrauded ten Middle Eastern banks to the sum of GBP£105million in a scheme involving fictitious metal shipments and was later imprisoned for two years.

**Investment fraud** relies on persuading investors to contribute to investment schemes which are either inaccurately described or non-existent.

**Computer and e-fraud** is a relatively new mechanism by which to carry out traditional fraudulent schemes. Computers can be used to electronically steal funds, intercept financial transactions and divert intellectual property in a way which requires new detection and investigation techniques.



## The Symptoms

More than likely, the perpetrator of a fraud is known to the company involved. In a recent survey in the UK, company employees were found to be responsible for 30% of fraud and management were responsible for a further 55 - making a total of 85% of fraud the result of inside jobs.

Opportunity is a key factor in committing fraud. The more trusted members of a company, such as bookkeepers, Directors and senior management - all of whom may work long hours with time alone in the office and access to privileged information - are the most likely to commit fraud.

There are some key warning signs of fraud and spotting these early can reduce the impact of fraud and the damage to a business:

- lack of complete management accounts
- poor recovery rate from debtors
- uneven turnover
- unusually high stock levels
- lavish corporate entertainment and high standards of living
- a dominant individual controlling a submissive Board
- high turnover of legal and accounting advisers
- excessive working hours and reluctance to take vacations
- inadequate credit checks on customers who later turn out to be uncreditworthy
- poor response to queries from management, colleagues, suppliers and auditors
- excessive payments to 'consultants'
- management preoccupation with share price

## The Solution

Prevention is better than cure and there are ways of making a business less vulnerable to

fraud. Careful screening of employees, staff training, the use of 'whistle-blowing' procedures and the structured deployment of technology can all help to reduce the opportunities for committing fraud and make it more detectable.

## Fraud Statistics

- Organisations lose an average of 6% of their total annual revenue to fraud committed by their own staff.
- The median loss caused by males is US\$185,000 and by females US\$48,000.
- The typical perpetrator is a well-educated male.
- Executive employees cause more than 16 times as much fraud as their staff.
- Occupational fraud includes asset misappropriation, fraudulent statements and bribery and corruption.

No matter how many safeguards are in place, fraud can still occur and when it does, the key to damage limitation is early detection. An early investigation of any of the above symptoms can save time, money and reputation. By the time you are absolutely sure that fraud is taking place, it is often too late to control the damage.

In contrast, fraud investigation can be a delicate matter. The most revealing and conclusive investigations are those where the perpetrators are unaware that they are being examined until it is too late to hide the evidence. Inconspicuous investigation has the added advantage of being invisible to the media, investors, share holders and clients.

Completing an investigation which is both low-key and thorough relies on TKM's blend of highly experienced ICT and financial expertise. With early involvement, TKM has already helped a number of businesses and public sector bodies to avoid the damage to finances and reputation which fraud can cause; if you recognise any of the symptoms above, contact TKM right away.

Information,  
Plans  
Owners details,  
Business strategy  
Development  
Research data,  
Future plans  
Staff  
Relationships,  
Samples, contracts

## What is it all about?

Protecting copyright, trademark and patent from third party infringement. This includes safeguarding designs, ideas and branding as well as finished products.

## Why is it important?

Intellectual property is at the core of any business with a portfolio of unique products or services. A company's ideas and designs may take a great deal of time and money to develop and this investment must be protected against plagiarism.

Carefully balanced marketing strategies may be destroyed by oversupply of imitation goods to a particular market. Worse still, inferior copies of a product which bear the original manufacturer's brand name can damage a company's reputation for quality and safety.

