



SECLORE FILESECURE

Share with Confidence !

Government Regulatory

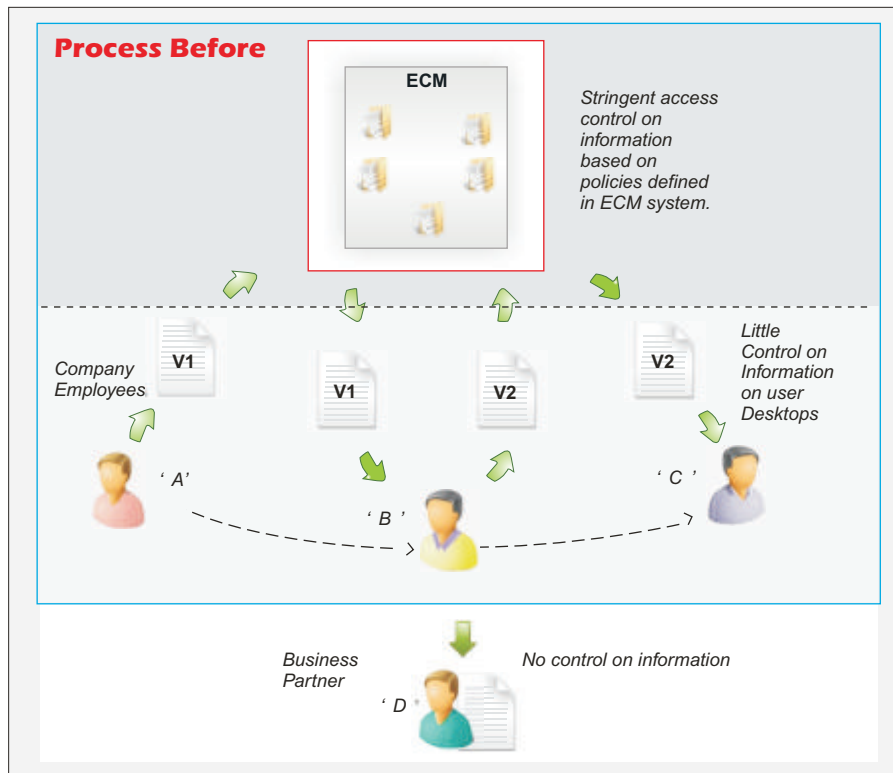
CASE STUDY

Background Of The Organization

The organization is one of the largest regulators of securities in the world. It is a nodal organization for managing the interests of the issuers of securities, the investors and the market intermediaries. The organization works with almost every financial services, publicly listed and law enforcement entity in the country.

Process Before

In an effort to reduce process cycle times and increase productivity and accountability, the organization has invested in an Electronic Content Management (ECM) system. Access to the ECM is provided to employees and to some business partners for the purpose of collaboration. A lot of confidential information relating to internal processes as well as personally identifiable customer information is handled by the system. To protect this information, stringent process and access control was implemented in the ECM.



Information risks and need for persistent security and usage control

All security measures that were implemented prevented unauthorized access to documents inside of the ECM. However, the risks of information breaches identified were as follows:

- Granular security policies implemented within the ECM system were rendered ineffective as soon as information was “downloaded” from the system.
- Authorized users parted with the downloaded content intentionally or unintentionally with users who were not supposed to be otherwise privy to the information.
- Centralization of information within the ECM system also posed a higher risk of “bulk” data theft i.e. Users “bulk downloading” the information for misuse.

The problem at the core was that once authorized users download the information there was no way of controlling its usage. Because of this there were serious information compromises which posed an enormous threat to the functioning of the organization.

Providing security for content outside the ECM without hindering collaboration was identified as a key success factor for the project. The following requirements were identified as key to achieving this:

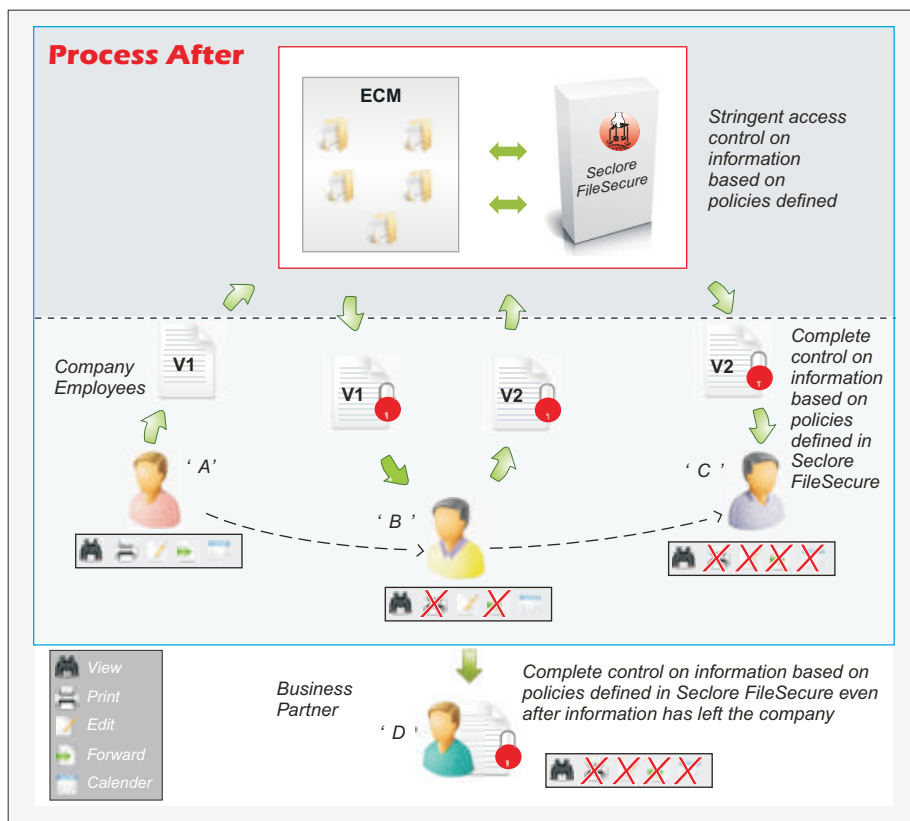
- Granular control on usage rights based on the role and task that is assigned to an individual. Eg- A simple workflow consisting of a document preparer (A) -> document editor (B) -> and document approver(C) should possibly have the following usage control rights.

User	View rights	Edit rights	Print rights	Distribute rights	Date Embargo
A	✓	✓	✓	✓	X
B	✓	✓	X	X	X
C	✓	X	X	X	✓ _(only after a certain date)

- Persistent end-to-end usage control on information throughout its lifecycle.
- Ability to integrate with existing identity management system of the ECM.
- Complete audit trail of authorized activities and unauthorized attempts performed on the information throughout its lifecycle.
- Ability to modify the usage rights of downloaded information.
- Automatic protection of a document before its leaves the ECM.

The Seclore Solution

Seclore FileSecure, integrated with the ECM system, enabled the organization to enforce usage rights on documents. Document creators could now give specific usage rights like WHO (people, groups) could use the document, WHAT (view, edit, print, forward, full control) can the person do with the document, WHEN (specific dates, time spans) can this be done & from WHERE (within the office, at business partner) can the document be used. Documents could also be “deprecated” such that access to old documents residing on desktops could be prevented. The “audit trail” feature not only guaranteed compliance to regulatory standards but also helped in detecting suspicious activities on documents by unauthorized users. Document rights could also be changed post distribution thereby providing additional control on distributed documents.



Benefits and ROI drivers

The above mentioned requirements were inherited when Seclore's IRM was integrated into the ECM. A few other key benefits were

- Information security outside of the “control area” of the ECM - Persistent security of information within and outside of the organization reduced the risks of information breaches significantly.
- Collaboration - By providing seamless security, Seclore FileSecure enhanced collaboration as information could now be shared with colleagues and business partners without worry.
- Compliance - Comprehensive tracking of information through the lifecycle of creation-storage-distribution-usage-archival-deletion provided audit trails and lowered the costs associated with compliance to frameworks.
- No process change - Capabilities to automatically protect information, use native applications like MS Office, Adobe PDF reader etc. to access the documents and single sign-on with the ECM system meant no change in the existing way of working for users, reducing costs associated with change and training.
- Low IT administration overheads - Capability to integrate with existing identity management system, existing storage system and existing web application infrastructure meant lower IT administration overheads.

About Seclore

Seclore is a high growth security software product company promoted by IIT Bombay. Seclore's products FileSecure and InfoSource help mitigate the risk arising out of information breaches and regulatory non-compliance whilst enhancing collaboration. This is done by providing ubiquitous technology for information control within and outside of the enterprise which seamlessly works with existing infrastructure. It is easy to deploy & use and comes with pay-as-you-use pricing.



SECLORE

Tel: +91 22 4015 5252

Email: info@seclore.com

Blog: <http://blog.seclore.com>

www.seclore.com