www.pwc.co.uk

Beyond cyber threats:

Europe's First Information Risk Maturity Index

A PwC report in conjunction with Iron Mountain

March 2012

pwc

Contents

Foreword

Information is the lifeblood of every business. Paper files and folders, back-up tapes and digital archives represent a treasure trove of customer insight, employee knowledge, business intelligence and innovation. At the same time, information presents one of the greatest legal and reputational risks to businesses of all sizes. You only have to pick up a newspaper to see what can happen to your customer relationships, brand reputation and sales if information is lost, damaged or exposed.

Like any other business asset your information is exposed to risk. You can only protect your information if you know where the risks are, how likely they are to occur, and how best to manage them.

To understand the levels of information risk within European mid-market businesses' and their capability to mitigate against this, Iron Mountain commissioned PwC to study 600 mid-sized businesses across Europe. The results reveal a deeply concerning picture of complacency, ignorance and lack of management that should sound an alarm bell across the European community.

The findings are particularly worrying at a time when companies of all sizes and in all sectors across Europe are producing and processing electronic and paper records at ever-increasing speed in an ever-more stringent regulatory environment.

Information risk is a board-level issue. If you only take one thing away from this report, it should be an understanding that the key to managing information risk starts and finishes with your people and business culture. Do not expect technology alone to solve the problem. People are often the weakest link when it comes to information security, but they are also a company's secret weapon when it comes to cost-effective information security management. Information risk management should be part of the cultural DNA of your business and establishing a culture of responsibility can only be successful when the drive and example comes from the top.

We hope that this report will encourage you to review the approach your business takes to information risk and take on board the recommendations and practical steps suggested.

We hope you take action not simply because your customers are calling for it, or the legislators demand it, but because it is the right thing to do. Take action because the success or even survival of your business could depend on it.

Christian Toon
Head of Information Risk
Iron Mountain Europe

Executive summary

This report presents the findings from Europe's first Information Risk Maturity Index. The Index clearly shows that European mid-market businesses have a long way to go to bring their information security practices up to acceptable standards.

Across our sample of 600 European businesses, the performance was poor, with an average index score of only 40.6 out of a maximum possible score of 100. In the current commercial environment, a score of anything less than 50 is bad news for companies, their customers and their collective peace of mind.

Our study reveals that 59% of businesses believe that investing in technology will facilitate data protection. This suggests, firstly, that data security is widely perceived by business as mainly an IT issue, which it is not. Secondly, and related to this, it suggests that investing in technology is often perceived as the appropriate solution. However, this ignores a growing body of evidence which shows that one of the biggest threats to data security centres around corporate culture and employee behaviour.

The evidence in this report illustrates why all businesses should take heed. The risks they face are extensive, with the potential to make the difference between success and failure.

Our study shows that over 60% of mid-cap businesses in the countries surveyed are not confident that their employees, or their executives, have access to the right tools to protect against information risks.

Based on the findings of our Information Risk Maturity Index, we have identified a set of steps and actions that, if put in place and frequently monitored, will help protect the digital and paper information held by businesses.

- *Step 1: Make information risk a boardroom issue* – ensure that it's a permanent point on the Board's agenda, that there's a senior individual on the Board responsible for it, and that it is embedded into the Board's dashboards that are used to monitor overall corporate performance.

- *Step 2: Change the workplace culture* – design and deliver information security awareness programmes, have the right guidance available for every person and at every level, and reward and reinforce the good behaviours throughout the organisation, from the most junior employee to the most senior.

- *Step 3: Put the right policies and processes in place* – and ensure these cover all information formats (electronic, paper or media), define any vulnerabilities relating to manual information handling, establish whistle blowing protocols, and review and test all systems and processes on a regular basis.

These actions are fundamentally about developing a business culture in which information risk awareness is at the core of day-to-day employee tasks and activities.

Businesses need to act, and they need to act now. Doing nothing is not an option. A step-change in business culture and employee behaviour is required. Anything less will simply not be sufficient.

1 Information: a priceless resource

> *"Information is a priceless resource that must be protected. There's currently a massive gap between what businesses are currently doing to protect themselves, and what they should be doing."*
>
> ***William Beer***
> *PwC One Security Director*

Company A lost a USB stick containing customer profile data. This resulted in extensive adverse media coverage, and more than £100,000 in cash costs.

A courier carrying financial services back-up tapes was robbed. This led to several man-weeks of investigation to check that the data had not been misused.

Source: Information Security Breaches Survey (ISBS) 2010, Infosecurity Europe/PwC.

In June 2011, Nintendo joined on-line games company Sony and US defence contractor Lockheed Martin, in admitting that their information had come under malicious internet attack. The announcement came just days after the UK's Chancellor of the Exchequer, George Osborne, told an international conference that British government computers receive over 20,000 malicious email attacks every month.

The message is clear: no organisation, of any size, in any sector and with information to protect, is safe.

Customer records, internal data, paper and digital, businesses handle a massive amount of data and information every day. The mismanagement and potential loss of this information ruins brand reputations, undermines customer and stakeholder confidence, removes competitive advantage and can cripple a business overnight.

The cost of rectifying the impact of this mismanagement can be huge. The capital and operating costs alone can cause irreparable damage, never mind the indirect or hidden costs associated with brand damage, loss of intellectual property or lost customer confidence.

Yet data mismanagement and loss, including small scale leakage, accidental deletion and high profile security breaches, is growing exponentially and this rise is expected to continue.

Our recent research study, commissioned by Iron Mountain reveals, however that mid-market businesses are not good at managing and protecting their information. PwC conducted a survey of 600 mid-sized businesses (those with 250-2,500 employees) across 6 European countries: the UK, France, Germany, the Netherlands, Spain and Hungary. This paper explores the various approaches taken to protect and secure business information and reveals that complacency, ignorance and poor management are widespread across the mid market.

Our Information Risk Maturity Index puts a spotlight on the massive gap that exists between what businesses are currently doing and what they should be doing. It highlights that most midmarket businesses are not looking after their (and their client's) data at all well.

