www.pwc.co.uk

Beyond awareness: the growing urgency for data management in the European mid-market

A study of attitudes, behaviour and best practice within European business, including an updated Information Risk Maturity Index

A PwC report in conjunction with Iron Mountain
June 2013

pwc

Contents

Foreword

Christian Toon
Head of Information Risk
Iron Mountain Europe

Navigating the information landscape

The information landscape in Europe has changed beyond all recognition. Every sector in every country is struggling to adjust to the transformation. Many are uncertain how to accommodate rapidly increasing volumes of information in multiple formats; the explosion of social media; the proliferation of mobile devices; changes in legislation and a rising malicious threat. At the same time, we are seeing a growing ambition to harness the value that can be contained in both structured and unstructured information. As a consequence, managing information is more complex today than it has ever been. And with increasing complexity comes increasing risk.

It is, therefore, timely that Iron Mountain and PwC have undertaken research to examine the state of information risk facing mid-sized businesses in Europe. This is the second information risk maturity index. Examining the data, it is heartening to see progress over the past 15 months. Awareness of information risk is growing, with businesses everywhere increasing their index score. The European average rose from 40.6 last year to 56.8 against a target of 100. Our research suggests that the increased awareness is creating uncertainty, as businesses recognise the need to act but remain unclear as to where to turn or what to do next.

What is now required is for the gains in awareness to be transformed into a strategy and set of actions to reduce exposure to information risk. This will require buy-in and involvement from the very top of the business. Those responsible for information management will need to learn to speak the language of the boardroom and open up a dialogue with other key stakeholders. The loss of customer loyalty, damage to brand reputation and the erosion of sales and revenue are key concerns for those tasked with managing the information, and these are concerns that should translate readily to board level. It is clear, however, that if real progress is to be made business should not only be concerned with the risk to reputation and customer loyalty but should also strive to realise the opportunity and value that can be unlocked when information is well managed as a business asset.

In producing this white paper we have aimed to not only uncover the level and complexity of the problem but to produce something useful for European businesses. The risk index and the online risk evaluation tool www.ironmountain.co.uk/risk-assessment are designed to provide insight that will help businesses to take the next step towards managing their information responsibly. This white paper outlines a set of actions that can equip businesses to improve their approach and thereby reduce their exposure to information risk and help them to harness the value of the information they hold.

Executive summary

'Put simply, the mid-market in Europe does not value its information enough, or understand its worth as a business asset.'

Claire Reid, Partner,
PwC Information Security

Businesses are struggling to manage the information they hold and as a result they are exposed to unprecedented levels of risk. Fraud, data breaches, and social media catastrophes are growing faster than businesses can respond. The mid-market in Europe is particularly exposed, yet remains complacent in its data management practices. Our study reveals that confusion about what to do next, is holding the mid-market back from acting to protect their businesses and realise the value of the information they hold.

Key findings of the study:

Awareness is no longer the problem. Our study shows that there is an increasing level of awareness among mid-sized businesses of the threat posed by exposure to information risk and a growing understanding of the need to take action.

- The average index score this year is 56.8 out of an ideal 100. This is a step forward from last year's score (40.6) when few were managing their information at a satisfactory level. Whilst there has been some improvement, the Index score is still low and there is a long way to go before data management practices reach acceptable standards.

- 68% believe a responsible attitude to information is critical to business success. Information, both paper and digital, customer and internal, is recognised as a valuable asset, and looking after it well can lead to untapped commercial benefits (as well as avoiding disaster).

- The survey results suggest that businesses are either unsure what to do next or remain ill-equipped to tackle the threat. Only 45% have an information risk strategy in place and monitor its effectiveness, while 44% expect the risk of a data breach to increase.

The information management challenge:

Our study shows that many are caught in a growing "swamp" of uncategorised paper and digital data that they don't know what to do with. As a result, confidential and sensitive information is more likely to be exposed to an increased risk of data breach.

- 36% keep all their information in case it is needed.

- 42% are worried about the security of their stored data.

A picture is emerging of confusion, contradiction and complacency around the management of information risk in the mid-market. Increasingly a gap is growing between attitude and action.

'93% of businesses employing more than 250 staff experienced a breach in the last year. The worst case average cost of every breach was £450k - £850k.'

Source: PwC Information Security Breaches Survey 2013

- 78% believe they need to do everything they can to prevent a data breach and yet a disappointing 47% say their Board does not see data protection as an important issue.
- The mid-market holds its suppliers to the highest security standards. Only 14% would work with a business that had experienced a data breach but businesses fail to hold themselves to the same standards.
- A high level of trust is placed in middle and junior management and support staff, in the absence of effective, monitored policies and controls to safeguard data. For example, 58% do not monitor their control systems for access to information.

In this paper we focus on the attitudes and behaviours that have emerged in our study. We highlight some key factors that are holding mid-sized businesses back from reaching their full potential.

Best practice to reduce information risk:

Building on last year's white paper, we have identified a set of steps and actions that will help the mid-market really raise its game and reap the commercial benefits that go hand in hand with protecting and valuing one of the most precious of business assets – paper and digital information. These actions include:

- **Take it to the top** - seek Board level support by taking a strategic approach to information management.
- **Take control of what you've got** - know what information you have, where it is, and decide whether you still need it.
- **Take your people with you** - operate a policy of controlled trust underpinned by a set of monitoring tools, policies and procedures.

The state of information risk today

The message is clear: every organisation with information to protect, regardless of size or sector, is at risk. At a time when data breaches, cyber attacks, and social media catastrophes are running at an all time high, businesses are being exposed to unprecedented levels of risk. Yet the mid-market continues to leave itself wide open to the irreparable damage that a data breach can cause.

Complacency, contradictory behaviours, poor data management practices and a lack of appreciation of the value of their information are not only placing businesses at risk, but are holding them back from reaching their full commercial potential. There is an evident lack of trust in organisations that have experienced a data breach, and those that can demonstrate that they look after their data well, will have a clear competitive advantage.