## The Symptoms

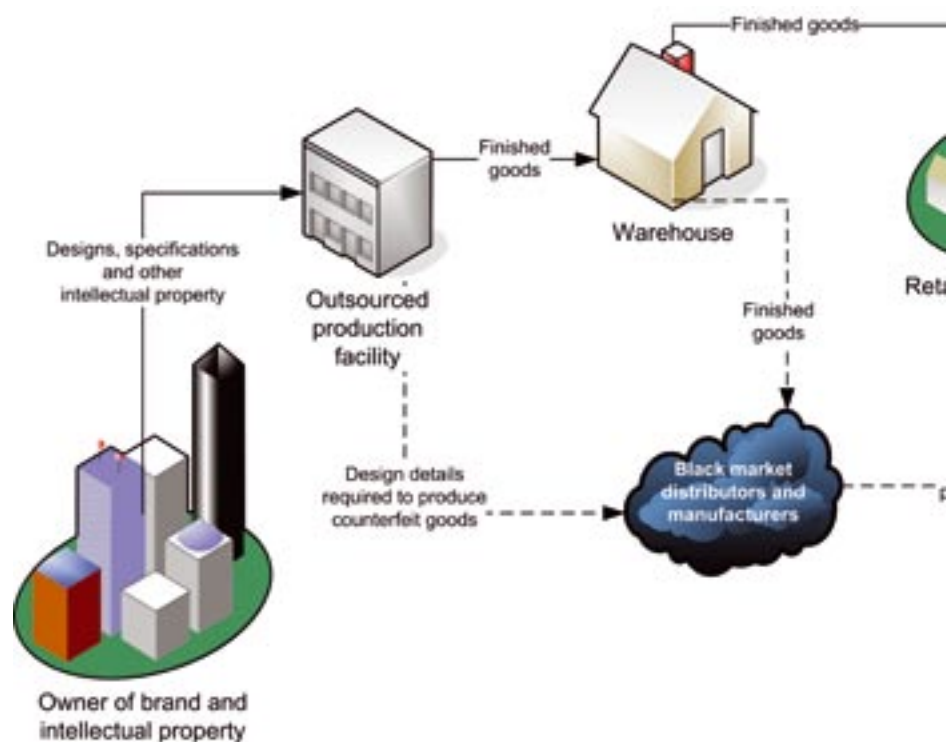
Often the first indication that intellectual property rights (IPRs) have been infringed comes when sales in a particular market decline despite strong consumer demand. This suggests that imitation products are entering the market either under the same brand name or as clear rivals. Sales of products in restricted markets and sales by unauthorised agents, dealers or retailers can also indicate that counterfeit goods are in circulation.

In many cases, imitation products and services are brought to light by dissatisfied consumers, who complain to the brand owner in the belief that they have made a genuine purchase.

## The Solution

Whether the product is automotive parts, electrical products, cigarettes, clothing or pharmaceuticals, IP investigations usually follow a similar pattern. TKM will begin by determining the identity of the seller, which is often disguised in the increasing number of Internet-based transactions. From this starting point a thorough investigation is begun to establish the point of manufacture, the trail of revenue and the extent of the infringement. Liaison can then be undertaken with civil or criminal law enforcement agencies to put a stop to manufacture and distribution as well as taking civil redress for damages where appropriate.

In the case of service-based infringement, the process is very similar, with a shift in emphasis from the product lifecycle to the flow of information. In both cases, TKM will use recognised investigative and reporting techniques which allow a case to build as the enquiry progresses. The result is a robust and reliable report which can form the basis of civil or criminal proceedings.



## What is it all about?

Investigating cases where individuals with significant influence or decision-making powers within an organisation are unfairly exercising their authority to the possible detriment of the business in return for financial reward or other personal gain.

## Why is it important?

Business stability and long-term growth rely upon the guidance and decisions of qualified senior staff. If these decisions are motivated by personal gain then the decision-maker is no longer acting in the best interests of the business and may behave in a way which damages the company either directly or in terms of reputation and image.

## The Problem

Those in senior positions within a business often have a free rein over the day-to-day decisions they make even though their actions can affect shareholders, investors and other senior staff. Because of the hierarchy of accountability, there is often no need for such individuals to justify their decisions until action has already been taken. Where the true interests of the business govern management decisions, this structure works well but it becomes potentially dangerous when executives make decisions based on an opportunity for personal gain.

