CLEARSWIFT

Information Visibility: Reducing Business Risk

with The Clearswift Aneesya Platform

Table of Contents

Overview

Since the Veterans Association data breach in 2006, there has been an ever increasing need for organizations to better understand and manage their electronic information. New legislation continues to be introduced both from national, as well as an industry sector perspective with a view to protecting the information, and more importantly, the people that the information relates to. This began with credit card, bank and financial details and has subsequently spread to healthcare (PHI) and other personally identifiable information (PII) and is now looking to protect Intellectual Property (IP).

On the face of it, the problem doesn't seem to be so great; understand the information of value, where it is located and then how to protect it. However, for all those who have been trying to do this, the challenge has never been greater.

Most organizations do not understand what information has the most value to them, why it has an associated value, where it is stored and who has access to it. The situation is made even more challenging due to changes in working practices with critical information being held on a variety of enablement devices, both corporate owned (CYOD – choose your own device) and BYOD (Bring Your Own Device), 'in the cloud' and on social networking sites. While it is a challenge for the CIO to understand information within their own locus of control, when it starts to travel outside, the challenges multiply exponentially.

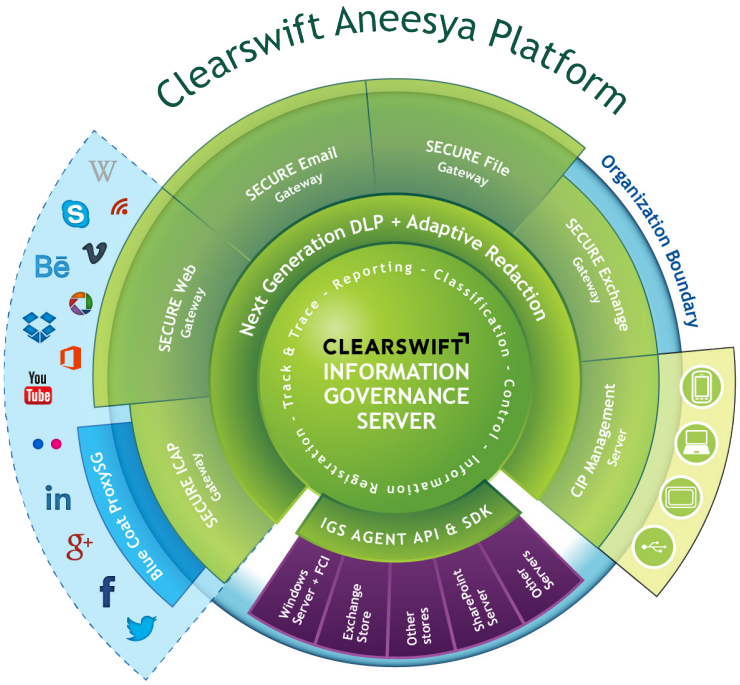

Figure 1: The Clearswift Aneesya Platform

The Clearswift Aneesya[1] Platform, see Figure 1, is designed to be a cornerstone of an Information Governance Strategy, enabling the CIO, Compliance Officers and other peers who have a responsibility to retain, secure and store critical information to take a pro-active attitude in addressing the growing complexity of internal and external operational and regulatory procedures.

The Aneesya Platform is centered around the Clearswift Information Governance Server (IGS) and is designed to work in conjunction with information sources, such as those provided by the Clearswift SECURE Gateways, which process email and web content[2]. The information sources process the data they control or manage and relay the required metadata to the IGS. The IGS then applies both policy and audit rules to the information it receives, feeding back policy actions as required. For example, an internal document containing critical information could be emailed internally and then a paragraph cut and pasted into a presentation, and the presentation sent out over unauthorized web based email. The Aneesya Platform would detect and block the sending of the presentation as well as alert the organization's Compliance Officer to the attempted breach. While detection in the past used to be solely based on key words or 'whole file' fingerprinting, the Aneesya Platform enables far greater flexibility and granularity.

[1] Aneesya: (ah-nee-see-ya) Cornish (an old Celtic language): to preserve, to secure
[2] The Aneesya Platform is extensible to enable any other information sources to be included through the use of the Clearswift Information Governance Server API and SDK.

Introduction

The Clearswift SECURE Gateways have been designed to provide best-of-breed security for email and web traffic, for both inbound hygiene and outbound data loss prevention. 2013 saw updates to the gateways to include Adaptive Redaction, a patented innovation which dynamically removes only the content that breaks information security policy while leaving the rest of information to continue to its destination unhindered. Clearswift also introduced two new gateways; the first is the Clearswift SECURE Exchange Gateway, which enables Deep Content Inspection (DCI) and Data Loss Prevention (DLP), with Adaptive Redaction, to be applied to internal email. The second new gateway is the SECURE ICAP Gateway, designed to enable Clearswift DCI/DLP to be applied to any ICAP compliant boundary device, for example web gateways from Blue Coat.