It highlights the widespread view that investing in technological solutions to keep data and information secure, is the answer. However the research also reveals a lack of focus on corporate culture and untrained, unmanaged and unchallenged employee behaviours leaves the mid-market open to a Pandora's Box of risks and dangers.

In January 2011 the World Economic Forum named cyber attacks as one of the top five threats facing the world. This paper highlights that cyber attacks are not the only threat to the integrity of information in the workplace.

Key study findings

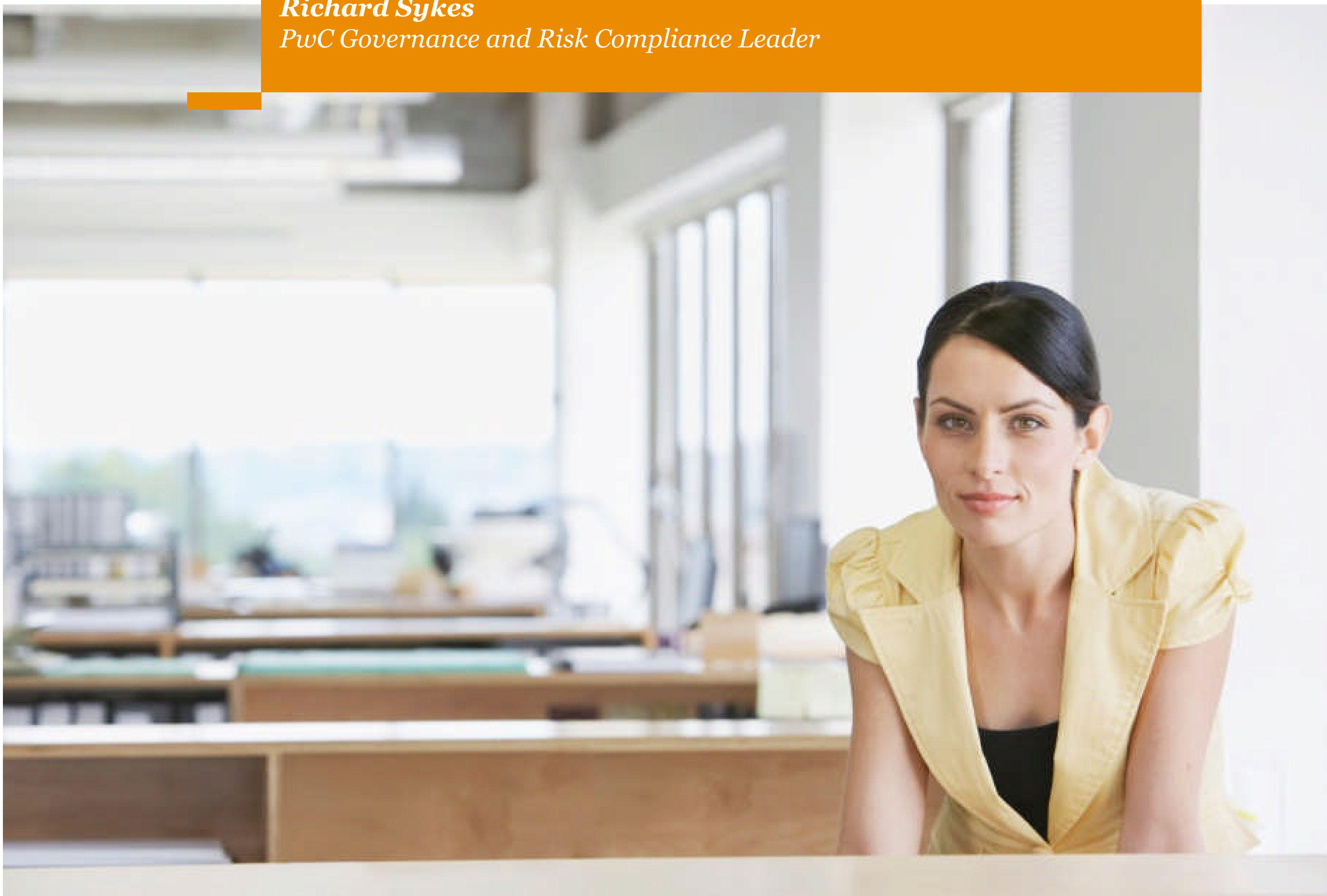
Only 50% of mid market businesses cited information risk as one of their top three overall business risks.

Just 36% of mid market businesses have a specific individual or team with responsibility for information risk, and whose effectiveness is monitored.

PwC/Iron Mountain Information Risk Study, 2011/12.

2 The mid market is at risk

> *"Business leaders ignore information security risk at their peril. Historically business leaders have tended to regard information security as a technology issue – as reflected by the traditional reporting channels – but this is a complete misconception and needs to change."*
>
> ***Richard Sykes***
> *PwC Governance and Risk Compliance Leader*



PwC's recent study on information risk, commissioned by Iron Mountain, reveals that most mid-market businesses are not good at protecting their data. Our Information Risk Maturity Index clearly shows that European mid-market businesses have a long way to go to bring their information management practices up to acceptable standards. The index measures the level of maturity of business practice in mitigating information risk.

Across our sample of 600 businesses, the performance was poor, with an average index of only 40.6. In a commercial world where any growth is good growth and where the rebirth of the service culture is driving client retention, anything less than 50 is bad news for companies, clients and their collective peace of mind.

So, 40.6 is a long way off the ideal world where every business has a full suite of strategic, people, communications and security measures to protect data and information in place.

Our Risk Maturity Index is based on a set of measures that, if put in place and frequently monitored, will help protect the digital and paper information held by an organisation. The index represents a balanced approach to information risk, including strategic, people, communications and security measures.

The full list of 34 measures aimed at minimising information risk, is set out in the appendix of this report. Some of the key measures are highlighted below.

Key elements of our Information Risk Maturity Index

Strategy

- An information risk strategy.
- A corporate risk register.
- Secure disposal of technology hardware and confidential documents.
- A corporate risk register.

People

- Internet usage and social media usage policy.
- Employee training programmes including induction and refresher courses on information risk.
- Personnel background checks.
- A specific team responsible for information risk.

