

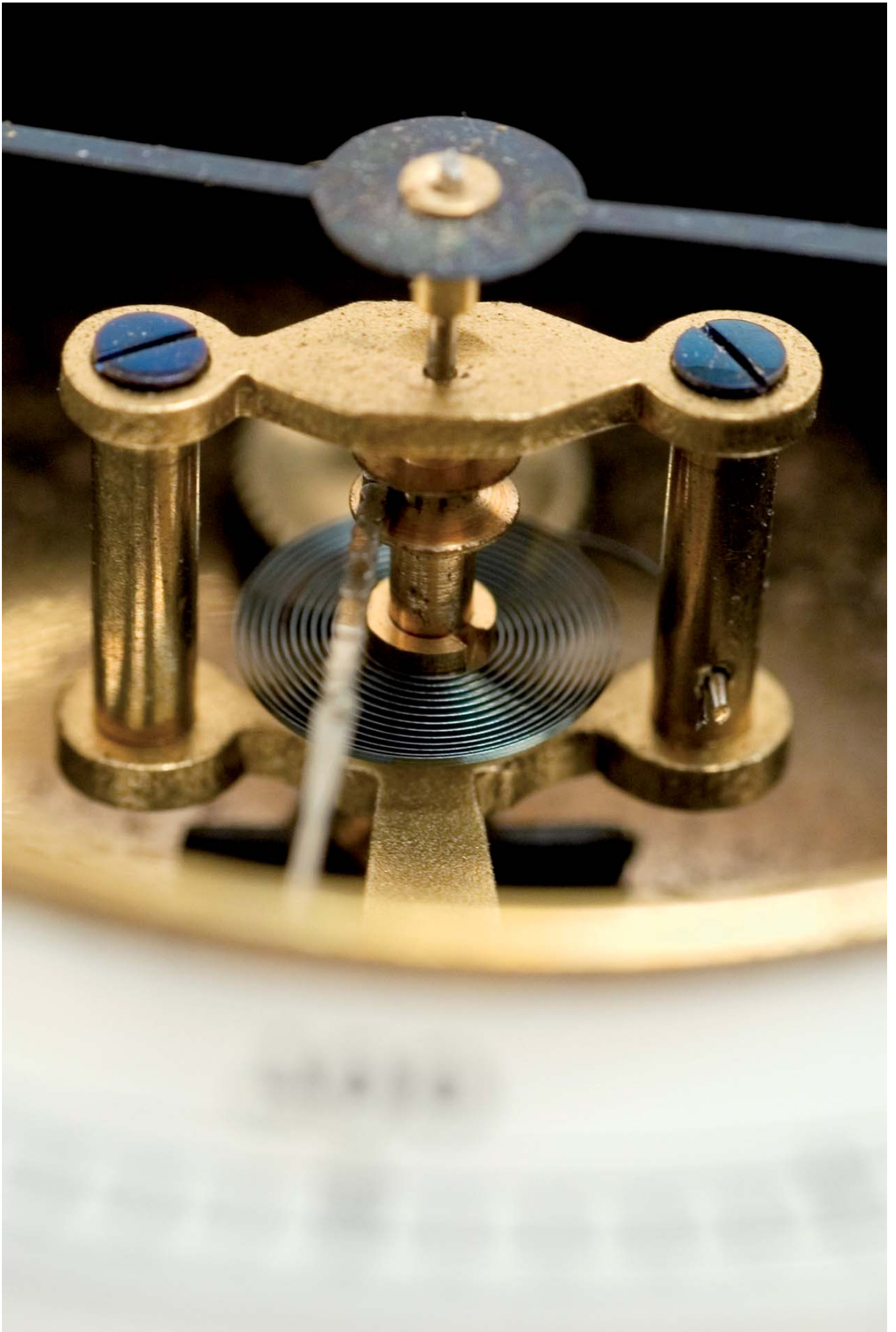


Data Loss Barometer

September 2008

ADVISORY


780





- 4 Executive summary
- 6 Methodology
- 7 Data loss
– the scale of the problem
- 9 Victims of data loss
- 10 Removable media
- 11 Sector analysis
- 12 Types of data loss
- 13 What you need to know
- 14 How KPMG can help

Executive summary

A photograph showing two business professionals in a control room. In the foreground, a woman in a dark suit is focused on typing on a laptop. Behind her, another person is holding a document. The background is filled with blurred lights and equipment, suggesting a busy, high-tech environment.