Our recent research study, commissioned by Iron Mountain, reveals that the mid-market is still not treating its data well. Whilst there is evidence of some improvement in data management practices across the European mid-market, poor data practice remains rife. PwC conducted the second of its annual series of surveys of 600 mid-sized businesses (those with 250-2,500 employees, defined as the mid-market) across six European countries: the UK, France, Germany, the Netherlands, Spain and Hungary. This paper builds on the findings of our 2012 report 'Beyond Cyber Threats', which introduced Europe's first Information Risk Maturity Index, and highlighted that the mid-market needs to become much better equipped to manage information risk.

The 2013 index indicates that there has been some improvement in the information security practices of the mid-market, but with an index score of 56.8, there is still a long way to go.

Information Risk maturity Index 'zone descriptors'

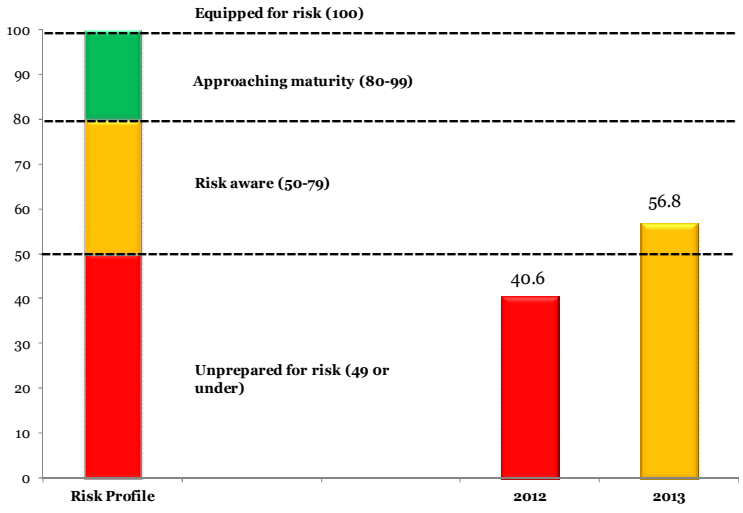
Equipped for risk Businesses have implemented a responsible approach that encompasses strategy, people, communications and security from top to bottom. They monitor, evaluate and improve their approach to manage effectively their exposure to risk.

Approaching maturity Businesses have established some measures and there is greater awareness from senior leaders. They have reduced their exposure but fall short of being able to implement a robust strategy.

Risk aware Businesses have woken up to the need to manage risk. However, they are uncertain about what to do or remain ill-equipped to tackle the threat.

Unprepared for risk Businesses are severely exposed to information risk. They are unlikely to have an information risk strategy in place and senior management are unaware of the potential impact to their business.

Information Risk maturity Index 2012-2013



Base: 600

Mid-market complacency continues...

Only 45% have an information risk strategy in place and monitor its effectiveness.

Only 38% have a formal business recovery plan.

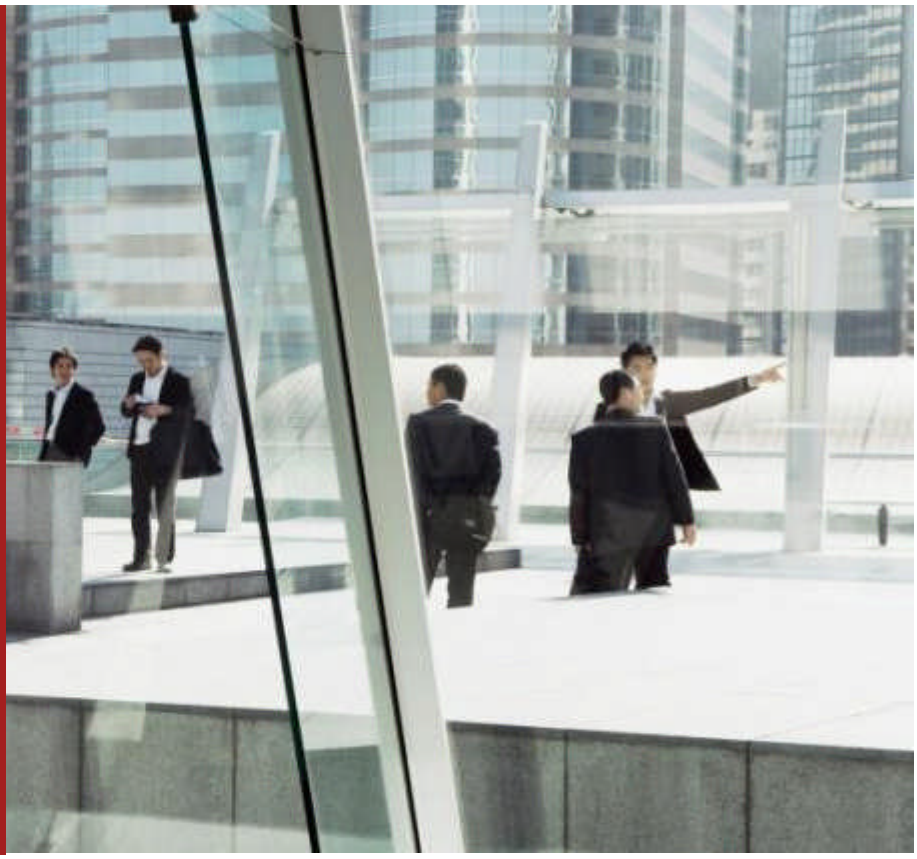
Only 32% monitor the effectiveness of their corporate risk register.

Only 28% run and evaluate employee communication programmes to re-inforce information risk procedures.

Only 45% monitor the effectiveness of the team responsible for information risk.

Only 39% monitor the effectiveness of their data classifications.

Only 26% evaluate the return on investment for their information security spend.

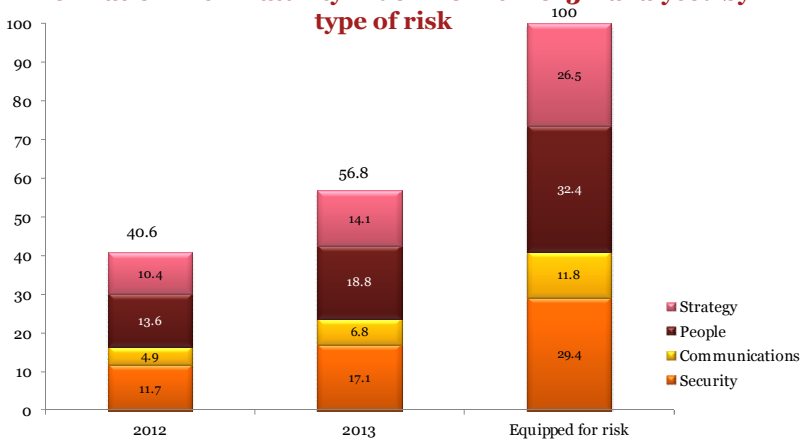


'Businesses must embrace a new way of thinking in which information security is both a means to protect data and an opportunity to create value to the business.'