Communications

- Employee communications programmes to reinforce information risk issues.
- Clear guidance on storage and safe disposal of physical and electronic documents.

Security

- An inventory of locations where information is stored.
- Clear, updated and recognised data classifications.
- Control procedures for access to buildings, restricted areas, company archives etc.
- A centralised security information management database.

Key study findings

60% of businesses were unsure whether their employees had the necessary tools to protect against information risks.

26% of business respondents do not conduct personnel background checks.

59% of businesses who experienced a data loss reacted by investing in protective technology.

PwC/Iron Mountain Information Risk Study, 2011/12.

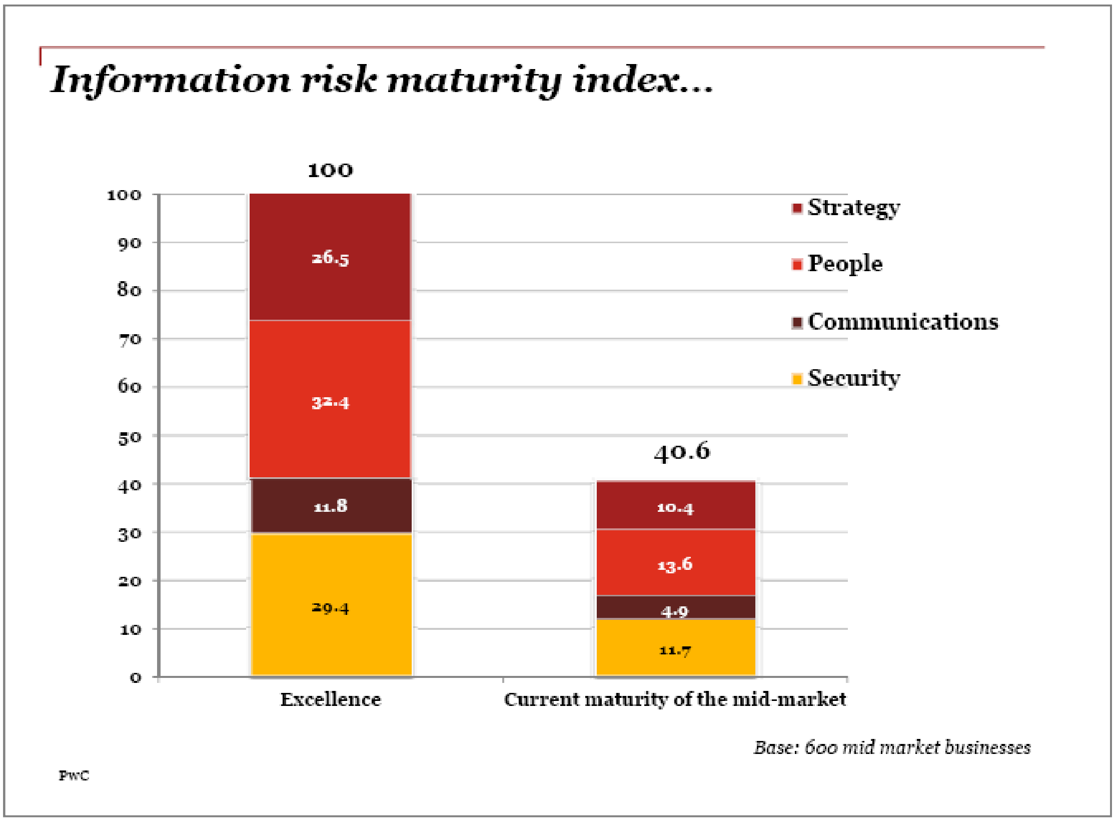
Businesses that have most or all of the measures in place, and regularly monitor their effectiveness, will score between 90 and 100. The average score for our sample of 600 European mid-market businesses is 40.6, illustrating the lack of attention being given to this issue – and the potential for a real information crisis.

The index also highlights that the area requiring most improvement relates to people and communications. This supports further evidence emerging from our study that mid-market businesses are failing to recognise that one of the biggest risks to information is untrained, negligent and disgruntled staff.

The study also reveals that 59% of businesses believe that investing in technology will facilitate data protection, suggesting that data security is widely perceived as an IT issue and investing in technology is the appropriate panacea. However, this ignores a growing body of evidence that one of the biggest threats to data security centres around corporate culture and employee behaviour.

These same businesses remain unsure if they have appropriate tools in place to help their employees reduce the risk of data loss. Furthermore, they are not undertaking personnel background checks, and failing to monitor the effectiveness of their information risk awareness programmes (where they exist). In summary, a substantial number of European mid-market organisations fail to recognise that investing in employee awareness and behavioural change will have a greater impact, lower cost and a more tangible commercial benefit than simply buying technological solutions alone.

This awareness gap is supported by evidence from the Computer Security Institute's Computer Crime and Security Survey, which reported that less than 1% of security budgets are allocated to awareness training. The study found that up to a quarter of businesses incurred more than 60% of their financial losses from accidental breaches by insiders.


Information risk maturity index…

Base: 600 mid market businesses

PwC

The risk of data loss is higher today than it has ever been. One of the biggest threats to an organisation and its customer's data is the behaviour and attitudes of its employees. This can be a result of many factors, some driven by the culture of the organisation, some employee centred and some a result of external factors. We have identified 8 issues concerning employees that can, and often do lead to incidents of data loss.

1. ***Lack of awareness*** or lack of understanding of the organisation's data protection policies, data loss risks and their implications.
2. ***Lack of training*** in the use of data management systems, leading to data being mistakenly deleted or misplaced unknowingly.
3. ***Negligence*** on the part of the employee – talking too loudly on the train, leaving confidential files in the bar on a Friday evening, leaving confidential papers on desks overnight.
4. ***Employee complacency*** and 'it will never happen to me' attitude, leading to carelessness and a lack of diligence such as 'forgetting' to encrypt sensitive emails, not locking confidential files away.
5. ***Misplaced curiosity***, leading to data loss mishaps or deletion of data.
6. ***Leavers* -** employees preparing to exit the organisation, and taking data that may be 'useful' in their new position.
7. ***Disgruntled and disengaged employees*** who feel their employer 'owes them'. Such feelings may emanate from unfulfilled promotion ambitions, pay freezes or perceived lack of appreciation of the employee's efforts.
8. ***Malicious insider attacks*** from employees seeking to make profit from their employer's data, or wishing to cause damage to the organisation.

