

# Can you ever be wholly leakproof?

Data leakage prevention (DLP) is beginning to appeal to many, but even the best products need careful deployment, says **Rob Buckley**

**P**reventing data loss or data leakage is now a priority for many organisations and their security functions. Data leakage prevention (DLP) technologies appeal to many as a way of attaining that goal. However, before implementing DLP, organisations need to consider what DLP is capable of, what they really want and what processes and technologies they're going to need.

With so many ways for data to leave the enterprise, there is an equally large number of technologies that can describe themselves as DLP or DLP-related: business continuity, intrusion detection, endpoint protection, encryption, auditing, email/web filtering, identity management, two-factor authentication *et al.*

It might seem obvious that all these technologies should be implemented. But to implement all aspects of DLP would require considerable budget, expertise and time, and not all of these are going to be available to the average recession-impeded security function.

More importantly, the idea of being able to prevent all data leakage, even with DLP technologies, is an illusory one, according to Grega Vrhovc, a researcher

for the Information Security Forum: "In terms of stopping malicious attempts to steal data, DLP is not as efficient. Systems differ in how effective they are. Many are good at monitoring anything sent in plain text, some can deal with zipped PDFs and more, for example, but can they deal with PDFs saved as Tiff images? Steganography? Encryption? Many can monitor the network and block activity, but there may be other business processes they haven't counted on that can bypass that." And even a perfect

DLP system can't stop people printing out information and taking it from the building if they have permission, or simply memorising, writing down or taking photos of data they see on-screen.

So counting on DLP to prevent all losses is impossible. Organisations should expect DLP to be able to block most forms of accidental leakage – but only the more amateurish attempts at malicious leakage that employees might perpetrate. Architecting the necessary security into existing apps is the only way to prevent more concerted malicious leakage.

A good starting-point for a DLP project is risk assessment to determine where the most likely vectors of data loss are liable to be. If these are anticipated to be on the network, it's possible to install network DLP software or appliances from many vendors on a trial basis and monitor activity to determine if and how data is already leaking. This should give you a greater idea of what kind of measures will be needed to stop further leakage.

José Grandmougin, consultant systems engineer at Fortinet, says that means "considering a layered strategy to DLP, with either one or several systems being



**Consider a layered strategy, with several systems combined to block possible vectors"**

**José Grandmougin/Fortinet**





## DATA LEAKAGE PREVENTION CASE STUDY: CITY OF LONDON POLICE

With 1,200 staff, including 800 or so police officers and just three police stations in its square mile of coverage, the City of London police force is the smallest territorial police force in England and Wales. Nevertheless, with hundreds of thousands of commuters and tourists passing into the area daily and the same compliance requirements as other police forces, the force still has to ensure that its data remains confidential.



**Brailsford-Hart: balance**

Gary Brailsford-Hart is the force's head of information management services and chief information officer. He joined as a warrant officer in 1997, but soon transferred to more technical projects to track warrants, after which he joined technical services.

"DLP came up straightaway," he says. "We moved from Windows NT to 2000 desktops six years ago. With NT, there was no USB and limited CD writers; with 2000, I knew I had to deploy a solution to

manage USB" – to prevent data being leaked from the force via removable media. Brailsford-Hart chose DeviceLock, because of its AD integration and group policies.

There is now only one USB device approved for transferring digital data, DeviceLock's Stealth MXI, picked in part because of its reliability. "There's nothing more destructive than police officers, and USB devices are fragile."

As well as being hardware-encrypted, it has a steel case and biometric access via fingerprint. There's an audit trail of who has copied what to the device.

Brailsford-Hart says he had to strike a balance.

"It's possible to get data loss paranoia. There's a balance between confidentiality and accessibility." Everyone in the force has the right to copy and use the data on the Stealth MXI, provided they can make the business case. But staff find it hard to understand why, "when you can go to PC World and buy a terabyte USB stick for £3".

USB devices aren't the only way data could leave the force, so it also uses other DLP technologies. At the gateway, M86's MailMarshal is used to scan email and web content for breaches, put a cap on the maximum size of email attachments and to prevent uploads of data via the web.

Staff have more or less accepted the controls as necessary: "Every now and then we offer a seminar to explain it." But Brailsford-Hart says the force is having to look at ever-more sophisticated DLP policies to deal with increasing computerisation.

"Some officers want greater access to social networking sites so they can use them for investigations," he says. That will mean not just changes at the gateway, but also additional education on how to use social networking safely.

