opinion piece

dimension data

Data Loss Prevention

Protecting the data that matters

Most organisations would agree that their employees and the data that they generate, process, and base decisions upon, is what enables them not only to survive, but to thrive. Inevitably, however, circumstances will arise that place your two greatest assets – your people and your data – at odds. And if you don't have an unbreakable chain of security links that prevent employees from accessing information they shouldn't, or using information to which they are entitled against you, or simply absent-mindedly losing or misapplying your information, your organisation is at risk.

So both the profitability and integrity of your business – and the productivity of your employees – depends on your protecting that data responsibly.

It uses technology to **prevent** and **control unwanted use of data**, accidental or otherwise.

The demise of the traditional corporate perimeter

In business today, effective communication and collaboration is the enabler of productivity. The ability for employees to gain remote and mobile access to enterprise resource planning systems, e-mail and messaging systems and mobile applications is not just enabling but actively fuelling intensified collaboration among internal and external stakeholders. Also, flexible working is now an accepted norm – which further extends the corporate network.

Increasingly, corporate end users are challenging what the IT department dictates – they are demanding the freedom and flexibility to create, consume and share information from any device, at any location, at any time. As a result, the flow of personal mobile devices into the workplace continues unabated. This trend has spurred the demise of the traditional corporate perimeter, with a sudden flood of devices that are no longer directly managed and controlled by the enterprise accessing corporate resources. With the business drivers loud and clear, technology and security professionals are no longer able to credibly represent a roadblock for the adoption of mobile technologies.

The issue here is one of meeting user expectations. What organisations need to provide is anytime access to information and the ability for employees to enjoy the same experiences in the workplace that they do in their personal lives, irrespective of their device of choice. But that doesn't mean having no authorisation processes or opening up the corporate network to the predations of the outside world. It simply means translating user expectations into a corporate environment, where security, governance, compliance, and commercial realities are part of the functionality.

Enter data loss prevention (DLP).

For the business, by the business

DLP allows organisations to set up, operate, and distribute an effective security policy for information flow in order to keep control of critical information such as blueprints, financial metrics, and source code, prevent accidental breaches of compliance and confidentiality policy, and support users' mobility while using laptops or smaller devices.

It uses technology to prevent and control unwanted use of data, accidental or otherwise. At the same time, it enables individuals to optimise the value of your data. DLP is, therefore, not as much a technical issue as it is a business issue.

In addition, because it focuses on data, DLP is very much a part of the larger compliance and privacy discussion. Most privacy legislation demands disclosure of lost, unencrypted data even if there is no evidence that sensitive data has been accessed by unauthorised users or used in a malicious way.

However, most security solutions are still perimeter-centric, encompassing firewalls and virtual private networks (VPNs) and focused on protecting perimeters and resources lik laptops and servers. While they are necessary components of a comprehensive security strategy, they only protect the infrastructure that contains and processes information, not the information itself. An additional shortcoming of a perimeter-centric security environment is the fact that when data leaves the protected assets or perimeters, it is often no longer secured.

All data was not created equal

Data can take many forms including web pages, e-mails, electronic and paper documents, data bases, to name a few. It also exists in various contexts: 'data at rest' resides on storage mediums such as endpoint devices; 'data in transit' traverses the network; 'data in use' passes through a computer's Central Processing Unit; and 'data beyond boundaries' is located outside of the organisation's direct control.

DLP cuts through this complexity and allows you to centrally control and monitor data flows and prevent leakages, irrespective of the location, type and profile of the data.

Data-in-use

DLP protects and controls sensitive information such as contracts, term sheets, and other business-critical documents that are being used at an end point.

Data-in-motion

DLP monitors, encrypts, filters, and blocks outbound content contained in e-mail, instant messaging,
file transfers, web postings, and other types of messaging traffic.

Data-at-rest

DLP discovers, protects and controls information on servers, databases, desktops, laptops, file/storage servers, USB drives, and other types of data repositories.

Data-beyond-boundaries

DLP encrypts data and manages access to it based on digital rights management principles, restricting access to and use of data based on identity and also providing an audit trail.

People – the building blocks of effective DLP

Together with your data, your people are your business' most important asset. It therefore stands to reason that you need to help your employees understand how to interact optimally with company data – and also how to contribute to IT security. Employee education is, therefore, one of the building blocks of effective DLP.

From a business case perspective, quantifying a return on investment in security education for employees is not any easy task. That said, it makes little sense to put sophisticated processes and systems in place and not ensure that employees are informed and equipped to make use of and benefit from them.

Steering ahead, securely

This journey towards securing your data need not necessarily be fraught with risk and uncertainty. With some focus, data loss prevention is achievable and will allow you to unlock the benefits that the new business paradigm of collaboration and mobility promises.

dimension data

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

For contact details in your region please visit **www.dimensiondata.com/globalpresence**

www.dimensiondata.com