It is the final one of these, malicious attacks, that is commonly believed to be the main 'insider' threat, however there is now strong evidence to show that the other seven are more prevalent and potentially just as damaging. Indeed all insider threats have the potential to cause greater financial losses than threats which emanate from outside the business.

However, the common element linking all seven high risk factors is behaviour.

Lack of training, poor communications, failure to set and enforce a company culture of 'do it once – do it right', complacent management, supervisors and workers, all combine to create the single greatest risk around the integrity of information in the workplace.

Case study examples

In February 2008, the Bank of New York Mellon sent 10 unencrypted backup tapes to a storage facility. When the storage firm's truck arrived at the facility, however, only nine tapes were still on board. The missing tape contained social security numbers and bank account information on 4.5 million customers.

HMRC lost the data of 15,000 people in 2007 after a hapless employee put a disc containing classified information in the post provoking a public outcry and widespread negative media coverage.

3 The impact of not safeguarding your data

> "A breach of internal control at this company resulted in a large fraud being perpetrated over a long period of time. The losses were in excess of £500,000 and the investigation cost more than £100,000."

Source: Information Security Breaches Survey (ISBS) 2010, Infosecurity Europe/PwC

The impact of data loss or theft can be far reaching. Counting only the direct cost of fixing the problem can be misleading. Many businesses are unaware of the significant hidden costs associated with data loss – hidden costs that can cause irreparable damage to brand reputation, customer confidence and public trust. Every business that holds customer or other sensitive information is potentially at risk; and it's only a matter of time until their complacency makes them a victim.

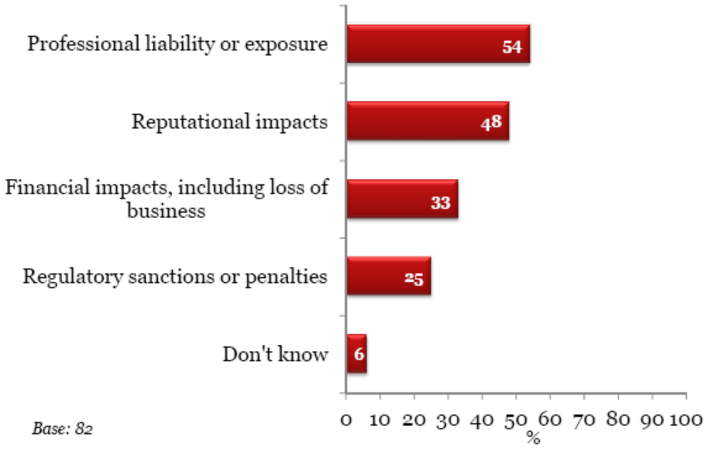
As the chart below highlights, the findings from our study suggests that professional liability or exposure and negative impacts to business reputation are the most prominent impacts for the mid-market market.

This finding was consistent across each of the markets and sectors and illustrates that businesses are conscious of the link between negligent internal practices and how they are perceived by their client's customers or market peers.

The Infosecurity Europe Information Security Breaches Survey report has quantified the main impacts on small and medium size businesses, and these are highlighted below:

- Business disruption – on average 2-4 days of lost business at an average cost of £15,000 - £30,000.
- Incident response costs, mainly staff time - resulting in an average cost of £4,000-£7,000.
- Direct financial loss, which may include fines, imposed by regulators and compensation payments to customers – on average £3,000-£5,000.
- Indirect financial loss such as the loss of intellectual property, revenue leakage, brand damage – on average £10,000-£15,000.

What were the main impacts on your business arising from lost or misplaced information?



Base: 82

PwC

Key study findings

Around six months ago an employee left their laptop in their car whilst out on a client visit and the car in which the laptop was in was stolen, which included a detailed supplier presentation. The major impact was to our reputation as we had to postpone our supplier presentation, whilst we investigated the issue and prepared a new version. The supplier appeared understanding; however, without doubt this had a negative impact on our reputation in their eyes.

Insurance company, UK.

As a company we recognise that the information losses that we have suffered do not look good on us as a business and this has a negative impact on our reputation. We always go back to the employee that made the error to make them aware of what they've done to help ensure that this is not repeated.

Financial services company, UK.
PwC/Iron Mountain Information Risk Study, 2011/12.

4 Responsibility for information risk

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

Bruce Schneier
International security technologist and author

Despite the global impact of information and data loss, startlingly, only 1% of mid-market businesses see information risk as being the responsibility of everyone in the organisation. More worryingly, only 13% see this as a boardroom issue, and have assigned the overall responsibility for information risk matters to the CEO or CFO.

A significant proportion (35%) continue to view information risk and data protection as an IT issue and have placed the responsibility in the hands IT security manager. The legal and insurance sectors are more likely to take an IT-led approach, with financial and manufacturing leading the way with a more holistic approach to avoiding data loss.

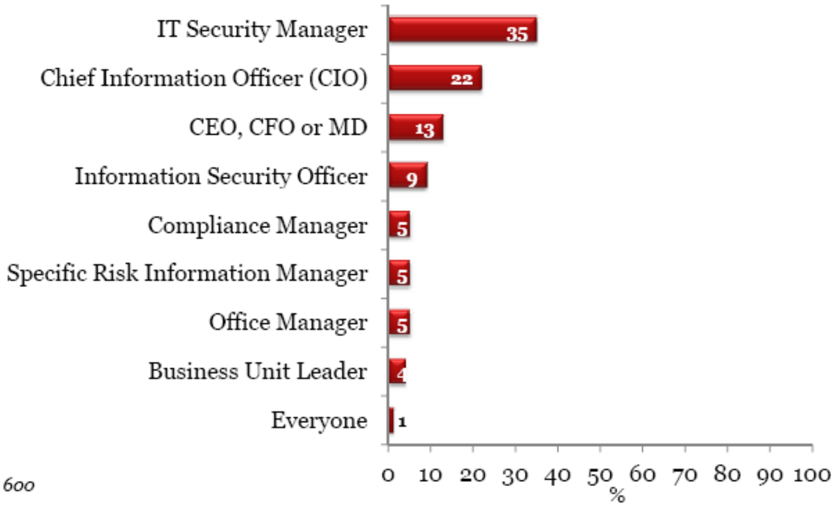
This lack of boardroom involvement and lack of ownership outside IT is deeply concerning. The findings illustrate both the high levels of complacency and low levels of understanding of the risks involved.

