SECLORE

MANUFACTURING BUSINESS USE CASES

MANUFACTURING

1. Protecting IP and Complying with ITAR/EAR
2. Protecting Sales and Forecasting Documents
3. Protecting Manufacturing Plant Designs
4. Consumer Electronics Manufacturer

SECLORE

Protecting IP and Complying with ITAR/EAR

How a major US Optoelectronics manufacturer uses Seclore's EDRM for protecting its IP and complying with US export regulations

Company Profile

Leading Global Manufacturer

- Manufactures security and inspection systems such as airport security X-ray machines and metal detectors, medical monitoring and anesthesia systems, and optoelectronic devices.
- US$595 million (FY 2010) in revenue Founded in 1987, includes three subsidiary companies
- 3,180 employees worldwide (as of June 2010)

Seclore Business Benefits

- Extend your Security and Risk Infrastructure outside your Corporate Borders
- Secure information sent to vendors and third parties
- Securely adopt file-sharing, Cloud Computing, BYOD, and mobile-device usage
- Comply with legal, regulatory and privacy obligations
- Prevent Negative Press, Loss of Consumer Confidence and Competitive Advantage

Seclore Capabilities

- Persistent Data Protection – Even Outside your Network
- Robust Usage Controls: Enforce View, Copy, Edit, Print, and Screen Captures, by User, Time, and Location
- Real-time Audit Trail and Usage Reports
- Remote-Control and Expire Files in Real Time – Wherever They Reside

It's not Just About Securing Information,
It's About Securing *Corporate Value*

Business Situation

This US optoelectronics manufacturer outsources its IT operations to a low-cost country in Asia. This has brought tremendous benefits - including world-class IT expertise at a fraction of US costs. The company focuses on its core business and leaves ancillary functions to the experts. And ends up saving money too. IT personnel – which are non-US citizens – perform routine tasks such as file backup and server maintenance. They possess complete access to all confidential files saved in numerous storage systems and servers. These files contain core Intellectual Property and information related to military and dual-use items that are exported to various countries.

Most importantly, many of these documents also contain technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended (Title 50, U.S.C., App. 2401 et seq.). Violations of these export laws are subject to severe criminal penalties. There have been numerous cases of manufacturers being heavily fined for violating export regulations defined under ITAR (International Traffic in Arms Regulations) and EAR (Export Administration Regulations). These documents – along with the actual export items – are sent to various re-exporters and agents (if any) and eventually the end customers.

Challenge

The challenges arising from the desire to utilize lower cost outsourcing are mainly two fold:

Loss of IP. There is absolutely nothing stopping IT administrators from obtaining unauthorized access to any file. And then doing with it whatever they wish: from editing its contents to sending it to a competitor. Losing such core IP – especially to market rivals – could directly affect bottom lines and even people's jobs. Forget malicious intent – even an innocent act of double clicking on a PDF file – if discovered during audits – could have costly consequences.

Non-compliance: The IT administrators are not US citizens. And they are certainly not licensed to access information pertaining to USML (United States Munitions List) items stored on the servers – information that is covered under ITAR and EAR. The mere act of opening a single PDF file could result in direct non-compliance for the organization and millions of dollars in fines. Repeated violations could result in the export license being revoked.

Seclore Solution

The documents used and generated are protected with Seclore's Enterprise Digital Rights Management solution. Once a file is protected, it can be freely shared with the relevant users without any threat of misuse or data leakage. Only specific team members have access to these protected files. Each user has access to his/her relevant files only. The operations that each authorized person can perform on the file i.e. viewing, editing, printing, copying content etc. are also controlled.

The same security and access permissions can be extended to external auditors and partners. Their level of access to this information is restricted. Files can also be sent out with time-based controls, so that they expire after a certain period of time and cannot be accessed any longer. Access permissions on any file can be modified centrally and dynamically. User access can be added or removed as desired. These changes come into effect immediately regardless of where the file is located at the time. All activities performed by all users are monitored and searchable – thus facilitating regular usage audits and enabling regulatory compliance as well.

The Results

Seclore's Enterprise Digital Rights Management solution has enabled this manufacturer to successfully protect its Intellectual Property and comply with the relevant US export control laws and regulations. They have also been able to systemically enforce the NDA and the EULA (End User License Agreement) and ensure that only authorized parties can access technical data governed under ITAR and EAR. Thus, a security solution – something that is usually looked upon as a hindrance – has unusually resulted in securing data, ensuring compliance, without drastically affecting usability, end user workflows, and work habits.

