

IT Analysis – Digital DNA

By Fran Howarth, Principal analyst, Quocirca Ltd

According to the old cliché, content is king. For many organisations today, the content that they produce could be considered as the crown jewels of the business, including highly sensitive and valuable data such as financial records, intellectual property and databases of customer records. There are many that would like to get their hands on those gems of information and preventing this data from leaking out of an organisation is of prime concern to governments, enterprises and small businesses alike.

But it is not just data leakage that organisations today fear. Most entities face some kind of regulation and many of those rules mandate that information produced by or received by the organisation, such as in the form of emails, must be kept for a specified period of time and that its integrity must remain intact. For example, by placing controls on who can access what information and what they can do with it so that records cannot be altered by an unauthorised person.

Most of those regulations mandate that all information must be recoverable so that it can be handed over to authorities should there be suspicions of non-compliance or illegal activity. And this is also occurring in private cases as well. Electronic discovery (e-discovery) lawsuits are now fairly commonplace in the US and are growing in importance in Europe, particularly in the UK. This means that organisations must be able to produce any documentation that could be relevant to the lawsuit—and in any format, from word processing documents and emails, to product designs on CAD-CAM systems.

An organisation that has taken steps to secure and effectively govern its information may think that it can prevent its information gems, or even dregs, such as derogatory comments made by an employee, from falling into the wrong hands. Or they may think that they are in a good position to answer regulatory or e-discovery demands with the minimum of fuss.

However, there is one common mistake that has scuppered a fair few organisations to date, but which is only just beginning to get the attention that it deserves. That is the failure to consider metadata. Metadata is defined as "data that provides information about other data". This can include information about who created a document and when, and who has made what modifications to it at which point. Essentially it is the digital fingerprint or DNA that identifies all activity related to a document and provides an audit trail of that activity.

Lawsuits demanding the production of metadata along with the documents to which they refer have been brought to court since the mid-1990s and are becoming increasingly common. High profile cases where metadata has been used to provide key evidence include WorldCom, Enron and the Martha Stewart investigations, mainly in the form of emails. In some cases, metadata has been used to reconstruct evidence in disputes over timelines, such as an accusation that someone has backdated documents.

Other gaffes involving metadata have included a report released by the UK Prime Minister's office regarding its contentions that Iraq was amassing weapons of mass destruction. Used by Colin Powell to make the case for war in an address to the United Nations, a search for metadata in the document revealed that parts of it had been copied from work produced the previous year by a graduate student. And pharmaceutical giant Merck suffered embarrassment when metadata revealed that it had deleted a story about the causal relationship between its drug Vioxx and heart attacks.

Although the problems with metadata have long been known about by technologists, today's highly regulated environment and the sensitive nature of much of the information produced by organisations are elevating the issue to the business level. Now more than ever there is a need for organisations to ensure that they have systems in place to control the information that they hold—including metadata that can be used

to prove when documents were created, stored, searched and retrieved. In practice, the best defence is a layered strategy, including employee education, technology tools such as metadata cleaning or mining software, and policies defining the responsibilities of staff when handling documents.

For those organisations that have such processes in place, the benefits that they reap may be more than just the avoidance of negative publicity or a large fine. Although less publicised, there are cases where organisations have been able to use metadata attached to business documents to prove that an allegation was false. For example, in one case, an organisation in the UK faced a lawsuit from another firm which claimed that it had certain information at its disposal. Through forensic investigation, however, the organisation facing the lawsuit was able to prove through examination of metadata, including that attached to previously deleted documents, that it had never been party to that information and thus it won its day in court.

Just as fingerprints left at a scene of a crime are regularly used to secure convictions or to prove that a person could not have been there, the digital DNA of documents, or metadata, can be used as evidence of wrongdoing or can be used to prove innocence. The importance of metadata cannot be understated and should be a key consideration in the development of an effective system of information governance.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, Dell, T-Mobile, Vodafone, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at
<http://www.quocirca.com>