



# Comment Article

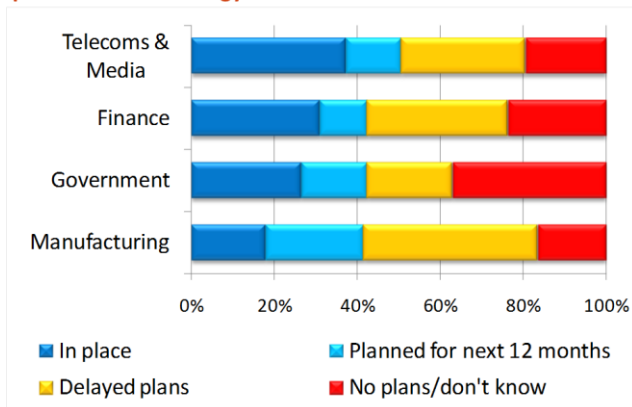
First published by the NCC Evaluation Centre

## Stemming data losses – Dec 2010

By Bob Tarzey, Analyst and Director, Quocirca Ltd

There is a clear case for using data loss prevention (DLP) technology. Recent Quocirca research shows that about a quarter of respondents had implemented DLP technology of some sort (figure 1) – and those with DLP in place were far more confident about their ability to protect data and intellectual property (figure 2). Overall, around 70% of respondents with DLP technology were confident they could protect their IP and personal data, compared to less than 10% of those without DLP systems.

**Figure 1: Has your organisation deployed data loss prevention technology?**



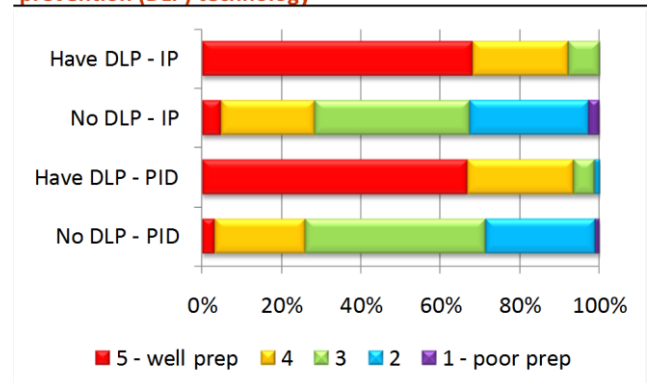
But if DLP can make such a difference, why aren't more organisations using it?

Certainly, there is no lack of awareness of the problems DLP sets out to solve. Our research shows that the safe use of data is a major concern for IT managers when it comes to IT security (figure 3). After malware, which tops the list, the next four issues all relate to data use: they are the internet, managing sensitive data and the activities of both internal and external users.

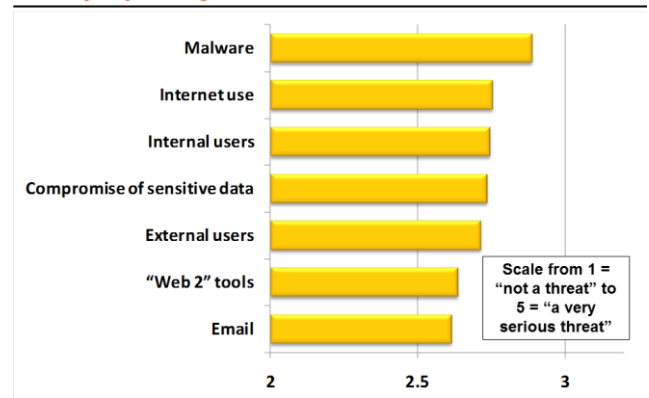
All four are related – and one of the main aims of DLP is to stop users sharing the wrong

information with the wrong people over the internet.

**Figure 2: Confidence to protect intellectual property (IP) and personally identifiable data (PID) relative to use of data loss prevention (DLP) technology**



**Figure 3: To what extent are the following a threat to IT security in your organisation?**



Data compromise is costly and Quocirca research shows that most organisations expect regulations and associated fines to get tougher. The area where regulation is expected to increase the most is data privacy. Already this year, the UK Information Commissioner's Office has been empowered to impose fines of up to £500,000 for the poor handling of personal data.

On top of this, it is becoming easier for employees to leak data – either intentionally or accidentally. First there is the range of communications tools that are now available, including email, instant messaging and social networking. Second there is the growing number of mobile devices with huge storage capacity to which personal data and IP can be copied – notebook and netbook PCs, smartphones and memory sticks, all regularly lost or stolen.