Information is the lifeblood of any organisation.
Protecting data from theft or unintentional disclosure
is critical to ongoing commercial success.



“We are living in an age where protecting your information has never been so important”

UK Information Commissioner's Office

Data loss incidents are increasing in number and significance every year. Such leakages are not only costly but damaging to corporate reputations.

This KPMG research takes a global look at data loss to identify types of loss, where losses occur and the impact on victims. The main findings of this analysis are:

Internal controls are vital

Human or procedural errors account for a significant number of losses. Due to the human involvement it almost becomes impossible to eliminate losses – such as a laptop left on a train or a CD that goes missing in the post – entirely.

Risks of errors are greatly reduced by implementing appropriate and clearly defined procedures around the use and handling of data. Staff need to understand what is expected of them with regularly implemented, tested and updated awareness, training and education programmes.

Portable media is highly vulnerable

Mobile devices such as laptops and removable media are invaluable to modern day business but carry an increased risk of data exposure.

To manage the risks, security guidelines must clearly communicate to all users when, where, how and what data may be transported. They should also set out appropriate actions in the event of the loss or theft of a portable device.

A lost or stolen device does not necessarily make your information vulnerable. Data protection measures, such as encryption, can prevent your data from falling into the wrong hands.

Hackers are a persistent danger

Unauthorised access presents a major threat to data protection. The malicious and often organised nature of hacking makes it more likely that the data extracted will be used for criminal and fraudulent purposes.

Regular risk assessments to identify threats and vulnerabilities, supported by appropriate mitigation, can help protect networks and system resources from hackers. Controls must be continuously monitored and regularly tested so you can gain confidence they work correctly and continue to meet your needs.

Incident response is key

Reputation is commonly regarded as an organisation's most valuable asset. Loss of reputation means a loss of customer trust and a loss of business.

Handled correctly, however, the reputational damage resulting from data loss incidents can be minimised.

Organisations must plan their incident response carefully. Security policies must include how to detect, escalate and resolve issues and appropriate action to take in the event of an incident. Consideration should also be given to how to manage influencers of public perceptions – such as customers and the media – in order to mitigate damage.

1034 incidents of data loss

280m people affected

25% involving **PC theft**

80% causing loss of **personal details**

51% of losses from an **internal** source

46% of lost data has **no protection**

Methodology

This research is based on publicly disclosed incidents of data loss.

“ Personal data remains a high-value commodity for criminals ”

UK Financial Services Authority

Although the incidents date from 2005 through to June 2008, much of the analysis focuses on events since January 2007. The incidents are worldwide, but predominantly originate in the US and UK.

In the US, legislation exists to ensure that data loss incidents are fully disclosed. Such information is freely available and publicly reported. Websites run by Open Security Foundation and Identity Theft Resource Centre are particularly useful information sources. Details of non-US incidents are taken from the media, internet searches and independent news or data feeds.

Care is taken to ensure that the data used in this report comes from reputable and independent sources. Availability, consistency and accuracy of information can vary between sources, countries and by type of incident. Furthermore, it should be noted that press reports are typically skewed to the issues deemed most relevant and interesting to the readership.

This report does not provide a definitive list of all data breaches, rather it is a snapshot of a global issue. Nonetheless, it is evident that incidents do occur, that data is lost and that confidential information and personal details are compromised.

Source information:

Open Security Foundation
www.datalossdb.org
Identity Theft Resource Center
www.idtheftcenter.org
Privacy Rights Clearinghouse
www.privacyrights.org
Attrition.org
www.attrition.org/dataloss
Information Commissioner's Office
www.ico.gov.uk
CIFAS www.cifas.org.uk
Factiva www.factiva.com
Bloomberg www.bloomberg.com
Guardian www.guardian.co.uk
Times www.timesonline.co.uk
Independent
www.independent.co.uk
Telegraph www.telegraph.co.uk
BBC www.news.bbc.co.uk
ITV www.itv.co.uk
Channel 4 www.channel4.com
The Register www.register.com
Silicon www.silicon.com
Security Focus
www.securityfocus.com



Data loss – the scale of the problem

Every year brings news of further data loss incidents. It is anticipated that there will be over 400 breaches in 2008 but that fewer people will be affected.