PwC Global State of Information Security Survey 2013

The mid-market has moved out of the danger zone but businesses should still be concerned about the level of risk that they are being exposed to. In a world where the daily likelihood of a data breach is increasing exponentially, businesses need to have better plans in place to protect themselves. There is no reason why all mid-market organisations should not aim for the maximum score of 100, meaning that they are equipped for risk.

Information Risk Maturity Index 2012 & 2013 - analysed by type of risk



To attain a score of 100, businesses need to put in place and monitor the effectiveness of the 34 measures set out in our index (described in the appendix of this document). None of these, in our view, are difficult to implement or monitor, yet our study indicates that the mid-market has a long journey ahead, and appears to be confused about what to do next.

It is positive that mid-market businesses are now more diligent about monitoring the effectiveness of their information management practices especially in the area of data security. The people agenda has also witnessed additional focus. On balance, however, around half of the businesses in our study still need to significantly improve their information management practices.

Key study findings

55% of French firms have a monitored information risk strategy in place compared to 34% in the UK and 45% overall

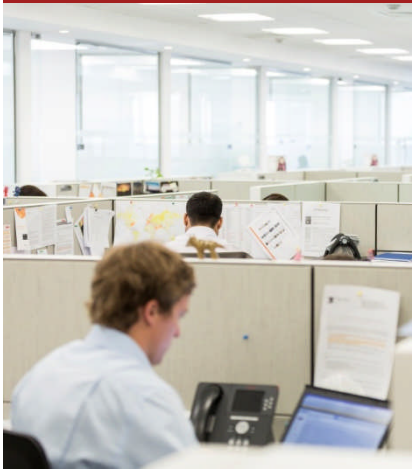
40% of Dutch and 38% of Hungarian firms have a monitored corporate risk register, compared to 21% in Germany and 32% overall

52% of Dutch firms have a strategy for the secure disposal of hardware and confidential documents. Only 26% have this in place in Spain, and 41% overall.

61% in Hungary and 59% in the Netherlands have clear employee guidance on the safe secure disposal of physical documents, compared to 50% overall and 36% in Spain.

35% of legal firms have a monitored information risk strategy in place, compared to 55% in the insurance sector and 45% overall.

54% of manufacturing and engineering firms have a specific team in place with responsibility for information risk. 34% of legal firms have this in place, and 45% overall.



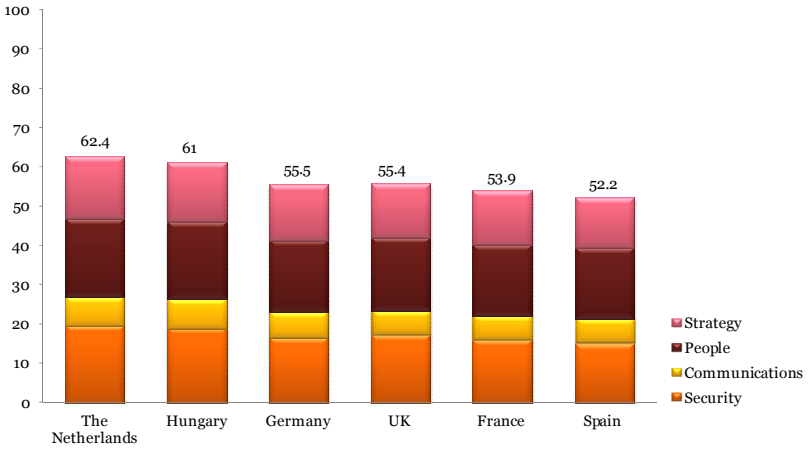
The key area for improvement relates to their lack of strategic focus on information management. More than half do not monitor the effectiveness of their information risk strategy, if they have one.

The mid-market needs to wake up to the fact that information is a critical strategic asset for organisations and must be treated and accounted for accordingly. In a period of recession this is even more important. Doing more with less requires working smarter, not just harder, and the most successful organisations are achieving this not only by approaching and exploiting information as an asset, but by also placing a value on this asset. They have realised that we only really take care of what we value.

Country variations

The Netherlands and Hungary have achieved the highest index scores, at 62.4 and 61.0 respectively, with the Netherlands witnessing a significant improvement in the past year.

Information Risk Maturity Index 2013 - analysed by country



Amongst the six countries involved in our study, the Netherlands stands out as being the most strategic in its approach to information risk. For example Dutch businesses are more likely than their counterparts in the other countries to have a contingency plan in place to respond to small scale data mishaps, a corporate risk register, a strategy covering mobiles, personal devices and laptop security and a strategy for the secure disposal of hardware and confidential documents. In addition, the Netherlands, along with France, was the most likely to treat information risk as a Boardroom issue.

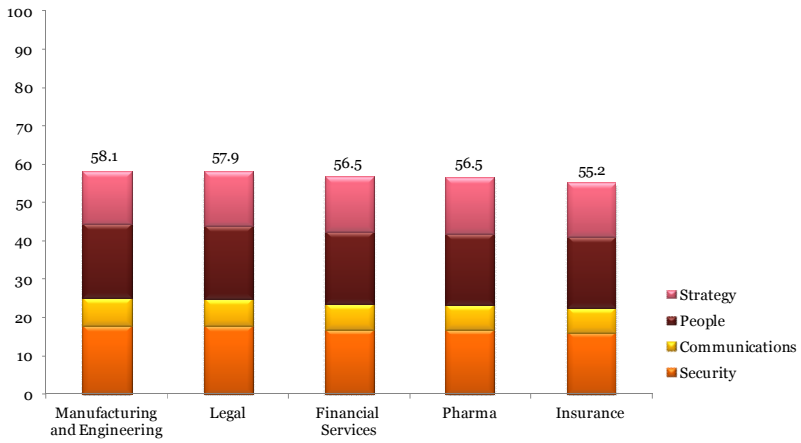
In Hungary the main improvements have related to employee training measures and communications, with a strong focus on providing employee guidance on the storage and disposal of electronic and physical documents.

