

FORENSIC

# Succeeding in Turbulent Times – Are you fighting information theft?

ADVISORY

May 2009

## Information theft – a high risk, a low priority?

In the current recessionary climate, many employees are uncertain about their futures. Each week there are fresh announcements of job losses across industries. Financial pressures continue to mount for individuals due to a stagnant housing market, savings rates at historic lows, uncertainties over pensions and crashes in stock prices.

It is perhaps unsurprising, that employees are more likely to be tempted, in these uncertain times, to act improperly and against the interest of their employer to preserve their own financial interests.

There is a danger that they see an opportunity in exploiting the valuable and potentially sensitive data that your business holds – by either selling or taking it to competitors, or using it to set themselves up in a competing business.

### Are you vulnerable?

Have you considered how vulnerable you are as an organisation to such misconduct by employees, and are you actively and effectively fighting information theft?

### In this issue

A rising trend	2
The perpetrators	2
Information theft to secure the next move	3
What information was stolen?	4
Rationalisation – “I did it because...”	4
How they got away with it	5
Industries at particular risk	6
Preventing data theft	6
Responding to data theft	7
Conclusion	8

This bulletin considers the following issues:

#### A rising trend

KPMG and Mishcon de Reya (MdR) have analysed over 100 employee-related data theft cases on which they have acted over the past three years, revealing an increase of more than 100% during that period.

#### The perpetrators

The vast majority (69 percent) of the data theft instances reviewed were carried out by either males operating alone or by groups of male employees.

#### Information theft to secure the next move

In 23 percent of cases, the reason for the data theft was to establish a competing business.

#### What information was stolen?

By far the most common data stolen was customer or client-related information (relating to customer relationships, levels of trading, pricing information, profit levels and so on) or customer lists.

#### Rationalisation – “I did it because . . .”

Many bright careers are now on hold whilst organisations assess the effects of the credit crisis and economic downturn.

#### How they got away with it

The most common method for employees to transfer stolen data was via email.

#### Industries at particular risk

Our analysis also looked at the business sectors where data theft is most common.

#### Preventing data theft

A focus on preventing, rather than only reacting to, incidents is essential.

#### Responding to data theft

Even if you have sophisticated data security controls, you may be caught out.

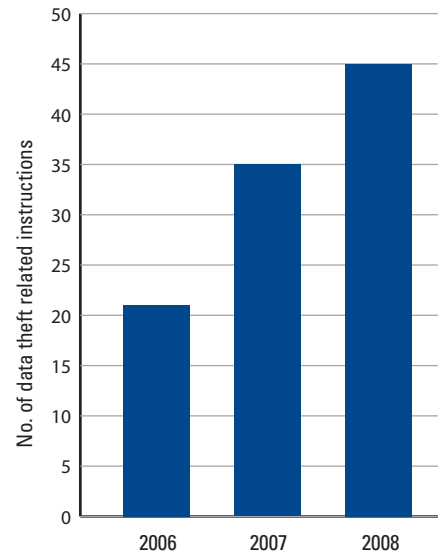
## A rising trend

KPMG and Mishcon de Reya (MdR) have analysed over 100 employee-related data theft cases on which they have acted over the past three years.

Our analysis highlights a number of common features:

Cases of data theft have risen year on year, more than doubling between 2006 and 2008 and culminating in 46 cases in 2008 where forensic investigation and legal redress was sought by the employer to protect its business interests.

In the current economic climate, the number of such incidents is almost certain to increase. KPMG's Data Loss Barometer predicts a 10 percent increase in reported incidents of data loss in 2009, some of which will inevitably be through deliberate design and intent to steal data. **Are you prepared with an effective response plan in order to minimise the potential damage to your business?**



Source: KPMG and Mischoon de Reya

## The perpetrators

The vast majority (69 percent) of the data theft instances reviewed were carried out by either males operating alone or by groups of male employees. Our analysis shows that only 22 percent of the data theft incidents were committed by women or groups of women. Nine percent of incidents involved both males and females.

Whilst many of the thefts were carried out by individuals, in a number of cases, larger groups were involved. In about 10 percent of cases, data theft was perpetrated by teams of employees working in conspiracy against their employer, either to set up on their own or to join an existing competitor. In one case, up to 15 employees were involved in a concerted conspiracy to defraud their employer through the theft of proprietary information.

Alarming, the study shows that in the vast majority of cases (93 percent), employees had already left the employer before the thefts were discovered. This is clear evidence that companies are not doing enough to prevent and detect information theft in a timely fashion.

