AUJAS
Managing Information Risk

MAKING DATA PROTECTION MORE EFFECTIVE

A step beyond technology implementation

By Jayesh Kamat & Chandra Prakash

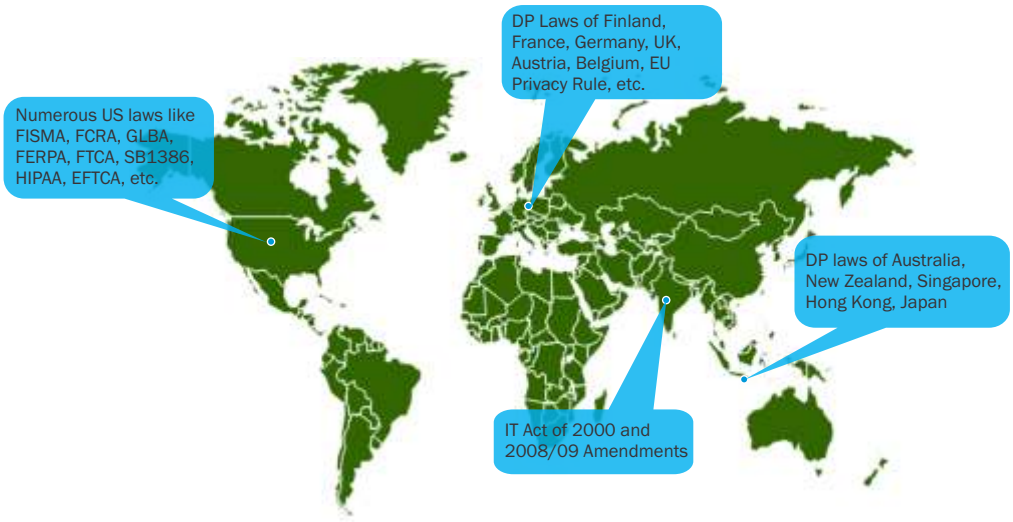
Introduction

Much has been written about data loss prevention ecosystem, including tools and technologies, end points security and the need for data classification. There are numerous statistics around data leakage as a credible threat to business and how many CIO/CISOs are sleepless across the world worrying about data security.

Now, there is enough awareness across the world around the consequences of data loss or leakage and more so in organizations that deal with personal (privacy), financial, and health care data either due to direct compliance requirement or due to contractual requirements of clients.

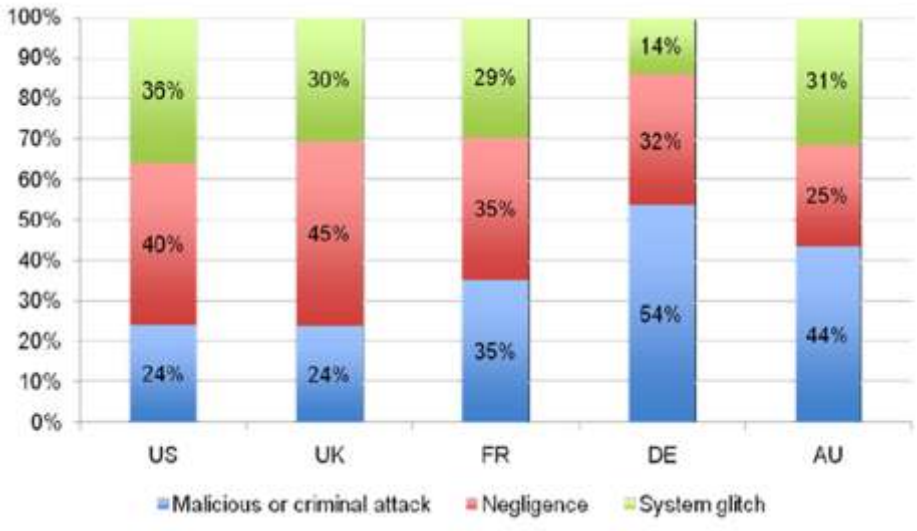
Growing Importance of Data Protection

Worldwide Data Protection is no longer optional, it has become mandatory with many laws being passed by most countries including India. With most businesses dealing with multiple countries it is essential for the continuity of business to protect data in accordance to the regulations.



> "The primary ownership and accountability of the data lies with the business while IT is the custodian tasked with managing and protecting data."

The figure below shows Ponemon institute 2010 research on cost of data breach across some of the developed nations. It can be seen that 60-70% of the breaches are due to malicious attackers or simply negligence. These statics make a compelling case for implementation of a data loss prevention tool.



