Foreword

Sue Trombley

Management Director of Thought Leadership

Iron Mountain North America

Christian Toon

Head of Information Risk

Iron Mountain Europe

In a world driven by knowledge, information is becoming an increasingly valuable business asset, and with this growing value comes greater risk.

This is the third annual study by PwC and Iron Mountain to discover how European mid-market companies (businesses with between 250 and 2,500 employees) perceive and manage information risk. The 2012 study revealed extensive complacency with regard to potential threats and vulnerability. Its 2013 successor suggested that the mid-market had responded but that its preliminary efforts to tackle information risk were being drowned in the swamp of big data.

This year we decided to explore whether the information risk management trends are confined to the European mid-market, or whether they are more widespread. The 2014 study, which yet again draws on the research strength and business insight capability of PwC combined with the depth of expertise of Iron Mountain, includes mid-market organisations in the US and Canada and larger enterprise-level companies (businesses with more than 2,500 employees) on both continents.

Everywhere we looked we found a shortfall between where organisations currently are in terms of their ability to manage information risk and where they want or need to be.

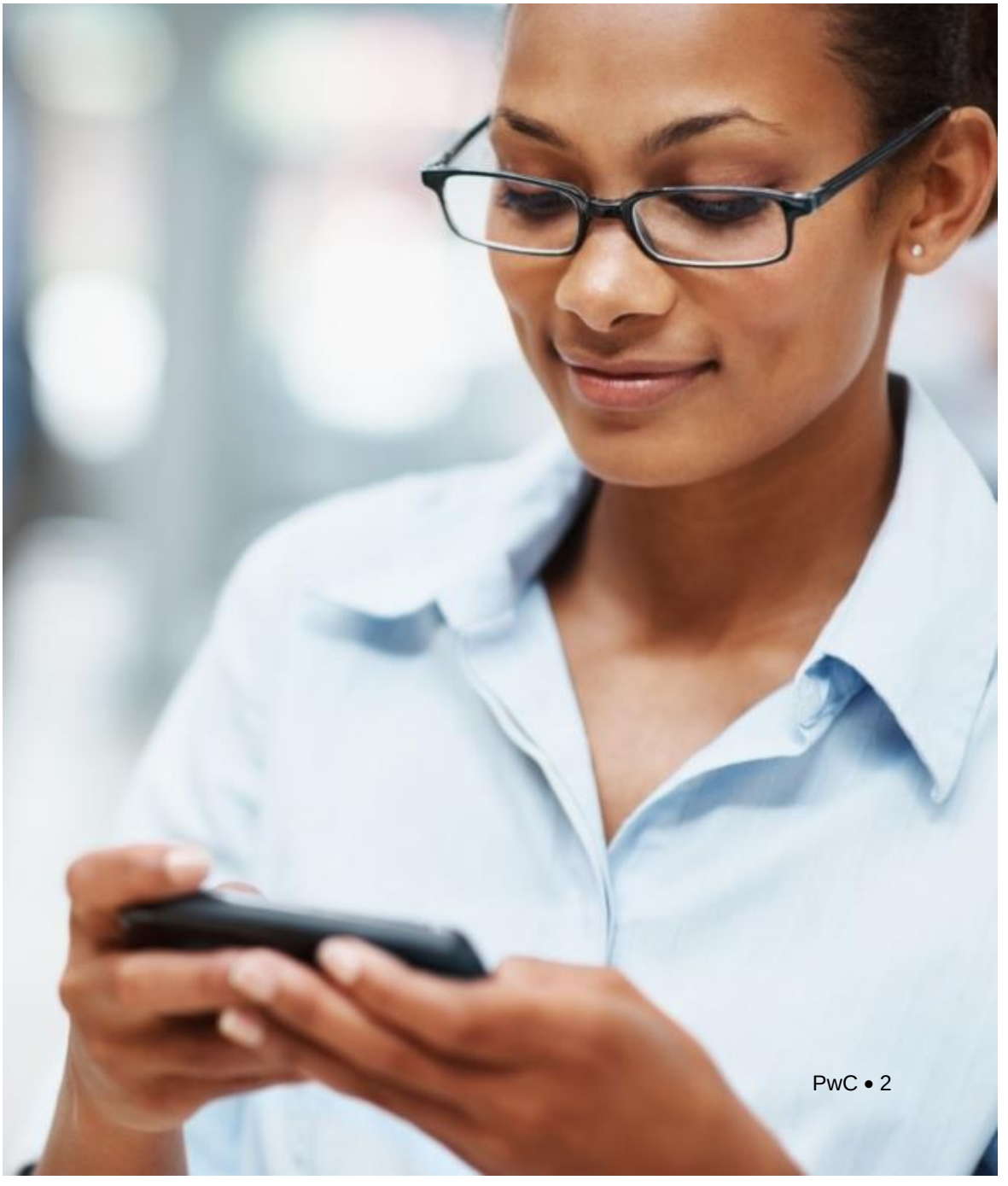
The top trends are universal:

- From the largest and most established enterprise to the youngest mid-market company, organisations find themselves unable to bridge the gap between having a well-intentioned plan or policy in place and making sure it actually works.
- Responsibility for information risk is invariably and almost entirely placed on the shoulders of IT, at a time when information is created and used by all functions across the business, and the potential impact of a data breach - reputational, legal, financial, and commercial - demands the attention of senior leadership and greater involvement of business units beyond IT.