In contrast, Spain has the lowest index score, at 52.2. Interestingly, Spanish firms are the least likely to see their employees as a threat to information security. At the same time they are behind their European counterparts with regard to the provision of employee guidance on internal policies and procedures, and are least likely to have some of the key security measures in place, such as due diligence programmes for the handling of personal, customer or employee information, intrusion detection systems and recognised data classification systems.

Sector variations

From a sectoral perspective, all five sectors in our study have raised their game and are at a similar level of maturity, whilst still at the lower end of the 'amber' zone.

Information Risk Maturity Index 2013 - analysed by sector



Legal and manufacturing & engineering have seen the largest increases since 2012. There is evidence to suggest that manufacturing & engineering firms are increasingly taking a more strategic approach, with more having an information risk strategy in place, and a formal business recovery plan. This sector is also much more likely than the others to consider employees as a threat to information security, and compared to last year have placed a stronger focus on people and communication measures.

The legal sector has improved across most of the 34 measures, but is still the least likely of all the sectors to have an information risk strategy in place, and a specific team or individual in place with responsibility for information risk.

Information Risk Maturity Index Ranking by country: 2012 – 2013.

Country	2012	2013
Netherlands	**5th**	**1st**
Hungary	**1st**	**2nd**
Germany	**4th**	**3rd**
UK	**6th**	**4th**
France	**3rd**	**5th**
Spain	**2nd**	**6th**

The need to manage the growing data swamp

'In today's hybrid paper-digital information world, firms risk drowning in a swamp of complexity and confusion unless they take charge of their information. A responsible and accountable approach to information is vital if businesses want to realise the benefits of this important business asset. Such an approach is critical if businesses are to deserve and preserve their hard-won brand reputation and customer loyalty.'

Christian Toon
Head of Information Risk
Iron Mountain

'Every hour, enough information is consumed by internet traffic to fill 7 million DVDs. Side by side they'd scale Mount Everest 95 times.'

IMS research for IBM, 2013

Many mid-market businesses are slowly becoming submerged in a "swamp" of unstructured data that they don't know what to do with. The data swamp has formed as a result of businesses not having policies, processes or technology in place to help categorise information and identify what should be retained, how it should be stored and what can be destroyed. As a result, many businesses are retaining all of their digital and paper information, often meaning that large amounts of confidential and sensitive data can be accessed by employees or contractors, increasing the chances of a data breach.

Over a third of the businesses in our study keep all of their information in case it is needed. A further third need to seek legal advice before deciding what to do with their data. It is well known that the amount of data, digital and paper, being created year on year is growing exponentially, so if businesses continue to keep everything, maintaining a growing data swamp will be costly and could expose the business to risk. For example, certain types of documents need to be securely destroyed according to legally mandated retention periods and failure to do so can result in fines and damage to the reputation of the business. On top of this, many businesses are concerned about the security of their stored data. Clearly, access to stored data must be managed, and appropriate controls put in place to prevent a data breach occurring.

The rise of digital data, across various remote formats, including the proliferation of shared data supply chains, is also creating an environment whereby the mid-market is struggling to control the "chain of custody". Critical business information is now available in multiple formats, and in hard and soft copy, to larger groups of people, again increasing the risk of a data breach.

The more information an organisation retains, the greater the likelihood of exposure to complacent, curious, untrained, disgruntled or malicious staff. As we pointed out in *Beyond Cyber Threats,* one of the biggest threats to the integrity of information in the workplace is the behaviour and attitudes of its employees. Organisations that have a growing swamp of uncategorised data, exacerbate this threat immeasurably.

'90% of the data in the world today has been created in the last two years'

IBM
Understanding Big Data - IBM Big Data Platform

'Three quarters of UK employers said they had no enforceable system to prevent employees gaining unauthorised access to company data.'

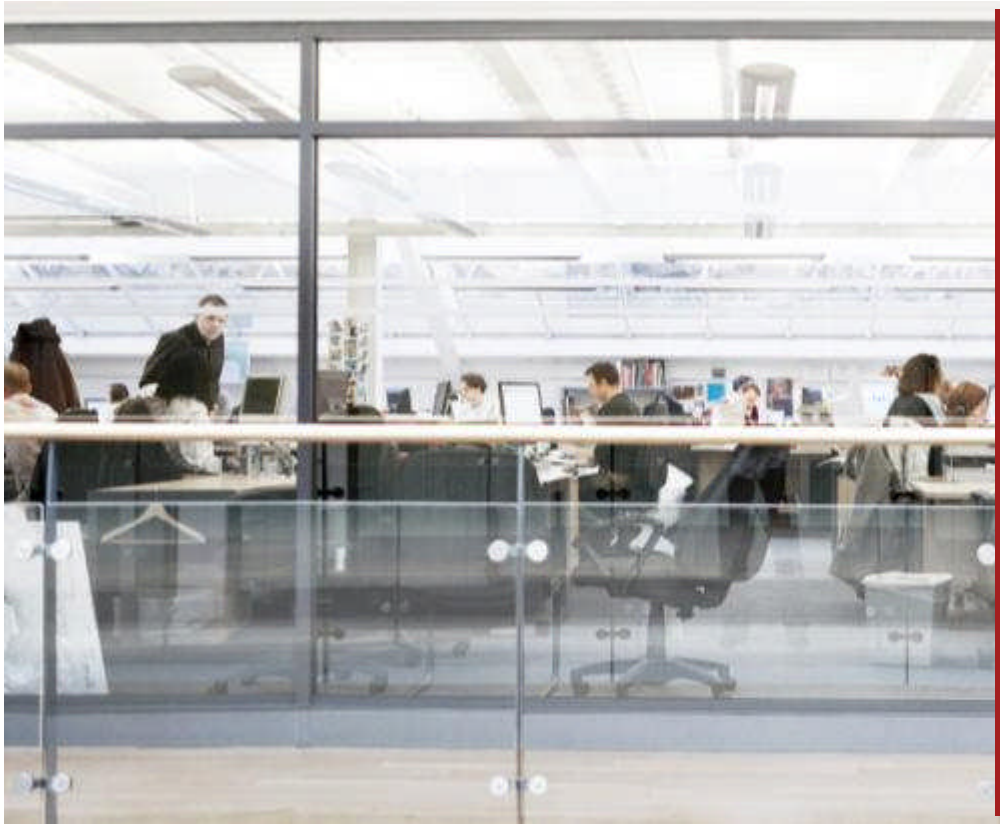
UK Insider Threat Survey, LogRhythm. April 2013

Even the front runners – businesses that lead the way in information security – are struggling with data retention. Our study shows that they are just as likely to keep everything just in case.

