WHY DLPS ARE COMMONLY KNOWN AS "DISASTROUSLY LONG PROJECTS"?

The effectiveness of DLP is based on the information it monitors. Unfortunately this is an extremely tedious task because DLP systems are essentially offshoots of anti-virus solutions. They are designed for use by IT staff and follow the anti-virus approach of centralised rule definition and incident monitoring. This approach results in the following problems:

1. **Gathering real sensitive information requires too much effort.**
   DLP systems apply security centrally; this requires IT security professionals to gather all the important sensitive information and secure it. This is an almost impossible task to achieve as information is produced within each department on a daily basis and end-users are too busy to manually categorise this information and pass it to the IT administrators. As such information that is being monitored is mostly outdated and in worst case scenario never monitored leaving DLP systems largely ineffective.

   a. **What is required is a mechanism where information is automatically secured at the source as it is being produced without involving IT or even the end-user**
   b. **What is required is an automated way for end-users to classify information and define what is important as it is being produced.**

2. **Lack of sharing of highly sensitive information with the IT staff**
   Real sensitive information such as financial records or board papers are never shared with IT staff as they are considered highly confidential and can change the nature of the entire business. As they can't be shared with IT staff they never get protected leaving the most important information always unprotected.

   a. **What is required is a mechanism where information owners can define restrictions on who can access the said information without involving IT staff. Further, the monitoring of this information is also limited to the information owners and not the IT department.**

3. **(Over blocking verses ease of Use) Changing sensitivity nature of information.**
   Information that is classified as sensitive can change in sensitivity level once the information has been made public or if more people are required to have access to this information. Again this becomes a major challenge for IT staff as they have to constantly update the restriction imposed on the information. For example tender specs are considered sensitive as long as they are not published and are blocked from being sent out. However once the tender is opened the procurement department can send them out to interested vendors. Any delay in allowing the procurement department from sending this information becomes an issue for IT Security who get blamed for stopping people from doing their business.

a. **What is required is a mechanism where end-users can take the responsibility to define who can access the information and who cannot. An override mechanism where they can override a defined restriction by giving a valid reason.**

1 THE SOLUTION → E-SAFE COMPLIANCE MANAGING SECURITY THE SMART WAY

e-Safe Compliance is an enterprise system for ensuring responsible, productive and secure use of IT resources. In addition to its productivity and auditing functionalities, e-Safe Compliance prevents data leaks but does so in a **smart** way and so avoids the problems listed above. The fundamental difference between e-Safe Compliance and DLP systems is that it treats data leakage as a business problem that needs to be tackled at an **operational level, rather than an IT problem**.

1.1 SECURES INFORMATION AT ITS SOURCE AS IT GETS CREATED, ENSURING INFORMATION IS PROTECTED ALL THE TIME.

e-Safe Compliance secures the information at its source by encrypting sensitive documents using **universal encryption.** Documents encrypted using universal encryption can only be opened on devices having e-Safe agent installed, along with the relevant user credentials, and are tracked throughout their lifecycle from creation to deletion using e-Safe. As such, if the users decide to send the documents to a 3rd party, or decide to copy it, they need the e-Safe agent to open them.

1.2 MONINTORING REAL SENSITIVE INFORMATION USING DECENTRALISED DLP RULE CREATION

e-Safe compliance offers both centralized rule creation as well as decentralized rule creation. Information owners using the **information tagging utility** can categorize a large amount of information themselves without involving the central administrators and can create DLP rules. Further, the information owners also receive reports for the information they have defined. This ensures that users who have defined information monitor the usage of that information and can detect any misuse by their staff.

1.3 PROTECTING HIGHLY SENSITIVE INFORMATION USING DOCUMENT RIGHTS MANAGEMENT

e-Safe Compliance solves the problem of classifying highly sensitive information by providing a built-in document rights management module while allows top management to define document sensitivity using mouse right click options. The following options are available:

1. Define the classification of sensitive documents as being
    a. Secret
    b. Confidential
    c. Office document

2. Define who can have access to the said information
3. Define the usage restriction on the information such as cut/copy/paste/print etc.

More importantly information owners receive usage reports of that particular information. This ensures that, if there is any misuse, the information owner, who understands the potential impact of the violation, is in a position to take action.

1.4 SOLUTION TO OVERBLOCKING VIA TRUST BUT VERIFY PHILOSOPHY

Normal DLP systems have two modes of operation:

i) Block sensitive document usage/transfer etc
ii) Allow document usage but monitor.

Restricting document usage prevents users from doing their job, whilst just monitoring document usage results in the reviewing of a large number of incidents. e-Safe Compliance introduces a third way – **"allow users to remove restrictions but require them to provide a reason for doing so".** By allowing authorised users to override restrictions by giving a reason means the users are no longer prevented from doing their job. Further the fact that they have to give a reason ensures that users are aware of the importance of the information and will be held responsible for any misuse. This automatically ensures security of information.