Data Leakage Prevention - the Human Angle

Michael Barwise

Automated Data Loss Prevention (DLP) systems sit on the network and/or at endpoints, monitoring and controlling the flow of documents according to rules that comply with the organisation's information management policies. Growing numbers of commercial offerings have emerged in the last few years, and an open source product (MyDLP) is now available. But in my opinion, although DLP certainly has a big part to play in preventing some well-defined kinds of data leakage - for example by controlling access via the network to classification-tagged documents or specific data such as credit card details - it's not for everyone.

I assert this for several reasons. Firstly, DLP rules are derived from the organisation's policies. So they can only be as good as those policies, and it is the inadequacy of policies that allows most data leaks to happen. Secondly, DLP can exercise no control over paper records or manual processes, both of which are still commonplace in businesses of all scales - and which are involved in a high proportion of data breaches. Then there's the burden of implementation. For a large organisation, the complexity of the required rules can be a significant concern. A few months back John Vecchi of Checkpoint told The Register *"Some of these technologies are sophisticated and impressive but it can take 12 months to discover and a further 12 months to classify data. ... so ... many firms who have bought the technology have not turned it on."* Furthermore, for smaller organisations the cost/benefit ratio of acquiring and maintaining DLP may prove rather poor.

I appreciate I'm taking a contentious position in an industry that seeks to reduce costs and improve efficiency by automating as much data management as possible, so to justify it I examined a sample of the most recent Data Protection undertakings published by the UK Information Commissioner's Office to see how DLP would have helped prevent the incidents they relate to.

Twenty-two undertakings relating to more than 33 incidents were issued between July 1st and September 15th this year. Eight incidents involved paper records left in public places. There were fourteen incidents of misdialling when sending faxes. Personal data was exposed inappropriately on web sites in four incidents. Three incidents involved lost or missing USB sticks. The remaining six undertakings cover four instances of sensitive emails sent to the wrong recipient, one of password mismanagement, one dumped CD, two stolen laptops and one record of unspecified type that could not be found when requested.

In terms of record count, by far the worst case was the lost CD - containing some 1.6 million unencrypted records and left in a filing cabinet that was sent to land fill. Second came 20,000 records on a USB stick that was created in emergency to cover for a network failure and was then lost. But well in excess of a thousand paper records containing sensitive medical and legal information were dumped or abandoned in public places in eight separate incidents. In the case of the laptop theft, the equipment was stored in a locked room, but the key was hung on a hook in an adjoining outer room. However some of the most sensitive information was associated with much smaller numerical losses. Although no actual data leakage was proven, for several months CEOP (the child protection agency) collected sensitive information via a web form over HTTP, and all the instances of fax and email misdirection involved single records containing highly sensitive information.

This sample demonstrates the number and significance of incidents that DLP could not have prevented. The eight paper records losses are the most obvious, followed by the fourteen fax misdirections. Although DLP can in principle manage email recipients by document type, it's nevertheless questionable whether it could reliably have prevented these incidents. In one case at least - a local authority - the diversity and almost daily changeability of the professional contact base would have made it very difficult to keep the requisite rules up to date.

The risk associated with the laptop thefts might have been reduced by enforcing disk or file encryption, which might possibly be managed by DLP. That's a lot of contingent "mights", and the physical loss would still have occurred. DLP-enforced file encryption might also have mitigated the effects of the loss in the cases of the CD and one of the USB sticks. But there are cheaper and simpler ways than DLP of enforcing encryption, should you misguidedly consider USB sticks - or indeed email - an appropriate data transfer vehicle for sensitive personal data anyway.

The two other USB stick incidents were both clearly outside the scope of DLP. In one case, a legitimate encrypted USB stick was copied illicitly elsewhere to an unencrypted one which was then

lost, and in the second, the 600-odd USB sticks were notionally encrypted but the encryption could be bypassed due to a flaw in the product. When this was discovered, all the devices were recalled but half of them were untraceable.

So even being generous in our assumptions, maybe nine out of more than 33 incidents could have been prevented by DLP. Almost all of them could, however, have been prevented by enforcement of good information management processes. Clearly DLP can deal with only a subset of potential real-world data leakage, and even there it is in practice only as good as the rules you provide it with. Those rules must be derived from your policies, and all these breaches suggest that poor quality policies - indeed even a lack of policies - is a commonplace. In the absence of a properly enforced effective information management framework, DLP may do little more than confer a false sense of security, which is worse than a known exposure. It's therefore a useful tool for security-aware mature organisations, but it's not a panacea and should be eschewed by those who have not yet got a sound grip on data leakage at the process level. It's a support - not a substitute - for robust information management.

Circulated as a white paper, September 2011