These findings illustrate the quandary most organisations face in the modern world. There is little doubt the risk/reward matrix favours the remote hacker, cyber criminal and economic criminal and this is where the greatest focus is in terms of protecting digital data in an increasingly digital world.

And while those threats cannot and should not be diminished, the focus and priority they receive often serve to reduce the day-to-day reality that statistically, an untrained and poorly managed employee is more likely to mishandle information. The 1% who agree that everyone shares the problem just serves to underline the magnitude of the threat.

Clearly it is time for businesses to wake up to the fact that investing in IT systems, whilst important, will not solve the whole problem.

Who is ultimately responsible for information risk within your organisation?



Base: 600

PwC

Key study findings

35% view information risk as the responsibility of the IT security manager.

Only 1% of mid-market businesses see information risk as being the responsibility of everyone.

PwC/Iron Mountain Information Risk Study, 2011/12.

5 How well are businesses protecting themselves?

> *"What is required now is a new approach in which an investment in understanding and influencing the behaviours of all those concerned is balanced against the continued investment in technology and processes."*
>
> *PwC Report, Protecting Your Business: Turning your people into your first line of defence*

Our survey shows that over 60% of businesses surveyed are not confident that their employees, or their executives, have access to the right tools to protect against information risks.

When asked what people measures they have put in place to minimise information risk, only a third of businesses in the survey had implemented each of the following and were actively monitoring its effectiveness. The remaining majority are clearly at risk, and in complacency mode, believing 'it will never happen to me.'

1. Information risk awareness included in induction programmes.
2. Ongoing training and awareness programmes for all staff.
3. Personnel background checks.
4. An internet and social media usage policy for all staff.
5. A code of conduct around employee behaviours in relation to information.
6. Easily available information for employees to refer to.
7. Tools to measure employee confidence in information risk procedures.
8. Employee communications programmes on information risk.
9. Employee guidance on procedures for safe disposal of physical and electronic data.

Businesses think the right thing to do is to invest in technological solutions to protect their data and information. 59% of businesses who experienced a data loss reacted by investing in protective technologies.

Industry sector variances

From a sectoral perspective, financial services and pharmaceuticals are the strongest sectors with legal falling some way behind. If we take the pharmaceutical sector for example, this sector is typically protective of its Intellectual Property (IP) largely as a result of the strength of various patents, which may in part explain its stronger overall performance on our index.

In a similar way, the financial services sector is highly regulated across Europe, with the impacts of data loss or mismanagement extremely high in terms of both reputational and financial costs.

In contrast, the legal sector, whilst in possession of a wide range of data and information, usually clients rather than its own, is predicated on a tradition of original documentation. Legal companies are often highly reliant on such original documentation which may help to explain why its index score is comparatively lower than those sectors, including financial services and pharmaceuticals, which do not have such reliance to the same extent.

In all sectors and countries, communication and measures to minimise the people risks are the areas requiring most attention.

Overall mid-cap businesses are failing to recognise that investment in employee awareness and behavioural change will have a greater impact, will cost less and will have a greater commercial benefit than technological solutions alone.