From a country perspective, France has the biggest data swamp, with half of the businesses in our study retaining all of their data. Spanish businesses have the lowest levels of retained data, and are the most likely to use a third party to manage data retention on their behalf.

It is more a case of not knowing what to do, than blissful ignorance. When asked what they considered to be their main challenge going forward, 41% commented that they are worried about managing their paper legacy. This was particularly true in Germany and Hungary, and in the legal sector across Europe, where almost half of the businesses that we spoke to felt challenged regarding the management of their paper documents. Another concern facing the mid-market is the security of stored data. 42% hold this concern, rising to 48% in France and 52% in the insurance sector.

As well as focusing on developing the right behaviours amongst staff, the mid-market needs to tackle its data swamp before it is too late. Getting up to speed with data retention legislation and guidance is essential. Classifying and securely storing data that must be retained, and undertaking secure destruction of unnecessary data is a must. Businesses need to act now before the swamp becomes uncontrollable and starts to leak.



Key study findings

36% keep all of their information in case it is needed

31% seek legal advice regarding data retention before taking action

41% see 'managing their paper legacy' and a major future challenge

42% are worried about the security of their stored data

61% do not monitor the effectiveness of their data classification systems, if they have them

The obligation to educate your people: can you trust the trusted?

Key study findings

Only 14% would do business with an organisation that has had a data breach

Only 25% believe that employees are a serious threat to information security

82% trust their employees to follow their information risk policy

45% do not monitor employee social media usage

Case study

An innovative move by Kent police to appoint a "youth" police commissioner has spectacularly backfired due to the teen's personal social media accounts. Paris Brown, 17, was chosen out of more than 160 applicants to act as the "voice of the youth" for Kent Police. However, it later emerged that her personal Twitter account was found to have racist, homophobic and crude tweets dating back months. The Kent Police Commissioner admitted the teen's social media accounts were not checked prior to her appointment.

The mid market is showing signs of confusion and inconsistency in its attitudes to information risk. Our study reveals that 58% would not do business with an organisation that has had a data breach, yet many continue to put their own data at risk. With only 45% having a monitored information risk strategy in place in their own organisation, this effectively amounts to a 'double standard' of external vigilance tempered by internal complacency.

Mid-market businesses need to start applying the standards they use when selecting suppliers and contractors, to their own business. They are failing to realise that their own customers are likely to have the same view, and will withhold business in the event of a data breach.

Last year *Beyond Cyber Threats* highlighted that a step change in business culture and employee behaviour is essential if the information assets of the European mid-market are to be safeguarded. This year's study shows that businesses are very aware of the impact of a data breach on their business, but continue to be unperturbed about the threat from within. 25% of the businesses that we consulted believe that employees are a serious threat to information security, yet 82% trust their employees to follow their information risk policy (if they have one).

Mid-market businesses continue to tell us that the IT security manager is the main guardian of their information, and the person ultimately responsible for information risk within the organisation. Ironically, when asked who they worry about as the greatest risk for a data breach, over half cited the IT team. It is understandable that the people who are given greatest responsibility for and greatest access to the most sensitive and confidential data are considered the greatest risk.

Who do you worry about as the greatest risk for a data breach?

'80% of UK employers said they did not believe any of their employees would steal confidential information, yet a poll of employees showed that 23% had accessed or taken confidential data from their workplace.'

UK Insider Threat Survey, LogRhythm, April 2013

Middle managers, junior staff, PAs and cleaners are perceived to pose a low risk of causing a data breach according to our study, presumably because of relatively limited access. However even the most trustworthy of employees have the potential to make a mistake, yet many organisations do not have controls in place to protect themselves against simple human error. For example, 61% of organisations that we spoke to do not monitor the effectiveness of their data classification systems, and 58% do not have or do not evaluate their control systems for access to company archives and other sensitive information.

Employee screening procedures were also found to be lacking in many mid-market businesses, with less than half checking employer references, and only 40% undertaking police checks or reviewing criminal records. In addition few are checking the easily accessed, publicly available information available on social media sites such as Twitter. It seems that many mid-market businesses are bestowing a large amount of trust on people that they know very little about. Many organisations also lack the commitment to communicating and training staff on their information policies and procedures (where they exist). Instead they place a high reliance on employee trust.

Having trust in employees can be a good thing but the problem is that many of the breaches that have occurred to date have been caused by human error. It is therefore important to operate a policy of controlled trust, and to have adequate policies, training courses, communications and security controls in place to protect information from both malicious intent and hapless blunders.

In a world where social media is everywhere, and with 88% of consumers using the same mobile device for personal and work purposes (PwC data), the potential for harm is huge and there are many high profile examples to prove it.

The average data thief is:

- *A current employee*
- *Male*
- *37 years old*

In about half of the cases studied the employee stole trade secrets, followed by business information (billing information or price lists) and in 75% of cases they had authorised access to the data they stole.

Insider Data Theft: When Good Employees Go Bad
Symantec, December 2011

The value of information

The business world has changed and companies in all countries and across industries, are now routinely sharing information across business borders, whether it's with business partners or employees' personal devices. It is no longer only an IT challenge; business leaders need to make sure they are protecting what is most critical to their organisation's growth and reputation.

Andrew Miller, PwC Information Security Director

Key study findings

59% believe that the costs of properly protecting their data outweighs the risks.

54% believe that the pace of change is staggering and they will never keep up with it.

Information is a strategic business asset, and treating it as such can offer the opportunity for a multitude of commercial rewards, not least a strong competitive advantage. Sadly, despite the fact that most mid-tier businesses believe that treating information as a business asset is 'the next big thing' very few are demonstrably pursuing that goal.

