

Preventing data loss - what's needed? The search for standards

By Bob Tarzey, Service Director, Quocirca Ltd

The UK's MPs may rue the day a disk listing details of their expenses was leaked to the Daily Telegraph from the House of Commons Fees Office earlier this year, but they were going to be made public at some point anyway, courtesy of the UK's Freedom of Information Act which the MPs themselves passed in to law in 2000.

The leak has not just exposed the actual expenses claims but the ill-defined and opaque policies that underlie them - herein may lie the bigger lesson for others.

There are plenty of examples of data that has reached the public domain that should never have done so, not least from other parts of the UK government.

This has led to a burgeoning demand for methods to control the use and dissemination of data electronically - so called data loss prevention (DLP) technology. Effective DLP requires that three things are understood and controlled: people, data and policy. Most organisations are on top of the first of these: they know who the people in their organisation are or at least have the means to do so. This includes not only employees but also external workers who need access to their IT systems.

Information about people is stored and referenced using directory servers. There are plenty of these around, including IBM's Tivoli Directory Server, Microsoft's Active Directory and Novell's eDirectory. While there is plenty of choice, they all largely comply with a widely accepted open standard known as LDAP (lightweight directory access protocol), so it is fairly easy for other applications to access information about users regardless of the specific directory in use.

The second area, data, is complex because it's all over the place and in many different formats based on various standards. Of course, there are

data repositories that limit what can be done with the information stored in them: content management systems for documents and databases for structured data.

However, the risk of leakage is greatest when data has been extracted from a repository and is being transferred by email, shared over the web or copied to some portable device. To ensure the sharing of data is authorised and safe requires that it is monitored - that the organisation knows when and where it is in use. DLP technology, supplemented by good end point security, helps to address all this.

Next comes policy. Policies define who can do what with different types of data. For example: only accountants can attach financial spreadsheets to emails; no one can move data onto USB storage devices; employee records must only be printed in a secure print room.

Defining and understanding policy across an organisation is the hardest part of the job. There are plenty of tools to help but the problem is selecting a policy engine that can be used by a range of applications that handle data.

There is no clear market leader and few standards in this area. The headache this causes should not be underestimated - a key reason for getting data use under control is to demonstrate compliance with various privacy and security regulations. To do that it is necessary to demonstrate policies are in place and enforced wherever possible.

IBM's recent announcements around DLP underline the problem. IBM Tivoli Storage Manager has a policy engine that the company claims can manage stored data "down to the individual file level". But this does not help with data being created on the fly or stored in places beyond Storage Manager's control such as end user devices.

Comment Article

To boost its offerings in the DLP market IBM has formed two partnerships over the last six months: Verdasys for the management of end points and Fidelis Security Systems for monitoring data in use. But the problem is both the new partners' products have policy engines too - so now to control the use of data using an IBM solution requires three policy engines. This means there's plenty of scope for duplication and inconsistency.

IBM is not alone. Security vendors have addressed DLP through multiple product lines developed in-house, acquired or via partnership. For example Symantec bought Sygate for end point security (now Symantec End Point Protection or SEP V11) and Vontu for DLP (now Symantec DLP V9), both of which had their own policy engines.

CA, EMC/RSA, Trend Micro and Websense have all made acquisitions in the DLP and end point areas and face similar problems with co-ordinating policy. McAfee has the most centralised approach. Its ePolicy Orchestrator (ePO) was developed in house and is core to its security suite. All its acquired technology is integrated with ePO as well as with 50-plus partner products, all done using McAfee's own proprietary software development kit.

For each vendor, the integration issues around policy will be addressed given time. However, there is a bigger issue: there are no widely accepted standards around the definition of and access to policy. It would make data security far easier to implement if there were and if a policy could read from any compliant policy repository, just as user details can be read from LDAP-compliant directory server.

The state of UK politics is a parody of this: it is easy enough to find out who your MP is but tying down the policies that control their behaviour is another matter.

Comment Article

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, O2, T-Mobile, HP, Xerox, 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>