CHAPTER 3

WHAT IS THE COST OF IGNORING INFORMATION RISK?

HOW TO MINIMIZE YOUR EXPOSURE

WHY YOU NEED THE INFORMATION ECONOMICS EBOOK

This five-part eBook will help you gain a full understanding of the role information plays in your organization. It examines every aspect of Information Economics.

1. What is Return on Information?
2. How do I gain access to my information to extract maximum value?
3. What is the cost of ignoring information risk?
   - Threats
   - Common mistakes
   - Opportunities for improvement
4. How can I design a program that works for our people and our business?
5. How will future trends in information management affect my business?

YOU WILL LEARN

How to recognize and prepare for the pitfalls of information management, avoiding risks like a data breach or non-compliance

INFORMATION ECONOMICS

THE INTERSECTION OF VALUE, RISK AND COST

Information Economics is managing and leveraging information created and received by an organization with a view to the bottom line. Every business needs an enterprise-wide information strategy that aims to reduce risk, ensure compliance, lower costs, and now with the emergence of big data, prepare for analytics. Information Economics provides a comprehensive and collaborative strategy to help organizations optimize information value and limit risk at every stage from the initial creation of records and information across their active life, right through to secure destruction.

CHAPTER 3:

RISK AWARE AND PREPARED

In the previous chapters of this eBook, we've looked at how to secure a Return on Information by extracting maximum value from your records and information. And, we've also explored minimizing costs by retaining records you're legally obligated to keep and putting the rest in permanent storage or arranging for secure destruction. But not every aspect of Information Economics can be transparently assessed in terms of cost or savings.

Information risk might seem difficult to quantify economically, but avoiding information catastrophe must be a top priority as the consequences can be so severe. The need to mitigate risk however, must be balanced with an organization's overriding need to allow its people the freedom to work efficiently, extracting maximum value from its information.

This chapter examines the individual threats and explains how to plan a strategy to avoid disaster and get a positive Return on Information.

INFORMATION RISK: THE FACTS

One very insightful piece of research on information risk comes from top global business consultancy PwC and Iron Mountain. Their 2014 report, *Beyond good intentions – the need to move from intention to action to manage information risk*, analyzes research on 600 European and the same number of North American companies with 250 – 2,500 employees.

The report defines best practice in minimizing information risk and quantifies performance against this benchmark using the Information risk maturity index. An index of 100 indicates that a business is equipped for risk, and the average index for North American businesses was found to be 54.5, showing that the vast majority of companies are exposed to considerably greater risk than they need to be.

THE AVERAGE NORTH AMERICAN BUSINESS SCORES

54.5%

ON READINESS FOR RISK

THREATS

DATA BREACH

The catastrophic data breach is every company's worst nightmare. While hacking is a serious threat, in PwC's 2014 Global State of Information Security Survey, almost as many executives cited current employees (31%) as a likely source of an information security incident as hackers (32%).

Recent government research in the UK and North America shows that 31% of the worst security breaches in 2014 were caused by human error, with a further 20% due to deliberate misuse of systems by staff[1]. The same survey shows that there has been a significant rise in the cost of individual incidents.

The top two information management priorities for businesses are avoiding data breaches and the consequences of non-compliance.

