SECLORE

INSURANCE BUSINESS USE CASES

INSURANCE

1. Protecting Investment Data
2. Training Content Major Private Life Insurance Company
3. Protecting Finance Reporting and Consolidation
4. Protecting Accounts Commission Information
5. Protecting Accounts Taxation Information

SECLORE

Protecting Investment Data

Company Profile

Major Insurance Company

- US $2.25 billion annual revenue
- 15,000 employees
- Over 400 customer centers

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

For this large insurance company with a huge revenue base, the investment function is a vital pillar of its operations and a key determinant of its profitability. The investment function in this

- Life Insurance firm comprises of three key teams: Front Office (FO): This team is in direct contact with clients and markets. They manage and maintain confidential enterprise information related to investments, sales, trading, research and risk management. This team generates a lot of sensitive data such as research reports prepared by analysts for recommendations to the fund management team, models & valuations, trading information, meeting notes of discussions with various companies etc.
- Mid Office (MO): This team ensures control and processing of transactions.
- Back Office (BO): This team monitors post market processing of transactions: confirmations, payment, settlement and accounting. The Mid Office & Back Office teams generate highly confidential Holding statements, Performance Summary reports, NAV & other working files.

The data is shared using emails and temp folders. A large amount of confidential investment data is stored in folders shared over the network.

Challenge

This information is sensitive and highly valuable to the organization and its usage should be restricted and monitored. These files can cause serious reputational and financial damage if leaked to the public or to competitors. Thus, protecting this information is a strategic business imperative. However, these confidential documents are shared via normal email and stored in network folders. The information in these files may easily be misused. Laptops or mobile devices containing this information may be lost, stolen, hacked or compromised. Anyone with access to these files can freely distribute them to unauthorized entities within and outside the enterprise without a trace.

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.

Solution Delivered

A network folder is configured to protect all the files in it.	All the working data related to reporting and consolidation would be saved on this central location only. Since this is the folder where the team saves and stores their in-progress content, there is no overhead, no change in work habits required by users, and no change in user experience. Only permitted users can open these files. All other users – including IT staff - cannot open these files even if they get hold of them.
Once a file is placed in a particular folder it would be permanently protected with the access permissions assigned to that folder.	The file would remain encrypted and protected even after it is taken out of the folder.
Information shared with other departments via shared folders would also be protected.	Authorized users of various departments would be free to copy these files onto their laptops or USB devices without compromising the security in any way.
Information shared with auditors or other external parties would be protected with similar controls.	The files could be shared over email or any other medium.
Activities performed on these files would be monitored by the the Finance Reporting and Consolidation 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.

In this era of cut-throat competition in a dynamic industry such as Life Insurance, protecting Investments and Trading information is of paramount importance. Using Seclore's EDRM, the risk of the confidential information being compromised was virtually eliminated. Thus, the organization has been able to achieve the important strategic objectives of securing its corporate value, its reputation, and its business.

SECLORE

Training Content
Major Private Life Insurance Company

Company Profile

Major Insurance Company

- One of India's largest private Life Insurance companies
- 15,000 employees over 400 branches across the country
- US $2.25 billion annual revenue

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

A major Life Insurance company has a large in-house Learning and Development (LnD) unit that handles the entire organization's training requirements. Life insurance in India is a fast growing, dynamic industry (with a high attrition rate) and employees need to be on a continuous training cycle to ensure that they are equipped to handle the ever changing product portfolio and customer needs. LnD designs and develops the training content and then delivers the training to the various departments. In an industry with astonishing attrition rates, LnD has served as a competitive differentiator for the company that is rated as among the best in the country has helped the company not only retain employees but also attract the best talent in the market. Hence, LnD activities are an important part of organizational strategy and market competitiveness.

Challenge

The Analysis and Design teams interact with the Business Stakeholders to collect their requirements and work on the Training content. During the design phase, drafts are shared with various internal stake-holders before the content is finalized. Until then, only specific individuals should have access to this data on a strict needto-know basis.

Multiple teams work on the content and design of the final material. External freelancers or consultants may also be part of the project team. Once the content is finalized in the form of Training Presentations, Facilitator Guides, Participant Handbooks etc. they are distributed to training centers across the country. Training instructors at various remote locations download the training content to their personal computers or storage (USB) devices and carry them to the training locations. This content may also reside on shared computers in the training facility. Data in all these shared locations is highly vulnerable to leakage.

The evaluation tests and assignments need to be approved by multiple Business Stakeholders before they can be incorporated into the online evaluation tool. The entire evaluation process could be jeopardized if the content is leaked out during the approval process.

