

## Straight Talking – Data leaks highlight need for content security

By Bob Tarzey, Service Director, Quocirca Ltd  
13<sup>th</sup> December 2008

The growth in the use of email and other forms of electronic communication between businesses in the last two decades has opened up a whole new area of risk. While there is an imperative to share information to keep business moving, all too often valuable data is getting into the hands of the wrong people.

The main danger is not so much that mishandled information will end up in the hands of competitors, although that should certainly be avoided, but more that the news of data leaks can cost businesses dearly in other ways. This includes direct costs such as regulatory fines and loss of assets, but also indirect costs, caused by reputational damage leading to lost orders and even share price devaluation.

Many of the high-profile data losses reported by the press in the last few years have involved lost laptops or disks used to move data from one place to another. Often there has been no proven compromise of data or even confirmation that misplaced disks have ended up in the hands of anyone who used the information on them inappropriately. But by the time the news gets to the media the damage has been done to the organisation's reputation, regardless of the actuality.

If the media was the only thing to worry about businesses might be tempted to try and suppress the news of data leaks. Unfortunately for them, there are other interested parties, namely regulators and courts, which cannot be brushed aside.

In most Western European countries data protection laws do not contain specific clauses requiring disclosure of leaks but that is likely to change. However given that the majority of data leaks involve "personally identifiable data", laws that protect privacy, most importantly the Europe Human Rights Law, come to bear. While these do not specifically require disclosure, not to do so would breach privacy, so the need to disclose is implicit as individuals must be informed if their privacy is likely to be compromised.

Human rights legislation and data protection laws give regulators teeth and they are using them to bite. At one level they are fining organisations for mishandling data and at another they are starting to impose restrictions on the way data is handled that require businesses to invest in technology - potentially creating costs even for those organisations that handle their data with the utmost care.

A seemingly minor data breach can lead regulators to take a more in depth look at the data handling procedures within an organisation. When the Nationwide Building Society reported the theft of a laptop from an employee's home in February 2007 it led to a fine of £980,000. The fine was not for the loss of the laptop per se, but for poor practices around data handling within Nationwide that were uncovered by the investigation into the lost laptop.

The underlying message here is that the starting point for any business wanting to address the way it handles data and mitigate the risk of data leaks has to be to formulate good internal policy, so that even when the inevitable occurs investigators can see that this was in spite of good policy rather than caused by bad policy or no coherent policy at all.

Policy needs to relate to how people use content. Most organisations already keep tabs on employees but they may need to extend that to external users. Organisations also need to be sure about which data they have stored and what it is used for - and too few organisations have clear policies about how people and content are linked.

Having a written policy that is well communicated to users is one thing - enforcing it is another. Here some organisations are getting ahead of the game but many others will end up lagging behind the requirements of the regulators.

It may sometimes appear that the regulators are adopting a knee-jerk response to high profile leaks; British data protection lawyers joke that the UK Data Commissioner has issued a directive

that data stored on laptops should be encrypted, for no better reason than encryption is something the commissioner had heard of. They may have a point. Encryption is not the be all and end all for data protection. Once someone has the keys to decrypt data, they are generally free to copy, email and print it as they like.

In future the data protection authorities in all countries are likely to hear about more and more so-called privacy enhancing technologies (PETs) as time goes by and may start to mandate them too.

One in particular is the fast growing availability of tools for data loss prevention (DLP). These have been around for some time but, as with many security technologies, DLP is now going mainstream as the big security vendors buy up the early innovators leading to pairings such as Symantec/Vontu (Nov 2007), Trend Micro/Provilla (Oct 2007) and Websense/PortAuthority (Jan 2007). Others such as Clearswift have developed DLP technology in-house.

Regardless of whether the regulators start to stipulate the use of DLP or not, businesses worried about data protection should take a look at it. DLP addresses two of the main issues in the people/content/policy triangle. First it enables content to be identified and monitored wherever it exists in an organisation. Then it allows policies to be defined about how people may use that data. It makes written policies such as "spreadsheets cannot be attached to emails" or "personnel data cannot be copied to laptops" enforceable.

Of course businesses need to allow their employees to share data both internally and externally. But with the regulators ever watchful, they are right to be nervous about it. The answer is to get their data handling policies under control and where possible use the technology available to enforce this.

Quocirca's report, [Content security for the next decade](#), is freely available at our website.

## 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>