The mid-market is also well aware of the impact of a data breach. Two thirds believe that a data breach will have a detrimental impact on customer trust and loyalty. Indeed the fact that most businesses in our study would not trust another organisation that has experienced a data breach also demonstrates this point. Around half consider that a data breach would be harmful to their brand reputation and believe it would damage sales.

In your view, what impact would a data breach have on your business?

'

Clearly, concern for customer loyalty, not compliance is the main motivation for organisations to better manage their information

We have spent over fifteen years and £100m developing high-speed brushless motors, which power our vacuum cleaners and Airblade hand dryers. We are demanding the immediate return of our intellectual property'. Dyson court papers supporting an industrial espionage claim. October 2012

.

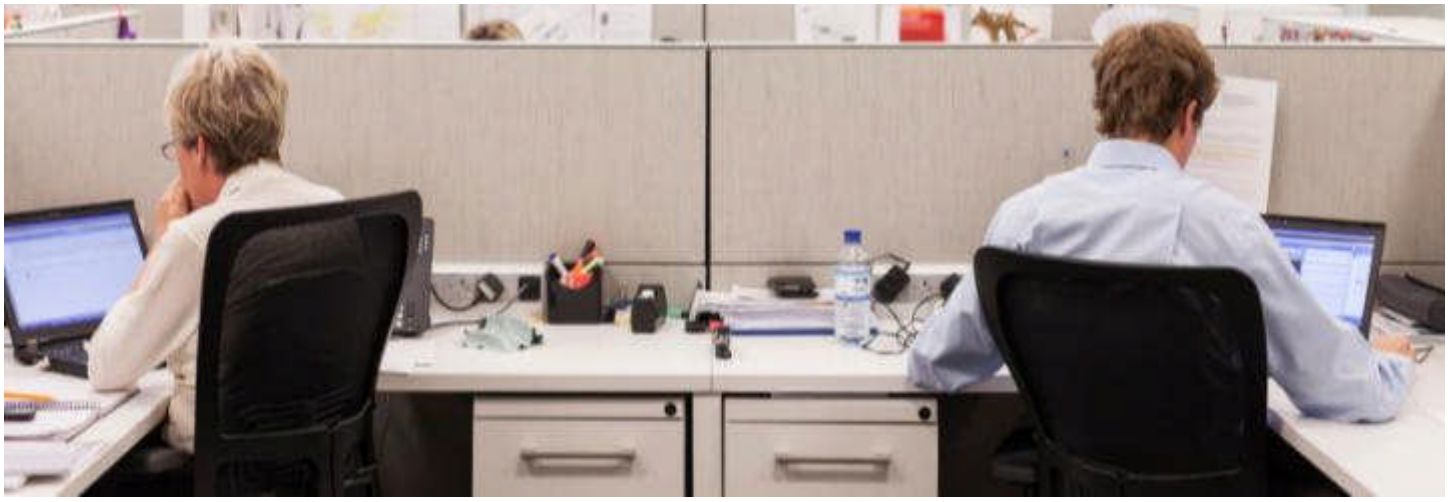
Members of the UK Civil Service Sports Club, of which there are 130,000 nationwide, have been informed that their names, addressees, dates of birth and national insurance numbers have been stolen from a central computer database. The details were then used in frauds.

Daily Telegraph 27.11.2012

We know that complacency is a big issue, but what else is holding organisations back? Our research suggests that the European mid-market is struggling most with the strategic aspects of information management. They are also worried about cost, and feel overwhelmed with the pace of change.

Only a minority of businesses are getting anywhere close to treating their information as an asset and even fewer actually place a value on it. Most (74%) do not measure, or know how to measure the return on investment for their spending on information security. Many do not have the capability and skills within their organisation to adequately manage their information asset and 35% consider this a challenge. People who don't know how to do things rarely do them well.

Academic research showing that companies consistently underestimate the value of information both absolutely and relatively in comparison to material goods supports our findings. Consequently, businesses must (a) invest, both capital and time, to develop effectively integrated and monitored information management programmes and (b) re-balance priorities towards viewing information from a business value as opposed to cost and risk perspective



Adopting best practice

'The only way to secure data in motion and data at rest is by designing an overall information security strategy based on a good understanding of threats to the business and implementation of a layered security monitoring approach which tackles data throughout its lifecycle.'

Claire Reid
PwC Information Security Partner

The findings presented in this report are challenges that are prevalent throughout the industry. Luckily security experts are finding solutions and actions which can reduce the risk of information loss. In our opinion, the following are some of most effective actions that can yield good results.

Step 1: Take it to the top

Get Board level support by taking a strategic approach to information management

- Develop an effective information risk strategy and monitor its effectiveness. Take a structured approach to developing a strategy, as follows:
    - Determine how data is stored, transferred and disposed across internal and external networks;
    - Determine the required technology, process and people controls for managing information at various stages of its lifecycle;
    - Design and implement controls using the fundamental principles of information security, resilience and reliability;
    - Foster a company-wide culture of information responsibility. Work with your HR team who have a leading role to play in the mitigation of information risk.
    - Don't forget your paper: simple steps, including document classification, secure storage and accessible shredding can help engender the company culture required to deliver this step-change.
- Place information security on the Board's agenda. Influence the Board's agenda by talking their language, and by finding out what is important to them. There is a linkage between continued customer loyalty and perceptions of how organisation's manage and protect customer data. Board level direction, in terms of behaviours and actions, can lead to a commercial advantage if implemented and monitored effectively.
- Value your data as an asset and demonstrate to employees that you mean it – put it on the balance sheet, or seek advice in terms of measuring the return on investment from your information security spend. Work out what it would cost to replace your data.
- Engender a culture of shared responsibility for information management amongst employees. Ensure employees realise that it's their personal responsibility too.

