IRON MOUNTAIN®

SEE INFORMATION DIFFERENTLY

RECORDS AND INFORMATION MANAGEMENT

GETTING IT RIGHT FROM THE START

THE BASICS OF RISK PREPARATION

INTRODUCTION

A QUICK GUIDE TO HELP YOU PLAN, EXECUTE AND BENEFIT FROM A PLAN TO LIMIT YOUR EXPOSURE TO INFORMATION RISK.

Success in records and information management takes planning, organisation and a strategy for taking control of physical and digital records from creation, through active use to secure storage, permanent storage or planned destruction. Done well, records and information management will help your organisation limit information risk, manage costs and lay the foundation for big data analytics.

From the largest and best established to the smallest and newest, organisations struggle to bridge the gap between a plan to limit information risk and effectively implement that plan.

THE TROUBLE WITH RISK

The reasons for the gap between the theory and practice of managing information risk are varied. On the one hand, information cuts across every team and business area. In many organisations, it needs to be readily available for multiple teams to access at any time and from any place. In our increasingly global business environment, information access must be fast, device-agnostic and secure.

With rapid growth in the volume, variety and velocity of information entering businesses, records and information managers not only have more information to deal with, but evolving formats to consider. From paper records to social media posts and emails, the challenges show no sign of receding. What's more, it's not necessarily easy to determine who should have access to what information and who shouldn't. And there are added questions around how people should access information and from where. It may be acceptable for the head of a business area to look at and use potentially sensitive information, but what happens if the information is printed out and left on a bus? Or, saved to a laptop that's left in a restaurant?

There are also risks connected to storing information. Digital databases can be breached and online communications are subject to malware, fraud and malicious attack. Paper records are easily lost or destroyed. It's one thing to intend to manage information risk, but it's another to put a comprehensive plan into action.

WHY WORRY ABOUT INFORMATION RISK?

The threat posed by information risk can't be overlooked. Adverse incidents that threaten some aspect of electronic security are increasing. According to Defending Yesterday - key findings from The Global State of Information Security (PwC 2014), there's been a 25% jump in detected incidents. In fact 24% of respondents to the survey reported a loss of data – an increase of 16% from the previous year. PwC's Information Security Breaches Survey 2014 suggests that there's been a significant rise in the cost of individual breaches. It also reports 10% of UK businesses that suffered an information security breach in the last year were so badly affected that they had to change their business entirely. Threats are increasing in frequency, severity and cost.

WHAT DOES THIS MEAN FOR YOUR ORGANISATION?

Information security isn't just nice to have. It's a business imperative. It can't simply be left in the hands of IT or even senior managers. Your information security strategy should assess your strengths and vulnerabilities in order to identify and manage risks. Your strategy should also adapt to the changing threat environment by identifying your most valuable information. Knowing where this information is and who can access it will help you prioritise your resources and investment.

STEPS TO TAKE

1 SHARE THE RESPONSIBILITY

Information management should be the responsibility of everyone in your organisation. If information becomes the sole responsibility of IT, there's a danger that the people who create and work with information every day won't understand the risks connected to it. What's more, if information isn't everyone's responsibility, your teams may not understand or adopt new ways of working. Policies aimed at keeping information secure should be visible at the very top of the organisation and understood at every level. The C-suite should openly promote good information security practices. Leaders are as responsible as managers, users and creators. After all, IT can't protect information if someone in marketing doesn't respect or follow guidelines.

73% in Europe and 74% in North America think IT should ultimately be responsible for information risk.

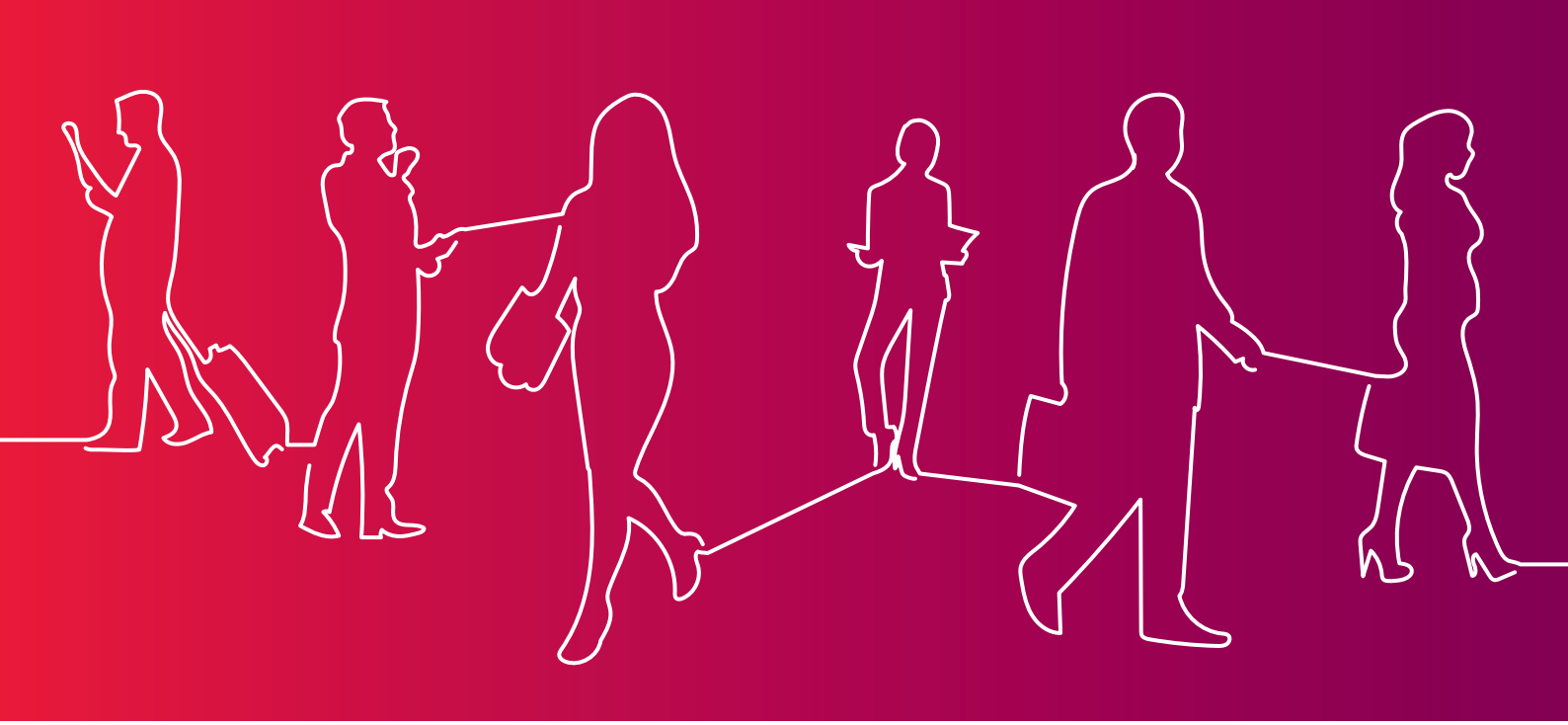
Beyond good intentions, The need to move from intention to action to manage information risk in the mid-market, PwC and Iron Mountain 2014