This is possibly a consequence of increased vigilance by organisations. However, as in previous years, one large scale incident can dramatically swing the statistics.

So how big is the data loss problem?

Is the number of incidents actually escalating or is it just the media coverage that is increasing?

As the general population becomes more aware of identity fraud and threats to their personal information, their concerns grow. Media interest inevitably follows and so reports on security breaches increase.

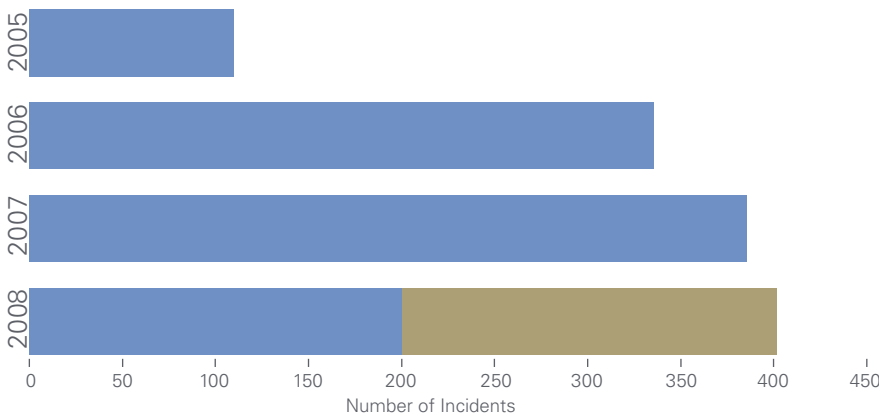
Businesses' reliance on technology contributes to the cause of security incidents. As they become more

technology dependent, new risks, vulnerabilities and threats to data emerge. Data protection points become more diverse and difficult to control. As a consequence, even with the most secure and comprehensive controls, it is almost impossible to achieve absolute protection against all conceivable threats.

Security incidents involving data loss are an unpalatable risk of business life. If, or when, security is breached, corporates must act swiftly, appropriately and decisively to limit the potential damage.



Data Loss Incidents Vs Year

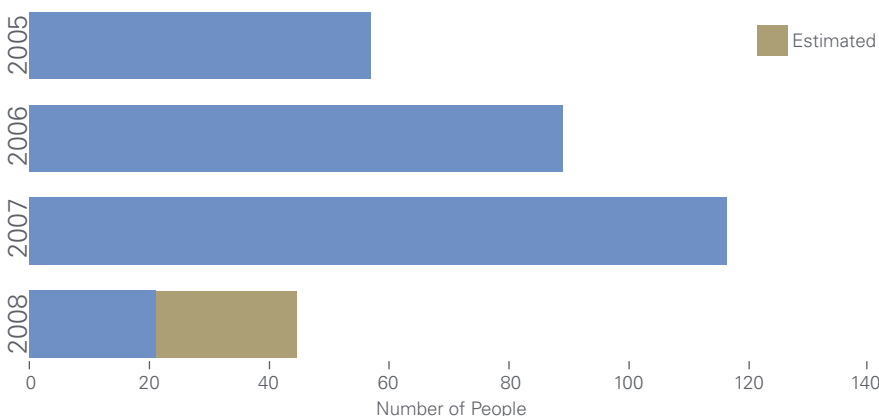


1034 data loss incidents since January 2005

280m people affected

404 incidents estimated for 2008

People Affected Vs Year



Incidents **increasing**

People affected **increasing**

Technology **increasing**

Public concern **increasing**

Data loss – the scale of the problem

Incidents of PC theft and hacking are common. Breaches initiated outside the victim organisation are most difficult to predict and control.



Technical safeguards, such as network perimeter security, are essential for guarding against external threats but internal controls have a part to play too.

The value of implementing and adhering to strict internal controls is evidenced by the reported number of internal incidents. In losses reported between 2007 and 2008, 50% emanate from internal sources and 44% originate from outside the organisation. Internal incidents include accidental web or network exposure, human or system errors, improper data disposal and the loss of removable media (see page 10).

Effective risk assessment is essential to identify the most vulnerable data and the associated internal and external threats to its security. Only by understanding the risks can the correct focus be applied to mitigate those risks and protect critical data. Furthermore, to ensure that technical and procedural controls are effective, staff must be fully aware of (and know the importance of) their obligations in respect of information security.

