

Data Leakage

In a simplified view, Internet content security is about keeping the 'bad stuff' on the outside of your company and keeping the 'good stuff' on the inside. Data leakage is concerned with keeping the 'good stuff' on the inside - securing and managing access to your intellectual property or sensitive information.

There are two primary data leakage elements to be concerned with: 1) what data you want to protect and 2) what constitutes a leak.

Data, or the 'good stuff', covers a range of corporate assets such as:

- Intellectual Property (IP) – this can be company secrets, product designs, mathematical formulas, research papers, source code, patents, schematics, recipes, proposals, reports, etc.
- Commercially Sensitive Information – this can be financial reports, employee payroll documents, contracts, strategic business plans, acquisition targets, product and marketing launch plans, budgets, customer databases etc.
- Confidential Information – this can be patient health records, customer financial information, legal contracts, employee resumes, confidential supplier information, pre-release reports, survey data, etc.

Leakage covers possible methods by which this data could be accidentally distributed or stolen. This could include:

- Emailing data to the wrong recipient or attaching the wrong file to an email.
- Employees deliberately emailing information to competitors.
- Disclosure of confidential information to the media.
- Emailing confidential information in an un-encrypted format.
- Internal staff using webmail or email to discuss confidential subjects with external parties.

How Common is Data Leakage?

It is very common. The issue with data leakage is not so much about how common it is, but its severity, the nature of the data and how it has been leaked.

In the 2006 CSI/FBI Computer Crime and Security Survey 68% of respondents reported they had internal security breaches. These breaches included loss of information and Intellectual Property theft. 39% of respondents reported more than 20% such incidents came from inside their organizations.

A recent IDC study found that 84% of all data leakage was generated internally, by employees, rather than being stolen by hackers or virus infection. Another study in the UK by Forrester Consulting found that more than a third of UK companies had suffered a leak of sensitive information in the previous 12 months.

The newspapers are full of high-profile examples where companies have been exposed for the leaking of confidential information. For example, Apple suffered significant embarrassment after two employees revealed secret new product information on their personal blog sites.

A statistician employed by the Palm Beach County, Fla., health department inadvertently emailed his colleagues the names of 6,600 locals known to be infected with HIV and AIDS. This was a serious breach of the Federal laws on handling patient information and ensuring patient privacy.

What are the Costs of Data Leakage?

There are many costs associated with data leakage. These can be anything from public embarrassment, to financial loss, reduced stock equity, loss of competitive advantage or even criminal investigation and prosecution.

In the case of Apple, where their employees revealed product information before it was released, the company's share price plummeted after the leak

A recent IDC study found that 84% of all data leakage was generated internally, by employees, rather than being stolen by hackers or virus infection.

Data Leakage

was revealed. The company was forced to fire the employees involved, resulting in embarrassment, lost productivity and legal costs.

In the incident with Palm Beach health department, the apparent violation of the Healthcare Insurance Portability and Accountability Act (HIPAA) could result in prosecution, not to mention the loss of patient confidence in the department's ability to protect their private information and identities.

The financial costs of data leakage are very hard to quantify. Consider a hypothetical scenario, where a company's new MP3 player designs and specifications are leaked to a competitor before it is launched. This breach in security could undermine the company's entire business and lose millions of dollars in revenue. In addition, this could result in embarrassment, loss of professional reputation and give a significant boost in the competitor's market share.

The Marshal Solution for Data Leakage

Marshal provides a range of tools which can be applied to protect against data leakage. These tools work in a policy-based framework to enforce security and prevent attempts to leak information. Marshal products can be adapted to identify data which is specific to your business and manage this data according to your unique policy requirements.