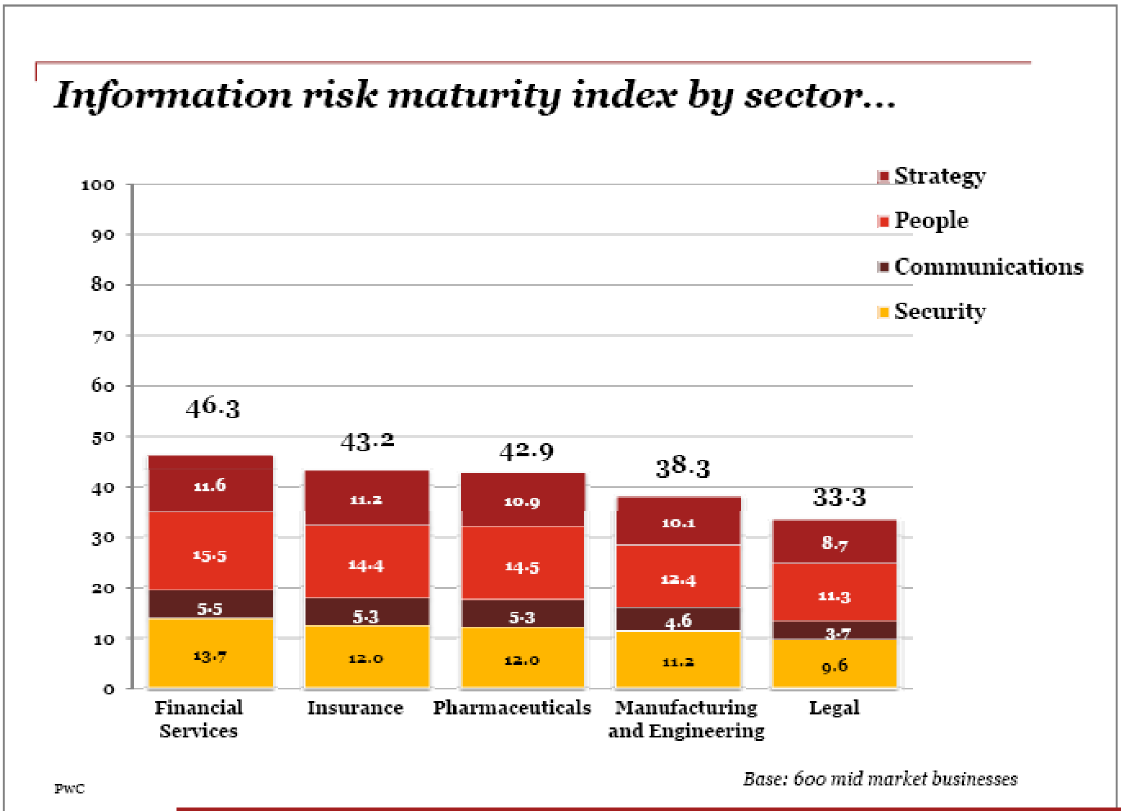
Key study findings

I became aware that an appointed Consultant had accessed confidential information beyond their responsibilities, which could have had huge impacts if this was to be released to our competitors. In a strange way this example was quite reassuring, as it at least showed me that our systems, aimed at detecting this sort of unauthorised access, were at least working effectively.

Manufacturing company, Netherlands.

Just 36% of mid market businesses have an information risk strategy or approach in place, which is effectively monitored.

PwC/Iron Mountain Information Risk Study, 2011/12.



Information risk maturity index by sector…

PwC

Base: 600 mid market businesses

Key study findings

Just 17% of UK businesses had a formal business recovery plan that was effectively monitored.

27% from the legal sector had no training programmes in place to brief employees on information risk issues.

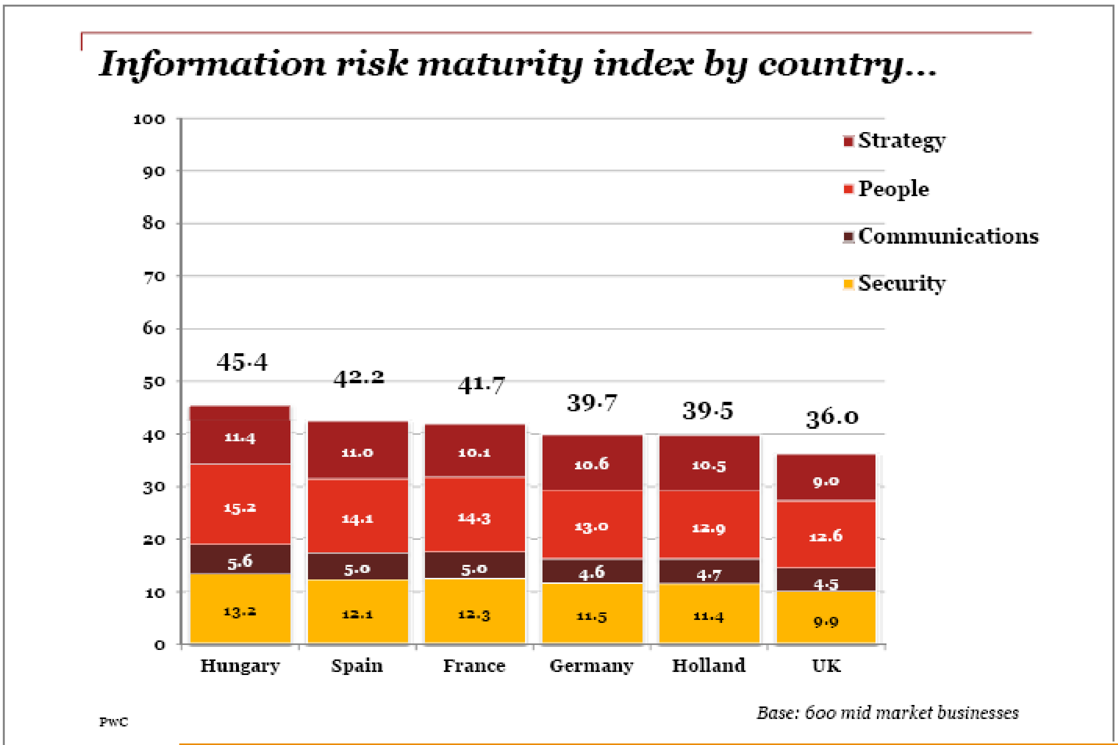
42% of Hungarian businesses had an information risk strategy or approach in place and monitored its effectiveness.

PwC/Iron Mountain Information Risk Study, 2011/12.

> *"Lack of knowledge, the complexity of protection and the problems of getting senior management to take notice are fundamental issues that must be addressed."*
>
> ***Christian Toon***
> *Head of Information Risk*
> *Iron Mountain*

Country variances

Whilst all of the countries surveyed require a huge step change in the way that they treat information risk, Hungary is in the strongest position, with businesses there more likely to have training programmes, clear guidance, codes of conduct and employee communication programmes in place. The UK is consistently below par on the people issues.



Information risk maturity index by country…

PwC

Base: 600 mid market businesses

> *"The contrast between Hungary – with its high level of ISO certification and monitored policies – and countries like the UK, where 41% of respondents don't even know if they have experienced a data breach, is concerning."*
>
> ***Christian Toon***
> *Head of Information Risk*
> *Iron Mountain*

6

What are the best organisations doing?

"We have an information security strategy... together with ongoing communications with our employees and a restricted access policy to systems which hold client information. The importance of respect for these measures is included in employee interviews and initial training."

Financial services company, The Netherlands.

PwC/Iron Mountain Information Risk Study, 2011/12.

Businesses that are good at protecting their data are more focussed not only on developing the right behaviours amongst their employees, but are also more clued-in to the commercial benefits of having a comprehensive information risk strategy in place. Such businesses realise that customers and suppliers would rather do business with companies they can trust to look after their data and keep it secure. They are very aware of the competitive advantage that an effective information risk management and security strategy can bring.

The front-runners - businesses that lead the way in information and data security typically exhibit a number of features. Firstly they have prioritised the importance of information risk by allocating overall responsibility at c-suite level, typically to the CEO or CFO. Front runners also have a team (or individual, depending on the size of the business) in place whose responsibility it is to manage information risk. This is not a team of comprised solely of IT professionals.

Front runners: how are they different?