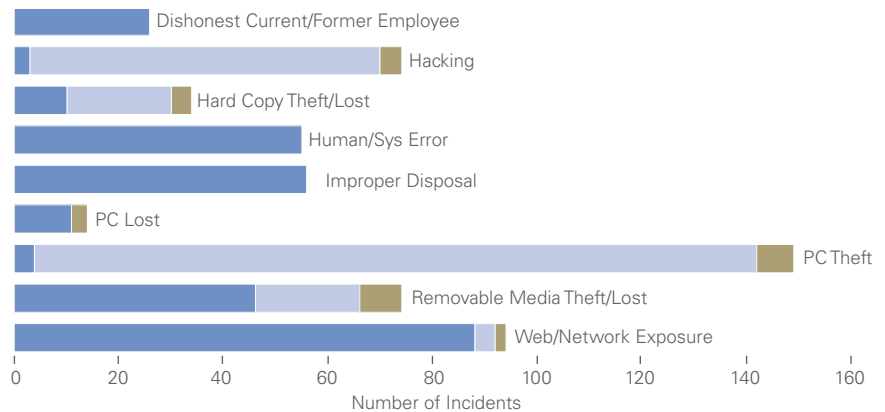
589 data loss incidents since January 2007

25% of incidents involve **PC theft**

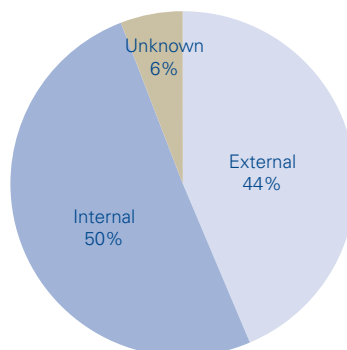
16% of incidents involve **web/network exposure**

13% of incidents involve **hacking**

Number of Incidents Vs Type of Breach



Security Breach Source



50% of incidents are from **internal** sources

44% of incidents are from **external** sources

Internal threat versus **external?**

Victims of data loss

Organisations that suffer data loss are most likely to experience breaches caused by hacking, loss or theft of removable media or web/network exposure.

Hacking, the most malicious and organised type of data loss breach, counted for over 60 million victims between 2007 and 2008. Data which is hacked rather than inadvertently lost is most likely to end up in criminal hands.

In 2007, three separate incidents accounted for the majority of victims of data loss. The incidents, which were widely reported in the media, include:

- An intrusion into the computer systems of TJX Companies in the US, threatening the credit/debit card details of over 45 million customers.
- The loss in the post of two CDs with HM Revenue & Customs details of over 25 million child benefit recipients in the UK.

- And the exposure, in the Netherlands, of the details of 15 million people on a legitimate health insurance website.

Leaving these three major incidents aside, reports of hacking and removable media theft/loss remain the most common breaches. However the incidents are more evenly distributed across the different types of breaches. This is further substantiated when another incident of hacking, affecting six million people, is removed from the analysis.

The victim statistics are approximations, as numbers are not always disclosed. Moreover, there is an often blurred relationship between the number of

people affected and the number of records lost. Even so, that there has been a potential 138 million victims since January 2007 illustrates the massive scale of the problem and the considerable disruption caused by data loss.

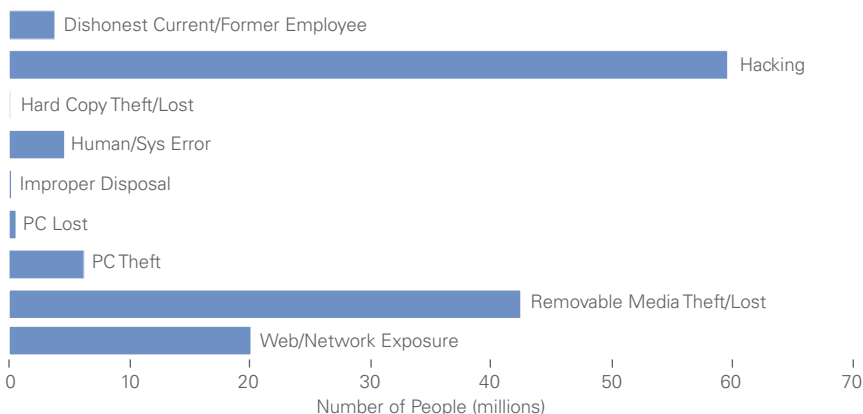
“ The rise in fraud should be of concern to us all ”