SECLORE

Protecting Sales and Forecasting Documents

Company Profile

Leading Global Manufacturer

- US $403.8 million annual revenue
- 2000 employees worldwide
- Presence in India, US, and Europe

Seclore Business Benefits

- Extend your Security and Risk Infrastructure outside your Corporate Borders
- Secure information sent to vendors and third parties
- Securely adopt file-sharing, Cloud Computing, BYOD, and mobile-device usage
- Comply with legal, regulatory and privacy obligations
- Prevent Negative Press, Loss of Consumer Confidence and Competitive Advantage

Seclore Capabilities

- Persistent Data Protection – Even Outside your Network
- Robust Usage Controls: Enforce View, Copy, Edit, Print, and Screen Captures, by User, Time, and Location
- Real-time Audit Trail and Usage Reports
- Remote-Control and Expire Files in Real Time – Wherever They Reside

It's not Just About Securing Information,
It's About Securing *Corporate Value*

Business Situation

At a leading API manufacturer, the marketing team shares confidential company information with different departments within the company - such as Production, R&D, Regulatory, Finance and the Senior Management – as part of daily business processes. This information is shared only with the relevant employees within these departments. The documents contain information that directly influences or is related to company strategy, for example:

- The Sales Forecast for a particular product would be shared with:
  - Brand manager(s) for that product
  - R&D and Production - to inform them of the quantity required to be produced for the next month/quarter
  - Finance - to enable them to calculate the projected profits based on the projected sales.

- The company's contract agreements with customers would be shared with the Legal and Regulatory departments. These contracts were required for reference at various points by the Regulatory and Finance departments to see the payment terms as well as well as the relevant clauses.

This information was shared with enterprises via company email or temp folders shared over the enterprise network.

Challenge

Since this information was shared via insecure emails or network folders, they could easily leak and find their way to unauthorized parties. Anyone could easily forward an email or send a confidential file to anyone else within the organization or outside it. Employees who were not authorized to access the files themselves possessed access to the network folder where the files where stored. This situation and business need presented the enterprise with a significant challenge: to share this extremely confidential data and collaborate on it in a secure manner. Leakage and misuse of this data could result in business and reputational losses, and a severe loss of competitive advantage. In essence, the challenges that the company faced were not only to ensure that unauthorized users don't obtain access to the information, but also that authorized employees are not able to misuse it in any way. For example, this included ensuring that:

1. A brand manager is able to view Product Forecasts for his product only
2. Sales Forecasts are available to selected employees only
3. Legal Contracts can be viewed by selected employees, who should be unable to edit or print them, or potentially leak the information in any other way (e.g. by screen grabbing etc.)
4. Customer contract agreements, that are themselves covered under NDA, are accessed by Legal and Regulatory departments only

Other employees should not be able to open these files even if they got hold of them.

Solution Delivered

The Marketing team would use Seclore's Enterprise Digital Rights Management solution to secure files containing this information. Different access permissions were specified for different files. Access to the file contents would be heavily restricted. Operations that each authorized person could perform on the document i.e. viewing, editing, printing, copying content etc. would be controlled. These access rights and security would 'stick' to a file and stay with it regardless of where it was stored or how it was shared – email, network folders, CDs, USB drives etc. All user activities on a file would be automatically tracked and a detailed, searchable log of this information would be available through a central web-based console. The solution (detailed below) successfully achieved the business objective of information security without interfering in business processes.

The Marketing Head protects Sales Forecast data with Seclore's EDRM solution.	Production and R&D departments can view these files, while the Finance team can view and edit them. Hence, the Seclore's EDRM solution mapped perfectly with business requirements. All these users can perform no other operation on the files, such as editing (for Production and R&D), printing, capturing screenshots etc. Any other user would not be able to open the files even if they got hold of them. Thus, everyone with access to the network temp folder for example, would still not be able to open the files within that folder if he/she does not possess the required permissions. The act of protecting files can also be delegated to a designated member of the marketing team.
The Marketing Head protects Legal Contracts with Seclore's EDRM solution.	Legal and Regulatory departments are allowed to view these documents, and do nothing more. No other action (editing, printing, taking screen captures, copying content etc.) can be performed by these users on those documents. Anyone else would not be able to open these documents even if they got hold of them.
Activities performed on the documents are monitored and logged in a central web-based console.	Every action performed by every user on every file would be tracked in the central web-based console. These logs can be filtered and searched by user, date etc.

Seclore's EDRM has helped the company ensure that the security guarantees given to customers go beyond paper agreements and NDAs. The solution caused little or no overhead or interference in existing business processes and workflows. Seclore's EDRM was able to seamlessly fit into a complicated business process – right from Technology to R&D to QA – and ensure maximum digital security at every stage. Thus, the organization has been able to successfully secure customer information as well as its reputation as one of the leading API manufacturers.