Seclore Solution

The documents used and created are protected with Seclore's Enterprise Digital Rights Management solution. The security and

access permissions reside with the file itself, they are equally effective in any environment – whether the file is lying in any computer anywhere in the world, in an inbox, on a network drive, on a USB stick, on a CD/DVD etc. In addition to the LnD team, only specific business stakeholders will be given access to view these documents. If the content design is being outsourced to external parties, the documents shared with them will be protected with similar access permissions.

Even though the design vendor is outside the organization's network, the security of the information remains enforced without any compromise. All activities performed by everyone are monitored and searchable.

Once the final training presentations and guides are ready, they will be shared with the training instructors across multiple locations with similar controls. Even if the files are stored on individual laptops or external storage/USB devices, the security and access permissions will always remain enforced. Authorized users can view the file but cannot edit, print, copy content out of it etc. Printing is tightly controlled with very few authorized users having print permissions on the files.

Solution Delivered

A folder on the file server is configured to protect all the files in it.	All the 'work-in-progress' training content and related documents would be saved on this central location only. Since this is the folder where the team saves and stores their in-progress content anyway, there is no overhead and no change in work habits required by users. Only people with access can open these files. All other users – including IT staff - cannot open these files even if they get hold of them.
The Learning and Development (LnD) team would manage the user access permissions.	After the initial configuration, the IT team does not need to be involved in the ongoing changes to the user 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 if it is taken out of the folder.
The information shared with training instructors via shared folders would also be protected.	The instructors would be free to copy these files onto their laptops or storage (USB) devices without compromising the security in any way.
Information shared with design vendors or other external parties would be protected with similar controls.	The files could be shared over email or any other medium.
Activities performed on these files would be monitored by the LnD 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.
The risk of data leakage - accidental or malicious – is significantly reduced.	The risk of the organization's Training and Evaluation information being available to unauthorized users or to their competitors was successfully mitigated with minimum overheads. The LnD and IT team are able to get a good night's sleep having ensured that this data is safe and secure.

For an organization that puts tremendous focus on their Training and Organizational Development initiatives, protecting training content was a critical strategic requirement. Using Seclore's EDRM, the risk of the content being leaked was very significantly reduced which ensured that the organization's strategic differentiator against their competition was maintained.

SECLORE

Protecting Finance Reporting and Consolidation

Company Profile

Major Insurance Company

- US $2.25 billion annual revenue
- 15,000 employees
- Over 400 customer centers

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

Financial Reporting and Consolidation reaches entirely new levels for this Life Insurance company, given its large Revenue and Consumer base. The management has always acknowledged transparent, accurate and timely financial reporting as a key area of corporate responsibility. For this organization, it is not just about legal and regulatory compliance, it is about business, brand reputation, and corporate strategy.

The Finance Reporting and Consolidation team comprises of the core financial reporting, regulatory reporting, and expense management and reporting verticals. This team also maintains enterprise information related to compliance reporting and audit co-ordination. It caters to requests from various departments and stakeholders regarding this information. Files and reports are shared using emails and temp folders. Critical information owned by the Finance Reporting and Consolidation team, such as shareholder reports, management analysis and reports, regulatory reports to insurance industry compliance, party-specific commercialdeal information, legal and compliance documents, board packs etc. are stored in shared network folders.

Challenge

This information is sensitive and highly valuable to the organization and its usage should be restricted and monitored. These files can cause serious reputational and financial damage if leaked to the public or to competitors. Thus, protecting this information is a strategic business imperative. However, these confidential documents are shared via normal email and stored in temporary folders on the network (known as 'temp folders') in unencrypted and unsecure form. The information in these files may easily be misused. Laptops or mobile devices containing this information may be lost, stolen, hacked or compromised. In fact, anyone with access to these files can freely distribute them to unauthorized entities within and outside the enterprise without a trace. Leakage or misuse of this information may lead to:

- Reputational losses: Negative media coverage, loss of shareholder and consumer confidence
- Financial losses: Loss of potential business and clientele, loss of customer confidence
- Legal and Compliance issues: Fines, penalties, expensive and endless litigation

Seclore Solution

Documents used and created by the Finance Reporting and Consolidation team are protected with Seclore's EDRM. Only permitted team members have access to these protected files. Each user has access to his/ her relevant files only. This security 'sticks' with the file and remains in effect regardless of the file's location.

A user may be allowed to view and edit a file, but not allowed to copy content out of it, print it or even take screen captures. The same 'need-to-know' access permissions also apply to external auditors, vendors, and other external parties. Certain files are shared with expiry dates - information automatically expires after its purpose is served and cannot be accessed further. The Business unit power user can centrally and dynamically modify access permissions on any file and can add or remove user access as desired. Changes made to a file's access permissions take place in real time and 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.