CIFAS

Media reports:

- <http://www.securityfocus.com/news/11455>
- http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm
- http://www.theregister.co.uk/2007/12/13/dutch_health_care_privacy_storm

People Affected Vs Type of Breach



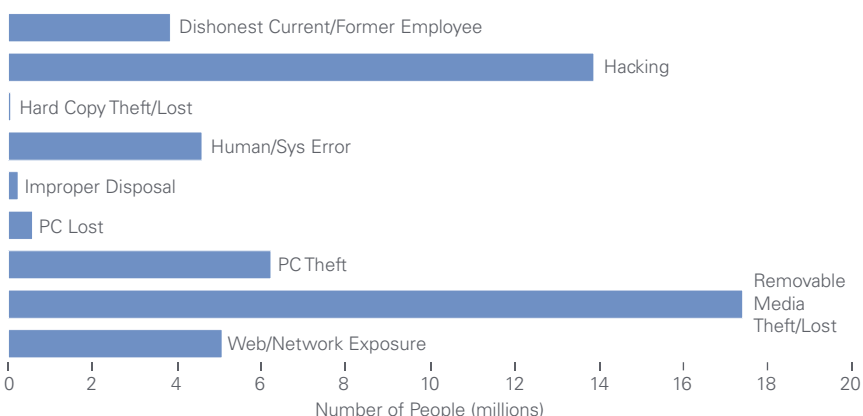
138m people affected since January 2007

60m people affected by **hacking**

42m people affected by **removable media** loss

62% of all people affected were victims of **three incidents**

People Affected Vs Type of Breach – excluding figures for three major incidents



6.2m people affected by **PC theft**

4.6m people affected by **human or system errors**

3.8m people affected by **dishonest employees**

5.0m people affected by **web exposure**

Removable media

The loss or theft of removable media is not only commonplace but affects large numbers of people. The media itself comes in many forms – such as CDs, tapes and memory sticks – each carrying inherent risks.

It is much more likely that a removable media device will be lost internally (62%) than stolen by an external perpetrator (27%). Furthermore, removable media is more often lost than stolen.

Encryption is widely accepted as an effective method of protecting information. Given the high probability of a misplaced portable media device, companies should take steps to ensure that all data is encrypted and cannot be accessed by unauthorised people.

In practice, however, encryption is rarely adopted. In the vast majority (62%) of reported losses or thefts of removable media, data was neither encrypted nor password protected.

Not included in this statistic are incidents where the level of protection was neither disclosed nor available. If such information were to be published, it is highly probable, that the number of breaches without data encryption would rise.

Protection by purely technical means is however not sufficient for most organisations. The highly mobile nature of these removable devices makes it easy to transfer data between business partners and contractors.

In addition to encryption, policies and procedures for secure data processing and handling are vital. These should be backed up by agreed legal contracts between parties.

It is the variety, flexibility and convenience of portable media devices that makes them popular. However, a balance must be achieved between implementing data protection at a manageable cost and maintaining the value of mobile devices and their benefits to business.

“ We may take enforcement action if firms fail to encrypt customer data taken offsite ”