- They treat information risk as a boardroom issue.
- They have a multi-disciplinary team in charge of information risk.
- They have a balanced information strategy and they monitor its effectiveness.

The businesses who do this well will put in place a team combining technological focus and strong people skills. The third key factor is continual vigilance - having in place, and regularly monitoring the effectiveness of, a comprehensive well thought-out information risk strategy that takes a balanced approach involving investment in people, processes and technology.

Our research reveals that these front runners not only have fewer incidents of data loss, but are also more aware of the number and types of incidents they have experienced. They are better equipped to deal with problems when they occur.

Incident awareness should not be understated, as extensive research into economic crime and cyber crime repeatedly warns that most organisations are actually unaware of the number of security breaches, with many unaware that they have been breached until told by regulators, security organisations – or the media.

Such good practice is most likely to be found in the financial services sector, and in Hungary and the Netherlands. The UK has the lowest incidence of front runners and linked to this, the largest number of businesses (41%) who don't know if they have lost any data or not. Unfortunately, in the mid-cap sector, businesses that look after their data well are few and far between.

Key study findings

Detailed customer information was lost by one of our sales people offsite. By losing the details of the customers' orders and requirements we lost their confidence, and that had a direct impact on our order book.

Manufacturing company, UK.

71% of businesses that we categorised as 'front-runners' have not reported a data or information loss within the past three years, much higher than the other respondent groups.

41% of UK businesses surveyed did not know or were unsure as to whether they had suffered any data loss incidents within the past three years.

PwC/Iron Mountain Information Risk Study, 2011/12.

7 Understanding the commercial benefit

"The true value of information to business is often overlooked. This leads to inadequate protection against risks to corporate reputation. If the business community would only wake up to information risk management, it would see greater business reward."

Marc Duale
President of International, Iron Mountain

The Index confirms that the market drives action. Businesses were more likely to implement an information risk strategy to meet their client's demands or gain competitive advantage, rather than respond to legal or regulatory policy.

More than half of businesses surveyed mentioned commercial factors as the main reason for putting in place an information risk plan or strategy.

However, companies that did implement an information risk strategy – regardless of the reason – were much better equipped to resist cyber attack, mismanagement of data by staff and data mishaps.

Commercial pressures remain a significant driver of compliance. It is our view that client companies should demand higher levels of compliance. This could be enforced through a contractual requirement. If more clients, customers and suppliers made better data management a condition of doing business, standards would improve.

But how are clients to know what differentiates front-runners from followers? The answer is often, regrettably, they can't. However, anecdotal evidence suggests that the best clients and the front-runners enjoy a symbiotic relationship, where clients ask key questions – similar to the questions in our survey – with the answers driving even greater levels of service provision amongst the front-runners.

This Index also supports and builds on the view that the commercial benefits of a well formulated and executed strategy to develop the right behaviours, compare very favourably with those from an increase in the level of investment in technology based solutions.

A well thought out approach to developing the right behaviours will ensure that all employees will be alert to risks, will want to act to protect their employers' data and will know that they will be actively supported in doing so.

What are the commercial benefits?

- Competitive advantage
- Meeting client requirements
- Avoidance of reputational damage
- Better placed to win work form clients
- Stronger, more trusted brand

Key study findings

More than half of the respondent businesses cited commercial factors as the main reasons for putting an information risk plan or strategy in place.

External auditors visited our office to conduct an independent audit concerning the extent of compliance with the firm's clear-desk policy. The subsequent report found that a number of employees had ignored this policy, with sensitive client information found to be easily visible to external office visitors which could have had serious impacts if stolen or removed from the office. The Audit Commission issued us with a stern rebuke.

This was very embarrassing and resulted in a series of employee communications from the Board of Directors reiterating the importance of complying with the policy and that this would be monitored closely by the senior leadership.

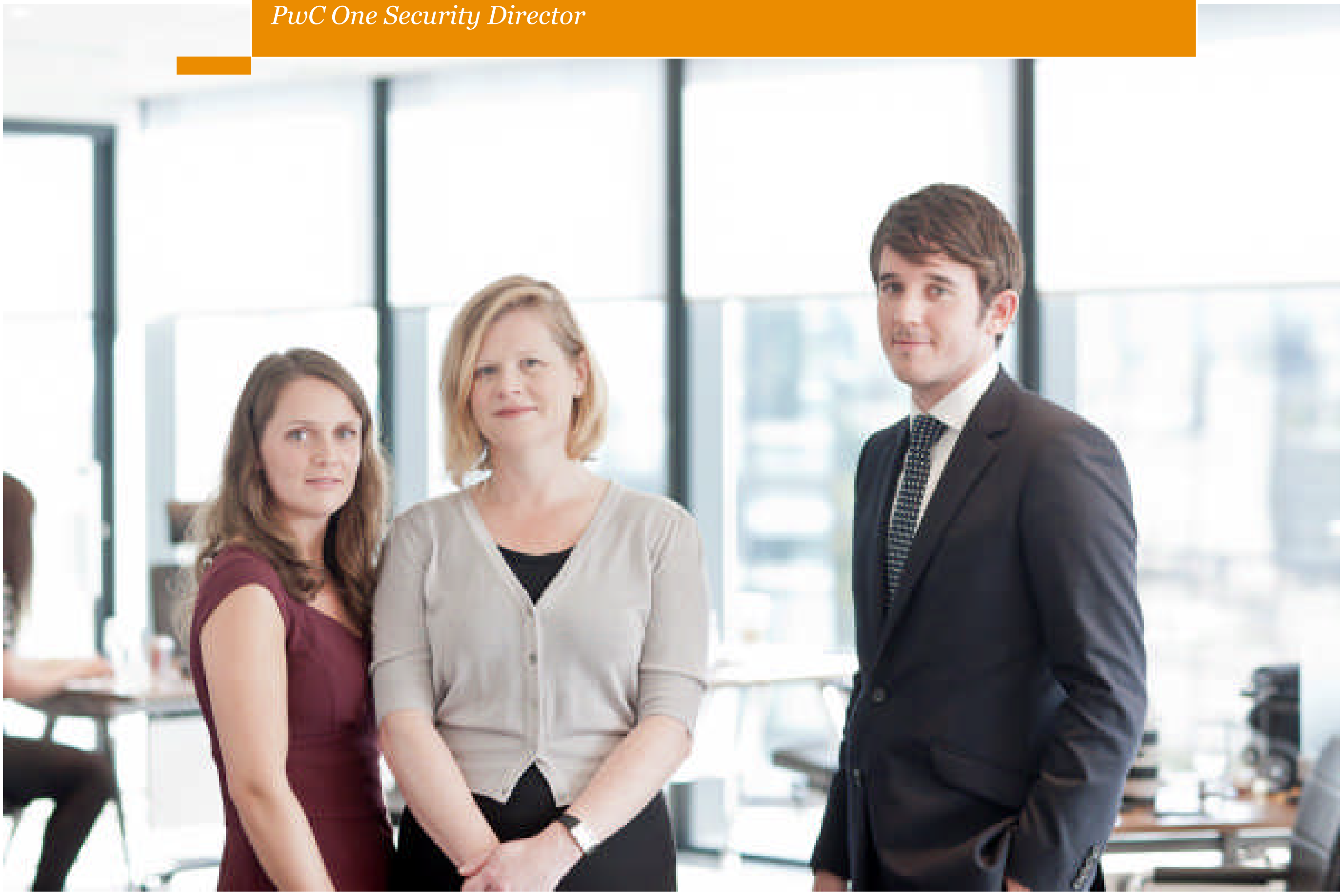
Financial services company, UK.
PwC/Iron Mountain Information Risk Study, 2011/12.

