Data Loss Barometer
Insights into lost and stolen information in 2009

Reputation at risk
Data loss can seriously damage a brand

Identity theft
Have you put too much personal information online?

Real or fake?
Screening out the dishonest job seekers

Insider knowledge
Are your employees leaking valuable information?
Data may be as valuable as gold, yet it can slip through your fingers like water...

In the digital age, protecting information has become a major priority for almost all organizations. If it gets into the wrong hands, your business could suffer. If the media hear about an embarrassing leak, your reputation could plummet. At the same time, holding on to data is becoming much harder, because information can now be stored and accessed in a greater variety of ways and in ever larger quantities.

In this publication we look at some of the ways data can be lost or stolen, using the latest findings of the Data Loss Barometer; our research into worldwide reports of data loss incidents. We also consider how to build an infrastructure and a culture that are geared towards keeping information secure – and which can respond swiftly when under threat.

As the global recession has led to an increase in intellectual property theft, now is the time to shore up your defenses.

MALCOLM MARSHALL
Partner
Information Protection and Business Resilience, KPMG in the UK

For an online version, go to wwwdatalossbarometercom
Data Loss Barometer
Insider leaks and other trends in lost and stolen information

Vetting staff
There’s more to hiring a credible employee than being impressed by his CV

Brand protection
A data loss incident can have serious repercussions for your reputation

Incident response
A well-drilled outfit won’t be caught out by a major security event

Trusting third parties
Outsourcing work can raise a whole new set of data security concerns

Succeeding in turbulent times
Are nervous employees sizing up your valuable data before they jump ship?

Portable media
When memory sticks go missing, you could lose more than just minor hardware

Preventing data leakage
How to stop vital information flowing out of your organization

Social networking
Why posting your pet’s name online could jeopardize your personal finances
THE ENEMY INSIDE

Malicious insider leaks were up by more than 50% in the first six months of 2009, according to the latest KPMG research

More and more people are being tempted to steal vital data from their employer – data that could be used in a crime or passed to competitors. This is one of the main findings of the 2009 Data Loss Barometer, KPMG’s analysis of lost and stolen information.

“A combination of economic pressures and tempting offers from organized criminals has led some employees to see theft as an option,” says Edge Zarrella, Global Head of IT Advisory for KPMG. Such a claim is supported, to take just one example, by the case of a U.S. employee working within an HR department who stole information on at least 10 fellow employees. He passed the information to a relative who used it to open accounts and buy thousands of dollars worth of goods. And earlier this year, a senior manager of a financial institution in Japan, with privileged access to its systems, stole and sold-on its entire customer database.

“People are often the weakest link in the chain,” says Zarrella, “so it’s more important than ever to keep a firm control on those individuals with access to sensitive internal systems and data.”

This rise bucks the overall downward trend in reported data loss in 2009. Almost a third fewer cases were reported than in the first six months of 2008. There are two possible explanations for the fall. Firstly, following several high-profile incidents in 2007, many organizations are more aware of the need to protect information. Secondly, media focus has shifted onto the wider recession.

The impact of data loss continues to rise, however, with more than 110 million people being affected during the first six months of 2009. A large portion of this figure relates to a breach at Heartland Payment Systems, where more than 100 million credit/debit card details were allegedly accessed by hackers. The incident is at present one of the largest data breaches in U.S. history.

Government plays catch-up

While many sectors are upping their game and reducing cases of data loss, one big exception is government. There has been an 18 percent increase over 2008 – and almost 30 percent over 2007. This is particularly worrying given the high public and media attention in such cases.

“It’s more important than ever to keep a firm control on those with access to data”

© 2009 KPMG International. KPMG International provides no client services and is a Swiss cooperative with which the independent member firms of the KPMG network are affiliated.
Tip of the iceberg
The Data Loss Barometer has recorded almost 2,300 data loss incidents, that have affected more than 700 million people. But, since the majority of breaches go unreported, this is likely to be just the tip of the iceberg.

One industry that appears to have got its act together is the financial services sector, which has seen incidents of lost information fall by more than two-thirds.

“Financial information and intellectual property is highly valued by an identity fraudster or criminal”, comments Zarrella, “so it is encouraging to see banks and other institutions placing greater focus on protecting this data.”

Despite such encouraging progress, he warns against complacency. “At a time when fraud in general is on the increase, criminals will continue to look for ways to access personal accounts. So financial companies cannot afford to take their eyes off the ball.”

What’s on that laptop or memory stick?
Although the theft of laptops is still the most common of all data security breaches, the total number of such incidents has almost halved since 2008. There has also been a significant drop (of 20 percent) in the number of portable media (USB keys, BlackBerrys, mobile phones, etc) that have gone missing, although cases are still all too common where personal data is inadequately protected. In Norway, a USB key containing records of psychological evaluations was lost and eventually found in a public car park.

It’s possible that such cases are so commonplace that they go unreported except in exceptional circumstances – for example, when memory sticks containing millions of names go missing. Such was the case in Germany, where a telecommunications
THE METHODOLOGY

The Data Loss Barometer analyzes data loss incidents reported around the world since 2005. This data is freely available in some countries thanks to legislation that requires full disclosure of data loss incidents. In other countries, information is obtained via KPMG’s network of international firms and consultants. Key information sources include the media, internet searches and independent news or data feeds.

Care is taken to use data only from reputable and independent sources. Availability, consistency and accuracy of information can vary between sources, countries and by type of incident.

A list of the information sources used is too large to include in this publication but particular thanks should go to the Open Security Foundation who have provided invaluable support and information.

company lost a disk containing details (names, addresses and contact details) of 17 million customers in 2006, only for the incident to be reported in 2008 following news that the data had been offered for sale on the internet.

