The Need for DLP now

A Clearswift White Paper

Ben Rothke, CISSP CISA

DLP (data loss prevention) is a powerful technology that can be used to plug the holes in the data leakage dam that is affecting a myriad organizations worldwide.

While DLP is a broad set of features, of which would require a much longer document, Clearswift is happy to offer this white paper as an introduction to the topic of DLP, which is one of the most important and powerful tools in the information security industry toolkit.

Introduction

Anyone who has tried to replace a laser toner cartridge in corporate America knows the hassle. If you are lucky and there happens to be one in the supply closet, then signatures and a few keys later, the toner can be removed from the hallowed sanctum known as the office supply closet. As soon as the toner is taken, the door to the supply room is closed and secured.

Evidently, firms feel there is a significant risk to leaving expensive toner cartridges unsecured, in the hands of employees who may pinch them. For some reason, these firms think that their employees can't be trusted with office supplies, which require them to be stored in locked areas.

The truth is that a few bad apples can quickly steal thousands of dollars' worth of office supplies and companies understand that they must be secured.

For similar reasons, companies will place asset tags on every chair, table, laptop, microwave, etc. If these items are left unsecured and undocumented, the worst will likely happen.

But when it comes to the terabytes of confidential and proprietary data on corporate networks, companies often use kid gloves to secure the data. This begs the question, why are office supplies subject to a higher level of security than valuable data?

First, take a moment and think of the myriad different types of data in your organization that need information security controls. Without much effort, you should be able to think of 10 types in under a minute. Data types such as the following are just a few that can probably be found in your organization:

- Finance/spreadsheets
- M&A
- Social security numbers
- Sales forecasting data
- Legal
- Contact information
- HR
- Customer private data
- Client lists
- R&D
- Credit card numbers
- Marketing strategies

For many years, Sun Microsystems noted that the network is the computer. With that, the network is the data, as data is the gold for many organizations. Imagine if it occurred that 500 office chairs were stolen, with asset tags. Not really such a big deal, as they are insured.

But if a few gigabytes of data are lost from an organization, that can often mean significant impact and consequences, including:

- Class action lawsuit
- Public embarrassment
- Expense to recover
- Compliance violation (PCI DSS, Sarbanes-Oxley, GLBA, EURO-SOX, HIPAA/HITECH, UK Data Protection Act, California Senate Bill SB 1386, and many more)
- Loss of customer trust
- Diminished competitive advantage
- Negative branding
- Financial consequences

With that, many organizations are turning to a DLP solution to help them gain control over their seemingly uncontrolled data stores.

Why DLP?

There are a number of reasons why you want to consider a DLP solution. Gartner notes in their ***2010 Buyer's Guide to Content-Aware DLP*** that content-aware DLP solutions offer a significant array of capabilities to organizations. Their key findings are that DLP:

- Helps organizations to develop, educate and enforce effective business practices concerning the access, handling and transmission of sensitive data
- Provides reporting and workflow to support identity and access management (IAM), regulatory compliance initiatives, intellectual property protection and data policy compliance management

Those two areas alone are domains which nearly every company is struggling with. Other areas where DLP has shown to be of significant value is:

- Helps organizations to develop, educate and enforce effective business practices concerning the handling and transmission of sensitive data
- Dynamic application of policy based on the classification of content determined at the time of an operation
- Early detection – which equates to earlier mitigation

For many originations, they see DLP software and hardware as the answer to their information security problems. As I wrote in ***DLP – A Security Solution, Not a Security Savior*** http://www.btsecurethinking.com/2009/12/dlp-%E2%80%93-a-security-solution-not-a-security-savior/, over the last few years. DLP has achieved critical mass. So what exactly is this security remedy called *DLP*? DLP refers to a set of software and hardware solutions that identify monitor and protect data, mainly via content inspection and contextual security analysis.

One of the main benefits of a DLP solution is that it can detect and prevent the unauthorized use and transmission of confidential (as defined by the organization) information. DLP sounds like a slam-dunk security solution that every organization can use. Yet, as important as protecting data is, there's more to DLP than simply rolling out a DLP solution.

As noted in the beginning of this white paper, many organizations have much better knowledge of how many pencils they have in their supply closets, than how much data they have on their networks. DLP tools have data discovery capabilities and can scan data repositories and identify data. A decision can then be made if that data needs to be part of the protections scheme. The data can also be indexed as a way in which to start a process of determining who the data owner is.

When looking at a product's data discovery capabilities, one key area to look at is how many different data types it is able to identify. There are literally hundreds of different file formats in use; from Microsoft Office documents, multimedia, encrypted, zip, source code and many more.

How does data leak?

There are literally hundreds of ways (many of them in a manner many organizations can't fathom) in which data can leak. The following table lists but a few of them.