2 KNOW YOUR STRENGTHS AND WEAKNESSES

Find out where your organisation's most valuable and most vulnerable information resides. Determine who has access to it. Your risk assessment should include the entire business; every aspect and location. Your risk assessment should also involve questions developed by people responsible for managing risk. Consider including IT security, compliance and legal, business units and records management. Look at physical and digital repositories as well as the cloud and mobile devices. Don't forget your third party providers. Use your results as a framework for planning and making decisions about the resources you invest. Revisit your conclusions regularly as the risk profile of different business areas can change.

87% of European and 80% of North American businesses don't believe that ex-employees have taken information owned by a business to a new employer.

Beyond good intentions, The need to move from intention to action to manage information risk in the mid-market, PwC and Iron Mountain 2014



3 ENGAGE YOUR PEOPLE

Risk management depends on your employees:

▶▶ As information's volume, velocity and variety increases, so does the need for people who can help organisations move beyond information policy. Employing data analysts will help your business determine the balance between value and risk. You can also make data science and analysis part of business functions.

▶▶ Develop and implement information training so your people are aware of risk and empowered to change their behaviours. Communicate with your people regularly to ensure the training becomes part of everyday working practices. Information is an asset and creating a culture of information respect will protect and promote its value. It should begin with stop executive and include all employees as well as third party suppliers and contactors.

▶▶ People leave jobs. And when they do, they often take valuable or sensitive information with them. Put a process in place to protect information from employees. Raise awareness and encourage good corporate conduct.

Only 26% of European and 20% of North American businesses follow up on their risk training to see if it's been effective.

Beyond good intentions, The need to move from intention to action to manage information risk in the mid-market, PwC and Iron Mountain 2014

4 REMEMBER PAPER

Paper is a major threat to information security. Consider investing in a combination of scanning and secure document storage. A hybrid solution can help you take control of your paper records. Iron Mountain's expertise and resources have stood the test of time and may be right for your organisation.

Around two thirds of the respondents listed paper records as a top risk concern. That's twice as high as the second place risk of external threats.

Beyond good intentions, The need to move from intention to action to manage information risk in the mid-market, PwC and Iron Mountain 2014

5 MEASURE AND MEASURE AGAIN

To be meaningful, change must be measured. Define your key performance indicators and establish reporting metrics as well as timings. Make sure people are aware of the measures you're putting in place by communicating your aims to senior management and offering training to key teams. Assign someone responsibility for assessing and reporting on your outcomes.

Only 37% of European and 47% of American respondents had a fully monitored information risk strategy.

Beyond good intentions, The need to move from intention to action to manage information risk in the mid-market, PwC and Iron Mountain 2014

6 PLAN FOR THE WORST

What will you do if, despite your precautions, the worst happens? Your business continuity and crisis management plans should include a strategy for handling the aftermath of an information breach. How you communicate with your employees, customers and the public will affect the outcome.

FINAL THOUGHTS

As information and the forms it can take evolve, so do the risks connected to it. In order for businesses to find and use information as an asset, they need to ensure that risks are consistently and effectively managed. In the future, the most successful businesses will find the balance between protecting information and setting it free to fuel innovation and growth. The aim is not to lock information away, but to use it to its full advantage.

To find out more about how Iron Mountain can help you manage information risk, download the recording of the webinar on developing your risk framework.

IN THE UK CLICK HERE

IN IRELAND CLICK HERE

Or, read the complete PwC report on information risk.

IN THE UK CLICK HERE

IN IRELAND CLICK HERE

IRON MOUNTAIN®

R.O.I 1800 732 673 | N.I. 08445 60 70 80 | ironmountain.ie
08445 60 70 80 | ironmountain.co.uk