IRON MOUNTAIN®

TAKING THE RIGHT RISKS

WHITE PAPER

CONTENTS

INFORMATION IS...
YOUR ADVANTAGE

Iron Mountain-sponsored business intelligence specifically geared to the needs of small business clients.

Some business risks are worth taking – opening your doors was one of them. But operational risks offer no chance of upside. Here's how records management can help you minimize those dangers.

INTRODUCTION

When you think about risks to your small business, the story of a mouse, told by Stephen Dubner, co-author of the best-seller *Freakonomics*, is instructive. A deceased mouse, as the story goes, somehow ends up in a lady's salad at an upscale New York City dining establishment[1].

Why are we telling this unpleasant, graphic tale? Because it's a valuable object lesson in operational risk. A rodent in the salad may be, for most restaurants, a once-in-a-lifetime circumstance. But think about it: This unfortunate confluence of events reflects a series of small operational failures in the restaurant's food preparation practices, quality assurance and, most of all, food sourcing. The result was literally stomach-turning.

Businesses that win at managing operational risks are much less likely to find themselves with their own version of "Mickey on a bed of lettuce." But, let's understand what "operational risks" actually represent. Inadequate processes, people, and systems are at their core – and these conditions are possible in nearly every small business task. Employee theft, civil, or criminal liabilities, cybercrimes, acts of nature, changes in compliance rules, and failures of technology are all causes (or effects) of operational risk.

Does this list sound too overwhelming to even begin tackling? Think again. By focusing on one aspect of your operations, you can mitigate many, if not all, of these risk areas. What's this not-so-magic bullet? A systematic records management plan that puts all your information in order.

[1] Freakonomics.com, Stephen Dubner, 7/21/11. http://freakonomics.com/2011/07/21/freakonomics-radio-a-mouse-in-the-salad-whats-the-worst-restaurant-experience-youve-ever-had/

DID YOU KNOW?

Operational risk is one of several business risks. Other types include financial, strategic, regulatory and reputation. You can mitigate all of these with better records management.

HOW (AND WHEN) RECORDS CAN WORK AGAINST YOU

Records mismanagement is a more insidious flavor of operational risk. And how do you mitigate it? A business owner can put a lock on the door, install software to protect company computers from viruses, or put excess cash into a bank account. But when it comes to vital documents, the solution may be less tangible at first.

Those pieces of paper that start piling up around the office seem harmless enough. But sooner or later, poorly kept records start affecting the bottom line. A company with inadequate records management might expose proprietary data or run afoul of customer privacy rules, harming its reputation. It could struggle to respond to discovery requests, or incur excessive storage costs by hanging onto paper it no longer needs.

Broadly speaking, business owners have a poor record of managing their records, though their intentions may be good. Iron Mountain conducted an extensive study in Q1-2014 with over 600 small businesses on document management. This study shows that 55 percent of small businesses have no formal paper document storage program in place.

LEGISLATION COMPELS BETTER RECORDS MANAGEMENT

One of the largest operational risks driving the adoption of smarter records management policies stems from the growing body of consumer-privacy legislation. For example, a doctor storing former patients' records, a financial planner sending out investment returns, or a retailer filing payroll or supplying 401(k) plan data to employees must all comply with a growing number of federal, state, and industry privacy rules.

One of the most pertinent privacy regulations impacting records management is the FACTA Disposal Rule. This law requires companies to properly dispose of sensitive consumer information once they're finished with it. These records can include employment files, insurance claims, medical histories, or credit reports, among other types of information[2].

[2] Federal Trade Commission, "FACTA Disposal Rule Goes into Effect June 1," June 1, 2005. http://www.ftc.gov/news-events/press-releases/2005/06/facta-disposal-rule-goes-effect-june-1

FAST FACT: More than one-third (36%) of respondents to A View into Unified Records Management: The Iron Mountain Compliance Benchmark Report offer no or very limited records-management training in the workplace.

FACTA: ONE OF MANY REASONS TO ACT

The FACTA Disposal Rule applies to any business owners who might collect consumer data, including landlords and even individuals hiring in-home employees like nannies or contractors. The standards for proper disposal are flexible; they require organizations to analyze the costs and benefits of different disposal methods and the sensitivity of the information. Naturally, the more sensitive the information, the more securely it must be shredded or otherwise destroyed.