And, as Zarrella warns, these devices are holding ever-increasing amounts of information. “You’re only one high-profile incident away from potential disaster,” he warns. “Organizations should be fully aware of the risks and have a platform for internal incident reporting and analysis.”

When it comes to theft of portable devices, criminals are likely to care less about the actual devices than the data they contain, which could be used directly or traded on the black market. Encryption of laptops and other portable devices should therefore be a minimum requirement. However, our research shows that, for 2009, no protection measures had been applied to at least 24 percent of lost or stolen portable devices.

Encryption is not an option for plain hard copy, of course, and the casual discarding of such papers continues to pose serious security risks. Incidents of improper disposal of hard copies are up by nearly a quarter this year, suggesting that many companies should look again at their handling of confidential waste.

“‘You’re only one high-profile incident away from potential disaster’

No room for complacency

Despite there being fewer than expected data losses in the first half of 2009, the continuing economic slowdown could well see the number rise to match the record tally of 2008 (703); malicious theft being a particular worry. Moreover, the trend in data loss reporting could also be on the rise, says Zarrella: “One of the potential influences [of this rise] is possibly the changes to laws on disclosure of lost data.”

It is likely that many national governments may mandate the public notification of data loss incidents, particularly in Europe where the e-Privacy directive has recently introduced a data breach notification requirement. The U.S. and, to a lesser extent, the UK have provided the bulk of reported cases to date, but Zarrella predicts that may change. “Don’t be surprised when the media start to take more interest once these laws are passed. We may start to hear a lot more from Europe, Asia-Pacific and beyond.”
An intruder at the gates

The person you’re interviewing may not be who they claim to be. Careful vetting of candidates should reduce the chance of criminals infiltrating your organization

By David Chernick, KPMG in the UK (david.chernick@kpmg.co.uk)

With unemployment rising and vacancies falling, some people can’t resist the temptation to cheat their way into a job. That’s depressing news for honest jobseekers, forced to compete with ever more brazen CV liars.

It’s also bad news for employers. As more and more candidates chase fewer positions, already under-resourced HR departments must cope with floods of application forms.

So how can organizations build a strong defense against phony intruders?

SCREENING OUT THE CRIMINALS

Inevitably, some employers have stronger controls than others – particularly if they’ve been victims of such crime in the past. In addition, many sectors and professions stipulate staff vetting regimes to protect themselves and their stakeholders.

But, worryingly, even more wary, risk-averse employers can often unknowingly grant access to identity fraudsters, CV/resumé liars – and worse. And that’s usually because either they don’t have the right policies and procedures in place, or if they do, they’re not executing them properly.

One common mistake is the vetting of potential employees by recruiters in the HR department who are more focused on the hiring than the background checking of employees. That hints at a conflict of interest within the onboarding process. Another trap is to trust candidate-volunteered sources, who could masquerade as ‘friendly referees’. Such
people may help to conceal earlier dismissals for dishonesty or to vouch for false qualifications.

**REAL OR FAKE DOCUMENTS?**
Anyone who’s had to check passports or visas knows that it’s almost impossible to spot the difference between a fake and the genuine article. Yet the onus is usually on the employer to ensure that any recruits are entitled to work in their country. And the problem isn’t getting any easier, as false documents are increasingly offered for sale on the internet.

The passport scanners found at most airports use highly sophisticated technology. Armed with such equipment, plus ‘watch lists’ of suspects, they can spot fakes in seconds. Fortunately, such scanners are becoming far more affordable, which should help to ease the worries of employers. Just make sure the person who turns up for work is the same one who presented the genuine ID during the recruitment process. Security badges with an employee photograph should be a basic control.

**RESUMÉ LIES**
Lies or exaggerations on CVs and resumés are nothing new. Recent research by the internet job site Monster suggests that up to a third of candidates would be prepared to lie on an application form to secure a new job. Phony qualifications, exaggerated job titles, misrepresented employment dates and concealed dismissals for dishonesty are popular fabrications. Just as worrying, too many employers still rely on candidate-supplied contact details for referees who may supply glowing but false references.

**TAKING A PRAGMATIC VIEW OF RISK**
Many employers struggle to decide what checks to make when recruiting, and end up either doing too much or too little. One simple approach is to build up a ‘risk matrix’ by considering the risks facing your organization, and the potential impact of different job roles on those risks. It’s definitely worth using an objective and skilled facilitator when you’re putting a matrix together. He or she should be someone from outside the business or the department in question.

**CHECKING INTERNATIONAL CRIMINAL RECORDS**
This task is complicated by the long list of differences between countries of what constitutes a crime, the reliability of convictions, the quality of data, and the ease of access to or even availability of records. Thankfully, the Centre for the Protection of National Infrastructure (CPNI) in the UK now publishes practical advice on how to undertake criminal records checks in 48 of the most commonly sought countries. They also include pointers for companies needing to maintain personnel security in offshore locations, especially within shared service centres, and those who face the challenge of recruiting offshore staff.

"Make sure the person who turns up for work is the same one who had the genuine ID when he or she was recruited"

**KEEPING ONE STEP AHEAD**
Fortunately for employers, there’s more information and support available these days than ever before as victims, law enforcement agencies and counter-crime experts increasingly join forces to reduce the harm caused by employment fraud. But well-networked and determined criminals won’t stop trying new ways to infiltrate organizations. Effective employment screening should be vigilant in keeping abreast of the fraudsters’ latest techniques, and constantly deploy better checking regimes. •
A security breach can seriously damage your reputation, so make sure you’re fully prepared should the worst happen

By Neil Stinchcombe, Director, Eskenzi PR (neil@eskenzipr.com)

When data goes missing or hackers break into your network, your first instinct may be to minimize the immediate threat to customers, employees and your business as a whole. However, many companies find themselves rushing to contain the incident without a well-prepared and coherent brand protection plan.

