Fragmenting DLP assessment, implementation, and management is counter-intuitive
Contents

Introduction 01
Having the cake and eating it 01
Holistic = end to end 01
The devil is in the detail 02
Local availability, global knowledge 02

opinion piece | fragmenting DLP assessment, implementation, and management is counter-intuitive
Data loss or leakage prevention (DLP) is a holistic approach to protecting and controlling an organisation’s data. It's not a single solution. It's a suite of appropriately data-centric solutions that work together to cover your data wherever it is in the organisation – whether at rest in storage or external devices, on the move across the network and in cyber-space, or being processed on CPUs.

Of necessity, therefore, the process of assessing your DLP needs by locating and classifying your data, implementing DLP models and technologies, and managing and maintaining your DLP systems, whether they are process, technically, legally, or human resources based, needs to be just as holistic.

We're seeing a dawning realisation of this fact in IDC research about the business value of DLP done in 2009 for Dimension Data. The survey involved 407 organisations in 18 countries across Western Europe, the Americas, the Middle East, Africa, and Asia/Pacific.

Just over 50% of the surveyed organisations said they would be implementing some sort of DLP model in the next 12 months – but that they would be looking for solution-oriented rather than problem-oriented DLP services. Specifically, they believe DLP services should include at least a centrally managed security policy for the entire infrastructure, insider threat management, enhanced and secured mobility, and compliance.

They also want their DLP business models to generate ROI, control data flows, and support business operations in tandem with engendering positive opinions on success enablement.

Having the cake and eating it

And, yes, they’re absolutely right to expect all that – if they don’t fragment the way they get it all done by their suppliers.

Also, if you’re looking for solutions-oriented rather than problem-oriented solutions, then you’re moving away from the concept of point solutions and towards integration and consolidation.

It’s very rarely possible to achieve ideal integration and consolidation if you’re working through a number of different suppliers, each with their own take on what DLP means to your organisation.

Also, it makes no sense, for instance, to have one organisation assess your IT and data assets and their DLP requirements and then have another organisation implement the recommendations that arise from the assessment, and still another provide managed services once the implementation is complete.

That’s like refusing to have on site while your house is being built the architect you chose precisely because he has a strong engineering background – and leaving the interpretation of his drawings and recommendations to the building project manager.

“IT’s very rarely possible to achieve ideal integration and consolidation if you’re working through a number of different suppliers, each with their own take on what DLP means to your organisation.”

There will, inevitably, be a gap between the architect’s vision and the project manager’s implementation, because the project manager has neither the architect’s specialised knowledge of engineering or his particular insight into your expectations of your house.

In the same way, if you’re going to consult DLP specialists, as IDC’s research indicates that 52% of organisations will, then you’re expecting from those consultants not only an in-depth understanding of your particular organisation’s DLP needs but also input from them on what is possible, what’s desirable, and what’s strategically optimal.

Accordingly, based on an assessment of your assets and requirements, those consultants will fuse their experience of other DLP models with best practice in order to design for you a chain of secure links that will protect your data and therefore your business against all known threats. In the process, they will provide you with a foundation on which you can quickly and cost-effectively build additional DLP tools as new threats make themselves apparent.

Any supplier not involved in that process is simply not going to have enough information to help you implement your DLP systems and processes so that they properly fulfill the intentions of the original design.

Holistic = end to end

Well, I hear you say, all I really need the implementation team to do is follow orders.

Actually, it’s not that simple. IT security and data usage are not static. Without a thorough understanding of the underlying principles incorporated into the original design, project-focused organisations can skew the implementation in less than helpful ways.

Because the underlying principles are, essentially, developed from the processes used for life cycle management, they provide a holistic picture of an organisation’s systems and, therefore, how the organisation handles data.

The first step involves a business discussion about the organisation’s network and data-related technology lifecycle, and existing and best fit longer-term network and system architecture, considering risk, cost and strategic factors.

Business and technical reviews are done with the key stakeholders to ensure that the relevant information is collected and lifecycle milestones as well as security and configuration issues are identified.

An asset list is developed and analysed against security, configuration, and end-of-life databases. A technology roadmap is created, based on the prioritised recommendations from the analysis.

“It’s very rarely possible to achieve ideal integration and consolidation if you’re working through a number of different suppliers, each with their own take on what DLP means to your organisation.”
The consulting house and the organisation’s key stakeholders must then determine how to act on recommendations based on risk, cost, and strategic factors. An action plan is developed.

Each of these steps forms part of a multi-year planning approach and many steps need to be executed in more than one financial period. In addition, networks, data, and markets are dynamic. Configurations will drift from best practice standards over time and additional products deployed will enter the end of lifecycle. In order to ensure the benefits of this approach over time, repeat assessments should be considered.

It’s very nearly impossible for continuity of all these steps to be maintained – over time and across multiple IT and operational disciplines – by an exclusively project-focused implementation partner that has not participated in the original assessment.

The devil is in the detail

Besides, data can take many forms, including web pages, e-mails, electronic and paper documents, and data bases. It can be 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’ passes through a computer’s Central Processing Unit; and ‘data beyond boundaries’ is located outside of the organisation’s direct control.

So, within the global assessment, each area of DLP is an area of specialisation in itself. Data-in-use DLP, for instance, includes solutions that protect and control sensitive information such as contracts, term sheets, and other business-critical documents as they are being used on or off the network. Data-in-motion DLP includes solutions that monitor, encrypt, filter, and block outbound content contained in e-mail, instant messaging, peer-to-peer, file transfers, web postings, and other types of messaging traffic.

Data-at-rest DLP includes solutions that discover, protect, and control information on servers, databases, desktops, laptops, file/storage servers, USB drives, and other types of data repositories.

Data-beyond-boundaries DLP includes technology that encrypts data and manages access to it based on Digital Rights Management (DRM) principles, restricting access to and use of data based on identity and also providing an audit trail.

Local availability, global knowledge

Then, of course, there’s the question of managing and maintaining the implemented DLP solutions on an ongoing basis. Most organisations don’t have the range of skills in house to do it effectively – and eventually turn to managed services.

Keeping continuity throughout the assessment, implementation, and management elements of ensuring optimal DLP implies the use of a global systems integrator with local skills on the ground. That way, the organisation gets the best of local and global capability in a single, coherent offering focused tightly on the organisation’s unique and best interests.

The point being that, if you’re going with a holistic approach by going with DLP as a concept, you would want your assessment, design, implementation, management and maintenance to reinforce rather than undermine that holism by being integrated and consolidated as well.