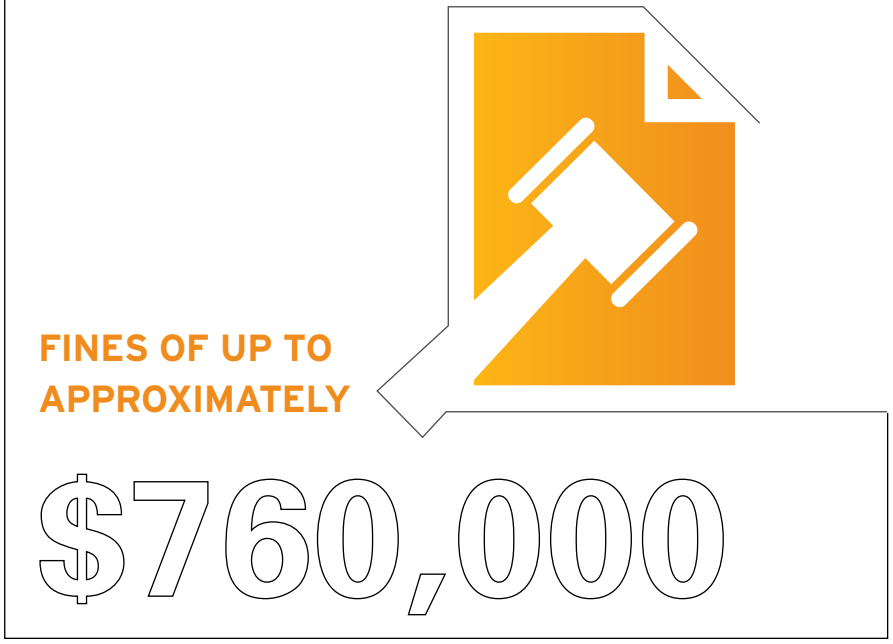
31% OF THE WORST SECURITY BREACHES IN 2014 WERE CAUSED BY HUMAN ERROR

[1] Information Security Breaches Survey 2014 - UK Department for Business Innovation and Skills

NON-COMPLIANCE

Chapter 1 of this eBook looked at Return on Information and the importance of reducing your records' burden in order to free up office space and improve access to information. An enforceable records retention schedule can help you do both – and achieve compliance. Data protection regulations are perhaps the most significant in terms of penalties with fines of up to approximately $760,000 for serious breaches[2].

When it comes to data losses, especially where sensitive customer information is involved, the fine can be the least of your worries. Reputational damage can cost you far more in the long run. 90% of companies that suffer a significant data loss go out of business within two years[3].



[2] UK Information Commissioner's Office
[3] London Chamber of Commerce

COMMON MISTAKES

IT-CENTRIC THINKING

PwC's report finds that 74% of North American businesses believe the overall responsibility for information security should rest with the IT security manager. However the same survey reveals that 62% ranked paper records as their biggest threat to their information security[4]. So it's not hard to see a flaw in the way that information risk is perceived.

Think about this: which is better protected by specific security measures, the data on your hard drives, or your paper records?

POLICIES AND TRAINING

The PwC findings here get to the heart of the general lack of preparedness for information risk among North American businesses. Only 18% have policies in place for the security, storage and disposal of confidential information. And just 20% follow up on information risk training to determine its effectiveness[5].

Information security is about everybody in the business doing the right thing every day. This means universal, ongoing training on policies and procedures, just like any other company-wide, business-critical aspect of operations.

74%

OF NORTH AMERICAN BUSINESSES BELIEVE IT SHOULD OVERSEE INFORMATION MANAGEMENT

[4,5] Beyond good intentions – A PwC report, 2014

OPPORTUNITIES FOR IMPROVEMENT

GOVERNANCE

Only 47% of North American businesses have a fully monitored information risk strategy in place. Reviewing companywide policies is a good place to start. Implementing them of course is another matter[6].

Getting the buy-in of key figures at all levels and across all departments, starting at the very top, is the way forward. Create an information management committee, who can lead your initiative, and raise the profile of the issue so that it cannot be ignored. Create a schedule for meetings and reviews and stick to it.

SECURE STORAGE

Of course information security has to be balanced with information access. Simply locking up your records will potentially keep them safe from theft and misuse, but can diminish their value to your organization if access is compromised. Other considerations include the risk of damage from fire, flood or even rodents. There are also the cost implications of storing onsite and office space can nearly always be put to more cost-effective use.

Offsite storage in secure, purpose built facilities with state of the art safeguards and pay-as-you-go access to records, usually offers the best Return on Information where paper records are concerned.

[6] Beyond good intentions – A PwC report, 2014

LOOK OUT FOR THE NEXT CHAPTER

CHAPTER 4: HOW DO I DESIGN A PROGRAM THAT WORKS FOR OUR PEOPLE AND OUR BUSINESS?

To reduce your information risk, download GETTING IT RIGHT FROM THE START, the basics of risk preparation

DOWNLOAD NOW

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.

IRON MOUNTAIN®

US-RM-EXT-TT-051215-001