Surprisingly, in many countries, there’s currently no law obliging organizations to publicize a breach. But trying to keep a lid on events can be risky. After all, you won’t look particularly clever if angry customers first hear about an incident through the media.

What’s the worst that could happen?

Before you react with a major publicity offensive, it is important to assess the potential harm that the breach could cause to your reputation.

Data such as medical or financial records are highly sensitive and affected parties should be informed straight away. On the other hand, some data losses are undoubtedly less serious and, if they’re swiftly resolved, loyal customers may well be kept happy with a letter of apology.

In 2008, for example, a major credit card provider sent out several thousand account statements containing personal information on other customers. The risk from this mix-up was deemed to be fairly insignificant and the company simply reissued the correct statements along with letters of apology.

On the other hand, some incidents may have financial repercussions and damage reputations. In mid-2009, a financial institution was fined more than US$5m (€3.5m) for failing to protect customer data from theft or loss. The penalty was reduced from over US$7m (€5m), due to their cooperation with the regulators to resolve the security matters quickly.

Offer clear instructions

All those affected should be told the steps (if any) they need to take to protect themselves. Similarly, you should clear the path for the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

In 2007, an unencrypted laptop belonging to a large retailer was stolen. It contained personal information on thousands of its employees, so the firm wrote to every one of those employees offering free credit checks to monitor suspicious activity.

Timing is critical

In some cases, though, immediate notification may not be the most appropriate action, as the case of another retail firm illustrates.

Having discovered that hackers had broken into customers’ payment details in 2006, it held back from making the news public while the police investigated. The delay proved you won’t look clever if customers first hear about an incident through the media.
crucial and led to several arrests and criminal charges. The company finally broke its silence with a press release providing a free phone number for customers, and advice that further information was available on its website. It also apologized unreservedly for the breach and outlined how its customer security had been improved. You never know when the worst may happen, so it pays to be prepared. In today’s 24-hour media goldfish bowl, organizations have to manage their image proactively to ensure they don’t get caught out. Above all, don’t make the all-too-common mistake of trying to deny or cover up what’s happened. This will only drop you in even deeper water and could destroy your credibility for good.

**Damage limitation in six steps**

Don’t simply wait passively for the unthinkable to happen. Your communication strategy should combine careful preparation and fast, decisive action, as any delay in response could be interpreted as a cover-up. But if, in your haste to act, your statement is ill thought-out you could look as if you don’t take the incident seriously. And remember, you may even find that a swift, appropriate response can actually enhance your reputation as a responsible organization.

1. **Put someone in charge** Establish who is responsible for containing and investigating a breach and for forming an incident response team.

2. **Form an incident response team** You’ll need input from individuals across the organization, including corporate communications, senior executives (as spokespeople), IT, HR and Legal. You may also have to involve external stakeholders and suppliers. Meet regularly to share information, brainstorm and update the plan.

3. **Have a clear plan** Identify the types of data you store and the various potential risks posed by its exposure. That should determine the appropriate action required to counter such risks. Work out who you may need to contact, what to tell them and how to reach them, taking into account different time zones. Once a breach has occurred, you should explain how and when it happened, what steps you have taken, and offer clear advice on how anyone affected can protect themselves.

4. **Involve third parties** You may also need to consider notifying the police, your insurers, other professional bodies, bank or credit card companies and other stakeholders. You should produce and regularly update a directory including relevant contact details.

5. **Role playing** By staging a simulated incident, you’ll get a good view of how ready you are to deal with the real thing, and be able to adjust your plans accordingly.

6. **Media Relations** You should have a coordinated media response strategy in place, including authorized spokespeople and a legal team to check that all communications comply with relevant regulations and legislation. The strategy should include:

   - A board-level spokesperson, chosen from a roster of media-trained and savvy executives
   - A prepared set of answers to all anticipated media questions
   - A role play with the spokesperson to prepare him/her for a potentially aggressive media
   - Communications that are as open, honest and candid as possible
   - A press release with quotes from appropriate executives and, if possible, relevant regulators or legal authorities. It should also include advice for organizations and consumers on how to minimize any risk
   - An apology (if you are at fault, of course!)
Why do so many organizations get caught out by unexpected security incidents? According to Greg Bell, it’s down to poor planning and communication.

Most of us are familiar with fire drills. We gather outside the building, get our names ticked off and return to work, knowing that all will be calm and straightforward should a real blaze occur. Yet, all too often, such ordered routine is nowhere to be seen when an organization’s data is attacked or compromised. There are a number of common flaws:

“I didn’t know that there had been an incident”
Employees are often unsure about what constitutes a “security incident” so may not bother to report it. Even if they are concerned, they may assume it’s someone else’s responsibility.

“Who am I supposed to report to?”
With no clear guidelines, an incident may well be reported to one of many help desks or a line manager, or possibly even to a security guard. Confused reporting lines may mean an incident isn’t resolved at all.

“I doubt anyone would do anything about it anyway”
Employees are often discouraged when they’re not kept in the loop regarding the progress of an incident they’ve reported. So, if someone does choose to report something and no feedback or updates are given, the individual may assume that the incident wasn’t especially important in the first place.

“But I told the person at the help desk”
Larger organizations, in particular, have a multitude of help desks, and they often operate autonomously. If you report an incident to the wrong desk, it may well end up being logged but not dealt with correctly. Even if it is sorted out, flaws in management reporting mean that the organization has no idea of how many incidents are taking place, and therefore no overall picture of where its weaknesses may lie.