So far, the force hasn't had a data breach. But, says Brailsford-Hart, the headlines other firms have garnered from their breaches have paradoxically been helpful. "It has been very useful in getting the attention of senior management, getting a little investment and raising our profile," he says.

combined to block the various possible vectors". Many security vendors, including Fortinet but not Symantec, for example, offer DLP features in the latest versions of their software, so it's possible that upgrading under an existing licence is all that's needed to gain access – with minimal investment – to the DLP features the organisation needs.

Since they are part of existing suites, you may find that integration between different security systems is easier and can be done through a single management console, without further programming. Although some DLP systems, including Symantec's Data Loss Prevention 10 platform, support technologies such as web services, others do not yet incorporate integration. Says Novell's senior technology sales specialist Mark Oldroyd: "In many data breaches, there's lots of evidence of data loss about

to happen. If you collect and monitor, you can see it before it happens, but the key is the ability to correlate data from individual systems."

A data assessment is also necessary, to establish which data is important and needs to be protected. "Unfortunately, this can be very difficult," says Martin Blackhurst, head of IT security at Redstone Managed Solutions. "You need to find out where the data is and whose responsibility it is."

Any organisation that has implemented an enterprise content management (ECM) system will at least have a good idea where the important documents are stored, and many DLP systems such as Websense's can integrate with ECM systems, but ECM might not know which documents are so important that they can never be checked out. ECMs that incorporate record management functions



**Encryption won't deal with an employee who puts a token in their laptop in Starbucks and then goes off to the toilet"**

**Neil O'Connor/Activity IM**



can also help to ensure data is only kept for as long as it is needed, points out Hitachi Data Systems' (HDS) field product manager John Hickman.

While ECM will help maintain a central store, many organisations will still find copies of information being stored on laptops and other mobile devices, as well as PCs. Encryption can help solve the problem of lost removable media and mobile devices being raided for data, although it can do nothing about someone who knows the password for the device, or, as Activity IM consultant Neil O'Connor points out, "an employee who puts the token in the laptop in Starbucks and then goes off to the toilet". Many DLP systems don't support operating systems such as Mac OS X or Linux, so can't be used to protect them automatically either.

Encryption is also useful on servers on desktops since, as HDS's Marcus Benham points out, all hard drives eventually leave an organisation. HDS's storage system can also write backups and data onto Worm media. However, 'data in motion', ie data transferred between datacentres or to backup, can still present a challenge, since encryption needs to be quick enough not to impede performance.

Performing that data audit might be something that an organisation can do for itself, or it might require an experienced data auditor to help determine how best to scan large numbers of documents. "Sometimes an external pair of eyes with external expertise is good," says Redstone Managed Solutions' Martin Blackhurst. "If you get a security VAR to come and talk to you, it would be sensible to seek advice.

"You need to be making sure you aren't missing a trick. But you have to have someone with expertise in data discovery and to be sure about the technology they're using to look – so don't rely on a VAR or a consultant."

Another option, not just for DLP but



for data discovery, might be to look for a cloud service. SecureWorks is planning to offer a cloud DLP service by the start of 2011 and is about to launch a pilot programme. According to senior product manager Kerwin Myers, the company is planning a staggered approach, with phase one offering monitoring of network traffic and phase two offering monitoring of 'data in use'. However, Novell's Oldroyd cautions against DLP in the cloud, saying that it marks "a step backward in security".

With a collection of sample documents that you want to prevent from leaving the organisation – and knowledge of how they might currently be leaking – you can choose an appropriate system or systems to defend against the loss. Most systems are able to scan Microsoft Office documents, PDFs, zip files and plain text, but if you use other file formats, be sure any DLP system that you choose can scan those additional file types.

Systems that allow you to selectively block documents will require you to set up rules to determine what kinds of documents to block, when – and what to do afterwards. Most vendors have created sets of rules applicable to certain industries or to deal with certain pieces of legislation, such as PCI DSS or the Data Protection Act. Simon Godfrey, director, security solutions at CA, advises larger organisations to check whether DLP vendors have sets of rules defined for countries other than the UK. "Germany

## HOW REAL IS THE INSIDER THREAT?

Are employees just there to help – or are they the company's biggest threat? The spectre of the malicious employee, using insider knowledge, is a threat that many organisations assumed would grow larger thanks to the recession.

