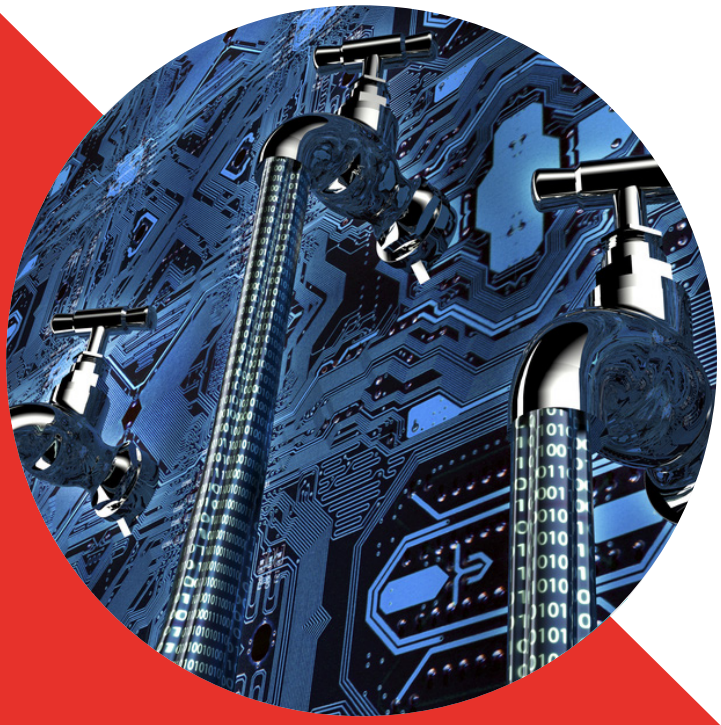
bsi.

...making excellence a habit.™

Data Loss Prevention

The essential elements for business critical information protection

A whitepaper



Executive summary

It should come as no surprise that as mass storage becomes increasingly cheaper and more readily available to organizations we hear more and more about data breaches, large and small. The advent of "Big Data" and the realisation that it can be utilised to drive business initiatives and objectives means that data is, more than ever, a critical business process.

A consequence of this is that if organizations are storing more and more information, the risk that this information may be misused or leaked also grows substantially.

Introduction

In spite of the fact data is arguably the most valuable and critical asset many organizations have, it is often neglected when it comes to ensuring that it is sufficiently protected

The lack of a Data Loss Prevention (DLP) policy could be costly to an organization who suffers a breach. Failure to adhere to regulations and standards such as the Data Protection Act or PCI DSS can incur large financial penalties for organizations that have a lax approach to the security of their sensitive data.

On top of this, a serious data breach can cause negative publicity in the press leading to a loss of customer confidence in the organization and the services it provides.

Some recent examples of large data breaches in terms of records stolen were[1];

- Mossack Fonseca, 11.5m
- Philippines' Commission on Elections, 55m
- Clinton Campaign, 5m
- Ashley Madison, 37m
- Ebay, 145m
- JP Morgan Chase, 76m

Organizations are looking at ways in which they can mitigate some of the common threats to their sensitive data, implementing a DLP programme is a good starting point. That being said, before a DLP programme can be put in place, organizations need to have a good understanding of the following:

- What sensitive data do you have?
- Where is your sensitive data stored?
- How is your sensitive data transmitted?
- What is your sensitive data used for?

This insight paper aims to discuss the factors that need to be considered to implement a robust Data Loss Prevention (DLP) programme and ensure your organization's sensitive data is not disclosed to the public domain in an unauthorized fashion.

1 http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Know your data

What data do you have?

A data classification policy is an important requirement here. Labels such as "Confidential", "Internal" and "Public" are common labels that many organizations use when trying to understand the types of data they have and how that data can then be controlled.

Sensitive data can take many forms, but for the purpose of this paper we have broken it down into three particular types as an example;

Confidential data	Internal data	Public data
• Intellectual property	• Meeting minutes	• Brochures
• Financial reports	• Internal memos	• Event information
• Customer lists	• Templates	• Public staff profiles
• Legal documentation	• Policies and procedures	
• Credit card information		
• Contract terms and conditions		
• PII		

Where is your sensitive data stored?

Data at rest can be defined as any information that resides in persistent disk storage such as a hard disk, tape or flash storage.

The portability of such devices and the amount of information that can be stored on such small devices can lead to data being easily lost or stolen. As such, it is important for organizations to protect sensitive data that is held in persistent storage using suitable encryption such as AES256 and access control mechanisms.

How is your sensitive data transmitted?

Data in transit can be defined as any information that is transferred over a public/private network.

Again, not all data will require protection e.g. reading a news site can be completed over insecure HTTP as there is no risk involved. However, what if we need to enter a password for online banking, enter credit card details to make a purchase or send an important legal contract?

In these cases we need protocols that can encrypt data while it moves between networks over the internet so someone snooping on the "wire" cannot read the data in plain text. Common examples of secure protocols include:

- Web - HTTPS
- File Transfer - SFTP
- Shell Access - SSH

Methods of Data Loss

While there are many methods whereby data can be leaked from an organization, some of the more common ones are as follows:

Inefficient hardware decommissioning

Organizations have to deal with obsolete hardware such as PCs, laptops, phones etc. on an annual basis.

However, many are unaware of the sensitive information they may be releasing by not having an appropriate process in place for disposing of this data correctly.

Organizations should have a data destruction policy to ensure that before hardware is recycled or sold that it is properly wiped using professional data wiping tools.

Human error / accidental publication

According to figures obtained by Egress Software Technologies via a Freedom of Information (FOI) request, human error was the cause of almost two-thirds of all reported incidents to the Information Commissioner's Office (ICO) in the UK.