“It took us by surprise”
Without a formal structure and process for managing incidents, people often panic and make poor decisions. They may shut down systems unnecessarily, destroy legal evidence, or fail to back up data.

Some staff do not even realize an incident has taken place

“Who’s in charge?”
In the absence of a senior, centralized security team, a potentially dangerous incident may not receive high priority. That makes it tough to mobilize appropriate support from public relations, HR, IT, Legal and other specialists. With no one taking overall responsibility, you could end up with an uncoordinated, piecemeal response. An effective incident management program, on the other hand, is run by senior individuals with the clout to obtain the necessary resources. They’ll be experienced enough to judge whether an incident is serious and respond accordingly.

What makes an effective program?
Everyone in the organization will understand the importance of security, and incident reporting will be quick and simple. Rules and procedures relating to incident management from reporting to resolution are clearly communicated to all relevant stakeholders. And the response team will have carried out practice runs, so they’ll know what to expect should the worst happen.

Hopefully, you’ll never face a major incident. But if you do, it’s better to be repeating a well-rehearsed drill than fighting an out of control inferno.

By Greg Bell, KPMG in the U.S. (rgregbell@kpmg.com)
Data loss at a glance

The latest trends and statistics for lost and stolen information (see pages 4-7 for a detailed narrative and description of the research methodology)

Number of incidents over the years

- 2006: 521 incidents
- 2007: 513 incidents
- 2008: 703 incidents
- 2009*: 570 incidents

Number of people affected over the years

- 2006: 250 million people
- 2007: 200 million people
- 2008: 150 million people
- 2009*: 100 million people

*Estimate based on figures for January-June 2009 (385 incidents)
Source: KPMG International, September 2009

Cause of data loss: people affected in 2009 (January-June)

<table>
<thead>
<tr>
<th>Incident type</th>
<th>No. of people affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer theft/loss</td>
<td>2,081,422</td>
</tr>
<tr>
<td>Hacking</td>
<td>105,505,536</td>
</tr>
<tr>
<td>Hard copy theft/loss</td>
<td>11,960</td>
</tr>
<tr>
<td>Human/system error</td>
<td>291,417</td>
</tr>
<tr>
<td>Improper disposal</td>
<td>102,035</td>
</tr>
<tr>
<td>Malicious insider</td>
<td>1,555,148</td>
</tr>
<tr>
<td>Malware</td>
<td>34,567</td>
</tr>
<tr>
<td>Portable media theft/loss</td>
<td>1,340,995</td>
</tr>
<tr>
<td>Unknown</td>
<td>49,413</td>
</tr>
<tr>
<td>Web/network exposure</td>
<td>2,700,300</td>
</tr>
</tbody>
</table>

Source: KPMG International, September 2009

Cause of data loss: number of incidents as % of total for 2009 (January-June)

<table>
<thead>
<tr>
<th>Incident type</th>
<th>% of total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer theft/loss</td>
<td>14%</td>
</tr>
<tr>
<td>Hacking</td>
<td>20%</td>
</tr>
<tr>
<td>Hard copy theft/loss</td>
<td>11%</td>
</tr>
<tr>
<td>Human/system error</td>
<td>11%</td>
</tr>
<tr>
<td>Improper disposal</td>
<td>11%</td>
</tr>
<tr>
<td>Malicious insider</td>
<td>11%</td>
</tr>
<tr>
<td>Malware</td>
<td>3%</td>
</tr>
<tr>
<td>Portable media theft/loss</td>
<td>12%</td>
</tr>
<tr>
<td>Unknown</td>
<td>12%</td>
</tr>
<tr>
<td>Web/network exposure</td>
<td>12%</td>
</tr>
</tbody>
</table>

Source: KPMG International, September 2009

Cause of data loss: number of people affected by...

MALICIOUS INSIDER

- 2008*: 0.1m
- 2009*: 1.6m

HACKING

- 2008*: 97m
- 2009*: 105m

Source: KPMG International, September 2009

Cause of data loss: number of 2009 incidents compared with 2008 (January-June)

<table>
<thead>
<tr>
<th>Incident type</th>
<th>% change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer theft/loss</td>
<td></td>
</tr>
<tr>
<td>Hacking</td>
<td></td>
</tr>
<tr>
<td>Hard copy theft/loss</td>
<td></td>
</tr>
<tr>
<td>Human/system error</td>
<td></td>
</tr>
<tr>
<td>Improper disposal</td>
<td></td>
</tr>
<tr>
<td>Malicious insider</td>
<td></td>
</tr>
<tr>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td>Portable media theft/loss</td>
<td></td>
</tr>
<tr>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>Web/network exposure</td>
<td></td>
</tr>
</tbody>
</table>

Source: KPMG International, September 2009

© 2009 KPMG International. KPMG International provides no client services and is a Swiss cooperative with which the independent member firms of the KPMG network are affiliated.
**Data loss by portable media:** number of incidents over the years

- CD
- Hard drive
- Tape
- Other

**Worst industries:** number of incidents as % of total for 2009 (January-June)

<table>
<thead>
<tr>
<th>Industry</th>
<th>No. of people affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education</td>
<td>838,385</td>
</tr>
<tr>
<td>Financial services</td>
<td>101,597,812</td>
</tr>
<tr>
<td>Government</td>
<td>3,577,353</td>
</tr>
<tr>
<td>Healthcare</td>
<td>389,190</td>
</tr>
<tr>
<td>Industrial markets</td>
<td>110,408</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>3,213</td>
</tr>
<tr>
<td>Insurance</td>
<td>165,670</td>
</tr>
<tr>
<td>Non-profit</td>
<td>76,800</td>
</tr>
<tr>
<td>Other</td>
<td>4,702,859</td>
</tr>
<tr>
<td>Professional services</td>
<td>1,694,380</td>
</tr>
<tr>
<td>Retail</td>
<td>41,506</td>
</tr>
<tr>
<td>Technology</td>
<td>475,217</td>
</tr>
</tbody>
</table>