Solution Delivered

A network folder is configured to protect all the files in it.	All the working data related to reporting and consolidation would be saved on this central location only. Since this is the folder where the team saves and stores their in-progress content, there is no overhead, no change in work habits required by users, and no change in user experience. Only permitted users can open these files. All other users – including IT staff - cannot open these files even if they get hold of them.
Once a file is placed in a particular folder it would be permanently protected with the access permissions assigned to that folder.	The file would remain encrypted and protected even after it is taken out of the folder.
Information shared with other departments via shared folders would also be protected.	Authorized users of various departments would be free to copy these files onto their laptops or USB devices without compromising the security in any way.
Information shared with auditors or other external parties would be protected with similar controls.	The files could be shared over email or any other medium.
Activities performed on these files would be monitored by the the Finance Reporting and Consolidation 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.

The serious risk of the organization's financial information being available to unauthorized users or to their competitors was successfully mitigated with minimum overheads. The Finance Reporting and Consolidation and IT teams have achieved the unique goal of information collaboration and its security both within and beyond their organization's boundaries.

For an insurance company that exists in a sector of cut-throat competition, protecting their consolidated financial statements and related documents was a critical strategic imperative. Using Seclore's EDRM, the risk of the content being compromised was virtually eliminated. Thus, the organization has been able to achieve the important strategic objectives of securing its corporate value, its reputation, and its business.

SECLORE

Protecting Accounts Commission Information

Company Profile

Major Insurance Company

- Among top 100 insurance companies in US
- Wide range of commercial and business insurance
- 1,200 employees

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

Timely payouts and commissions is something this private Insurance firm takes very seriously - given its large revenue and customer base. The Commissions department manages and maintains confidential enterprise information related to pay-outs and commission paid figures. It provides data and reports to internal as well as external entities. Highly confidential information such as Pay-out Data, Commission MIS Reports, Regulatory and Compliance Reports, MIS Reports and Data to Auditors and other stakeholders etc. – changes hands on a daily basis. All this sensitive information is shared via emails and 'temp folders' shared over the enterprise network.

Challenge

The confidentiality and sensitivity of this information can hardly be overemphasized. Extremely high liability is attached to this data. Exposure and misuse of this information could expose the organization to serious risk. For a life insurance company, operating in an industry where the competition is cut-throat, protecting this information is not just an IT activity but a critical strategic imperative. Currently however, all this information is shared amongst various teams in unencrypted and insecure form – and is highly vulnerable to leakage. Anyone obtaining unauthorized access to files containing this information could potentially misuse them. In fact, even authorized and legitimate users of this information could leak it.

Information related to taxation and documents intended for Regulatory Agencies are particularly sensitive in nature. If leaked, they can lead to serious financial and reputational losses for the enterprise.

Seclore Solution

The relevant documents are protected with Seclore's Enterprise Digital Rights Management. The security and access permissions reside with the file itself and thus equally effective in any environment – whether the file is lying in any computer anywhere in the world, in an inbox, on a network drive, on a USB stick, on a CD/DVD etc.

Only selected employees possess access to these protected files. The operations that each authorized person can perform on the file i.e. view, edit, print, copying content etc. are also

controlled. Print outs are tightly controlled with very few authorized users having printing access. All activities performed by everyone are monitored and searchable. Even what external users (vendors, partners etc.) can perform with these files are controlled. Files have in-built expiry dates so they are automatically made un-usable after their purpose is served. The Business unit power user (the Business head or a designated team member), who is the owner of this information, can modify the security and access permissions on these files and can add or remove user access as desired.

Solution Delivered

A folder on a network drive is configured to automatically protect all the files in it.	All working data related to reporting and consolidation would be saved on this central location only. Since this is the folder where the team has historically saved and stored their in-progress content, there is no overhead and no change in work habits required by users. Only people with access can open these files. All other users – including IT staff - cannot open these files even if they possess access to the folder. The Accounts Commission team would manage the user access permissions.
Once a file is placed in a particular folder it would be permanently protected with the usage permissions assigned to that folder.	The security would remain permanently attached to the file, so that the file remains secure even if it is taken out of the folder.
Information shared with auditors and other external parties would be protected with similar controls.	The files could be shared over email or any other medium – and the security would still remain intact. The file security provided by Seclore's EDRM is independent of transmission medium (email, SFTP etc.) and storage mechanism (network folders, USB drives, CD/DVD etc.).
Activities performed on these files would be monitored by the Accounts Commission team.	Every action performed by every user on every file would be tracked in a central web-based console. These logs can be filtered and searched by user, date etc.

Seclore's EDRM solution helped the organization achieve the critical strategic imperative of securing this information from misuse and leakage. The risk of the content being compromised was virtually eliminated.