Source: 2010 Ponemon Institute : Global Cost of Data Breach

Besides selecting a right DLP tool, there is also sufficient literature around best strategies for implementation of the tool, data discovery and finally policy implementation based on data discovered, etc. and like everything else this causes more confusion then it clears

Tool vs. Process

Thanks to increased regulatory requirements and competitive forces, most organizations have either some data loss prevention tool implemented or are contemplating the same. With most end point security technology companies buying and consolidating the specialist DLP vendors and integrating the technology into the end point security suites, DLP tools have the potential to reach every desktop.

The DLP technology is designed to address both, data in motion and data at rest and it relies on data discovery scanners to identify potentially classified/critical information that needs to be protected. Once identified policy templates are assigned to either block or monitor data from a central console based on data classification and its corresponding policy.

Seldom does any tool solve business problem, it is the people and process part along with technology that makes the difference in effectiveness and efficiency of the tool to meet business objective.

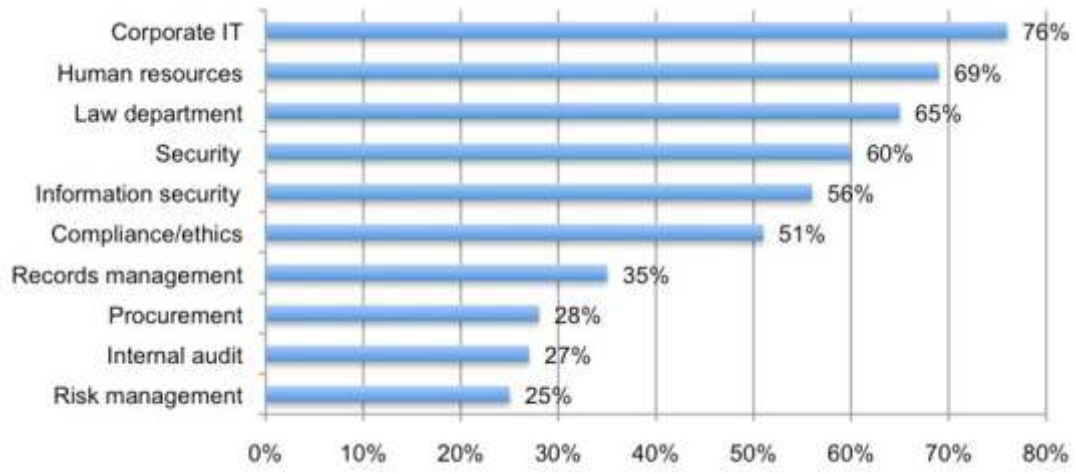
Depending on pure technology to scan, classify and configured rules is that, it fails to consider business either completely or at least partially. The primary ownership and accountability of the data lies with the business while IT is the custodian tasked with managing and protecting data. If the business fails to identify all pieces of data or fails to classify the data appropriately no amount of DLP security employed by the IT will protect data. This '**disconnect**' between IT leading the DLP implementation and business owning the data decreases the efficacy of data protections within the organization.

This usually manifests in large number of DLP false positive incidents, to which IT administrators have to address quickly to avoid business being affected. Usually they operate DLP tool in '**observe**' mode to avoid the back log that the false positives cause making the tool ineffective.

> "The principles of data governance, data classification and the DLP tool need to work as one solution, to effectively protect data in an organization."

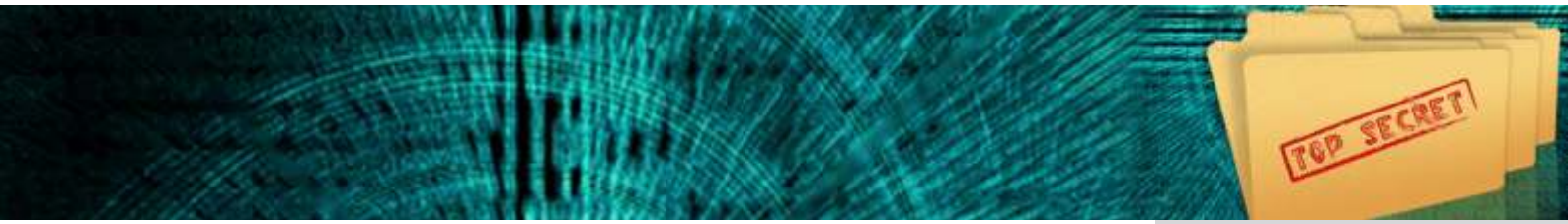
The following figure shows Ponemon research paper on business case for data protection showing most respondents feeling collaborating with IT is most important (76%) for data protection.

What business functions need to collaborate to achieve data protection goals



Source: 2010 Ponemon Institute : Business Case for Data Protection

AUJAS
Managing Information Risk



What is needed?

A more holistic approach is needed for protecting data that goes beyond the tool and addresses data at its source, the business. The principles of data governance, data classification and the DLP tool need to work as one solution, to effectively protect data in an organization.