There are wider-ranging implications for businesses which are subject to regulation either formally by Government or informally by investor interests. The biased awarding of contracts, selection of expansion sites, cartel agreements and 'under the table' dealings can all tarnish a company's image and often precipitate civil or criminal action. In the worst cases, history has recorded the collapse of companies of all sizes as a direct result of corporate corruption.

## The Symptoms

Business decisions generally follow logical reasoning and it is an early warning sign when this trend is broken, especially where an



individual or other business stands to benefit significantly as a result. Preferential allocation of contracts, research projects and acquisitions in the absence of supporting evidence might all indicate the presence of an undeclared incentive.

Unexplained accounting holes and incomplete legislative documentation are the hallmarks of far more serious corruption and are often discovered during the investigation of company insolvency and fraud.

## The Solution

In virtually all cases, corruption occurs through personal gain being placed above corporate responsibility. This usually results in a trail of money or other benefits which TKM can trace to identify the individuals involved.

Just like legitimate business, corruption does not succeed without planning and communication. TKM should be involved immediately that suspicions are aroused to recover e-mail traffic and computer-based evidence which might yield valuable insight.

Investigation of corporate corruption is challenging and delicate work and TKM utilises a blend of highly experienced ICT and financial expertise to ensure that business stability is not compromised by the pursuit of personal gain at the expense of business security.



# Parallel Trading

## What is it all about?

Goods being bought and sold wholesale by third parties between markets and customer groups where third degree price discrimination normally exists.



## Why is it important?

The practice of parallel trading is a significant threat to revenue for many multifunctional companies who sell their goods at different prices to different markets. By trading between these various markets, parallel importers offer customers a way to circumvent pricing policies, reducing profitability for the manufacturer.

Importing branded goods into a market where the local trademark owner has not given consent leaves the importer of these so-called 'grey goods' liable to injunctions, claims for damages and stock seizure.

## The Problem

Parallel trading has traditionally been a major problem for the pharmaceuticals industry but the practice now affects any manufacturer of goods who supplies to multiple markets.

Through the sale of grey imports, manufacturers lose out but the practice of imposing market supply quotas has so far proved ineffective.

Even the most diligent companies experience difficulties in identifying genuine cases of parallel trading. It is true that a price difference between the source and destination markets is a necessary condition but the issue is complicated

by factors such as product availability, ease of establishing a stable supply line and the magnitude of the price difference.

Predicting the flow of grey goods isn't always straightforward. The assumption that goods will pass from traditionally 'low cost' markets to 'high cost' ones in an oversimplification. There is documented evidence of pharmaceuticals, for example, being exported from Country A to Country B despite being more expensive on paper in Country A. In this case, the drug involved was supplied to hospitals in Country A at a discount and it was this hospital stock which was being exported.

Consumers are increasingly aware that grey goods are not necessarily of inferior quality and attempts by manufacturers to restrict long-term support for their goods to originating markets only (for example, vehicle servicing) has fuelled the growth of an industry dedicated to the support of grey imports.

## The Symptoms

Unexplained fluctuation in demand for a product in a specific market is a common symptom of parallel trading.

Foreign packaging, poorly translated instruction booklets and batch modifications can also indicate that goods have been imported from a different market.

## The Solution

TKM can identify trends in product supply to determine the likely source and destination markets for parallel trading, before conducting enquiries into regional distributors.

Once the likelihood of parallel trading has been established, TKM will monitor the physical shipping of sample batches of goods to identify their exact route from supplier to consumer. Using sophisticated tracking technology and supply line analysis, TKM can work across geographic boundaries to determine the extent of the problem and identify the parties involved.

## What is it all about?

Preventing the loss of valuable staff members and the skills they possess to competitors.

## Why is it important?

Staff are the backbone of any organisation, small or large. As such they are a valuable commodity to any business both in terms of the labour they offer and the skills and knowledge they possess.

## The Problem

Members of staff who offer a company more than just their labour - research skills, specialist knowledge, close client relationships and so on - are usually retained on contract whereby their usefulness to a competitor organisation is restricted either permanently or over a period of time. This reduces the potential for the staff member to move their labour to a competitor.

Nevertheless, successful approaches of staff by competitors do occur and are sometimes successful even with the tightest employment contracts in place.