Careless mistakes, often when doing repetitive mundane tasks	Accidently sending email to a group rather than an individual	Fat finger	Disgruntled worker
Attaching the wrong file	Not being careful when rushing to a deadline	Hitting the "send" button too early	Malicious intent
Corporate espionage	Outsourcers, business partners, contractors, etc., with poor security practices	Poor firewall rules	Lost USB, memory card, DVD, etc.
Lost smart phones	Lost backup tapes	Data storage devices not properly sanitized	Phishing
Malware	Insecure transmission of personal identifiable and other restricted data		

Ultimately, think beyond DLP

It is important to note that when considering a DLP solution, many companies are far too myopic and think that DLP works in a vacuum. Pragmatic firms don't take such an approach and are sure to integrate DLP as part of their overall information security framework. They use DLP as one spoke in the larger information security wheel. By integrating DLP with other technologies and tools, including end-user awareness and training, DLP can be a very strong link in the information security chain.

A multi-step approach to DLP nirvana

So how does one take the theory of DLP and put it into practice? The following are a few steps to protect your data if you choose to deploy a DLP solution:

Step 1 – Level set

Realize that the DLP solution will not solve all of your data security issues, or mitigate its risks. DLP is but one part of a larger set of information security tools.

Step 2 – Know where your data is

Every year, public companies produce annual reports. In the balance sheet section, a company notes how much cash it has on hand. These companies are expected to accurately know this and other crucial financial details.

Yet how many of these companies can produce an annual report for their data? The following should be a simple question for an organization - *how much data resides on your networks? How much of that data is in long-term storage? Archived?* Perhaps 1 in 100 organizations can produce a reasonable answer regarding their data libraries.

The main point to consider is that there is far too much data in motion that companies are oblivious to. It is impossible to protect data an organization is unaware of, where it is stored, or where it is traversing.

Therefore, the first step in data protection is to identify where the corporate data is. By performing a data discovery project, you can find all the data on your network. Note though that this is a detailed endeavor. Expect it to take weeks, if not months, to locate, diagram and document all of your major data storage locations.

Step 3 – Data classification
Not all data is equal. You therefore need a project to classify data to understand what needs to be protected and why. Detail the risks to confidentiality and list common risk scenarios that may arise from inappropriate data leakage.

Think of security as insurance for your data and you only need to insure items of value. The first step in a DLP endeavor is to define what your valuable or sensitive data is.

How much of your data is secret? More than you think. According to Forrester http://www.rsa.com/products/DLP/ar/10844_5415_The_Value_of_Corporate_Secrets.pdf, secrets comprise two-thirds of the value of firms' information portfolios. Despite the increasing mandates enterprises face, custodial data assets aren't the most valuable assets in enterprise information portfolios. Proprietary knowledge and company secrets, by contrast, are twice as valuable as the custodial data. And as recent company attacks illustrate, secrets are targets for theft.

Step 4 – DLP strategy
A DLP solution can't be deployed in a vacuum. Organizations need to develop a formal DLP strategy that details specific business and technology needs and requirements. Many vendors position their DLP solutions differently, so it is important that you document their DLP solutions differently. And it's important that you document your requirements, and not simply map them to a vendor's DLP product offering.

A mistake that too many organizations make is that they get into the minutia of DLP, before developing their high-level DLP strategy. Start with the high-level objectives, and only then, go deep into the requirements.

When you do get to the requirements phase, realize that DLP is not strictly an IT solution. Organizations that have effectively deployed DLP did it with input from various entities in their origination.

While this is not a definitive list, ensure that at the very least, these departments are included:
- Business owners
- Legal
- IT audit
- Finance
- Internal audit
- Information security
- Technology operations

Note that the legal department is mentioned in the above list. For many IT professionals, working with legal is a foreign concept; but that should not be the case.
Given that DLP includes monitoring of proprietary and personal data, your corporate legal department needs to give their approval to the DLP project to ensure that the monitoring does not violate any laws or requirements. For those entities in the European Union, this can't be overemphasized as EU directive on data protection can quickly be violated with DLP if you are not careful.

As you develop your strategy, take into consideration that DLP is a long-term endeavor; read: years not months. DLP is undoubtedly not a "plug and play technology." From the time you start thinking of DLP, until the point that it is fully deployed and optimized, it requires time and dedication.

What do you do when the CIO wants the DLP working now, not next year?

Note that the previous paragraph uses years and DLP in the same sentence.

But what about those firms that don't want a full-blown enterprise DLP solution, but rather an interim solution to get up and running quickly? What do you do when the CIO balks about the extended time to production and insists that the DLP solution be up and running *this quarter*, not *next year.*

The Clearswift Secure Web and Email Gateway solutions are the answer for those that want the functionality of a DLP solution without the extensive time and effort required.

The Secure Gateways incorporate basic as well as advanced DLP capabilities natively. From built-in e-mail encryption, to anti-spam/anti-malware capabilities and more, the Gateways have been well-received by large clients, as well as small and midsize businesses (SMBs) with DLP deployments of fewer than 3,000 users.