SECLORE

Protecting Manufacturing Plant Designs

Company Profile

Large Diversified Industrial Conglomerate

- Second largest producer of viscose filament yarn
- US $4.75 billion diversified conglomerate
- ISO 9001:2000, 14001:2004 & OHSAS18001 Certified

Seclore Business Benefits

- Extend your Security and Risk Infrastructure outside your Corporate Borders
- Secure information sent to vendors and third parties
- Securely adopt file-sharing, Cloud Computing, BYOD, and mobile-device usage
- Comply with legal, regulatory and privacy obligations
- Prevent Negative Press, Loss of Consumer Confidence and Competitive Advantage

Seclore Capabilities

- Persistent Data Protection – Even Outside your Network
- Robust Usage Controls: Enforce View, Copy, Edit, Print, and Screen Captures, by User, Time, and Location
- Real-time Audit Trail and Usage Reports
- Remote-Control and Expire Files in Real Time – Wherever They Reside

It's not Just About Securing Information,
It's About Securing *Corporate Value*

Business Situation

A large industrial conglomerate has purchased a chemical manufacturing plant from a European firm. The existing plant, based in Europe, will be dis-assembled and every individual part will be shipped to India for re-assembly. The plant seller will also provide the existing plant's mechanical, electrical and process specifications. These specifications are an important reference for the project team that is responsible for re-assembling the plant at the new location.

The Indian firm (buyer) has signed a confidentiality agreement that enforces significant financial penalties and legal liabilities if the plant specifications and designs are leaked. Ensuring the security of these documents was the highest priority and was part of the project team's responsibilities.

Challenge

Ensuring that the design specifications are not be leaked out to an unauthorized user was a key priority for the Project Head. A document lead was appointed to ensure that documents were accessed by selected project team members only. Furthermore, each function – Civil, mechanical, Electrical etc. was to be allowed access information related to their work only. The plant specification documents were physically secured by putting them on a single computer which was isolated from the network. Individuals were required to sign-up for accessing that particular machine and the document lead was required to supervise.

This was terribly inefficient for the project team members, since they could not access the documents when they really needed them. Considerable time was required to be put in by the documentation lead to be physically present when the information is being accessed. The physical security was time-consuming and cumbersome.

Seclore Solution

All the documents are now made available on a centrally located shared folder. Unauthorized users cannot these documents. Every authorized user has access to his/her relevant files only e.g. the mechanical team has access to mechanical drawings and documents only, the electrical team has access to electrical drawings and documents only and so on. These files continue to

remain secure even after they are removed from the folder Authorized users can view the file only and are unable to edit, print, copy content out of the files etc. The document lead can modify these access permissions and can add or remove user access at anytime from anywhere. The need for physical security of this information is completely done away with. Printing is tightly controlled with only 2 or 3 users having print access. All user activities are automatically tracked and a detailed, searchable log of this information is available through a web-based console.

Solution Delivered

The folder on the file server is configured to protect all the files in it.	All existing plant specifications would be stored and accessed from this central location only.
The data is re-arranged into functional sub-folders for each of the departments	i.e. Civil, Mechanical, Electrical, Process, Instrumentation etc.
For each function (folder) a separate set of access permissions is defined.	These function specific access permissions are used to secure files in the respective folders.
Once a file is placed in a particular folder it would be permanently protected with the access permissions assigned to that folder.	The security would remain permanently attached to the file, so that the file remains secure even if it is removed out of the folder.
Activities performed on these files would be monitored by the document lead.	Every action performed by every user on every file would be tracked in the central web-based console. These logs can be filtered and searched by user, date etc.
The risk of data leakage - accidental or malicious – is significantly reduced.	The financial and legal risk is mitigated and contractual obligations are met with minimum overheads. The project and IT team are able to get a good night's sleep having ensured that this data is safe and secure.

These additional security measures have caused no impact on existing business processes and workflows. Thus, the organization has been successfully able to meet contractual obligations and avoid a potential loss of reputation and business.

SECLORE

Consumer Electronics Manufacturer

Company Profile

Large Diversified Industrial Conglomerate

- Fourth largest television manufacturer in the world
- $70 billion annual revenue 300,000 employees worldwide
- Owner of over 140,000 patents 580 subsidiary companies

Seclore Business Benefits

- Extend your Security and Risk Infrastructure outside your Corporate Borders
- Outsource and Collaborate Securely
- Securely Adopt File-Sharing, Cloud, BYOD, and Mobile Device Usage
- Reduce Enterprise Risk and Liabilities
- Comply with Legal, Regulatory and Privacy Obligations
- Prevent Negative Press, Loss of Consumer Confidence and Competitive Advantage

Seclore Capabilities

- Persistent Data Protection – Even Outside your Network
- Robust Usage Controls: Enforce View, Copy,
- Edit, Print, and Screen Captures, by User, Time,
- and Location
- Audit Trail and Usage Reports
- Remote-Control and Expire Files in Real Time
- – Wherever They Reside

It's not Just About Securing Information,
It's About Securing Corporate Value

Business Situation

One of the world's largest consumer electronics manufacturers has a large distributor base. The commercial team shares region-wise pricing and commission structures with the distributors every quarter.