## The Symptoms

The grade of staff members usually involved in cases of poaching is such that they have relatively complex employment arrangements, possibly involving a range of benefits and incentives. Any move to a different employer means securing better employment terms and this usually requires discussion between the staff member and the potential new employer.

Much of this negotiation will typically be conducted in person and may necessitate the individual taking time away from the workplace. This 'holiday' time will often be arranged at short-notice and will be sporadic and distinct from more normal vacation time.

Other methods of communication will also be used and these might include e-mail and telephone. Uncharacteristic use of these facilities could indicate discussions with a third party and might be particularly suspicious if the

employee is secretive or reacts with unusual sensitivity to polite queries.

Careful collation of research notes, client contact details and other valuable information is often a symptom of an impending move and this could have more serious implications in terms of the loss of intellectual property to the new employer.

## The Solution

TKM can take an objective view of the actions and situation of a staff member and provide an assessment of the likelihood that a case of staff poaching exists.

Once this has been determined, we can conduct a thorough investigation of the staff member and their prospective new employer. We can examine trends in the company data accessed by the employee as well as taking steps to ensure the security of valuable intellectual property.



All of TKM's investigations in cases such as these are designed to be subtle and unobtrusive to avoid the risk of alienating the suspect employee in the event that there is no imminent danger.

## Acceptable Use Policies

As cybercrime becomes more prolific, the owners of corporate computer equipment are increasingly being held responsible for the actions of users. Downloading pornography, sending offensive e-mails and posting defamatory messages are all examples of actions by staff which have landed their employers in hot water.

Unfortunately, companies which have tried to distance themselves from the actions of their staff by dismissing the offenders often find that they face a barrage of legal challenges and employment issues.

The solution is to make sure that staff are clearly aware of what they can and can't do with company ICT equipment and the best way of doing this is to have a clear and comprehensive acceptable use policy. Once all staff members have signed up to the agreement as part of their contract of employment, it becomes a simple matter of procedure to police ICT usage.

To make sure your business is covered by a comprehensive ICT acceptable use policy, TKM offers a full consultation service, during which we examine each area of ICT usage in your business and deliver a use policy which covers practically all eventualities.

## Procedural Policies

There are many routine procedures which are pivotal to the ongoing operation of a safe and secure corporate ICT system. Unfortunately, many of these are overlooked in the busy schedule of a typical IT department.

TKM has developed a range of procedural policies which can help your ICT staff to keep on top of routine security tasks such as password changes, expired user removal, access rights review and so on.

With input from your own ICT staff, we can assemble a schedule of operations, each of

which is accompanied by a concise guide to best practice. By following this calendar, you can be assured that you are taking reasonable precautions to protect your ICT infrastructure without tying up staff resources or compromising usability.

