Case Study | Information Risk Advisory Services

AUJAS
MANAGING INFORMATION RISK

Turning a Bank's DLP from Liability into an Asset

Overview

Aujas leveraged its data flow analysis and data protection governance framework to turn around a ineffective DLP implementation

Aujas Solution

- ✓ Design a data protection governance & incident management framework
- ✓ Conduct a comprehensive data flow assessment
- ✓ Identify data classifications
- ✓ Create a web-based repository for sensitive data
- ✓ Align the rule base to business data flow
- ✓ Use a PMO-based approach to ensure the engagement's success

Introduction

Our client is a large international bank with a global network of branches, remittance centers, and ATM kiosks. Over the past three decades, the bank has expanded and now provides a full range of banking products and services to its retail and corporate customers. It also offers home financing and heavy equipment leasing services.

Considered a technology leader, the bank is known for its award-winning customer center, and online and mobile banking services. In keeping with its reputation as a leader, the bank implemented a Data Loss Prevention (DLP) technology to help it comply with regulatory requirements and security standards.

The Business Need

The bank's DLP solution was not aligned with the business usage of sensitive data, limiting its effectiveness. An inconsistent incident management process also hampered implementation. In addition, the bank knew it wanted to establish a database of sensitive data that could be updated by departmental representatives. With these needs in mind, the primary challenges for this engagement included:

1. *Designing the data protection governance and data leakage incident management framework* – For consistent data protection, a framework had to be created for managing the DLP technology, rule design, and deployment. The incident management framework also had to be redesigned so that the bank could manage the consequences of data leakage more effectively and consistently.

2. *Assessing more than 25 key business functions* – Sensitive data within each function had to be recorded along with classification levels and data flow. The goal was to identify all sensitive data and not just customer credit card numbers.

3. *Addressing structured as well as unstructured data* – One of the notable challenges for this project was assessing both structured and unstructured data for the bank's key applications and databases.

4. *Creating a data repository for sensitive information* – A point-in-time exercise would not have been effective because the bank's data and business systems changed often. A bespoke application was therefore needed to allow bank representatives to maintain and periodically update a repository of sensitive information within their individual functions. The Data Repository could also be accessed to help create DLP rules.

5. *Creating and testing DLP rules*– Once the database was populated, the rules had to be designed to protect sensitive data. A combination of keywords, RegEx, and fingerprinting techniques needed to be leveraged. The rules had to be tested and made live.

About Aujas

IDG Ventures

- Aujas is an IDG Ventures company
- IDG Ventures is a $ 3 Billion Group

- Offices in USA, India and UAE
- More than 300 clients and 500 projects across 23 countries
- Over 170 professionals

Practices:

- Information Risk Advisory Services
- Security Intelligence
- Identity and Access Management
- Application Security

Aujas Solution

Aujas conducted this engagement in four phases: Framework Design, Data Flow Assessment, Data Repository Tool Rollout, and Rule Design.

Framework Design

- Created **a framework** for data protection governance and data leakage incident management to ensure ongoing **effective and consistent DLP management.** The framework was finalized after multiple rounds of discussions with stakeholders.
- Ensured the framework consisted of **roles and responsibilities, processes, teams responsibilities, communication plans, reporting and measurement metrics**.
- Presented the framework to the bank stakeholders for final approval and implementation.

Data Flow Assessment Phase

- Identified business representatives, and scheduled interviews with them.
- **Conducted workshops** to orient business representatives to the need for and nature of the assessment.
- Interviewed business representatives to **capture business sensitive data along with the classification levels, compliance requirements ,and flow of data** across functions.

Data Repository Tool Rollout

- Designed the **workflow for the data repository** tool.
- Developed the Data Repository tool.
- Deployed **the Data Repository tool, loaded the sensitive document details** captured during the assessment.
- Configured the **approvers and reminder notifications**.
- **Trained business representatives** on its usage.

Rule Design

- **Assessed sensitive data** to identify the appropriate means of identification (**keywords, RegEx, fingerprint**).
- Created **rules based on the data flow** (approved senders, methods, etc.).
- Tested the **rules in monitoring mode**.
- Moved rules into production and the **low false positive ones into blocking mode**..

Key achievements:

- Assisted the bank to establish a **framework for on going data protection**
- Helped the bank to **identify data that is relevant to business**
- Enabled the bank to maintain an **updated repository of sensitive and regulated data**
- **Built awareness of data protection** in the business functions
- Built **rules for protecting what matters** and **confidently implemented** them

Benefits and Learning

The bank was able to implement business aligned rules and was able to **move rules from monitoring to blocking mode with confidence that data were protected**. The bank's IT team was also able to showcase and manage how effectively they could **detect and manage data leakage incidents using the newly created governance framework**.

The **business functions were able to realize and appreciate** the nature of data they were working with, understand **classification levels** and the **need to protect** the data.

The bank now had at its disposal a **lifecycle approach, using the data repository to manage data protection rather than relying on a one-time exercise.**

About Aujas

IDG Ventures

- Aujas is an IDG Ventures company
- IDG Ventures is a $ 3 Billion Group

- Offices in USA, India and UAE
- More than 300 clients and 500 projects across 23 countries
- Over 170 professionals

Practices:

- Information Risk Advisory Services
- Security Intelligence
- Identity and Access Management
- Application Security