Step 2: Take control of what you've got

Know what information you have, where it is, and decide whether you still need it

- It is easy to think that your stored data is just electronic information, but don't forget your hard copy records, how these are handled, and other formats you may use.
- Identify senior business sponsors to champion information responsibility, to each of these formats across the organisation.
- Identify what you've got, the amount of electronic storage by file types or database, quantities of physical records and/or multimedia. Ideally break this down by business function or type.
- Identify where it is located. Is it in-house, with a third party, your home country, outside the EU?
- You should identify what you have and where it is located. This will drive priorities to manage your risk and costs.
- Develop and communicate a process of information governance which must include data classification, storage protocol, data handling conditions, data retention or review rules and back up.
- Information retention periods are crucial for managing costs and compliance. Don't keep it longer than you need to.
- Once you have a classification policy, make sure you set an access control process for access to sensitive information and restrictions on large amounts of data to be transferred.
- Call an 'amnesty' period for internal employees to get their act right and comply with the information governance model. This would mean that employees either store data in allocated storage servers or get rid of all local data which is no longer needed.
- Reward positive behaviour and address poor performance when it comes to information management.
- Have your business sponsors monitor and review your information governance model.

Step 3: Take your people with you

Operate a policy of controlled trust

- It is important, and of benefit, that business leaders trust their employees. However, with ever growing threats (both malicious and unwitting) this trust must be in a controlled context.
- This is defined by an agreed set of monitoring tools, policies and procedures that underpin and complement the overarching trust.
- Develop a clear social media usage policy for staff, and run a training programme to educate them.
- Promote social media usage through the appropriate channels, including clear guidance in terms of what can, and cannot, be said.
- Be specific about what employees can and cannot post. For example prohibiting "inappropriate comments" is too vague. Tell them not to mention company names, specific projects and people.
- Encourage and empower employee "champions" to become brand ambassadors, by saying positive things about your business as a place to work on their personal social media sites.
- Run controlled internal monitoring drills to provide insight on how employees behave when confronted with a potential security threat.
- Communicate the purpose and nature of the monitoring drills, and use this as an opportunity to educate employees on how to react in the event of a data breach.
- Become more disciplined in the way confidential data is drafted, constructed and stored. For example, confidential documents being labelled and master documents designed in a manner that can be caught when taken out of the organisation (through data loss prevention tools).
- Control email traffic going to personal email destinations by implementing controls on the email gateway.

Appendix: research methodology

Introduction

In order to support this paper, PwC and Iron Mountain developed a robust research methodology to support the conclusions presented. This methodology has built upon the insights and lessons learned as part of the 2012 study. In the first instance, we worked closely with Iron Mountain to assess the themes which emerged from the 2012 study, and using these insights developed a comprehensive questionnaire which was largely based around the key themes of the paper, in terms of the extent and effectiveness of business approaches to managing information risks from a people, communications and security perspective.

This was supplemented with a series of 'attitudinal statements' to form a deeper understanding of why such practices pertained at both an overall level and at the sector and country levels. For comparability, the overall statements that underpin the risk maturity index were kept in the same format as 2012. The questionnaire was designed by PwC's in house team of research specialists with expert insight and contributions from the PwC Risk Assurance team, led by Claire Reid.

We worked closely with our research fieldwork partner, Coleman Parkes, to ensure the design of the questionnaire was in a compatible format to be uploaded to their computer assisted telephone interviewing suite (CATI) and that this was available in the native languages of our respondent sample base.

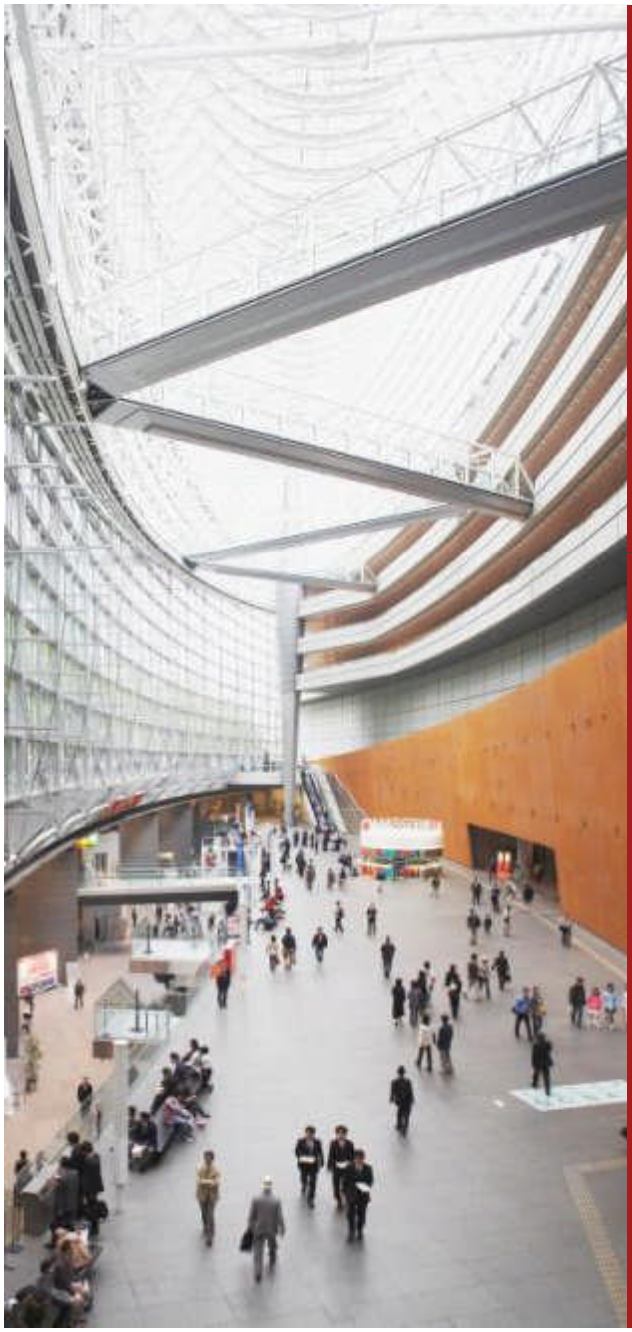
Who did we speak to?

Respondents to the telephone survey were typically CEO's, CFO's, CIO's and Directors in order to provide a senior business perspective and insight into the nature and extent of the most pressing information risks and of how these are being managed. The telephone interviews were conducted proportionally with respondents from the key markets and sectors in order to allow for a detailed level of comparative analysis to be undertaken.