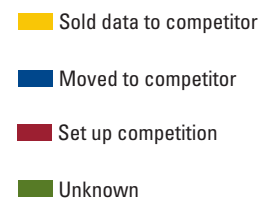
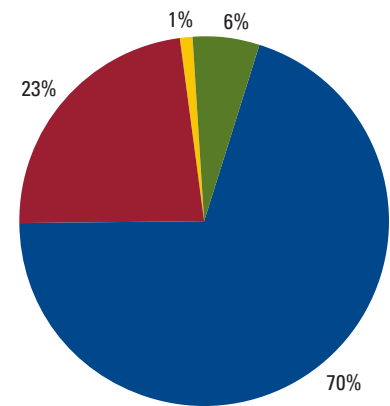
Even where companies had put restrictive covenants in place into employment contracts to protect their business, these appear to have had little deterrent effect. In 69 percent of cases, such covenants were breached by those stealing data. Tightly drafted restrictive covenants were key to obtaining restraining orders against offenders after the data theft had taken place.

Employers need to consider how vulnerable key business data and its value is to employees, especially opportunist male employees who appear to have little respect for business confidentiality or their contractual (and moral) obligations to their employer.

## Information theft to secure the next move

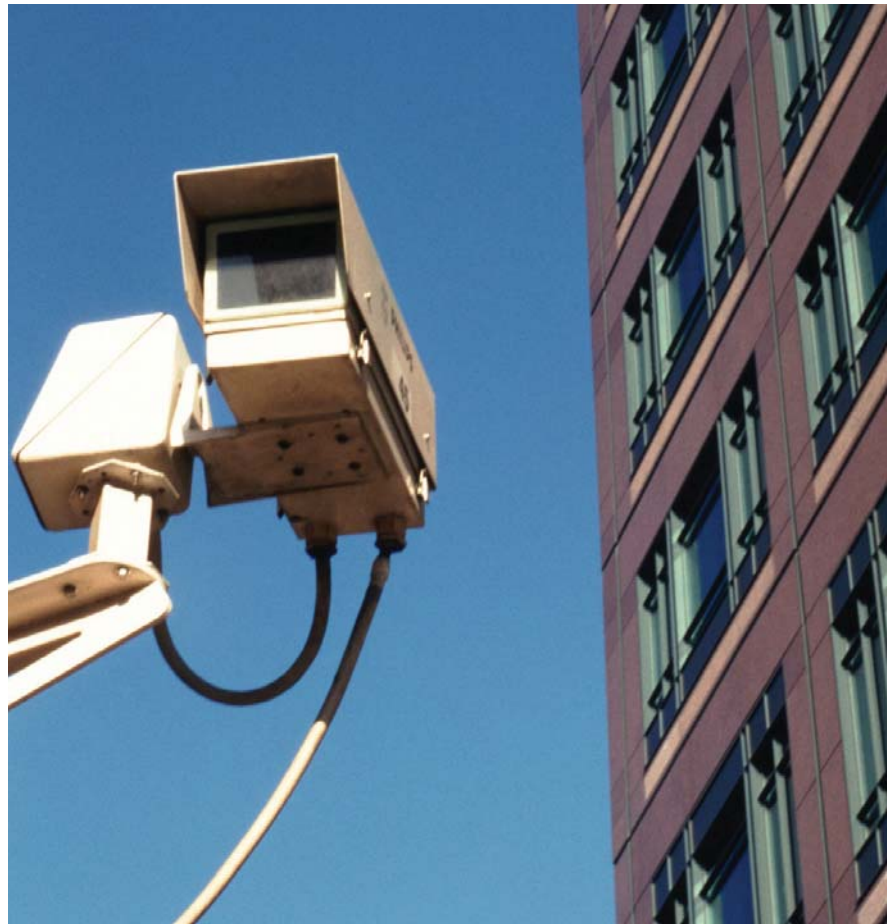
In 23 percent of cases, the reason for the data theft was to establish a competing business. In 70 percent of cases, the perpetrator(s) moved to work for a competitor company. Such data often proves to be part of a 'dowry' that an information thief brings to secure employment with a rival. This also raises serious questions about how much a new employer needs to know about the nature, and source, of information that a new employee brings with them.

In a mere 6 percent of cases, the intended use of the data was unknown, the theft having been discovered before it was clear what the data thief planned to do. In such cases, the person stealing the data may have taken it as 'insurance', in case it had potential value in the future.