Opinion varies as to how real that threat actually is. The 2006 e-Crime Watch Survey conducted by the US Secret Service and SEI CERT for *CSO Magazine* found that in cases where respondents could identify the perpetrator of an electronic crime, 32% were committed by insiders. A survey last November by Actimize of 70 financial institutions worldwide found that 82% believed the threat of employee fraud was growing and 78% saw the employee fraud problem increasing due to the slower economy. Other surveys go as far as 98% of crimes having an 'insider connection'.

IDC research last year painted a slightly different

**82%**  
of global financial institutions believe the threat of employee fraud is growing

picture. Of 400 organisations surveyed, 52% characterised their insider threat incidents as accidental. Only 19% believed the threats were deliberate, while 26% believed they were an equal combination, with 3% unsure.

"I don't think it's hyped up. It does happen," says Martin Blackhurst, head of IT security at Redstone Managed Solutions. "I've seen employees take customer data with them. Salespeople are doing it, because of the type of people they are. It is a very real threat."

"Malicious employees are always a threat," says Caroline Ikomi, technical director for Check Point. "People have been stealing off companies for donkey's years." However she puts the risk considerably lower, somewhere less than 10%, arguing that while insiders can be a threat, usually the damage they may cause is accidental rather than deliberate.



## Data loss



and France have very different privacy rules, much stronger than the rest of the EU's," he says. Customers at larger organisations should look into DLP systems with tried and tested rulesets for as many territories as possible, he adds.

Customising these rules for your firm requires work, which may require consultants with experience in the area to help you avoid the common pitfalls.

Some systems employ a 'Bayesian' approach, with users able to train systems by giving them documents already selected as confidential, as well as documents that are not, so the system can learn which is which. Others require users to create rules that use keyword searches, regular expressions and other forms of analysis to decide which files are confidential: typical flags might be credit card numbers or social security numbers.

While some systems rely purely on this level of detail, one of the biggest issues with DLP systems is false positives – they can err on the side of caution and flag up too many possible documents. To avoid this kind of overload, tying actions to identity can significantly reduce admin issues. Either using standalone identity management systems or by tying typically into LDAP or Active Directory, you can define certain actions as allowable by certain users or groups of users. "If someone in finance is sending a financial report, that might be fine, but someone in IT shouldn't be able to – and someone in a call centre shouldn't even be able to access it," says Lior Arbel, managing consultant, DLP of Websense. This ability to identify users can also be used for an audit trail and to monitor user activity for patterns of behaviour.

With most systems able to run in 'monitoring' mode at first, a testing period after installation is vital, since it allows the organisation to test the rules and refine them. Arbel highlights the case

of an organisation that chose the keyword of 'confidential' to determine if a document was confidential or not – but would have ended up blocking every single outgoing email in a live system, since its standard email footer also included the word 'confidential'.

This kind of training period can take from two weeks to 18 months, depending on the caution of the organisation, says Glen Vondrick, Sendmail's COO. He says many email delivery teams find that to maintain the service level agreements (SLAs) for email delivery times, they're unable to run some systems in anything except monitoring mode, as the large rulesets of some organisations mean their DLPs would slow email to an unacceptable level in live mode.

With a DLP system set to intercede rather than simply monitor, organisations need to consider what actions they'll get their DLP to perform if a potential breach is detected. Many DLP systems offer a variety of responses. "Specific actions can be soft touch," says Symantec's Andy Ng. "They can notify users when they copy data, or email notifications to a manager. They can block via email, or quarantine files from data copies." Sendmail can perform as many as 50 actions, while Symantec's platform offers organisations the ability to craft Java applets for specific actions. Your organisation should pick a system that provides the flexibility in action that your business processes require.

However, if users are prevented from doing what they legitimately want to do, they'll need to be able to contact an administrator to override the action. Set the rules too coarsely and there'll be too many alerts and a huge administrative burden; set the rules too finely and some confidential data is likely to leak out.

So, many organisations, unless they're heavily regulated and have a significant admin budget, will find that a middle path works better: instead of simply blocking the data from being sent, either the system will be set permanently to monitor mode or the DLP will alert the user that an action has been stopped and give them the option of overriding it. For this to work well, technology is not enough: a user education programme needs to be in place, so users understand why DLP has been introduced and the implications for the organisation if data does leak – which is why SecureWorks is planning to include it in its cloud service.

DLP is a great way to stop the loss of data that some users might cause by accident, as well as to monitor less obvious causes of data loss. DLP can't stop all losses, but it can help. ■



**Malicious employees are always a threat. People have been stealing off companies for donkey's years."**

Caroline Ikomi/Check Point