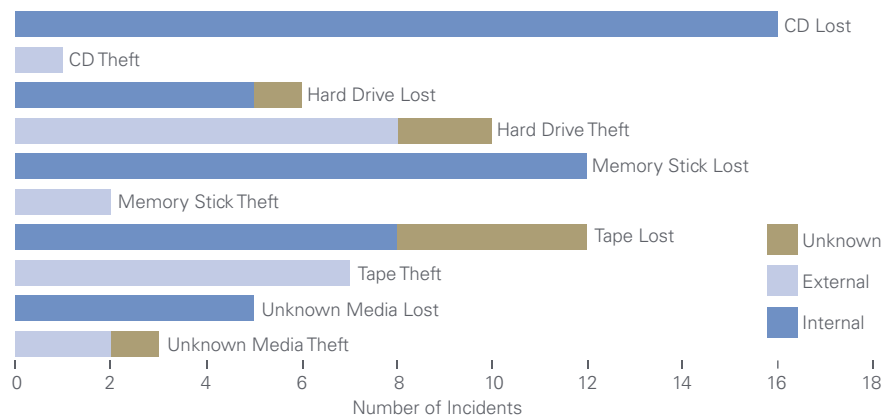
UK Financial Services Authority

62% of removable media incidents are internal

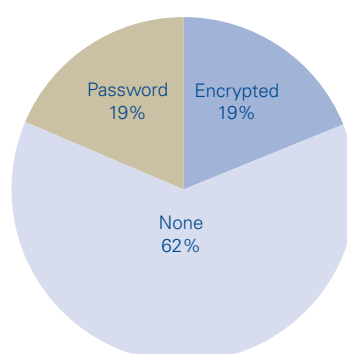
27% of removable media incidents are **external**

69% of removable media incidents are due to **loss** rather than **theft**

Number of Incidents Vs Removable Media Types



Removable Media Theft/Lost –Data Protection



62% of removable media incidents involved data with **no protection**

48% of all incident reports did not reveal the level of data protection

46% of all incidents involved data with **no protection**

Sector analysis

Which sectors are most vulnerable to data loss?

In the education and healthcare sector, it is the sheer number of personal records and the culture of the establishments that makes them vulnerable to data loss. Furthermore, they tend to have restricted security budgets which makes it more difficult to provide adequate protection.

Government organisations do not fare so well. They were accountable for 19% of data loss incidents between 2007 and 2008, affecting relatively large numbers of people. Furthermore, such agencies attract intense media scrutiny and criticism. Given the personal data they store and the relevance to the general public, it is essential that government organisations reduce the amount

of personal data they store and ensure this is securely stored.

Financial services organisations store customer data that is highly valuable to criminals. Such firms are often required to comply with strict laws and regulations governing data privacy, but significant lapses illustrate that the industry continues to expose itself to significant risks.

Consumer markets account for just over half of all people affected. However, as already described, just a single incident accounted for the vast majority of victims in this sector. The Payment Card Industry Data Security Standard has been introduced as a mechanism to improve security within organisations

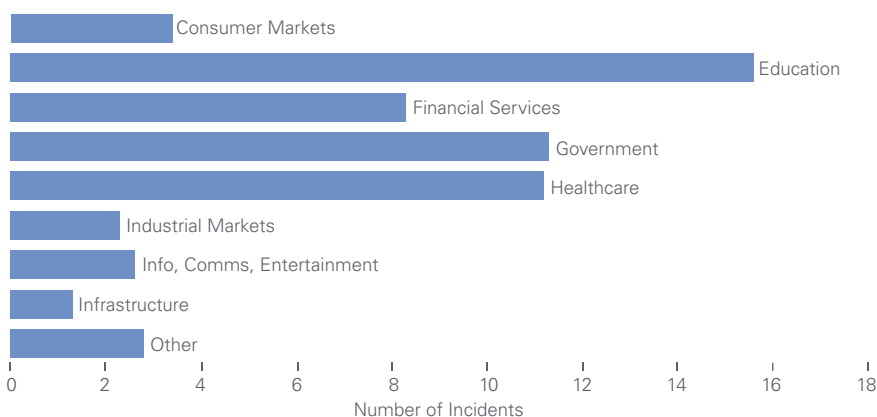
that are involved in card transactions, however compliance with this does not guarantee security. Implementation of its requirements could reduce the impact of a potential security incident though.

The threat of data loss is universal. It exists across all businesses, sectors and geographies. Every organisation may be vulnerable and must commit resources to reduce risks and keep their own and their customers' data secure.

“ Organisations which process personal information must ensure it is held securely. This is an important principle of the Data Protection Act ”