Source: KPMG and Mischcon de Reya

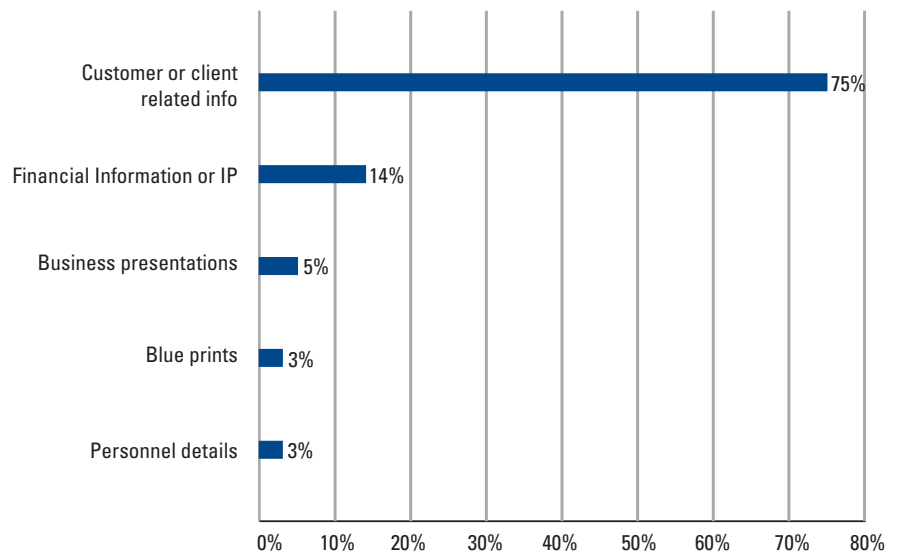
Employees are more likely... in these uncertain times to act improperly and...see an opportunity in exploiting the valuable and potentially sensitive data that your business holds.





## What information was stolen?

By far the most common data stolen was customer or client-related information (relating to customer relationships, levels of trading, pricing information, profit levels and so on) or customer lists. This occurred in 75 percent of cases. Financial information (such as internal accounts, business plans, projections and forecasts) represented 14 percent of thefts. In 5 percent of cases the data stolen was proprietary business presentations. However, even blueprints and personnel details were subject to theft, with these categories of data each being stolen in 3 percent of cases respectively.



Source: KPMG and Mischcon de Reya

A recent e-Crime Survey commissioned by KPMG and AKJ Associates supports the view that insiders and former employees represent a significant threat to business. Results drawn from the responses of over 250 IT personnel in Europe show that 63 percent of respondents believe that customer data is at risk from insiders or ex-employees, and that 61 percent of respondents consider that intellectual property or business sensitive information is at risk from this group. Asked what business assets were most at risk, 75 percent of respondents identified customer data, 59 percent considered customer identification data at risk, with just over 50 percent of respondents also identifying account information and password or log-in details at risk.

## Rationalisation – “I did it because . . .”

Many bright careers are now on hold whilst organisations assess the effects of the credit crisis and economic downturn. The so-called ‘Generation Y’, often defined as those born between the mid-70s and 2001, but also referred to as the ‘net generation’, have grown up in a booming world economy. They have often enjoyed rapid career progression and lucrative rewards. Generation Y employees are sometimes seen as being most loyal to themselves. With careers stalled or stalling, some may regard the theft of sensitive data – whether to take it to a rival

business or use it to start up their own venture – as the most effective way to restart their own professional and financial progression quickly.

The analysis shows that those who were caught stealing data justified their actions either by claiming that the information was already in the possession of the competitor (60 percent) or that the information was already in the public domain (30 percent). The latter highlights the challenge of defining what data within your business should be considered proprietary, and also when and why it may be construed as publicly information.

In 10 percent of cases, no defence was offered by the perpetrator when the theft was discovered.