IT departments face challenges with centralised IT provision too. The increasing use of cloud computing services, both at the infrastructure and application level, has lots of benefits. But there are downsides too when it comes to data protection; there is a need to make sure that data protection practices extend to the third parties charged with managing such data and that rules about the geographic provenance of data storage are adhered to.

For example, the UK Data Protection Act (DPA) does not allow personal data to be stored outside the EU; yet many cloud providers will routinely transfer data for primary or secondary storage to offshore data centres.

### **Need for compliance**

Increasing regulations, the range of end-user tools and innovations in the way IT is delivered are all well and good, but they tend to leave IT departments worried when it comes to protecting data.

Our research shows that most organisations struggle with a lack of time and resources, too many manual processes and do not have an overall compliance vision. This last point is regrettable – if they did have such a vision and put in place what Quocirca calls a “compliance oriented architecture” (COA), many of the other problems would disappear.

A COA is defined as “a set of policies and best practices, enforced where practicable with technology, that minimise the likelihood of data loss and that provide an audit trail to investigate the circumstances when a breach occurs”. It requires that three fundamental things are understood and controlled: people, data and policy.

Most organisations have some understanding of the first of these – they know who the people in their organisation are, or at least have the

means to know through the use of some sort of directory, most of which these days comply with the LDAP standard (lightweight directory access protocol).

However, research shows that most do not have what we would term full identity and access management in place. This includes being able not only to manage employees, but also understand external workers who increasingly need access to a given organisation’s IT systems and some of the sensitive data stored within them. It also includes the management of privileged users who can, if not checked, override the security that applies to normal users.

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 – and these are increasingly encrypted to ensure greater security.

But there is also a lot of ad-hoc data on files servers and user devices.

Encrypting data is important, especially on mobile devices, but ultimately data is of no use if at some point it is not decrypted so that it can be used.

It is when data is in use that it is at its most vulnerable. What is needed is the ability to identify the specific information that is in use at various levels (document, paragraph, sentence, word) and the ability to put controls in place. This must include pre-existing data and new data being created.

For example, it is possible to search all existing documents and identify those that contain payment card data, but that does not stop an employee entering such data into an email on the fly.

The third area is 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;

credit card data must never be included in emails.

Defining and understanding policy across an organisation is one of the hardest parts of protecting data. 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. Many DLP systems have a policy engine at their core which could serve such a purpose.

Yet many companies still end up using multiple policy engines. 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, which is tough if policy management is not centralised.

#### **Products on offer**

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.

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 perhaps 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.

CA has also moved into the DLP space through its acquisition of Orchestra in early 2009. Since then it has provided close integration with its existing identity and access management products, claiming to be one of the few vendors to offer all the components for a compliance oriented architecture. Most of its DLP competitors integrate with widely used third-party directories, principally Microsoft Active Directory, which CA can also do.

Vendors that have been traditionally associated with network firewalls are also entering the DLP market. Check Point made an announcement this year, Cisco has made acquisitions in the content filtering space that could take it in the direction of DLP, and unified threat management firewalls from vendors like SonicWALL are starting to provide DLP-like functionality.

Newer entrants to the firewall market such as Palo Alto Networks claim their application-level view of the world makes them well-positioned to handle many of the issues DLP addresses. However, it must be remembered that firewalls generally only deal with the network edge and not the internal use of data or end points (especially when they are off-network).

For each vendor, the integration issues around policy will be addressed given time. However, there is a bigger problem – 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 be read from any compliant policy repository, just as user details can be read from LDAP-compliant directory server.

But perhaps the main reason why 75% of organisations are yet to address DLP is that they simply have not got around to it. The market is young and the issues it addresses – security, compliance and employee enablement – are fast changing.

A few years ago, many IT professionals would have understood the problems of data security but not have heard of the term DLP. With the market consolidating so fast and all the major vendors having offerings, they will most likely have done so by now. Many more people will likely recognise the value of such tools and implement some form of DLP in the next few years.

Quocirca's recent report titled "You Sent What?" includes primary research on the state of the DLP market. The report is freely available to readers at:

[www.quocirca.com/reports/475/you-sent-what](http://www.quocirca.com/reports/475/you-sent-what).

## 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>