Source: KPMG International, September 2009

**Data type:** number of incidents as % of total for 2009 (January-June)

- Bank account details
- Credit/debit card info
- Financial information
- Government ID number
- Medical records
- Miscellaneous/unknown
- Other personal info

Source: KPMG International, September 2009

**Other personal info**

<table>
<thead>
<tr>
<th>Data type</th>
<th>No. of people affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank account details</td>
<td>449,001</td>
</tr>
<tr>
<td>Credit/debit card info</td>
<td>100,112,381</td>
</tr>
<tr>
<td>Financial information</td>
<td>2,535,218</td>
</tr>
<tr>
<td>Government ID number</td>
<td>4,126,103</td>
</tr>
<tr>
<td>Medical records</td>
<td>560,571</td>
</tr>
<tr>
<td>Miscellaneous/unknown</td>
<td>2,784,251</td>
</tr>
<tr>
<td>Other personal info</td>
<td>12,780,643</td>
</tr>
</tbody>
</table>

Source: KPMG International, September 2009

**Worst industries:** people affected in 2009 (January-June)

**Worst industries:** number of incidents as % of total where a third party was involved (2009, January-June)

**Data type:** number of 2009 incidents compared with 2008 (January-June)

Source: KPMG International, September 2009

© 2009 KPMG International. KPMG International provides no client services and is a Swiss cooperative with which the independent member firms of the KPMG network are affiliated.
Trusted third parties – an oxymoron?

Outsourcing can place sensitive data in the care of third parties. If the data goes missing, it could be more than just your reputation that suffers

By Pieter van der Merwe, KPMG in Australia (p.vandermerwe@kpmg.com.au)

During August 2009, three men were charged with hacking into the IT networks of Heartland Payment Systems in the U.S., compromising more than 100 million credit and debit card details. This major credit card payment company processes millions of transactions a month for 175,000 retail merchants. Such an incident – while registering as probably the largest data breach in U.S. history – is just one of a stream of high-profile cases involving third parties.

In a global marketplace, outsourcing has become increasingly popular as an ever-wider range of functions are handled externally. They range from data centre operations, payroll, data processing and disaster recovery, all the way through to marketing and communication services.

The trouble is that the abundance of third party suppliers for various services can often lead to reduced information ‘visibility’. This may be good for your bottom line, but third party relationships pose a whole new set of security risks – risks that are not priced into the cost of outsourced services. Yet it seems that both public and private sectors have been slow to realize the dangers. Executives are often happy to accept the risk until problems arise and their company’s reputation is in jeopardy.

Recent headlines have now made third party supplier management a top concern. In India, earlier this year, credit card details were stolen from a call centre used by a global IT firm. In 2007, a laptop was stolen from a printing company used by a top UK retailer; the laptop contained personal details (such as salary details and national insurance numbers) of the retailer’s 26,000 employees.

Have we seen it all?
Surprisingly, however, according to KPMG’s Data Loss Barometer, third parties have accounted for a minority of security incidents (11%) in 2009 so far. But is that just the tip of the iceberg: how many cases go unreported?

From our member firms’ experience helping organizations address their third party risks, third parties can often be unable or unwilling to report security incidents. With this in mind, how many companies are being left in the dark?

Protecting data that’s beyond your control
Many organizations should understand that they are liable for data protection breaches happening on third party premises. They are responsible for managing activities conducted through third party relationships, and for identifying and managing the risks that arise from those relationships – to exactly the same extent that they would if such activities were conducted within their own organization.

So, once that is understood, how does an organization go about safeguarding the data it has entrusted to third parties?

Five steps to trusting third parties

- Assess the risk
- Perform due diligence
- Develop sound service contracts
- Implement controls on your own turf
- Monitor and assure

First, you must decide, through risk assessment and due diligence, whether or not to enter into a third party relationship.

Next, ensure that contracts are structured to cover the necessary aspects of information security: what are the respective roles and responsibilities of the parties involved; how
We’re in this together…but who’s at fault if it all goes wrong?

Of course, when dealing with contracts, you should also seek legal counsel. And stand your ground if you encounter resistance over the time and cost of security provisions. The initial outlays are definitely worthwhile if they lessen the impact of a security incident.

Next, put controls in place in your own organization to ensure that data is properly managed, secured, stored and processed. Each process and third party relationship will differ, of course, so the risks and controls will vary too.

Finally, organizations should be vigilant in ensuring not only that services are provided as agreed, but that security is tight. No system is foolproof, so you’ll also need effective strategic planning. Third party relationships are here to stay, but those who take the necessary precautions will, hopefully, avoid making headlines for all the wrong reasons.

DIFFERENT THIRD PARTY RELATIONSHIPS

- The IT provider managing your network, who has access to the raw data travelling across your pipes.
- The software publishing house whose developed code you trust, and who you allow to support production systems.
- The data modelling firm to which you send your data by email, CD and online for data analysis.
- The finance and accounting back office provider who processes the payment of your outgoings and monthly salaries of your staff.
- The records management organization you use to archive or destroy your data.

The list goes on…
During the current recessionary climate, many employees feel stressed and uncertain about their futures. Every week fresh announcements are made of job losses across industries. Financial pressures continue to mount for individuals, and there are many reasons: the stagnant housing market, savings rates that are running at historic lows and uncertainties over pensions and stock markets.