- Despite the fact that organisations everywhere understand that information has value, the majority are far more likely to lock it away to avoid a data breach or legal action than they are to use it to drive competitive advantage, innovation and growth.
- Last, but not least, as businesses focus on digital initiatives, they are finding it hard to manage the risks associated with their paper records. These risks are listed as the top concern by around two thirds of respondents, twice as high as the second placed risk of external threats.

All this is leaving organisations vulnerable to data loss and damage. Yet this doesn't have to be the case. We found businesses with a clear and effective approach to Information Governance and managing information risk – organisations who understand the threats to their information and how to get value from it. Later in this white paper, we set out the key characteristics of these front runners and offer practical advice to help others make the same journey.

Good intentions should be the start, not the destination, of the journey to managing your information risk.



Executive summary

Information is the oxygen of business, it is essential and everywhere. It includes knowledge and learning, system generated data, product and customer information, day-to-day communications, archived paper documentation, together with corporate intellectual property.

But with a larger volume, variety and type of business information comes risks – risks that are wide ranging and if not properly managed and/or mitigated can have a critical and damaging business impact.

A recognition and understanding of these risks, threats and potential impacts is more prevalent today than in recent years. The mid-market business community, in both Europe and North America, has responded to the widely publicised data breaches, leaks and incidents of espionage by adopting more organisational strategies, internal action plans and processes, and by investing in security technology and internal communication programmes.

Nevertheless, our research has found that whilst this is a positive and welcome development, there is a growing gap between 'good intentions', determined by stated commitments through organisational policies and internal programmes, and practical action, in the form of effective enforcement of these policies and programmes.

This gap should be a key concern because it plays a part in exposing the mid-market business community to a wide range of information risks that could create long-lasting and potentially irreparable impacts on overall viability and competitive advantage.

Moreover, whilst this gap between stated commitments and practical action is contributing to a greater exposure to information risks, it is also restricting the extent to which mid-market businesses can effectively utilise their information as a valuable and, potentially, a market-distinguishing asset.

Many businesses in the North American and European mid-market recognise that their information has value but are failing to use their information to gain a competitive advantage. Our study has found that the mid-market remains unduly passive and protectionist as opposed to proactive and innovative with regards to how it utilises its growing information portfolio.

Interestingly, this is an issue that crosses borders, industry sectors, continents and business of all shapes and sizes – irrespective of employee numbers or resources. Therefore, the challenge is universal.

In our view, the mid-market has a significant need to translate organisational policies and objectives into practical and enforceable actions, the majority of mid-market businesses are neither sufficiently well protected nor in a position to fully optimise the data/information they possess.

Key findings of the study:

- The risk maturity index score, covering a sample of European and North American mid-market businesses, is 55.3 out of an ideal 100.0.
- A score of 55.3 rests in what we have defined as the 'risk aware' segment of the index. This is symptomatic of businesses that have woken up to the need to manage risk but remain uncertain about what to do or remain ill-equipped to tackle the threat.
- It is the lack of properly enforced and monitored actions, policies and procedures that is in part preventing the mid-market from reaching a more 'mature' state.
- Just 37% of European and 47% of North American businesses have a

fully monitored information risk strategy in place. This should be the bedrock upon which appropriate protective measures are built – yet more than half of mid-market businesses are not doing this.

- Only 26% of European and 20% of North American businesses follow up on their information risk training programmes to determine how effective they have been.
- From a responsibility and appropriate skills allocation perspective, 46% of European and 32% of North American businesses cite the IT Security Manager as having ultimate responsibility for information risk. When asked who such overall responsibility should rest with this increases to 73% and 74% respectively. In our view, this restricts an organisation's ability to anticipate and react to the full breadth of risks through a wider lens – above and beyond an IT perspective.
- More than half of businesses do not believe that they have any information management skills gaps amongst their workforce. This appears unduly optimistic but also reflective of the lack of understanding of the skills required to both protect and optimise business information appropriately.
- 87% of European and 80% of North American businesses do not believe that ex-employees have taken information owned by their organisation to a new employer. At best this is optimistic, at worst this is further evidence of a naivety that information of all types and levels of sensitivity is not being exposed by existing and future employees in a way that could serve to advantage other competitors and/or pose a threat.

To properly meet and exceed the fundamental twin objectives of sufficient protection and value optimisation of business information the mid-market needs to address a number of issues.

Bridging the gap between commitment and enforceable actions

(1) Organisational strategies, people initiatives, communication programmes and security processes need to be reviewed, tested, evaluated, refined and fully understood to be impactful.

Senior mid-market leaders must coordinate and effectively assign appropriate information risk responsibility

(2) Information can be visible or invisible, physical or electronic, online or on paper and therefore senior leadership must coordinate how this is both managed and/or optimised so that ***everyone*** knows both their role and the potential impact of non-compliance.

Information can only represent a value to business if properly managed and effectively utilised. This requires a proper audit of skills gaps, addressing such gaps and the appropriate allocation of skills.

(3) Information management and optimisation should not rest primarily in the hands of IT professionals. Data must be more widely shared with analysts and innovators throughout the organisation.

A confidence in employees should be safeguarded and underpinned by evaluated and controlled processes.

(4) Investment in security hardware and protective and enabling technology is important. However, this should be underpinned by monitored and controlled people/employee processes to stifle threats that may emanate from within organisations which can often be the most common and damaging sources of exposure.