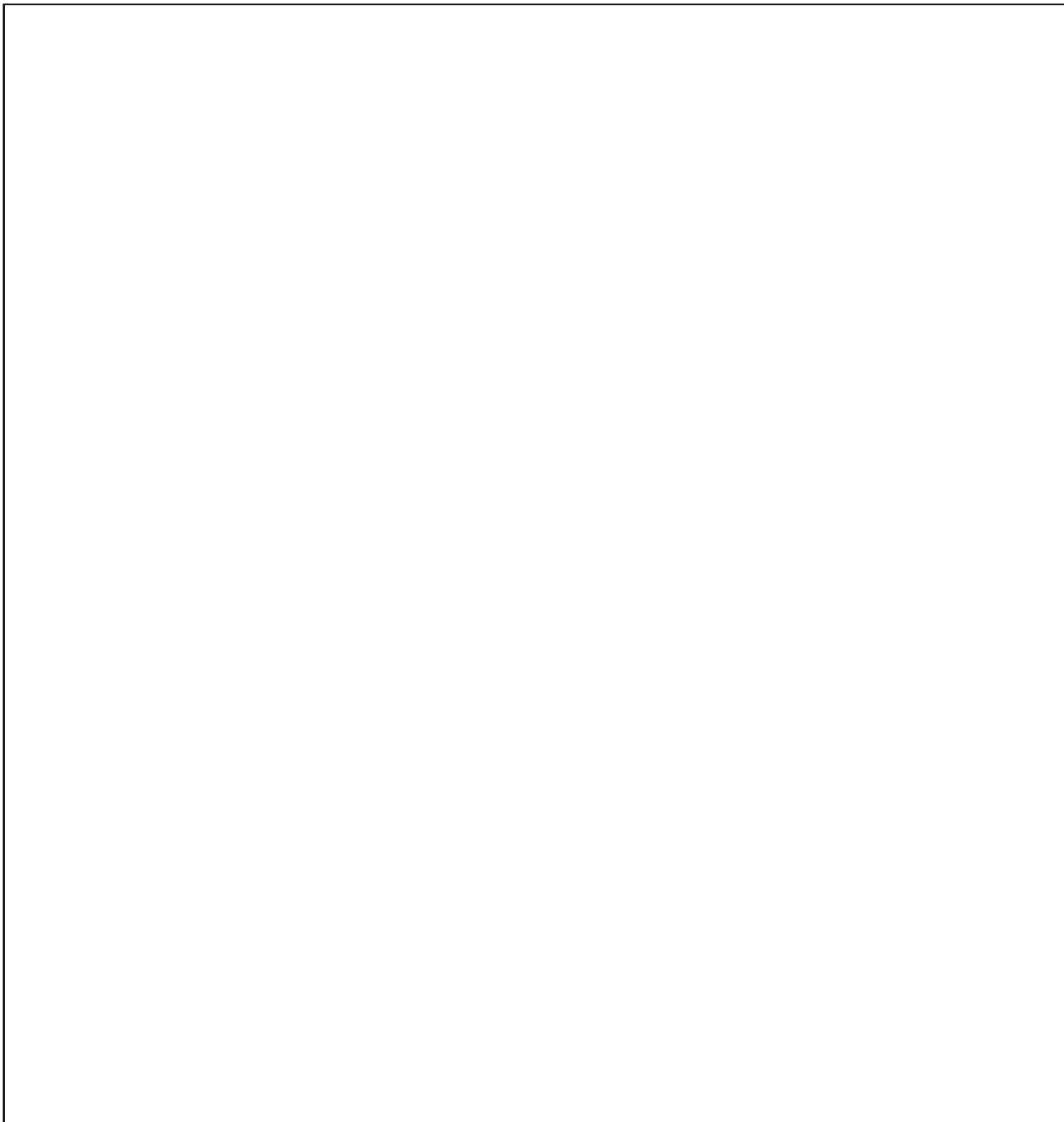
## Incident Response Manuals

For medium to large organisations, it is important to have a clearly defined and documented procedure for dealing with incidents involving ICT equipment. This avoids the sort of improvised approach which can lead to incomplete investigation and unreliable evidence.



The scope of a written incident response manual varies depending on the size and complexity of your organisation. In any event, making sure that front-line technical staff are briefed on procedure is the best way of ensuring that any incident is handled properly and with the greatest chance of successful resolution.

TKM provides a number of pre-defined procedures as part of our incident response manuals, each of which has been designed with evidence handling and legal considerations in mind. Any custom procedures are first approved by our legal advisory team before incorporation in a response manual to make sure that they provide adequate protection in the event of civil or criminal proceedings post-incident.



International Headquarters  
96a High Road, Beeston  
Nottingham NG9 2LF UK

t: +44 (0)1773 770 267

f: +44 (0)1773 770 268

e: [enquiries@tkmnet.co.uk](mailto:enquiries@tkmnet.co.uk)

[www.tkmnet.co.uk](http://www.tkmnet.co.uk)

International Headquarters  
96a High Road, Beeston  
Nottingham NG9 2LF UK

t: +44 (0)1773 770 267

f: +44 (0)1773 770 268

e: [enquiries@tkmnet.co.uk](mailto:enquiries@tkmnet.co.uk)

[www.tkmnet.co.uk](http://www.tkmnet.co.uk)