So it is unsurprising, perhaps, that some employees are likely to be tempted, in these uncertain times, to act against the interests of their employer as they try to shore-up their own financial position. There is a danger that they will see an opportunity to exploit the valuable and potentially sensitive data that your business holds – either by selling it or taking it to your competitors, or else using it to set themselves up in a rival business.

ARE YOU VULNERABLE?
Have you considered how vulnerable you are as an organization to such misconduct, and are you actively and effectively fighting potential information theft?

In a recent paper, KPMG in the UK and a law firm, Mishcon de Reya, analyzed more than 100 employee-related data theft cases on which they have acted over the past three years.

Such thefts have a number of features in common, as our analysis shows. Cases of data theft have risen year on year (more than doubling between 2006 and 2008), culminating in 46 cases last year in which forensic investigation and legal redress were sought by the employer to protect its business interests. In the current economic climate, the number of such incidents is almost certain to increase further.

THE PERPETRATORS
While most thefts were carried out by individuals, in about 10 percent of cases, the perpetrators were teams of employees working against their employer. Their aim was either to set up on their own or to join an existing competitor. In one case, up to 15 employees conspired to defraud their employer by stealing proprietary information.

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

INFORMATION THEFT TO SECURE THE NEXT MOVE
Further, our research showed that in 23 percent of cases, data was stolen in order to establish a competing business. In most cases, though – 70 percent – the perpetrator(s) moved to a rival company. That raises serious questions about how much a new employer needs to know about the nature, and source, of information a new employee brings with them.

In only 6 percent of cases were the data...
thieves’ intentions unknown, the thefts having been discovered before it was clear what they planned to do. In such cases, the person stealing the data may have taken it as ‘insurance’, in case its potential value could be exploited in the future.

So, what sort of information is being stolen?

By far the most common data – 75 percent – was customer or client-related (dealing with customer relationships, levels of trading, pricing information, profit levels and so on) or customer lists. Just 14 percent of the thefts consisted of financial information (such as internal accounts, business plans, projections and forecasts).

RATIONALIZATION – “I DID IT BECAUSE...”

Many bright careers are now on hold while organizations 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. Generation Y employees are sometimes seen as being loyal, first and foremost, to themselves. With careers stalled or stalling, some may regard the theft of sensitive data – whether they take it to rivals or use it to start up their own venture – as the most effective short-cut to restarting their own professional and financial progression.

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 in the public domain (30 percent). This latter statistic highlights the challenge of defining exactly what data within your business can legitimately be considered ‘proprietary’, and which should be accepted as public information.

In only 10 percent of cases was no defence offered by the perpetrator after the theft had been discovered.

HOW THEY GET AWAY WITH IT

The most common method of transfer of stolen proprietary data by disloyal employees was via email (46 percent of cases examined); 22 percent of cases were through taking hard copy print outs. Surprisingly, perhaps, USB memory sticks, data CDs or DVDs were used in only 9 percent of cases, despite their low cost, relative ease of use, and (especially in the case of USB sticks) conveniently small size. This may be an indication that data thieves are relatively unsophisticated, or that they simply do not believe they will be caught.

The misuse of newer technologies is likely to become more prevalent from now on since data can also easily be stolen using smart phones, MP3 players, digital cameras and other types of digital media. Social networking websites have also provided data thieves (in at least one case) with a way to remove data. Generation Y is, of course, very familiar and comfortable with such technology.

Such data leakage, and the ease with which data can be stolen, is therefore clear evidence that too many companies are not doing enough to detect and prevent information theft in a timely fashion.

RESPONDING TO DATA THEFT

Don’t be complacent. Even if you have introduced sophisticated data security controls, you could still be caught out.

Where data theft is discovered or suspected, an immediate and decisive response is essential. For example, you may well be able to minimize potential loss by taking legal action against perpetrators to recover stolen data before its release can cause you damage.

Of the 100-plus incidents handled by Mishcon de Reya, the average elapsed time from instruction to legal relief, whether in the form of restraining injunction, undertakings,

<table>
<thead>
<tr>
<th>HOW STOLEN DATA IS USED</th>
</tr>
</thead>
<tbody>
<tr>
<td>1% Sold data to competitor</td>
</tr>
<tr>
<td>70% Moved to competitor</td>
</tr>
<tr>
<td>23% Set up competition</td>
</tr>
<tr>
<td>6% Unknown</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>METHOD OF DATA THEFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>46% Email</td>
</tr>
<tr>
<td>22% Hard copies</td>
</tr>
<tr>
<td>9% Electronic storage device</td>
</tr>
<tr>
<td>16% Other</td>
</tr>
<tr>
<td>7% Suspicious database searches</td>
</tr>
</tbody>
</table>

Source: KPMG and Mishcon de Reya
In these uncertain times, employees are more likely to seize the opportunity to exploit valuable data.

damages or apologies, was just over two and a half weeks. In more than 55 percent of cases, specialist forensic technology or forensic investigation services were required to image computers, retrieve emails or 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 may provide you with evidence of the timing behind such actions, 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 rogue employees.

IN SUMMARY
Data theft by employees is a genuine threat to organizations, particularly in the current economic climate.

In the future, there is likely to be an ever-rising trend among employees attempting to steal confidential data for their personal benefit when leaving their current employment. It is possible for businesses to take effective action against such fraud, both in response to actual and attempted thefts of data, and to minimize the likelihood of data being stolen in the first place.

Effective data protection policies, and the creation of a climate in which everyone recognizes the value of, and need for, integrity in the handling of sensitive commercial data, is vital if such thefts are to be prevented.
Sometimes your biggest problems are little ones

As more and more data is stored on memory sticks, phones and MP3 players, how can you stop confidential information falling into the wrong hands?