8

A call to action

"The business needs to act, and it needs to act now. Doing nothing is not an option. Many of the actions are straightforward to deliver and can have a big impact. But it's clear that business culture and employee behaviour both need to change."

William Beer
PwC One Security Director



In our view the following steps, if implemented and effectively monitored, will significantly help prepare and equip the mid-market business community to meet the threats posed from information risks.

Step 1: *Make information risk a boardroom issue.*

- Make it a permanent Board agenda point.
- Identify an individual to take accountability and responsibility.
- Articulate information risk in a language the Board will relate to – the financial implications of not safeguarding information.
- Include information risk on your risk register, and provide regular status reports to the Board.
- Embed it into your existing practices and create monthly dashboards to monitor progress.

Step 2: *Change the workplace culture*

- People are the weakest link – screen all applicants before offering employment. Re-screen at regular intervals.
- Design and run well thought out information risk awareness programmes, starting at induction and with annual refresher courses. Support training initiatives with security briefs, and mix the delivery channel to keep it interesting.
- Reward and reinforce good behaviours. Enforce sanctions for failure.
- Identify individuals throughout the organisation to champion information security.
- Put effective communication channels in place to communicate new messages. Too much communication and the message is lost, too little and it doesn't get through. Enable a two way communication process.
- Have user friendly and easy to access guidance information available. Every workstation should have clear guidance for data handling.
- Embed information risk into the daily routines of employees e.g. clear desk policies, document shredding, use of confidential storage.
- Build information risk into staff objectives and embed into annual performance reviews.
- There is always a better mousetrap – find it. Identify technology that is fit for purpose and secure enough for your needs. When it is implemented maintain it, and ensure that you get sufficient logs and records from your systems. You need to know when something goes wrong and this information will support your investigation.

Step 3: *Put the right policies and processes in place*

- Ensure that you include all information formats – electronic, paper or media.
- Secure duplicates and originals in the same way.
- Undertake detailed assessment of current and future needs, threats, risks and determine the best course of action.
- Make sure you have the correct access policies and retention periods.
- Identify information asset ownership.
- Test systems regularly.
- Identify all manual information handling and define vulnerabilities.
- What happens when the technology falls over? Establish whistleblower protocols and be prepared to use them.
- Build your processes with information security at the core. That way it is not seen as a burden on the day to day business.

Appendix

Research methodology

Introduction

In order to support this paper, PwC and Iron Mountain developed a detailed and robust research methodology to support the conclusions presented. In the first instance, we worked closely with Iron Mountain to develop 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. 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 William Beer.

We also worked very closely with our research partner, Coleman Parkes, to ensure that 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 made available in the native languages of our respondent sample base.

Overview of our approach

The research methodology consisted of the following:

- A telephone survey of senior business executives from the mid-cap market.

- The completion of a total of 600 depth interviews with respondents from the UK, Germany, France, The Netherlands, Spain and Hungary and representative of the Financial Services, Insurance, Legal, Manufacturing and Engineering and Pharmaceutical sectors.

- A programme of 14 qualitative depth interviews, with senior business personnel across the same markets and sectors, to probe some of the key issues in more detail.

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 at a senior level.

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 at this level.

The qualitative strand of the study probed some of the key issues identified in the telephone survey in a more detailed way, particularly in terms of the prevalence of information and data losses together with the steps and corrective actions that these businesses have sought to put in place to minimise the occurrence of such incidents or losses.

In order to develop as much insight from each strand of 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 as well as drawing comparisons with previously published reports.

As part of our methodology, we also 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 follows:

Which of the following does your organisation have in place?

1

Strategy

1. An information risk strategy or approach in place?

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?

2

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)?

3

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?

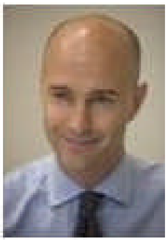
34. Incident notification processes, for example, how to spot something that shouldn't be there?

Report authors

David Armstrong

Partner, PwC International Survey Unit

T: +44 (0)28 90 245454
M: +44 (0)7713 680266
david.m.armstrong@uk.pwc.com



William Beer

Director, PwC One Security

T: +44 (0)207 2127337
M: +44 (0)7841 563890
william.m.beer@uk.pwc.com

William Rimington

Senior Manager, PwC Risk Assurance

T: +44 (0)207 2121027
M: +44 (0)7843 329723
william.j.rimington@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

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.co.uk

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

Design: RD-2012-02-22-10 50-VC