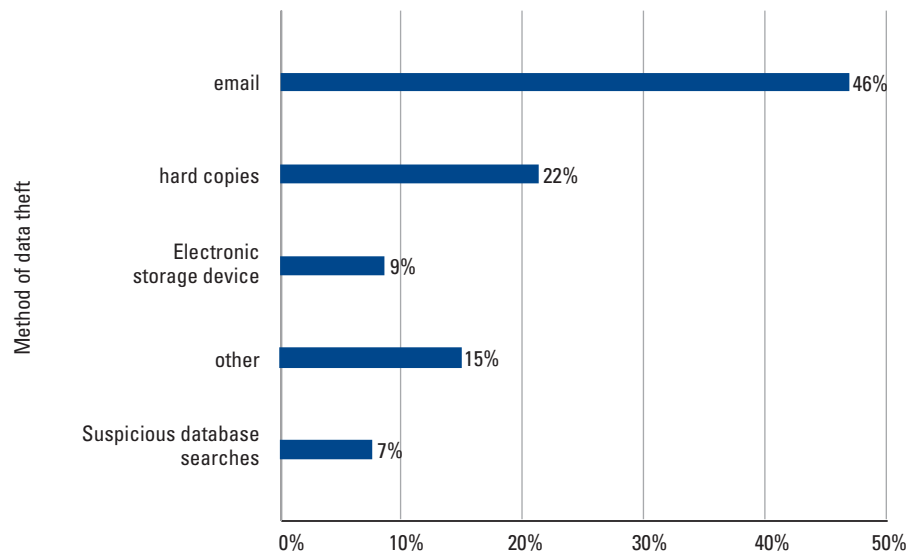


Cases of data theft have risen year on year, more than doubling between 2006 and 2008.

## How they got away with it

The most common method for employees to transfer stolen data was via email. In 46 percent of cases examined, this was used as the primary route to improperly remove proprietary data from the business. Taking hard copy print-outs of data was the method employed in 22 percent of cases. Surprisingly, the use of USB memory sticks, data CDs or DVDs was only present in 9 percent of cases despite their low cost, relative ease of use, and (in the case of USB sticks) small size. This may be an indication that data thieves are relatively unsophisticated, or that they simply do not believe they will be caught. Organisations can use forensic tools and techniques to capture digital evidence of such electronic data theft. The analysis also found a case where someone had installed software on a system that facilitated the recording and theft of data.

The misuse of newer technologies is likely to become more prevalent since data can easily be stolen using smart phones, iPods, digital cameras and other types of digital media. Social networking websites have also provided data thieves with a way to remove data in at least one case. Generation Y is, of course, very familiar and comfortable with such technology.

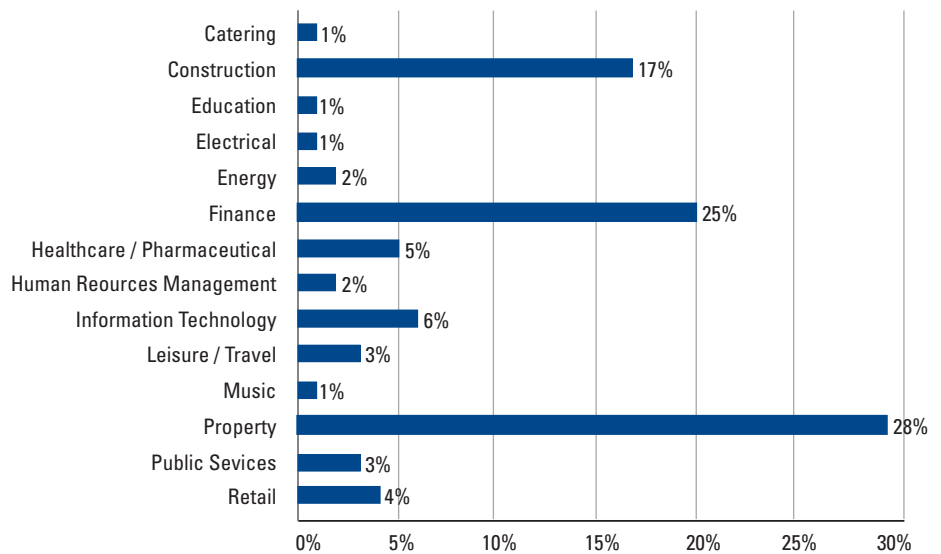


Source: KPMG and Mischcon de Reya

## Industries at particular risk

The analysis also looked at the business sectors where data theft is most common. Businesses operating in or servicing the property, finance and the construction sectors accounted for more than 70 percent of all cases, and it is these sectors that are under particular pressure in the current economic climate.

However, the study also shows that data theft is a problem across many business sectors. It can therefore be concluded that if data is held electronically, and if it has value to someone else, then it is vulnerable.



Source: KPMG and Mischcon de Reya

## Preventing data theft

A focus on preventing, rather than only reacting to, incidents is essential. Employers should consider the resources currently deployed to assess and manage the risks to their critical business data.

Information security guidelines must be up-to-date and communicated clearly to all data users within the business. These should give clear guidance on when, where, how and what data may be moved. Encryption and close control over who has access to data may provide additional lines of defence.

Consider the questions below to gauge how well this is currently being done:

- Do you have measures in place to mitigate the risk of data theft by employees? How would you detect such theft?
- Can you, and do you, enforce restrictive covenants in employee contracts with respect to theft or misuse of proprietary data?
- Are you aware of the forensic and legal steps you can deploy in the first instance to protect your position and mitigate the business impact?