These tools include:

- **Lexical Analysis** – the ability to control email based on the presence of certain keywords and phrases. Marshal can identify passages of confidential text either in the message body or buried within an attachment. With respect to web browsing, Marshal can detect attempts to upload confidential text to websites. For example, attempts to use webmail (like Hotmail or Gmail) to send confidential information.
- **User Management** – the ability to restrict rights for distributing confidential information to authorized persons only. This could mean that financial reports can only be emailed externally by the CFO, or product designs can only be emailed by members of the Executive Team. If another user tries to email a confidential document to an external email address, the message can be blocked and a notification can be sent to your security officer, a supervisor or other appropriate email address. User Management also allows you to restrict the ability to upload certain attachment types to websites. This can prevent unauthorized users from uploading Excel spreadsheets or CAD files to the Internet without permission.
- **File Management** – Marshal products allow you to control over 175 different file types. This control can encompass file type, who the sender and recipient are, the presence of key words and other elements. Marshal products identify files by the characteristic code

signatures of the file type, rather than relying on the name of the file, or the file extension for identification. Using the file extension for identification is an unreliable method used by some competitors that can easily be circumvented by a user by simply renaming the file extension. There are a wide range of file management options available to protect against data leakage. For instance:

- **Embedded signatures** – you can embed code words or alphanumeric markers in confidential documents such as "CODEWORD123," for example. These markers can be made invisible to the reader by making the font white, but MailMarshal can still detect the code word and block any document featuring the code word being sent by an unauthorized user.
- **Fingerprinting** – you can save a copy of any confidential document or file into MailMarshal's "fingerprint" folder. Any email with an attached copy of a file saved in the "fingerprint" folder can then be detected. Any attempt to email or access a restricted file can be blocked and reported.
- **File Type** – specific file types such as CAD, Microsoft Project plans or password protected zip files can be automatically restricted to authorized users only. This prevents general users from emailing files that are not intrinsically related to their job function. MailMarshal can also detect files embedded inside of other files, such as a Word file inside of an Excel

Marshal provides a range of tools which can be applied to protect against data leakage. These tools work in a policy-based framework to enforce security and prevent attempts to leak information.

Data Leakage

spreadsheet or a database file inside of a zip compressed archive file.

- Recipient Blacklisting – this allows you to define specific email addresses or domains that you wish to control email communication to. For example, with MailMarshal, you can set a wildcard rule that states “block all emails to *@mycompetitor.com unless from the Authorized Users group.” This rule would block any email going to your competitor’s email domain, coming from an unauthorized email address.

- Webmail Blocking – WebMarshal provides the capability to completely block access to blacklisted webmail accounts. However, if you wish to allow users restricted access to webmail for limited personal use, you can block users from uploading certain file types or even adding confidential text.

- Anti-virus & Anti-spyware – Marshal products support the use of many popular third-party anti-virus and anti-spyware scanners. These block Trojan worms and malicious spyware entering

your organization via email or the Internet, at the gateway. Viruses and spyware are the most common tools employed by hackers bent on gaining access to confidential information within your organization. By employing a layered approach to virus and spyware protection at the server level, Marshal products also help to prevent data leakage by external parties.

Why Marshal?

Today, Marshal is the solution of choice for more than 18,000 organizations worldwide, protecting in excess of 7 million users.

- 10 years experience in total content security solutions
- Solutions for companies from 10 to 100,000+ users
- Global 24/7 support team
- TRACE team insights and updates
- More than 40% of the Global Fortune 500 companies rely on Marshal solutions for email and Internet security needs
- More than 60% of the European Fortune Top 50 Companies use Marshal
- 45% of the USA’s Fortune Top 170 Companies use Marshal
- 40% of Asia’s Fortune Top 50 Companies use Marshal



Marshal’s Worldwide and EMEA HQ
Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Email: emea.sales@marshal.com

Americas
Marshal, Inc.
5909 Peachtree-Dunwoody Rd
Suite 770
Atlanta
GA 30328
USA

Phone: +1 404 564 5800
Fax: +1 404 564 5801

Email: americas.sales@marshal.com
info@marshal.com | www.marshal.com

Asia-Pacific
Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email: apac.sales@marshal.com