



## Storage Home

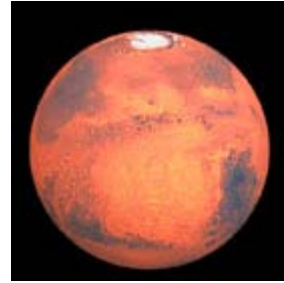
### Articles

### Related Areas

- ▶ IT Subject Areas
- ▶ Browse Subject Areas

## Total recall

Growth in the volume of electronic storage is putting pressure on IT managers, while the regulatory risks of document retention policies are rising.



With so many changes occurring in the storage arena John Lang, IT director of Epiq Systems reports on what IT staff need to know to get on the front foot.

When it comes to designing their document retention strategies, IT managers face a growing minefield of legal and regulatory requirements. Many companies are subject to the Sarbanes-Oxley Act, which has very strict guidelines on which documents should be retained. Meanwhile financial, tax and other regulators around the world all have their own varied stipulations about which documents should remain available for inspection - and for how long.

Moreover, for most companies, this is becoming more than a theoretical risk. One response to the financial and corporate failings that led to the credit crunch has been to give regulators considerably enhanced investigatory powers and the official encouragement to use them. In practice, this has led to a sharp rise in the number of dawn raids and information requests.

### Latest Articles

- ▶ Total recall
- ▶ A life in data
- ▶ Size matters
- ▶ The future of infrastructure design
- ▶ Greener datacentre top ten

### Latest from our blogs

#### oddIT Blog

Weird route, interesting stuff

Brian Runciman - 7 Jan 2009

No comments



#### Johny's Data Migration Blog

Data Migration - Free Training

John Morris - 7 Nov 2008

Comments (1)



These present a particular challenge for companies because of the tight timetables that regulators usually impose on their targets. For many companies, document retention and discovery policies have generally been formulated in anticipation of litigation rather than regulatory interventions. However, where the timescale for discovery in litigation can usually be measured in months, sometimes years, regulators commonly expect to receive the evidence they require within 30 days.

The increasing powers of regulators mean that knowing where your data is and how to find it is more important than ever. This task is monumental as the sheer volume of electronic documents continues to expand exponentially; such has been the growth in the number of documents generated since computers replaced paper as the main medium of business communication and record keeping. In the past, reviewing 50,000 documents would have been considered a big project; it is now not uncommon for the number of items involved in document reviews to run into the millions.

This is an issue that many companies have yet to fully address - a survey by Legal Week magazine last year found that only 41 per cent of general counsel thought that their boards had a 'reasonable appreciation of the risks' of failing to robustly manage their electronic data.

So, faced with a review of your company's document retention policy, where do you start? We would suggest a number of key steps to ensure that you are ready if and when the regulator knocks on the door.

It is essential to develop and maintain a holistic information (including email) management policy, across all of your company's locations. Developing an information policy is a three-stage process. What documents does your company generate and where are they located? Which of these are reasonably likely to be

required, given the rules of the regulators that your company is subject to and the company's litigation history? For how long do they need to be retained?

A common mistake is to assume that every document must be kept in perpetuity, which means that when an inspector calls, they waste enormous amounts of time and money by regurgitating thousands of documents which are of no use to anybody. This is not only an enormous waste of money, but can also give the impression to regulators that your record-keeping systems are inadequate - itself often a regulatory offence, as some recent eye-watering fines for banks and other companies has demonstrated.

Similarly, it is also essential to regularly check your company's back-up policy and restoration procedures. How effective and efficient are they? A poorly-conceived back-up and storage system can make the e-discovery process extremely slow, which has, in itself, led to regulatory penalties being levied on companies when the response to an information request is too slow.

An inadequate back-up procedure can also lead to the loss of key documents, especially emails, and the failure to produce important pieces of evidence will almost always be viewed adversely by courts, tribunals or regulators.

The key to this is to locate where your company's documents are stored, especially when your company has offices overseas. For multi-national companies, it does not automatically follow that each office's documents will be located on its own country's servers. Data can end up on servers a long way from its source of origin. It is also important to monitor the policies and practices of any third party data storage contractor your company may employ, to ensure that they are both keeping your documents and email safely and destroying them when appropriate.

In the event of an information request, the most important thing is to define exactly what it is that the enquirer is asking for. While the scope of regulatory information requests is often wider than that for the discovery phase of litigation, companies very often waste time in recovering every document.

When the heat is on, it is also often useful to bring in a specialist solutions provider. Specialist e-discovery platforms can help to identify and categorise the key document set, which can save many hours of review time.

Finally, the best advice for IT managers and directors is to share the burden of document retention with their employers. Very often, document retention policy is left solely to the IT department to deal with. However, when it comes to deciding how much to invest in document retention policies and infrastructure, the cost versus risk analysis is a fundamental business decision for companies and is a decision that needs to be taken by the business as a whole.

### **About the author**

John Lang is IT director of Epiq Systems, International. Prior to joining Epiq Systems, Lang spent 18 years managing global IT programmes across all aspects of the business with companies such as Hostway, Gap Inc and Toys R Us online division.

January 2009

[Legal and Privacy Notices](#) | © Copyright BCS 2009 | [Systems Status](#)

The BCS is a registered charity: No 292786 Patron: [HRH The Duke of Kent KG](#)