This is clear evidence that companies are not doing enough to prevent and detect information theft in a timely fashion.

- Have you had any incidents of data theft in your organisation in the last two years? How would you know if this had happened?
- Does your company have a high staff turnover? Is it a business which relies upon proprietary information for its ongoing viability?
- Are employees aware of threats to sensitive data, would they recognise warning signs of attempted theft and the implications for the business?
- Does your business, or business sector, suffer from a culture of data theft?

If you are unsure about the answers to any of these questions, you may need to review your existing procedures relating to theft of proprietary data.

## Responding to data theft

Even if you have sophisticated data security controls, you may be caught out.

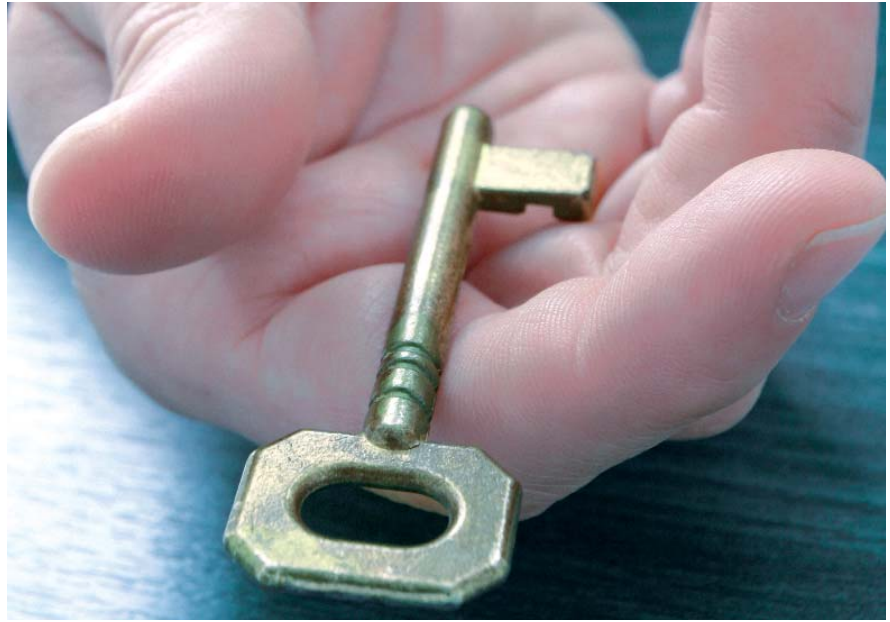
Where a data theft is discovered or suspected, a decisive and immediate response is essential. By doing so, you may be able to minimise potential loss, take effective legal action against perpetrators and recover stolen data before its release causes you damage.

Of the 100 plus incidents handled by Mishcon de Reya, the average time from instruction to legal relief whether in the form of restraining injunction, undertakings, damages or apologies was just over two and a half weeks.

In more than 55 percent of the cases, specialist forensic technology or forensic investigation services were required to image computers, to retrieve emails or to quantify the financial impact from the theft of the proprietary data.

In many situations, where a competing business is being set up, specialist corporate intelligence researchers can provide you with evidence of the timing behind such action, the names and addresses of those involved, and even identify others in your business who may continue to pose a risk. Such research can be a key part of building an effective legal case against the rogue employees.





For more information contact



**Hitesh Patel**  
Partner

KPMG Forensic  
Tel: +44 (0) 20 7311 3571  
e-Mail: hitesh.patel3@kpmg.co.uk



**Dan Morrison**  
Partner

Fraud & Insolvency Group,  
Mishcon de Reya  
Tel: +44 (0) 20 7440 7124  
e-Mail: dan.morrison@mishcon.com

## In conclusion

Data theft by employees is a real threat to organisations, particularly in the current economic climate. There is likely to be a rising trend in employees attempting to steal confidential data for their personal benefit when leaving their current employment. Businesses can take effective action both to respond to actual and attempted thefts of data, and to minimise the risk of data being stolen in the first place.

Effective data protection policies, and creating a climate where everyone recognises the value of—and need for—integrity in handling sensitive commercial data, is vital to prevent data theft from taking place.

KPMG and Mishcon de Reya both have extensive experience in assisting clients protect their data. For further information please contact us using the details to the left.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2009 KPMG LLP, a UK limited liability partnership, is a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. Printed in the United Kingdom.

KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.

Designed and produced by KPMG LLP (UK)'s Design Services

Publication name: Succeeding in turbulent times

Publication number: RRD-137721

Publication date: May 2009

Printed on recycled material.