By Jörg Asma, KPMG in Germany (jasma@kpmg.com)
The risks posed by portable data devices have been around since the invention of the floppy disk 40 years ago. And, as each new advance brings an exponential growth in the amount of memory on tap, many organizations have been struggling to find ways to protect confidential data.

Some organizations briefly stemmed the tide by banning CD burners and locking the slots for additional hard disk and floppy disk drives. But with the advent of USB interfaces – particularly memory sticks – the threat level has leapt up again. After some embarrassing high-profile losses in previous years, the number of reported losses of portable media fell by around a third between 2008 and 2009 – although the figure is still up on 2007.

Memory sticks may be a life saver for anyone involved in presentations, sales pitches and complex projects, but they’re proving a real headache for those responsible for data security. The average storage size of such devices doubles every two years, and with prices going in the opposite direction, the typical employee may well have a handful of them in his or her possession.

Apart from the risk of loss or theft, there are other ways that data can escape fortuitously. Most of us have at some time handed over a stick at a conference to download a presentation. Yet do we always consider that unrelated information already on the device could be downloaded without our knowledge? Some devices are even craftily designed to transmit data from your computer straight to the internet.

Keeping track of the actual data on USB sticks is well nigh impossible, as most users

Some devices can transmit data from your computer straight to the internet

store information from multiple sources. And now, with the emergence of smart phones and even memory cards for digital cameras, the danger is multiplying.

The blurring of lines between personal and company media means that an employee may well have a lot of highly confidential data on one or more personal device. Consequently, attempts to forbid staff from carrying notebooks or laptops across borders are often rendered meaningless, as much of the content may already be on their phone or MP3 player.

Without doubt, the relentless march of technology will ensure that portable media continue to proliferate. So what measures can be taken to combat such risks? At the very least, organizations should make employees aware of the need to exercise extreme caution. Better still, companies should encrypt data files on each and every device that may contain any type of sensitive information. Such a move would strike a blow against those who would seek to profit illegally from your valuable intellectual property.

**PORTABLE MEDIA SECURITY RECOMMENDATIONS**

Here’s how to enjoy the benefits of modern communications devices while reducing the security risks:

**Enforce a clear user policy**
- Allow only approved portable devices
- Restrict usage to employees with genuine business need
- Classify the type of information that can be stored and processed on portable devices
- Monitor and audit the use of such devices.

**Make users aware**
Communicate the policy to all users, explaining the rationale behind any restrictions. Make sure that all those involved in policing the policy fully understand their roles and responsibilities.

**Keep a record**
Know what devices you have and who’s using them.

**Restrict connections**
Allow only approved devices to be connected to your system. That may involve locking USB ports. Restrict the types of files that can be run on portable media.

**Central control**
Deploy central controls so that missing devices (e.g. smart phones) can be locked or disabled remotely.

**Dispose of devices safely**
If portable media are re-used or donated, this must be done securely. Alternatively, the devices should be destroyed.

**Encryption**
Centrally controlled encryption can ensure that devices such as USB sticks automatically encrypt information as soon as it is saved.

**Authentication**
Restrict access using safe passwords or two-factor authentication.

**Digital rights management (DRM)**
DRM technologies control use of digital content, wherever it is stored.
Information is the lifeblood of any modern organization. So how can you ensure it flows freely while avoiding embarrassing and damaging data loss?

Leaders and managers are constantly looking for ways to use knowledge to gain a competitive advantage in the information age. Yet while encouraging the free movement of information, they should also be on constant guard against data being lost or stolen. Remember, just as organizations vigilantly protect their physical assets, they should also adopt a holistic approach to keeping data safe.

**STEP 1: CREATE A FRAMEWORK TO PREVENT LEAKS**

Adopting such a framework is part of a wider change in an organization’s culture, where information is acknowledged to be the vital strategic asset it emphatically
is. To address data leakage, you should therefore consider the following:

**People** Identify when and where people come into contact with information as it flows around your organization. Then you’ll be able to highlight the need for security at those connection points. It’s also vital to confirm who ‘owns’ the data and make them fully accountable for, and aware of, their responsibilities.

**Processes** Understand the times and points where data is most likely to be leaked. It could be during a system upgrade or transaction, or when an employee leaves. Look at all the controls put in place to protect data and, in addition, set up a procedure to deal with any violations.

**Data** You should understand in detail the end-to-end flow of information, from the point at which it enters the organization to where it’s stored, processed, transferred and ultimately destroyed. This can help you secure the points at which employees can access data.

**Physical infrastructure** Make use of appropriate technology to protect your information. You should also restrict physical access to equipment, prevent eavesdropping and safeguard media such as laptops and memory sticks.

---

**STEP 2: PUT A PROTECTIVE BLANKET AROUND YOUR ORGANIZATION**

Any leakage prevention system should be flexible enough to cope with structural changes, such as mergers, acquisitions and disposals. It should also be able to adapt to higher levels of security prompted by marketplace threats or new legislation.

**Know what you own** By identifying all the information within your organization – and where it’s located – you can build a comprehensive inventory. You should take particular care of your most valuable data, confirming who can access it and where you’ll permit it to be transferred.

**Put a value on information** Although such a process cannot be completely precise, it is vital to estimate the real value of data – and therefore the cost to your organization if it is compromised.

**Control access** Whether it’s physical hardware or information systems, it is essential that only authorized individuals are permitted access to it. Make sure you spot any weak points and tighten them up.

**Rules, rules, rules** There should be a set of clear and unambiguous rules and procedures to prevent activities that pose a risk to your information. They should be consistent across the organization, have the full support of management and be clearly communicated through awareness programs.