If your firm fails to comply with FACTA, you could face severe civil liabilities and penalties. Statutory damages can run as high as $1,000 per employee, and civil fines can go up to $2,500 per employee[3]. On top of that, FACTA could require you to cover attorney's fees. These fees and penalties can add up fast—and all because you may have failed to comply.

Consider the mortgage company that the Federal Trade Commission fined $50,000 for improperly disposing of customers' sensitive personal information. On more than one occasion, the firm dumped such confidential documents into an unsecured dumpster. Many of these documents were in open trash bags, in clear view of prying eyes[4].

Your business would probably never be so flagrantly irresponsible (or you wouldn't be reading this now), but, like the mortgage firm, you may lack a systematic method for getting rid of documents. Iron Mountain's Compliance Benchmark Report found that 47 percent of companies either have an ad hoc method or no policy at all for destroying hard-copy records.

Without formal policies and follow-through, businesses of all sizes run a far greater risk of running into legal trouble. Besides the risk of enforcement actions, your business could also incur unnecessary storage costs by retaining documents you no longer need.

E-DATA POSES A SERIOUS CHALLENGE

Just as improper disposal puts companies at risk for security breaches, shoddy records management carries its own risks. Running up storage costs by hanging onto documents you no longer need is one thing. Much more hazardous is haphazard or disorganized retention of documents that must be kept for legal or business purposes. Losing track of documents kills productivity, since employees need to hunt down information or spend time re-creating it—especially in critical situations like a legal discovery. Scattered and/or lost records put your firm at risk for not responding to such queries in a timely manner.

Adding to this organizational challenge is electronic data, which is expanding exponentially. According to global market research firm IDC, the digital universe is on course to double every two years: By 2020, it will reach 40 trillion gigabytes. IDC expects much of this data—such as that generated through social media—to be difficult to control. And although consumers create the majority of data in the digital universe (68 percent, according to IDC), businesses are directly or indirectly responsible for nearly 80 percent of it, due to consumer privacy and compliance issues[5].

PCI COMPLIANCE

Just like a sandwich, the Payment Card Industry (PCI) has layers. First, you have the credit card companies who created the standards for PCI compliance. Next you have the acquirers (banks) who manage the merchant's credit card transactions. Lastly, there are the merchants, businesses with credit and debit transactions.

With any aspect of records and information management (or a restaurant), PCI compliance also involves teamwork. The risk here is not only to small businesses, but to the acquirer as well. Therefore, working together helps ensure full PCI compliance. It is important to find out specific requirements or concerns the acquirer might have and get to know them. As a side, a business can reach out to a Qualified Security Assessors (QSAs) who can help make PCI compliance a more straightforward process by linking the business and the acquirer together.

[3] riskVue, "Employee Identity Theft: Employers Beware," Warren, McVeigh & Griffin, Inc. http://www.riskvue.com/articles/rb/rb0509b.htm

[4] Federal Trade Commission, "Company Will Pay $50,000 Penalty for Tossing Consumers Credit Report Information in Unsecured Dumpster," Dec., 18, 2007. http://www.ftc.gov/news-events/press-releases/2007/12/company-will-pay-50000-penalty-tossing-consumers-credit-report

[5] IDC IView, The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East, December 2012. http://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf

The federal government has granted HHS enforcement to make sure small businesses follow the rules: Fines range from $100 to $50,000 per transgression, with a $1.5 million maximum per year.

HIPAA COMPLIANCE: CHANGES THAT AFFECT SMALL BUSINESSES

In 2013, the Department of Health and Human Services (HHS) modified how it regulates and enforces privacy and security rules under the Health Insurance Portability and Accountability Act (HIPAA). The revised regulations, which are modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules (often referred to as the Omnibus Rule), affect many small businesses – in particular, any business that comes into contact with health records by virtue of its business partnerships and client relationships[6].

It's no longer just hospitals, health insurance plans or other healthcare associates who are affected by these changes and as a result, many small businesses that process, analyze, and transmit medical records are also directly regulated by HIPAA.

Small businesses that handle patient records must:

- Produce any medical records that a patient can't otherwise get from a hospital or insurance company (e.g., if the patient's provider doesn't have a duplicate of the same record) in a timely manner.
- Implement adequate safeguards to prevent disclosure of medical records to unauthorized parties.
- Document and account for any and all disclosure(s) of a patient's records.

