

searchSecurity.in

Reliance Capital's DRM and DLP team up for data protection

By Dhvani Pandya, Principal Correspondent, SearchSecurity.in

Today, Indian organizations are fairly aware of external information security threats, and have sufficient controls in place to deal with such issues. However, the scenario is not so rosy when it comes to the now quite common issue of insider threats. This is why Reliance Capital Ltd.'s data protection project deserves special mention.

Reliance Capital (part of the Reliance Anil Dhirubhai Ambani Group) recently executed a data protection project across its five group companies. One of India's fastest-growing financial service companies, the organization has five key lines of business (LOB): mutual funds, life insurance, general insurance, consumer finance and broking and distribution.

Formed three years back, Reliance Capital Ltd. initially set up its basic security hygiene with solutions like firewalls, an intrusion prevention system and gateway antivirus/spam controls. However, Reliance Capital soon realized the need for control over data moving across systems, geographies and group companies. "Data sent to third parties for processing and other outsourced activities are usually insecure and provide avenues for misuse. The issue is about whether enterprises know the valid nature of these data transfers and whether these are malicious in nature," observes Murli Nambiar, the vice president and head of information security for Reliance Capital.

To answer these critical questions, Reliance Capital drew up a "Data Shield" project. It consisted of three components: data flow analysis, a document rights management (DRM) rollout and a data loss prevention (DLP) implementation.

Identification of critical data

Through data flow analysis, we identified aspects such as who generates the data, where it is kept, where it was passed on, etc. This helped us identify the system's leak points.

Murli Nambiar
Vice president and
head of
information
security
Reliance
Capital

Data flow analysis was the first and foremost phase of the data protection project, which began in September 2008. Reliance Capital started to study the data flow of core applications in each LOB. The company initially involved Ernst & Young as a project consultant for this analysis. "Through this data flow analysis, we were able to identify aspects such as who generates the data, where it is kept, where it was passed on, etc. Tracing the entire data flow helped us identify the system's leak points," Nambiar says.

Although Reliance Capital already had an information security policy, after data flow analysis the decision was made to have a specific data confidentiality policy as well. This policy defined people's roles, responsibilities and access rights. According to Nambiar, the data flow analysis helped Reliance Capital realize the entire issue's seriousness as well as the extent of risk.

With strong support from its management, Reliance Capital also created a data confidentiality awareness campaign for employees. The LOBs' CEOs sent emails to their respective teams, highlighting the new data confidentiality policy and the repercussions of policy violations. This message was then reinforced through screensavers and poster campaigns.

After identifying leakage points, Reliance Capital secured vulnerable areas using a combination of DRM and [DLP](#). The company uses separate solutions for DRM and DLP from Seclore Technology Private Ltd. and Websense Inc., respectively.

The right blend

Although the evaluation process included other established security vendors that provide DRM solutions, Reliance Capital chose to go ahead with Seclore (a relatively new player). This move was taken purely due to the flexibility provided by Seclore in terms of solution capabilities and customization.

Seclore customized its FileSecure solution for Reliance Capital with features such as mandatory data classification. "While using a DRM solution, you cannot leave things to users. For example, many users may never bother about things such as data classification. Hence, we decided to design a dialog box which pops up every time a new document is created or if the user forgets to classify a document," Nambiar explains.

Reliance Capital's DRM solution has been in use since April 2009. The DRM solution's implementation took around a month, and user acceptance testing took close to three months. "In terms of DRM, we did face a major challenge when it came to ironing out various integration issues with third-party products like Microsoft Office and OpenOffice," Nambiar says.

On the DLP front, Reliance Capital evaluated several options before it selected the Websense solution. "Though all the evaluated DLP solutions were quite mature, we decided to opt for Websense's DLP solution since the cost-benefit worked out well for us," Nambiar says. Reliance Capital took around two months to deploy the DLP solution.

The Websense DLP system's main components are modules for email, Web and endpoints. The Web component resides on the proxy server (to monitor Web traffic); endpoint agents on desktops/laptops (to monitor data on removable media and data cards, or being printed); and the email module alongside the email systems (to monitor outgoing mail).

Reaping the fruits

Today, the FileSecure DRM solution helps Reliance Capital lock down data with relevant rights and enforce and assign rights (view, print, copy, etc.) on its documents. The DRM solution provides granular rights to control each document.

After protection, the document can be distributed through means such as CDs, emails, pen drives, instant messengers, FTP and shared folders. Persistent file security provides file protection irrespective of its location. A document's rights are centrally managed by a server that defines the policies. FileSecure supports more than 115 document formats, which include Microsoft Office, OpenOffice and other text-based documents, as well as images.

Reliance Capital's DLP solution can be considered a second layer of security. It protects unclassified legacy data that may not be rights protected. DLP also helps protect the data that may be incorrectly classified by employees (with or without malicious intent).

According to Nambiar, implementation of these solutions has reduced the exposure of critical data for potential misuse or frauds. "We believe that since only authorized critical data leaves the organization, the business benefits are tremendous," Nambiar says.

06 Oct 2009

All Rights Reserved, [Copyright 2009 - 2010](#), TechTarget | [Read our Privacy Statement](#)