These pricing and commission structures are different across regions. It has been observed that distributors in different regions manage to get hold of the other regions' documents. The commercial team needs to justify this differential pricing to the distributors on a frequent basis. A few distributors are actively misusing this sensitive information.

Challenge

The commercial team has to ensure that the region-wise pricing structure is available to the distributors in that particular region only. The organization should be able to easily track and monitor these pricing sheets and if necessary make them inaccessible.

The conflict between the distributors and organization needs to be reduced to the maximum extent possible, by making sure that access is restricted to the region-specific distributors only.

The organization also has to prevent this information reaching their competitors via these distributors. Any data leakage or sharing should be traced back to the distributor leaked the information so that appropriate actions may be taken.

Seclore Solution

The commercial team protected these region-wise pricing sheets with the appropriate access permissions before sharing them with the distributors. Distributors across different regions can open only the files they are authorized to access. Regardless of how the files are shared (email, SFTP, CD/DVD etc.) or where they are stored, the security and access permissions are permanent and cannot be compromised.

The overhead of this security was minimal for both the organization as well as the external parties. There was no restriction on the datasharing mechanism and these files could be shared over emails. The organization can monitor and track the use of their files even when they are being used on a computer that is outside the enterprise network. It was observed that the conflict with the distributors reduced once the pricing sheets were not accessible

across regions. In case of any conflict or if the distributor relationship comes to an end, all shared files can be made inaccessible instantly with a click on a button.

Solution Delivered

The folder on the file server is configured to protect all the files in it.	All the pricing data would be initially saved in this central location only.
Sub-folders are created for each region with the corresponding user access permissions defined for each.	The region-specific folders would ensure separate access permissions for each region.
The data on the server is secured with 'file-level' access permissions.	So even IT administrators would not be able to open these protected files.
The commercial team would manage the user access permissions on these files.	After the initial configuration, the IT team does not need to be involved in the ongoing changes to access permissions.
Once a file is placed in a particular folder it would be permanently protected with the access permissions assigned to that folder.	The security would remain permanently attached to the file, so that the file remains secure even after it is taken out of the folder.
Activities performed on these files would be monitored by the commercial team.	Every action performed by every user on every file would be tracked in the central web-based console. These logs can be filtered and searched by user, date etc.

Hence, data leakage – whether accidental or malicious – has been virtually eliminated. The risk of the organization's pricing information being available to unauthorized distributors or to the competitors was successfully mitigated with minimum overheads. The commercial and IT team are able to peacefully sleep at night knowing that the data would be safe and secure at all times.

About Seclore

Seclore offers the market's first fully browser-based data-centric security solution, which enables organizations to control the usage of files wherever they go, both within and outside of the organization's boundaries. The ability to remotely enforce and audit who can view, edit, copy, screen share, and redistribute files empowers organizations to embrace mobility, file-sharing, and external collaboration with confidence. With over 2000 companies in 29 countries using Seclore to protect 10 petabytes of data, Seclore is helping organizations achieve their data security, governance, and compliance objectives.

Learn how easy it now is to keep your most sensitive data safe, and compliant.
Contact us at: info@seclore.com or CALL 1-844-4-SECLORE.

USA – West Coast
691 S. Milpitas
Blvd.#217
Milpitas CA 95035
1-844-473-2567

USA – East Coast
420 Lexington Avenue
Suite 300,
Graybar Building
New York City
NY 10170

India
Excom House Second Floor
Plot No. 7 & 8,
Off. Saki Vihar Road
Sakinaka, Mumbai
400 072
+91 22 6130 4200
+91 22 6143 4800

Gurugram
+91 124 475 0600

Singapore
Seclore Asia Pte. Ltd.
AXA Tower, 8 Shenton
Way
Level 34-01
Singapore – 068811
+65 8292 1930
+65 9180 2700

Europe
Seclore GmbH
Marie-Curie-Straße 8
D-79539 Lörrach
Germany
+49 151 1918 5673

UAE
Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City, PO Box
73030, Dubai, UAE
+9714-440-1348
+97150-909-5650
+97155-792-3262

Saudi Arabia
5th Floor, Altamyoz Tower
Olaya Street
P.O. Box. 8374
Riyadh 11482
+966-11-212-1346
+966-504-339-765

SECLORE