PROTECT AND PROMOTE:

HOW TO MANAGE INFORMATION RISK

ARE YOU CLOSING YOUR INFORMATION GAP?

A QUICK GUIDE TO HELP YOU LIMIT YOUR EXPOSURE TO INFORMATION RISK

From the largest and well-established to the smallest and newest, many organizations' information management plans suffer an awareness-to-action gap. This is the difference between having a plan to limit information risk and effectively implementing it. And, for some, this gap is getting wider.

If you're a procurement professional, you'll know that managing information risk is not just about storage. Given the business-critical role of data in today's world, it's impractical to do it all yourself. That's why businesses are increasingly turning to external expertise – to work with a trusted partner. They will be able to provide you with the skills, capabilities and the innovative information management solutions you need. As a result, you can minimize risks and be in a stronger position to extract more value from your information.

THE TROUBLE WITH RISK

The reasons for the gap between the theory and practice of managing information risk are varied. In many organizations, information cuts across every team and business area and needs to be readily available for multiple teams to access. In our increasingly global business environment, information access must be fast, secure and accessible from any device.

The rapid growth in the volume, velocity and variety of information adds pressure on procurement professionals to make sure their organization is working with the right providers. And that everyone has the information management tools to manage risk effectively.

From paper records to social media posts and emails, the challenges show no sign of receding. It's not always easy to determine who should, or shouldn't, have access to certain information or how people should access information, and from where. It may be fine for a department head to access potentially sensitive information, but what happens if the information is printed out and left on a bus? Or a mobile device is stolen?

There are also risks connected with storing information. Digital databases can be breached and online communications are subject to malware, fraud and 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 cannot be understated. According to key findings from The Global State of Information Security (PwC 2016), 38% more security incidents were detected in 2015 than in 2014. The number of incidents attributed to suppliers also climbed 22% in 2015 — a cautionary note for procurement professionals who have a key role in choosing the right companies to work with.

The study also reports that in the last year, 10% of UK businesses suffered an information security breach that caused them to change their business entirely. Threats are increasing in frequency, severity and cost – and it's not just the 'big boys' who are being targeted by cyber-criminals.

What does this mean for your organization?

Information security isn't just nice to have. Your information security strategy should assess your strengths and vulnerabilities in order to identify and manage risks. So when the threat environment changes, you know where your most valuable information is, and who can access it. This will help you prioritize your resources and investment.

SECURITY IN SIX STEPS

SHARE THE RESPONSIBILITY

Information management should be the responsibility of everyone in your organization – from procurement to sales. If it is 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 to it. Policies aimed at keeping information secure should be visible at the very top of the organization and understood at every level. Working with the executive team you 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.

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

KNOW YOUR STRENGTHS AND WEAKNESSES

Find out where your organization's most valuable and most vulnerable information sits and who has access to it. Your risk assessment should include the entire business – every aspect and location. Involve the people who are actually responsible for managing risk and supplier relationships, including procurement, IT security, compliance and legal, business units and records management. Look at physical and digital repositories as well as the cloud and mobile devices. And remember your third party suppliers. Use the results as a framework for planning and making decisions about the resources you invest. Revisit regularly as the risk profile of different business areas can change.

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

*Source: 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 EVERYONE IN THE BUSINESS

Risk management depends on the business as a whole:

- As the variety of information being stored and managed grows, so does the need for people who can help organizations develop 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.
- Offer training that helps teams become more aware of risk and empowers employees to change their attitude to information management. Communicate with your people regularly to ensure the training becomes part of everyday working practices. Information is an asset and creating a culture of respect will protect and promote its value. It should start and stop with executives and include all employees as well as third party suppliers and contractors.
- 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 leavers. Raise awareness and encourage good corporate conduct.

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

4 THE PAPER RISK

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

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

*Source: 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. MEASURE. REPEAT.

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

6 PLAN FOR THE WORST

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

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

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

FINAL THOUGHTS

As information and the forms it can take evolve, so do the risks connected to it. Balancing the priorities of protecting information and providing access to it only add to the complexity of managing risk consistently and effectively.

In the future, every successful organization will have struck the right balance between protecting information and setting it free to fuel innovation and growth. The end goal is not simply to lock information away, but to develop a management framework that's flexible enough to unlock value and use information to its full advantage.

To find out more about how Iron Mountain can help you manage information risk, call us on 1-800-899-4766

Find out more about how choosing the right information management supplier can help. Get the Vendor Checklist

CLICK HERE

SHARE YOUR THOUGHTS WITH US ON:

IRON MOUNTAIN®

ABOUT IRON MOUNTAIN. Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company Web site at www.ironmountain.com for more information.