



STAYING AFLOAT IN THE SEA OF DATA: MANAGING YOUR INFORMATION RISK

BY BOB TENNANT, CEO OF RECOMMIND

Corporations are drowning in data. Twenty-five years ago, individual computer storage was measured in thousands of bytes; 15 years ago, in millions; 5 years ago, in billions; today, in trillions. IDC recently estimated that 1.2 million petabytes of digital information would be produced in 2010, the equivalent of 1.2 zettabytes of data. The numbers are getting to the point where they're actually hard to fathom.

Despite the enormous amount of data created every day, the average employee gives no thought to managing it. Individuals have little incentive to classify or file information. It's a time-consuming, tedious chore, so most of the time, it doesn't get done—and without technological assistance, never will. It seems so much easier to save everything, in case it's needed later.

Unfortunately, the 'save everything' approach results in enormous costs that are ultimately borne by the organization, not the individual. These fall into two main categories: the cost of storing the information and the cost of information risk from keeping information that should have been deleted in a timely manner.

The 1.2 zettabytes of data produced in 2010 are now being stored on top of all of the information created, stored and not deleted from previous years. The cost of retaining data is often mistakenly identified with the cost of disk space, which leads some to the mistaken conclusion that information storage is cheap. That might be true for your home desktop, but for a corporation, the real costs of storage are not in disk space. They're in increased network complexity and network management, the energy costs associated with energy-hungry disk arrays, the additional IT staff

required to support unnecessary systems, and many other costs that are very real but don't fit under the "disk space" line item on a budget. In fact, despite the enormous rise in total storage costs, the most expensive, unpredictable, and threatening cost to an organization is information risk.

THE NEXT GOVERNANCE ISSUE: INFORMATION RISK

In 2010, the Department of Justice collected almost \$2.5 billion in fines in bribery prosecutions, and the SEC collected more than \$500 million on top of that. The FSA (the financial regulator in the UK) assessed fines in 2010 that were triple what it assessed in 2009. Every corporation is engaged at any given time in a number of lawsuits, and for every fine paid to the government or lawsuit taken to court, many more investigations and suits were initiated and either subsequently dropped or settled.

In the context of these investigations or litigations, all pertinent data (what in legal parlance is known as "responsive") requested is required to be produced, regardless of where it is stored and even whether you know it is there, sometimes (especially in the case of government investigations) on extremely tight deadlines. This is difficult even for companies with excellent document destruction policies. For companies without a real document lifecycle management policy—one which is both implemented and enforced—this means every production will cost many times what it needs to.

For example, a typical business presentation might go through 10 drafts before the final version. With poor preservation policies, a company



might need to produce all 11 documents in an investigation instead of just one copy of the final product. Data duplication at a document level increases the cost of identifying, collecting, analyzing and producing documents manyfold, in addition to increasing overall storage costs. To make matters worse, the most expensive part of the production process has nothing to do with IT. It's the cost of lawyer or paralegal time to review documents before they get produced. Review makes up 70 percent of the total cost of e-discovery, but it comes out of the legal department's operating budget, so is often unaccounted for in IT planning.

Because these costs are spread across departments, they are not easily classified—but at least they are predictable. In some instances, poor information management can result in unexpected, sometimes catastrophic, penalties from courts and governments. In the recent Alcatel-Lucent settlement, for example, Alcatel's initial failure to cooperate increased its penalty, according to one calculation, by \$23 million. Incomplete disclosures can give the impression of concealment, ruining all prior efforts at cooperation.

MANAGING YOUR INFORMATION RISK

These consequences can be avoided with a greater focus on information governance. Proper information governance includes consideration of the type of data to be stored, the role of the employees who create it and how it is accessed and used. When documents are classified by type, for example, a company can apply rules to it, including the date of its destruction. But because employees' tend to take a 'save everything' approach, with little thought to classification or destruction, implementing a people-oriented process around this risk is unlikely to succeed. Older technological methods, like keyword searching, can help, but are limited and not as reliable as purpose-built applications employing more sophisticated technology.

Such applications are software solutions that

learn and improve categorization over time as they encounter new data. Rules-based categorization or machine learning can automatically set the shelf life of information based on best practices for different types of content. Companies are using this same advanced technology to improve storage lifecycle management and to implement information governance policies. The reason? Technology succeeds where behavioral control fails.

ACHIEVING FINANCIAL CONTROL

Once companies have implemented better technological controls, they can add better financial controls by charging business units for overall storage costs. The better the business unit's document control policies, the less they are charged. Sophisticated tools such as predictive information management enable companies to take a cost-effective approach to data management while reducing their exposure to information risk.

In summary, companies that do not seriously assess their storage lifecycle management processes leave themselves vulnerable to increased costs and risk. Implementing a comprehensive storage strategy that includes an automated information lifecycle management process is one smart business decision that can act as both a shield and a sword in protecting a company in the age of the zettabyte. ♦



BOB TENNANT, CEO OF RECOMMIND