UK Information Commissioner's Office

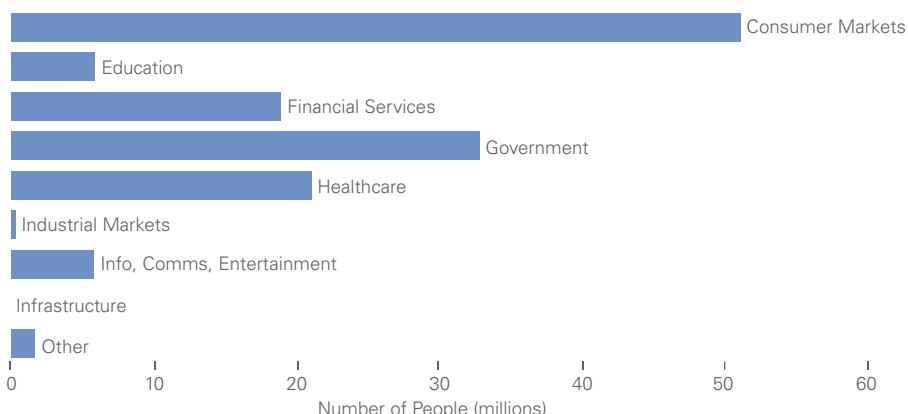
Data Loss Incidents by Sector



19% of data loss incidents linked to **Government** organisations

14% of data loss incidents within **Financial Services**

People Affected by Sector



33m people affected by incidents linked to **Government** organisations

51m people affected by incidents within **Consumer Markets**

Types of data loss

At 80%, incidents of lost personal details¹ are most common. These are typically details which are stored to identify an employee or a customer. In the US, social security numbers are often used for identification purposes.

For organised criminals, financial data has the most immediate value and it is this that they commonly target. Adding together lost bank account or card details with other financial information, such as pensions and investment details, means the majority of lost data is finance-related. Between 2007 and 2008, the financial details of 139 million people were wrongly disclosed, where ordinary citizens are affected, media and public interest is always high.

Criminals are adept at finding ways to use personal details for financial gain. Identity fraud is a growing concern which is costing individuals and businesses millions of pounds each year. In addition to financial loss,

victims can suffer significant disruption, distress and damage to their reputations. CIFAS, the UK's fraud prevention service, estimates that it can take between three and 48 hours' work for a typical victim of identity fraud to put right the damage and clear their name. In the case of a 'total hijack' where 20 or 30 organisations are involved, it can take more than 200 hours and cost up to £8,000. In that time, an individual's credit status may be considerably, albeit temporarily, impaired.

Across business sectors, no organisation is immune to the threat of data leakage. And a growing and widespread reliance on technology suggests that the risk is likely to

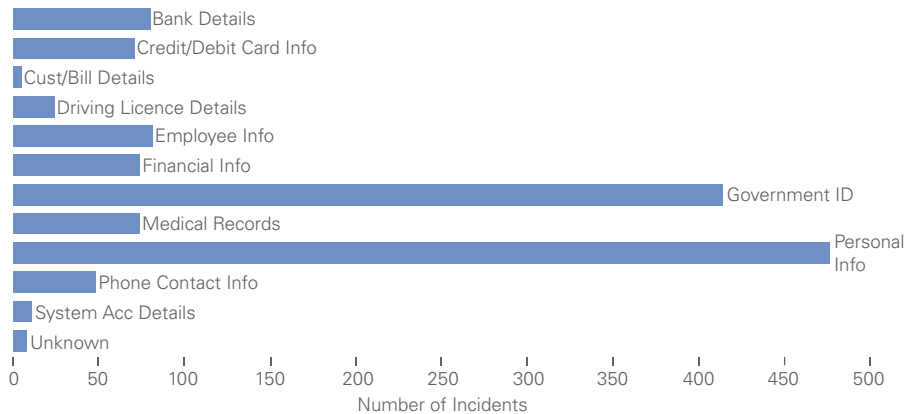
increase in future years. Tactics that focus on prevention, rather than reacting to an incident when it happens, are key to keeping identity and personal data secure, private and out of criminal hands. This can be achieved by allocating resources to assess and manage the risks around valuable business data.