**Monitoring and responding to incidents** Use a system that monitors and instantly flags up attempted or actual violations. Once an incident has taken place, there should be a procedure for responding quickly to limit any damage. Ensure lessons are learned and used to continually improve incident management procedures.

---

**STEP 3: AIM FOR CONTINUOUS IMPROVEMENT**

The expectations of any program should reflect, realistically, the existing and aspired level of security. We believe there are five levels to aspire to, level 1 being the most basic:

**Level 1 Informal** You know you’re not protecting information adequately and are doing little about it. Any awareness of leakage has probably been caused by specific incidents of data loss or unauthorized access.

**Level 2 Planned and tracked** At this level, you’re able to address some of your data leakage issues, but not until some time after they have occurred. Critically, you’re unable to address the root causes of problems or, indeed, predict when they may occur in the future. When issues do arise, you will often need to call for external help.

**Level 3 Well-defined** Your organization can stop leaks before they occur by addressing the root cause of any potential problem. And as you continually monitor data quality, you can quickly resolve incidents.

**Level 4 Controlled** With a mature set of information management practices, you proactively identify and deal with any issues. What’s more, leakage prevention has become an integral part of your technology strategy.

**Level 5 Continuous improvement** At this highest level, the management of information is treated as a core competency influencing all parts of the organization. Any data leakage is resolved at source, and the organization is always looking for ways to refine and improve its security systems.

As with any major change program, preventing data leaks calls for strong, high-profile leadership from the top, a mandate clearly communicated to all staff and full commitment across the organization. Identifying your most critical information assets is a fundamental first step. Then only a combination of measures covering business processes, technology and people can allow for information to be adequately managed and protected.

---

© 2009 KPMG International. KPMG International provides no client services and is a Swiss cooperative with which the independent member firms of the KPMG network are affiliated.
Most information and IT security departments have spent many years and countless millions protecting their corporate IT facilities from hackers. Yet while they’re barricading the electronic walls of their organization, they’ve often overlooked the human factor, which frequently comes in the form of polite, charming people with the ability to extract vital personal details from employees and consumers.

These chameleon characters blend in easily and often go by the nickname of ‘social engineers’. As the world-renowned hacker Kevin Mitnick explains in the book The Art of Deception: Controlling the Human Element of Security: “It is human nature to trust our fellow man, especially when a request meets the test of being reasonable.”

A clever social engineer may strike up an apparently innocent conversation at a bus stop with a lady with her dog. A couple of banal questions later she’s released the name of her first pet. Over time the fraudster may manage to elicit further snippets of information until he/she has the passwords for banking and other personal finances, enabling impersonation, identity cloning and, finally, account takeover.

It’s good to share… or is it?

In the past few years the task of such criminals has been made a whole lot easier with the rise of social and business networking sites such as Facebook, MySpace, Bebo and LinkedIn. As their popularity booms, an increasing number of people are cataloguing, indexing and archiving the details of their lives on the web. Many of us, it seems, are quite happy to share data online that we wouldn’t tell anyone face-to-face. On Facebook there is even a quiz entitled: “How well do you know me?” It encourages users to complete a questionnaire to test their ‘friends’ by asking them questions such as: “What is my mother’s full name?” “What was the name of my first pet?” “What are the names of my children?”

By cruising through various sites, it’s all too easy to build up an impressive understanding of an individual’s personal profile, stopping off at Facebook for educational details, before moving on to LinkedIn to pick up career history.

An increasing number of people are cataloguing their lives on the web

Which brings us back to your mother’s maiden name. We’re all aware of the questions we get asked either online or over the phone to access a bank or other financial service. These may well include your mother’s maiden name, date of birth, memorable address, memorable date and pets’ names. And passwords, as every fraudster and opportunist knows, often relate to personal details such as loved ones’ names, birthdays and so on… all of which may be available online. It’s low-hanging fruit just waiting to be plucked by a cunning cyber-thief.
Keep it to yourself

In the same way that those using cashpoints have grown accustomed to guarding their PINs from prying eyes, so employees and consumers must learn to exercise caution with personal account and log-in details. The financial services industry, regulators and professional services firms all have a role to play in educating customers on the importance of personal security.

There has been some progress, however. Many online banking websites remind customers to keep their password safe and use only trusted computers. However, much more is needed, possibly in the form of partnerships with the social networking sites themselves. Employers also have a role to play in keeping criminals at bay, and there are more cases of employees being disciplined for Facebook misuse.

The hunting ground of the social engineer may have shifted from the bus stop to cyberspace. But by making people more aware of the value of personal data – no matter how apparently innocuous – perhaps we’ll all learn the old-fashioned truism that some things are just meant to stay private.
Data loss can weaken a company’s foundation.

KPMG member firms can help you identify threats to your organization and navigate a safe path through the application of sophisticated technology tools and consistent methodologies.

We can help simplify complex issues: explain threats to your business, advise on the application of compensating controls and embed processes to help ensure consistency.

Our firms’ services are delivered by information security and forensic professionals, able to assist you on a global level.

We can help you to keep your reputation on high ground.

Contacts:

Europe, Middle East and Africa  Malcolm Marshall  e-Mail: malcolm.marshall@kpmg.co.uk  Tel:  +44 20 7311 5456

Jörg Asma  e-Mail: jasma@kpmg.de  Tel:  +49 221 2073 6233

Americas  Greg Bell  e-Mail: rgregbell@kpmg.com  Tel:  1 404 222 7197

Asia Pacific  Rob Goldberg  e-Mail: rhgoldberg@kpmg.com.au  Tel:  +61 (2) 9335 7728

For more information, go to www.kpmg.com