The content security gateways can be quickly deployed to stop data leakage issues, and you can see the positive effect within hours.

Many organizations prefer this approach, as it can be executed rapidly, showing direct results.

For those organizations that want to take this approach, the first step would be to identify the data in transit *today* so that accidental leakage (such as inadvertent transmittal of confidential documents) can be detected by the email and web gateways and stopped.

In fact, Gartner writes in *2010 Content-Aware Data Loss Prevention FAQs* that firms should "develop a two- to three-year road map for the deployment of capabilities from initial monitoring only to active blocking". For those that don't want to wait for that two- to three-year road map to complete, Clearswift Secure Web Gateway is an effective answer.

Gartner also write that organizations can balance DLP feature richness against cost by knowing at the outset what the type and scale of the problem is that you are trying to solve. From this, you can then develop both the business requirements of the technology and the supporting processes, and also the tolerance for operational costs that are likely to be incurred post-deployment.

Finally, many DLP initiatives get immediately blackballed when organizations see the price tag, which is often exorbitant. In *Budgeting the Costs of Content-Aware DLP Solutions* - Gartner in the report notes that the average DLP full solution price ranges from $350,000 to $750,000. The Clearswift Secure Gateways are available at a fraction of that cost, for virtually any organization.

So why does it often take a year or more to fully deploy a DLP solution? This is due to the fact that yet another mistake organizations make is attempting to take their data anarchy, and have it managed by DLP. Making DLP work means taking small steps at first, and then expanding on that. Many IT projects fail due to too large of an initial scope. Therefore, start small, achieve initial victories and successes, and then expand.

At the commencement of the project, start with the most critical and sensitive data; such as confidential data, laptops and mobile devices. Once you get that in order, then move to other systems and those with less critical data. Most organizations have far too much data to try to secure with DLP in one fell swoop.

Since laptops were mentioned, note that while laptops and notebooks are great productivity tools, they are also one of the busiest avenues in the world of data leakage and data theft. Their level of convenience and accessibility are in direct response to the raw amount of data that can be compromised. In fact, a committed adversary will target the laptop of an executive or senior manager, given the treasure trove of data residing on it.

It is worth noting that this step does not have anything to do with vendors, as that is in step 5. Your *ready for primetime* DLP strategy should be complete before engaging with a DLP vendor.

Many DLP projects sometimes lose funding between the strategy stage and the deployment stage. In order to gain greater management support and business justification for the project, a good idea is to determine the number of DLP violations that have occurred in your organization. Showing management DLP metrics such as how many credit card or social security numbers were quarantined is a great way to demonstrate the value of DLP technology.

Finally, for those serious about a DLP strategy, the report from Gartner entitled ***Develop an Enterprise Strategy for Data Loss Prevention*** http://www.gartner.com/ DisplayDocument?id=1383713 can be used as a guide.

Step 5 – Product selection, testing and deployment

Once the requirements are documented, the next step is to create a pilot to test a number of DLP products. Ensure various use cases are tested to analyze the product in different scenarios. Have specific and objective metrics to ensure value controls are tested and that your outputs are accurate.

Conclusion

Overall, DLP is a great security technology, but it is not security "pixie dust" that can magically secure your network. The steps listed here are a few of the many that need to happen as part of a formal DLP rollout. By taking such a tactical approach to DLP, you can ensure that it really does prevent your data from being lost.

For many organizations, an enterprise-grade DLP solution may be overkill. Given the cost and effort required, many organizations are finding that it is better in the long run for them to start with the Clearswift Secure Gateway solution, given the short-term benefits and immediate interim success it can provide.

These organizations find that once they have the Secure Web and Email Gateway solutions fully deployed and working, it is only then that they decided to consider a full-blown DLP package.

About the author

Ben Rothke, CISSP, CISM, CISA is a New York City based senior security consultant with BT Professional Services and has over 15 years of industry experience in information systems security and privacy.

His areas of expertise are in risk management and mitigation, security and privacy regulatory issues, design & implementation of systems security, encryption, cryptography and security policy development, with a specialization in the financial services and aviation sectors.

Ben is the author of ***Computer Security - 20 Things Every Employee Should Know*** http://books.mcgraw-hill.com/getbook.php?isbn=0072262826&template=osborne (McGraw-Hill), and writes a monthly security book review for Security Management magazine. He is also a frequent speaker at industry conferences, such as CSI, RSA, and MISTI, holds numerous industry certifications, and is a member of ASIS, CSI, Society of Payment Security Professionals and InfraGard.

Unifying Information Security

CLEAR SWIFT

Clearswift Ltd
161 Gaither Drive
Suite 101
Mt. Laurel, NJ 08054
856-359-2360
www.clearswift.com