To develop as much insight from this study, we embarked upon a comprehensive "mine" of the data by supplementing the topline findings with specific cuts, particularly in terms of market and sector specific trends. This analysis also included assessing the key changes identified between the 2012 and 2013 insights supported and informed by the attitudinal statements. We also sought specific input from our PwC network subject matter experts from each of the European countries represented in the research.

In a similar way as in 2012, we devised an information risk maturity index. This index was populated through applying a weighted average of each individual company response to 34 statements which were included in our study. The 34 statements were grouped under the four defined business areas of 'strategy', 'people', 'communications' and 'security' and categorised as shown overleaf.

Which of the following does your organisation have in place?



Strategy

1. An information risk strategy or approach.
2. A formal business recovery plan or strategy.
3. A contingency plan to respond to small-scale information 'mishaps' or data losses.
4. Regular privacy policy reviews.
5. A corporate risk register.
6. An information security strategy covering mobile, personal devices and laptop security.
7. A strategy for managing structured and unstructured information in digital and physical forms across multiple locations.
8. A strategy for the secure disposal of technology hardware and confidential documents.
9. A strategy that prioritises access to business-critical and highest risk documents that arise most often in compliance requests.

People

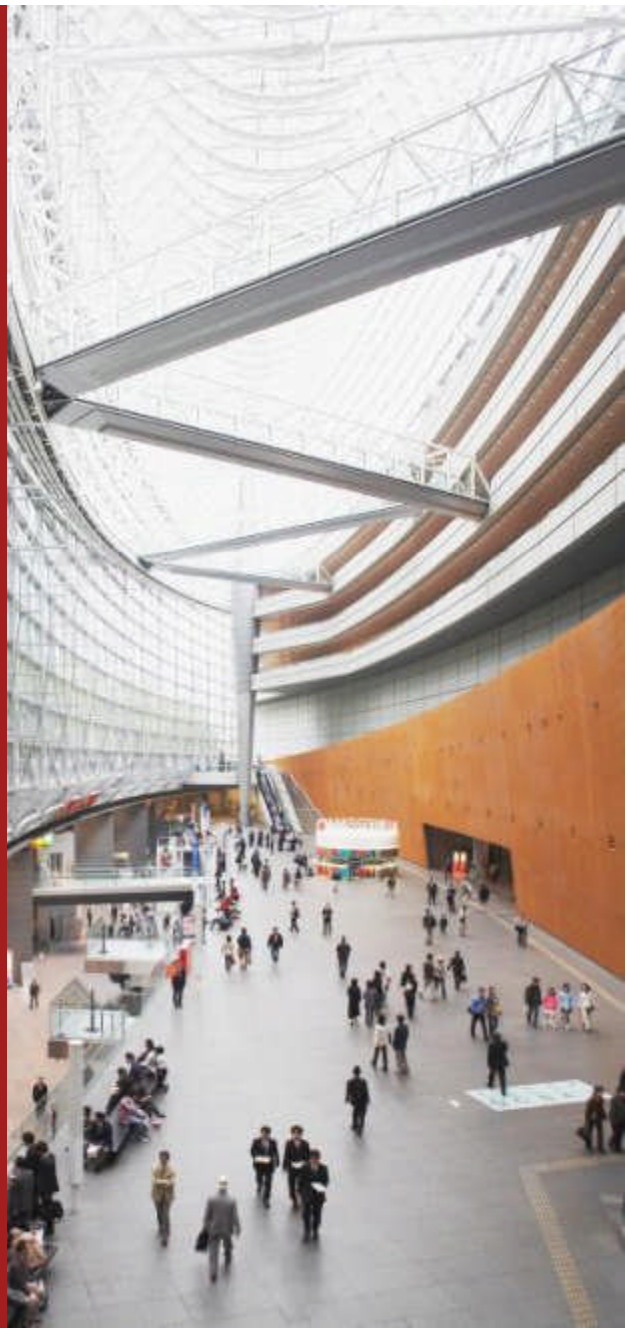
10. A specific individual or team responsible for information risk within your organisation.
11. An exit process for employees who leave your organisation to prevent the stealing or copying of information.
12. Training programmes to brief employees on information risk issues.
13. Information risk awareness included as part of induction training.
14. Ongoing 'refresher' training programmes.
15. Effective computer-based information risk training programmes.
16. Personnel background checks.
17. A code of conduct concerning the correct behaviours for all employees.
18. A tool to measure employee confidence in the effectiveness of your information risk activities.
19. An internet usage policy for all staff.
20. A Social Media usage policy for all staff (for example, Facebook, Twitter and LinkedIn).

Communications

21. Availability of easily accessible risk information for all employees.
22. Employee communication programmes to reinforce information risk procedures.
23. Clear employee guidance on internal procedures for the safe disposal and storage of physical documents.
24. Clear employee guidance on internal procedures for the safe disposal and storage of electronic documents.

Security

25. Company policies for the safe security, storage and disposal of confidential information.
26. Due diligence programmes regarding the handling of personal, customer or employee information.
27. An inventory of the locations of where your information is stored.
28. A centralised security information management database.
29. Technology to look at intrusion detection systems and intrusion prevention systems.
30. Third party validation, for example penetration testing.
31. Clear, updated and recognised data classifications.
32. Control procedures in terms of access to buildings, restricted areas, company archives and other sensitive information.
33. The use of different rules and processes for storing data taking into account different document retention periods and data protection requirements.
34. Incident notification processes, for example, how to spot something that shouldn't be there.



Report authors

Claire Reid

Partner, PwC Risk Assurance

T: +44 (0)207 212 5513

M:+44 (0)7734 607594

claire.reid@uk.pwc.com

David Armstrong

Partner, PwC International Survey Unit

T: +44 (0)28 90 245454

M: +44 (0)7713 680266

david.m.armstrong@uk.pwc.com

Julie McClean

Senior Manager, PwC International Survey Unit

T: +44 (0)28 90 245454

M: +44 (0)7738 313241

julie.mcclean@uk.pwc.com

Biju Mukund

Senior Manager, PwC Risk Assurance

T: +44 (0)207 213 1701

M: +44 (0)7850 907913

biju.mukund@uk.pwc.com

Kieran Jones

Senior Associate, PwC International Survey Unit

T: +44 (0)28 90 245454

M: +44 (0)7845 635383

kieran.p.jones@uk.pwc.com

www.pwc.com