Due to the overwhelming challenge of meeting HIPAA compliance, some have chosen to leave the healthcare business. However, as long as records are properly organized, then HIPAA requests are easy. By having documents properly tagged, indexed and classified, a business can easily and efficiently locate records when they need most.

By archiving all information, both paper and electronic, in a unified system where businesses can quickly search and access all of their records businesses, allows them to be compliant with HIPAA regulations.

LEGAL DISCOVERIES UNDERSCORE THE NEED FOR ORDER

Vast amounts of unstructured data are the main ingredient in a recipe for e-discovery disaster. In the event of a subpoena, your company could have as little as six weeks to identify and gather documents, including what could be tens of thousands of emails and social media missives[7]. You probably aren't prepared for that kind of last-minute digging, and neither are most of your counterparts.

A majority of companies (61 percent) say they struggle to meet discovery requests, according to Iron Mountain's Compliance Benchmark Report[8]. This puts them at risk for incurring penalties. Implementing a records management system will help you in the future if you have to face down a discovery request in a lawsuit or audit. A systematic, automated approach helps to ensure that your discovery processes are legally credible. It also greatly reduces the stresses and costs of what might otherwise become a mad dash for data.

[6] COSO, Risk Assessment in Practice, October 2012.
http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf
[7] 2013 Cost of a Data Breach
https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf
[8] A View into Unified Records Management: The Iron Mountain 2012 Compliance Benchmark Report, Iron Mountain and Bradyn SMB Q1 Report, 2014

MOBILIZE YOUR FIRM TO FIGHT OPERATIONAL RISKS

Take control of your company's operational risks with this five-step risk assessment:

1 STEP ONE

Develop the criteria you'll use to assess various records management risks. These can include failure to comply with regulations or slow response to an e-discovery request. A five-point scale, for example, can assess risks in terms of both their likelihood and impact.

2 STEP TWO

Assess risks first through a qualitative method, such as interviews or surveys. Then conduct a quantitative analysis that assigns numerical values to key risks and opportunities.

3 STEP THREE

Risks don't exist in isolation. Assess how they are connected and impact one another.

4 STEP FOUR

Prioritize risks by comparing the level of risk against your tolerance for it.

5 STEP FIVE

Respond to a risk by examining your options. You can accept it, reduce it, share it with an outside vendor – or avoid it entirely. Then perform cost-benefit analyses and formulate a risk-response plan.

A growing body of consumer-privacy laws underscores the operational risks of poor records management.

Just as improper disposal puts companies at risk for security breaches, shoddy records management carries its own set of risks.

Iron Mountain Recommends: Take Steps to Contain Your Risk

Did you know a data breach costs an average of $188 per record in the United States? Reduce your chances of suffering information breaches, identity theft and other security risks by engaging a trusted partner to help execute these best practices:

- Authorize and limit records access
- Tag information according to its level of confidentiality
- Securely destroy records you don't need or aren't required to keep
- Properly dispose of old computers and devices, where sensitive information might still reside
- Set strict policies for social media use
- Comply with privacy stipulations for handling and destroying private information

If you team with a trusted partner for offsite storage and other services, confirm that your vendor:

- Vets all employees who will have records access
- Enacts global security measures to ensure a proper chain of custody
- Securely stores records in facilities well out of the path of disasters such as floods, hurricanes and earthquakes
- Maintains, tests and updates a workable disaster recovery plan

REPUTATION IS EVERYTHING, ISN'T IT?

The most significant risk any company faces may well be damage to its reputation. As renowned investor Warren Buffet famously said, a company's reputation takes 20 years to build and five minutes to ruin. Just like that poor mouse in the salad, a garden-variety operational failure could prove to be the spoiler—or it could be a breach of customer trust stemming from improper handling of personal information.

Getting your operations house in order is the best investment you can make toward protecting your company's reputation, and instituting a comprehensive records management program is a great place to start. Not only can organized, accessible records help lower risks to your hard-earned reputation, they can keep you compliant, protect your customers' privacy, and help you respond to legal discovery and tax audits.

With all of these risks minimized, your company's proverbial salads should remain mouse-free.

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 website at www.ironmountain.com for more information.