If you consider how easy it is for a naive user to send a sensitive piece of information by replying to a phishing scam or accidentally sending an email to the wrong person due to the email client's autocomplete feature being switched on, it's easy to see why there were so many incidents reported for this reason.

Configuration/code errors

Configuration/code errors in online applications can unintentionally lead to sensitive data disclosure. Consider for example a login page to a website that is vulnerable to SQL injection. A well-crafted SQL command could give an attacker a database dump of the user's table via the application which would likely contain information that

could be considered personally identifiable.

Cybercrime

Cybercrime has become big business over recent years. The ease at which criminals can orchestrate phishing attacks aimed at tricking unsuspecting users to reveal their bank details, or launch a ransomware attack on an individual or organization rendering potentially critical files or other data useless until the victim makes a payment to get it back.

Couple this with jurisdictional boundaries and it means that the criminal has very little chance of ever getting caught save for cross border cooperation from police forces means that cybercrime is more attractive than traditional criminality.

Malicious insiders

The threat of malicious insiders is all too real as UK communications regulator Ofcom found after a former employee stole and passed on commercially sensitive information to his new employer.

Organizations have for quite some time attempted to manage the removal of data from their premises with the help of firewalls, proxies, email filters and end-point protection to block the use of USB ports. While these methods of protection will certainly help organizations limit the amount of data that leaves their organizations, the threat of shadow IT looms large in many organizations. Shadow IT is a term that is often used to describe the usage of cloud services within an organization but without explicit organizational approval.

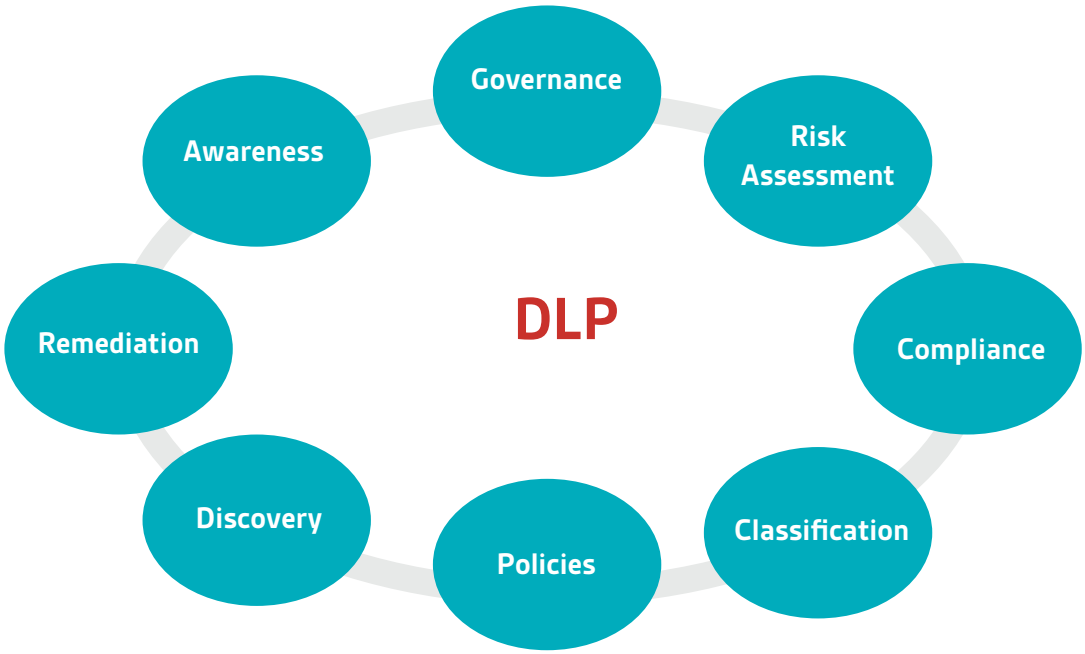
DLP enforcement

In order to properly enforce a DLP programme, we need to consider what elements allow us to do this.

Below are some of the elements that need to be considered when deploying such a programme[1]:

- **Data governance –** Monitoring the flow and storage of data in your environment based on its classification which will be based on confidentiality, integrity and availability
- **Risk assessment –** Identify threats, vulnerabilities and impacts to the business and prioritize a list of actions to reduce the risks
- **Compliance –** Understanding local and international regulations regarding the types of sensitive data the business has and how it must be used
- **Classification –** Classify business data according to its value to the business and protect data in accordance to its classification
- **Policies –** Flexibility in policy should be available to allow the business to easily adapt when industry standards or business objectives change
- **Discovery –** Finding sensitive data in areas you don't expect it by identifying broken processes and data drift
- **Remediation –** Identification of root causes of data loss incidents and mitigate using incident response procedures
- **Awareness –** A lack of awareness is often the weakest link in the chain when it comes to data loss. Ensure that employee education and awareness is at the forefront of your DLP programme

1 http://www.slideshare.net/sarfarazchougule/isaca-webinardlpaug82013final-v128451



Cybersecurity and Information Resilience services

Our Cybersecurity and Information Resilience services enable organizations to secure information from cyber-threats, strengthening their information governance and in turn assuring resilience, mitigating risk whilst safeguarding them against vulnerabilities in their critical infrastructure.

We can help organizations solve their information challenges through a combination of:

Consulting

Cybersecurity and information resilience strategy, security testing, and specialist support

Training

Specialist training to support personal development

Research

Commercial research and horizon scanning projects

Technical solutions

Managed cloud solutions to support your organization

Our expertise is supported by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CYBER ESSENTIALS

CSA cloud security alliance℠

bsi.

Find out more

Call UK: +44 345 222 1711

Call IE: +353 1 210 1711

Visit: bsigroup.com