

Five Steps to Effective Data Leakage Prevention



The prospect of data loss represents a concern for **every business**. Barley a month passes without an organisation suffering negative publicity as a result of **unauthorised disclosure** of sensitive data. And unbeknown to many organisations, their information is not only a **prime corporate asset**, but also a **sought-after commodity** on the black market.

The sheer volume of data in the typical business environment makes it difficult to control and heightens the risk of leakages at multiple points. Adding to the complexity is the fact that data takes various forms: web pages, e-mails, electronic and paper documents, databases and is also found in various contexts. 'Data at rest' is located on storage mediums such as endpoint devices; 'data in transit' traverses the network; 'data in use' is passing through a computer's central processing unit; and 'data beyond boundaries' is located beyond the organisation's direct control.

Three letter word

You, like many organisations may view data loss prevention (DLP) as a valuable 'string to your bow' in tackling the ongoing challenge of data or information loss. Yet harnessing the full potential of DLP requires focus and planning. DLP is not an 'off-the-shelf' product or a quick-fix. Vendors typically use the term for a portfolio of solutions that prevent accidental leaks or exposure of sensitive enterprise or customer information outside authorised channels. Despite implementing controls prescribed by vendors, organisations are still suffering from incidents of data leakage. Most organisations have firmly embraced authentication and access control. However, in isolation, these tactics do not represent a panacea for data protection issues. Protecting data effectively calls for a holistic approach that covers people, process and technology.

The issue here is that oftentimes, organisations view DLP as an isolated matter that needs to be addressed by the IT department. DLP, however, is very much a business issue – the implications of a data breach, loss or leakage are broad and business related.

Making DLP work for you

Make DLP a priority – but not a stand-alone project

Data leakage can cause an organisation untold public embarrassment and loss of revenue. Decision-makers therefore need to address the risk of data loss or leakage in light of a broader security strategy and roadmap. Look at DLP from a risk management perspective, not just as another IT security project. The best results will be achieved when a project team, of which the risk manager is a key stakeholder, is appointed and sponsored by executive management.

Understand information flows

One of the cornerstones of effective DLP is ensuring that sensitive information can be monitored and managed within the organisation. The location of sensitive information within the environment and how it moves from one user or process to another are referred to as 'information flows'. Unauthorised information flows constitute a data leakage event.

What organisations require, therefore, is full visibility of information flows within their environment. That said, the task of identifying all potentially sensitive data and defining the relevant protection policies is a potentially time consuming and resource draining task. The good news is that DLP tools often provide data discovery capabilities that facilitate the discovery and classification of information across the entire network.

Bear in mind that any discovery exercise must be supported by an underlying data/information classification policy. Such a policy will allow you to define different levels of security classification and determine the appropriate levels of control.

Implement technical and non-technical procedural controls

Another hallmark of effective DLP is having tactical control of data leakage risk points within your organisation. Theft and loss of mobile devices, such as laptops and mobile telephones, and the transfer of sensitive files over public networks without appropriate security, are key culprits here. Device encryption and port control solutions and secure file transfer solutions can provide you with the levels of control you require. They are also relatively cost effective, easy to implement and non-intrusive to the environment.

Create user awareness

Data leakage incidents are not necessarily the result of malicious intent. Employees may transfer sensitive data to external media devices such as iPods, smartphones, USB memory sticks or e-mail to home addresses, just so that they can continue working from home. User education provides an opportunity for the business to articulate the risk of information mismanagement to all employees, without limiting their productivity.

Ask for help

Complex business issues such as data leakage require comprehensive, easily manageable and integrated solutions. To be truly effective, your DLP initiative must stretch across the entire IT ecosystem and include classic network security (routers and switches), perimeter security (firewalls, IPS), endpoint security (PCs, mobiles, servers, etc.), application security and data security.

Few organisations retain the in-house security skills required to effectively address DLP. It's not uncommon, therefore, for organisations to enlist the services of an IT partner that is vendor agnostic and can recommend the optimum mix of technologies, without fear of favour.

One step at a time

DLP needs to form part of your overall security roadmap and reach across your entire IT estate. Threats are continuously evolving which means that there are no guarantees in the IT security world. However, embracing a holistic approach to information security (people, process and technology) will put you firmly on track to ensuring that your information is appropriately protected.



MIDDLE EAST & AFRICA

ALGERIA • ANGOLA
BOTSWANA • GHANA • KENYA
MOROCCO • NAMIBIA • NIGERIA
SAUDI ARABIA • SOUTH AFRICA
TANZANIA • UGANDA
UNITED ARAB EMIRATES

ASIA

CHINA • HONG KONG
INDIA • INDONESIA • JAPAN
KOREA • MALAYSIA
NEW ZEALAND • PHILIPPINES
SINGAPORE • TAIWAN
THAILAND • VIETNAM

AUSTRALIA

AUSTRALIAN CAPITAL TERRITORY
NEW SOUTH WALES • QUEENSLAND
SOUTH AUSTRALIA • VICTORIA
WESTERN AUSTRALIA

EUROPE

BELGIUM • CZECH REPUBLIC
FRANCE • GERMANY
ITALY • LUXEMBOURG
NETHERLANDS • SPAIN
SWITZERLAND • UNITED KINGDOM

AMERICAS

BRAZIL • CANADA • CHILE
MEXICO • UNITED STATES