The risk of data leakage - accidental or malicious – stood significantly reduced after implementing Seclore's EDRM.The risk of financial and accounting information being available to unauthorized users or to their competitors was successfully mitigated - with minimum overheads. The Accounts Commission and
IT teams achieved the unique goal of information collaboration and security. Seclore enabled them to not only secure information that remains inside their organizational network – but also secure information that goes outside the company for legitimate business reasons.

SECLORE

Protecting Accounts Taxation Information

Company Profile

Major Insurance Company

- Among top 100 insurance companies in US
- Wide range of commercial and business insurance
- 1,200 employees

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

Accurate and timely management of digital information related to taxes payable by a company - as well as its propagation to various related entities – is not just an IT initiative but a legal binding and corporate responsibility. The Accounts Taxation team at this Life Insurance company manages and maintains confidential information related to direct and indirect taxes. It shares information with internal as well as external entities on a regular basis. The information shared includes various payroll analysis reports, audit reports, tax notices, data for Auditors and Consultants as well as information private to the team itself (such as certificates) etc. Additionally, the team also caters to requests for information from various departments and other stakeholders. The data is shared using emails and temp folders. A lot of information is also stored in folders shared over the enterprise network.

Challenge

Concerns related to data leakage are centered primarily on tax MIS reports. Leakage of these reports could cause maximum risk to the organization. Critical data of the Taxation team is stored in network folders and shared via emails or 'temp folders' in unencrypted and insecure form. This information is sensitive and valuable to the organization and should be shared on a strict 'need-to-know' basis. Currently however, any employee possessing access to these files and reports can freely distribute them to unauthorized entities within and outside the enterprise without a trace. This information – if leaked - could cause serious financial and reputational losses for the enterprise.

Seclore Solution

The documents used and created are protected with Seclore's Enterprise Digital Rights Management. The security and access permissions reside within the file itself and are thus equally effective in any environment – whether the file is lying in any computer anywhere in the world, in an inbox, on a network drive, on a USB stick, on a CD/DVD etc. Only selected employees possess access to these protected files. Even operations that each authorized person can perform on the file i.e. view, edit, print, copying content etc. are also controlled. Printed copies are tightly controlled with very few authorized users having printing access. All activities performed by everyone are monitored and searchable. Even what external employees (vendors, partners etc.) can perform

with these files are controlled. Files have in-built expiry dates so they are automatically made un-usable after their purpose is served. The Business unit power user (the Business head or a designated team member), who is the owner of this information, can modify the security and access permissions on these files and can add or remove user access as desired.

Solution Delivered

A shared folder on a network drive is configured to automatically protect all the files in it.	All working data related to taxes and expense reporting would be saved on this central location only. Since this is the folder where the team has historically saved and stored their in-progress content, there is no overhead and no change in work habits required by users. Only people with access can open these files. All other users – including IT staff - cannot open these files even if they possess access to the folder. The Accounts Taxation team would manage the user access permissions.
Once a file is placed in a particular folder it would be permanently protected with the usage permissions assigned to that folder.	The security would remain permanently attached to the file, so that the file remains secure even if it is taken out of the folder.
Information shared with auditors and other external parties would be protected with similar controls.	The files could be shared over email or any other medium – and the security would still remain intact. The file security provided by Seclore's EDRM is independent of transmission medium (email, SFTP etc.) and storage mechanism (network folders, USB drives, CD/DVD etc.).
Activities performed on these files would be monitored by the Accounts Taxation team.	Every action performed by every user on every file would be tracked in a central web-based console. These logs can be filtered and searched by user, date etc.

Seclore helped the organization achieve the critical strategic imperative of securing this information from misuse and leakage. The risk of the content being compromised was virtually eliminated.

The risk of data leakage - accidental or malicious – stood significantly reduced after implementing Seclore's EDRM solution. The risk of financial and accounting information being available to unauthorized users or to their competitors was successfully mitigated - with minimum overheads. The Accounts Taxation and IT teams achieved the unique goal of information collaboration and security. Seclore enabled them to not only secure information that remains inside their organizational network – but also secure information that goes outside the company for legitimate business reasons.

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 6000 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
157 S. Murphy Avenue
Sunnyvale, CA 94086
1-844-473-2567

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

India
Excom House Ground 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

Bengaluru
+91 080 46586900

Singapore
Seclore Asia Pte. Ltd.
#08 -01
80, Robinson Road
Singapore – 068898
+65 8292 1930
+65 9180 2700

Europe
United Kingdom
Suite 4B, Linwood Point
Paisley, PA1 2FB
+44 141 433 7902

UAE
Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City, PO Box
73030, Dubai, UAE
+97155-990-1570
+9714-440-1348

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

© 2018 Seclore, Inc. All Rights Reserved.

SECLORE