This is a short introduction to the key steps Company85 recommends you take to achieve a successful data loss prevention (DLP) implementation that enhances, but doesn’t hinder, your organisation.

While DLP tools are very powerful, integrating them meaningfully with the business requires clear understanding of the policies, culture, objectives and statutory obligations affecting data protection. In practice, similar instances arise within similar organisations, which is why Company85’s experienced consultants can help fast track DLP programmes.

Key points

- Protect your data wherever it is
- Engage the business
- Invest in event processing
- It’s about a lot more than just the tools
- Measure maturity
**TIP 1: PROTECT YOUR DATA WHEREVER IT IS**

Ensuring you have good DLP coverage across all the places where your data is stored, transferred or used is critical. Many firms focus on data loss from their corporate local area networks (LANs), where sensitive data travels across the network and only leaves via web or email that can be tracked for policy violations.

While this approach typically exposes many DLP events, the problem is that more and more corporate data now resides outside the corporate LAN, on mobile devices. And when these leave your corporate LAN, so does your data.

Once outside the corporate LAN many DLP implementations are unable to protect the data. That means it will find its way onto public email and cloud services where you can’t control access and are potentially giving away your intellectual property. So you need to make sure your DLP solution is capable of monitoring and managing data on any devices that are connecting to your network and transferring data out. These could be corporate laptops, smartphones, tablets or, increasingly, ‘bring your own’ devices.

You also need to consider DLP controls for data stored by third party suppliers, such as when data related to your corporate applications is hosted in the cloud.

**TIP 2: ENGAGE THE BUSINESS**

Engaging the business and getting its support will stop you making costly mistakes.

The flow of data between you, your partners and customers is critical to keeping your revenues flowing, but we’ve seen a number of clients treat DLP simply as a technology solution and who have therefore implemented it ‘silo’d off’ from the business.

At best, the business then receives a stream of security events with no context and that are considered to have little value. DLP is seen as an annoyance, not a business benefit; as a result the business will probably ignore these alerts. At worst DLP stops or slows down a critical business process. This, in turn, stops the flow of money into your business, and (having lost money) the business will probably now do its best to proactively resist DLP.

Getting the business process working again often takes time because of the lack of engagement between business and IT. Security needs to work in partnership with the business, understanding the value of data and where it needs to travel as part of the business process. Potential data loss events should be routed back to relevant business stakeholders first wherever possible. A business-aligned stakeholder will be able to better interpret the value of data and therefore to understand the risk of the incident than a security analyst.

Where sensitive data needs to be transferred by a business process, IT security can provide secure transport mechanisms and use DLP to enforce their use. Where data shouldn’t be transferred, these events can be used to target and improve business-specific user education around policies and best practice. The result is the business sees DLP as a benefit and will actively promote it.

**TIP 3: INVEST IN EVENT PROCESSING**

The different types and sources of sensitive data within a firm are usually large, and as the volume and value of data used by the business grows this is only going to become more difficult to manage.

We’ve seen clients using out-of-the-box configurations for their DLP solutions. Vendor rule sets are a good place to start but they are not tuned to your business or data, and are only likely to catch the most obvious data loss events. The chances are that a lot of stuff you want to protect is flying right past your DLP monitoring while, on the flip-side, if you expand your rule-sets to try and catch too much you achieve the opposite effect. The people reviewing events are inundated with false positives, and they become overwhelmed as they can’t filter these events manually. As a result, events go through without review – and buried within these are the real data loss incidents.

Getting the balance right involves a significant investment in setting up and tuning DLP event monitoring, which should be gradually expanded to analyse as many events as possible. Filtering out false positives requires the right tools to start with. They need to be content-
aware and capable of sophisticated configurations to achieve your objectives. This will leave you with a manageable stream of real DLP events on which your business and security operations can focus.

**TIP 4: IT’S ABOUT A LOT MORE THAN JUST THE TOOLS**

For DLP to work you need to deliver change across multiple areas.

Ask yourself if your policies and standards around the control and handling of sensitive data are easy to access and understandable. Education and awareness for your users are key to preventing data loss. Stopping it before it happens is more effective than trying to monitor or block it.

When it does happen, ensure you use the information from actual data loss events to target individuals or departments that need more training and to feed back your business-specific data loss examples into training material.

Build DLP into your enterprise architecture. Making DLP an integral part of building new business apps is much more effective than retro-fitting it afterwards.

Make sure your staff can identify and classify sensitive data and understand how it should be handled. Use DLP tools to enforce handling (for example, the use of encryption or secure transfer methods).

A good operational model is required. You need to be able to quickly react and resolve events to keep the business running. Continual review and feedback between IT security and business is essential.

When all this is working together you’re in the best position to reduce the risk of data loss and to increase protection around your data.

**TIP 5: MEASURE MATURITY**

The data that businesses rely on is rapidly growing and becoming more complex. This means there is no quick fix to implementing DLP. DLP practices need to mature over a period of time.

At Company85 we talk about five levels of maturity:

1. **At risk.** This applies to organisations with no or poor DLP implementation. These firms are at serious risk of reputational damage, financial loss or regulatory fines from data loss events. Preventative actions are difficult for them as they can’t identify the root cause or source of data loss events.

2. **Assessed.** The organisation knows where critical data is, and is able to conduct forensic investigation into data loss events. It can now take preventative action to stop data loss before it happens – and when it does happen it has the information required to respond quickly and effectively.

3. **Key data protected.** By this stage the organisation has identified its particularly sensitive or valuable data. DLP is being used to enforce business processes around this data – where and how this it can be stored, transferred and used. Anything outside the standard business process is blocked and escalated by DLP processes.

4. **Protected.** This covers the same as the previous level but includes a much wider coverage of data. By now the organisation has confidence its data is protected and it can demonstrate compliance to regulators and audit using its DLP tools.

5. **Assured.** DLP is now integrated into any new business process. Risk of reputational damage, financial loss or regulatory fines is low.

Each level of maturity requires coordinated change across business, technology, people and information governance. In Company85’s experience, building maturity like this typically takes years and needs to be part of a structured programme or initiative.

Understanding your maturity level helps you understand progress, where to focus next, and helps set expectations with your internal and external stakeholders. It also enables you to ensure the people, process and technology changes are moving forward together so you can deliver a joined-up solution.
About Company85

Company85 is an independent IT consulting firm specialising in enterprise-class information protection, transformation and service management.

Headquartered in London, we provide advisory, implementation and managed services to FTSE100 companies and public sector organisations across the UK, Europe, Africa, the Middle East and the US.

Our clients include AstraZeneca; BBC; Betfair; Deutsche Bank; EE; Financial Times; Greater Manchester Police; J.P. Morgan; JLT; Lloyds Banking Group; Lloyds of London; LOCOG; NHS; Pfizer; RBS; Roche; Royal Mail; and Vodafone.

- Small Supplier of the Year, BCS UK IT Awards 2012
- Information Security Consultancy of the Year finalist 2013
- Specialist Business Continuity Company of the Year finalist 2012
- Channel Service Provider of the Year finalist 2013