Approach

1. Develop a Strategy:- This will help develop an organization wide data protection strategy
2. Develop a data classification policy and a program- Individual business processes should identify all forms of data, its classification and its authorized movement and document the same.
3. Governance Program- Fix up accountability, roles & responsibilities for data protection and data ownership.
4. Create and ensure awareness and training for business users- To ensure that the data protection remains a strong focus within the organization the council should ensure users are made aware of their roles & responsibilities around data protection.

How can we help?

Aujas is a global IRM (Information Risk Management) services company that specializes in advising its customers in information risk management including data protection. We at Aujas believe that while tools are important to enforce and automate processes it is the processes that need to be addressed for overall improvement.

Aujas data protection service focuses on assisting organizations extract maximum value out of their investment in security technology and solutions. We build the governance framework, data protection strategy, data protection program and assist organizations with identifying and documenting data flow analysis to identify data movement within and between processes, the forms data takes and the user awareness training. This data flow analysis translates into effective DLP policies while the governance framework and strategy translates into continuous data protection for the organization.

"Aujas data protection service focuses on assisting organizations extract maximum value out of their investment in security technology and solutions."

Case Study

Client's Profile:
A leading financial conglomerate having consumer finance, general insurance, life insurance, mutual fund companies under its umbrella

Client's Requirement:

The implemented leading DLP and DRM solutions were ineffective as the user community unaware of:

- The critical data movement and storage within their processes
- Usage of DRM to protect critical data

In addition, the IS team was struggling

- To identify the sensitive documents and fingerprint them
- Sheer number of DLP Incidents and large numbers of false positives

Aujas Approach:

Data flow analysis across the business processes was conducted to identify the critical data and its path within the processes ,across departments and with third parties

Based on the analysis the sensitive documents:

- Were identified for fingerprinting
- Were classified for DRM with appropriate distribution rights

In addition, training were conducted on securing the critical documents using DRM in the context of each department's critical documents

Value Proposition

- User community more aware about critical data and how to classify and protect the same
- IT Productivity augmented through enhanced use of DLP/DRM tools
- Effective usage of DLP & DRM solution

About the Authors

Jayesh Kamat

Jayesh has over 13 years of experience in information technology and information security arenas, his experience spans across the areas of IT and IS strategic consulting risk and compliance management and assisting customers with IS governance, certification readiness, IT/IS Risk Management, security technologies, tools and security architecture design. He has worked with clients from various industry verticals such as Banking & Financial Services, Insurance, Life Sciences, Oil & Gas, Media and Technology.

Jayesh currently heads the information Risk Advisory Practice at Aujas. Prior to Aujas he has worked with Deloitte & Touche AERS IPL, Microland Ltd in the information security space.

Email: jayesh.kamat@aujas.com

Chandra Prakash

Chandra Prakash is seasoned business and technology professional with over 11 years of experience, specializing in the area of Information Risk Management. He has served several fortune 100 clients in the BFSI and TMT industry in managing their risk and compliance program in a cost efficient manner. Besides strategic risk management projects he has executed several information security projects like implementation of ISO 27001 & BS 25999, KRI dashboard, automation of RCSA and creation of operational risk management framework and more.

Chandra Prakash currently co-heads the information Risk Advisory Practice at Aujas. Prior to Aujas, he has worked with Deloitte & Touche AERS IPL, Nokia and Delphi Computech.

Email: chandra.prakash@aujas.com

About Aujas

Aujas is a Global Information Risk Management (IRM) services company. We provide management consulting and technology lifecycle services in the area of information risk. Our objective is to offer effective IRM services on business and technical issues.

Our Service portfolio Includes Information Risk advisory services, Secure Development Lifecycle services, Identity and Access Management services, Managed Information Risk services, Vulnerability Management services and Converged Security services.

For more information, write to **contact@aujas.com**

Asia:

No. 4025/26, 2nd Floor, K.R. Road,
Jayanagar, 7th Block West,
Bangalore – 560 082
Phone : +91 80 40528527

Americas:

2500 Plaza 5, Ste # 2536
Harborside Financial Center
Jersey City, NJ 07311. USA.
Phone: +1 201 633 4745

Europe:

The Orchard,
2 Yew Tree Lane,
Tettenhall,
UK
Phone: +44-7989-609077

Karlsruher Strasse 87A,
75179 Pforzheim,
Germany
Phone : +49 (0) 7231 1571 70

Middle East:

Executive Suite: Q1-1-081,
P.O. Box No. 122376,
Saif Zone, Sharjah,
UAE
Phone : +97 1566940614

AUJAS
MANAGING INFORMATION RISK

www.aujas.com