80% of incidents cause loss of **personal details**

69% of incidents cause loss of **Government ID numbers**

Number of Incidents Vs Data Type

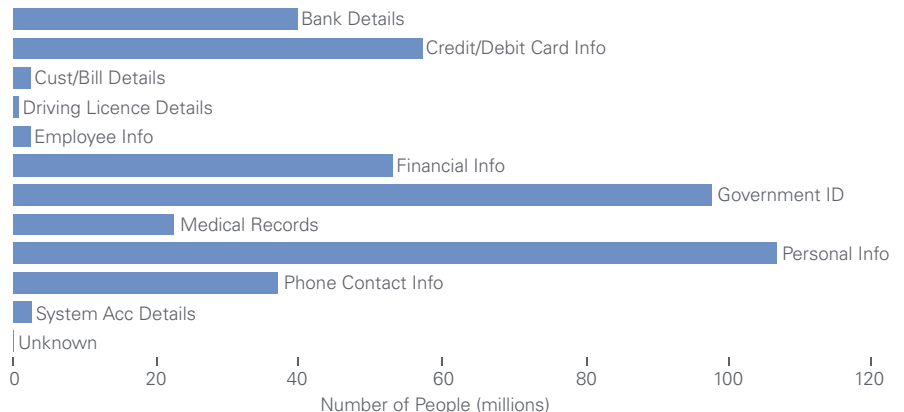


77m people had **personal info revealed**

62m people had **Government ID numbers** revealed

139m disclosures relate to **financial information**

People Affected Vs Type of Data



¹Personal information includes names, date of birth, addresses etc. Government ID numbers include Social Security numbers in the US and UK National Insurance numbers.

What you need to know

Data breaches pose a serious threat to all organisations. The impact on brand reputation is high and customer trust can be severely compromised.

Even the most secure and comprehensive controls do not provide absolute protection against all conceivable threats. To ensure that your business is as equipped as it can be to withstand or deal with a breach, test yourself on a few vital questions.

Do you know where your data comes from, where it is stored and how it is used?

Without knowing the source of information, how it is processed and how it is used, you cannot fully understand its value to your organisation. This will make it very difficult to evaluate the potential risks and to allocate the appropriate investment in information security.

Do staff understand the importance of good data handling?

A significant number of data losses are down to procedural error. Errors will occur when humans are involved in activities but where employees know what is expected of them in terms of data handling, they will be better positioned to identify the dangers and help counter incidents.

Where good internal controls are in place and there is a robust compliance culture, the risks of data leakage can be reduced.

Are you confident that your IT networks and systems are secure?

Malicious and skilled hackers do not only pursue high profile organisations. Businesses with poorly configured systems and weak network defences are easy targets for hackers.

Across all sectors, businesses need to protect themselves from attack. They should undergo regular assessments of their IT security arrangements.

Do you have a clear plan of what to do should you lose data?

Even businesses with the most sophisticated controls can get caught out by a data breach. Upfront planning on how to deal with a breach can help:

- reduce the impact of the loss
- preserve evidence for investigation
- maintain good relations with the public and the press
- prevent future reoccurrence.



How KPMG can help

As one of the world's largest providers of security advice, KPMG can help you assess and manage your data loss risks.



With market leading experience, we help organisations transform the protection of their information assets, to counter increased risks and address the concerns of customers and regulators.

Security assessment and assurance

KPMG offers a wide range of services to help you understand and identify weaknesses in your information handling systems and processes.

Services range from in-depth technical reviews of IT systems, to external and internal penetration tests, to evaluations of governance and policy arrangements.

Understanding where you are most vulnerable is key to actively managing the risks you face and reducing the chances of data loss.

Incident management

KPMG can help you to assess, manage and respond to the consequences of data loss. We help you to confirm the extent of the breach and assess how likely it is that the lost data will be used fraudulently.

We work with you to notify relevant authorities and affected customers; to define and implement recovery strategies and to assist your collaborations with regulators and legal advisors.

Awareness and training

KPMG can help you improve your employees' security awareness and handling of confidential information.

Based on our years of experience with other organisations, we help devise behavioural change programmes to enable staff and key suppliers to understand and fulfil their individual responsibilities for protecting critical data. We develop their awareness and understanding of how to respond when something goes wrong.

"We require a new and imaginative approach to accountability and to winning people's trust in the ways in which information is held and used"

UK Prime Minister – Gordon Brown



The contacts at KPMG in connection with this research are:

Malcolm Marshall

Partner KPMG LLP

Tel: +44 (0)20 7311 5456

malcolm.marshall@kpmg.co.uk

Matthew Martindale

Executive Advisor KPMG LLP

Tel: +44 (0)79 1755 2588

matthew.martindale@kpmg.co.uk

Ross Leaning

Advisor KPMG LLP

Tel: +44 (0)20 7311 5103

ross.leaning@kpmg.co.uk

Daren Das

Analyst KPMG LLP

Tel: +44 (0)75 0756 1456

daren.das@kpmg.co.uk

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.

© 2008 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: Data Loss Barometer

Publication number: RRD – 102553

Publication date: September 2008

Printed on recycled material.