2013 also saw the introduction of the Clearswift Information Governance Server; this is fully integrated into the Clearswift Gateway solutions and is the intelligence engine of the Clearswift Aneesya Platform.

This paper introduces the concepts and ideas behind the Aneesya Platform as well as giving details of some of its key features, such as Adaptive Redaction and information discovery and tracking through the Information Governance Server.

Business Trends

In today's business environment we are witnessing considerable change, from the way that business is carried out, to the way in which IT is delivered. These changes bring with them not only increased business agility, but also increased business risk. The risk is to the critical information an organization holds and the way it is securely managed. Failure to manage information frequently damages the corporate brand as well as harming competitiveness and customer loyalty. Media stories relating to mismanaged information are a regular occurrence and the problems are getting worse. But before we can identify a solution, we first need to examine some root causes in the business trends and the risks they create.

While there are many new business trends, they share one thing in common – easy access to corporate information. With this access comes greater risk through loss of control of the critical information.

Cloud Computing

Top of the buzzword list; cloud computing offers a fast and easy implementation of IT solutions which cannot be installed in-house at the same price point, flexibility of operations or in the timely manner that the organization requires. Missing out on 'the cloud' can mean missing out on vital business opportunities. Yet for many organizations, the risks still outweigh the benefits. The cloud offers little control over access or security policies, or over who can see your information and when. Changes in organization structure or roles often results in complacency of policy enforcement providing more people to have inappropriate access and control than necessary.

Social Networking

Social networking used to be seen as 'social' and not connected to 'business', however there are very few organizations today who do not have a presence on social networking platforms such as Twitter, Facebook and LinkedIn, amongst others. Furthermore the presence is not a cursory one; it is used as a communication and commercial platform to customers, suppliers and partners. Significant information is circulated using the platforms and when it has happened, there is nothing an organization can do to control its connected movements. A blanket ban on use is not practical as there are good business reasons for use, so preventing unauthorized sharing of critical information is the only way in which control can be asserted.

BYOD

'Bring your own device' is a trend driven by employees using their own (often far superior) hardware to carry out their corporate work. Although this frequently provides organizations with a more cost effective IT solution, it also gives the CIO more headaches – specifically around information security. It is considerably more difficult to assert control over critical information which is viewed or shared on the proliferating next-generation devices and cloud services than it has been over corporately owned devices. As mobile working practices become commonplace for business agility, there is a misnomer that needs to be challenged and addressed by organizations to clearly understand the limitations that mobile device management (MDM) provides to deliver adequate levels of security for both the device and information being utilized.

Collaboration

The desire to collaborate for organizations and individuals has grown in tandem with the adoption of cloud, social networks and mobile working: the ease with which documents can now be shared internally and externally can significantly improve the efficiency of working practices within a business. However, many companies that wish to collaborate in this way are deterred by the security implications. Once again, critical information can become lost once the data leaves the organization and moves beyond the control afforded by use of corporate devices.

From a security perspective, these new business practices have a potentially negative impact; it is the combination of these trends that gives today's businesses their agility and competitive edge. Not engaging with, or blocking them is not an option as this portrays a negative attitude to evolutionary practices. Data can be created on employees' own devices and then uploaded to the cloud for collaboration with others. Control over the devices, and more importantly the information, has shifted from the IT organization to the individual. The result is substantially increased business risk – and one the organization needs to reflect on and address. Which information is critical, where is it, who has access – is it adequately protected?

Business Risks

All businesses run on risk, without risk there is no benefit. It is how organizations manage risk which helps give them the competitive advantage. Today it is information which creates business advantage but accompanying it are multiple risks. The Aneesya Platform is designed to help mitigate the next generation of information risk that organizations are required to deal with.

Data Loss

The biggest information risk facing businesses today is data loss. Not only does data loss frequently result in regulatory fines, but it can also incur substantial additional costs associated with reputation damage[3]. Another concern is the possibility of losing intellectual property to competitors. While it's crucial for an organization's success to allow their employees to communicate in a free and collaborative manner, social-networking tools pose significant risks to organizations that don't protect themselves. While 40% of losses are attributed to malicious behavior[4], the overwhelming majority of data loss comes from inadvertent or accidental incidents.

Lack of understanding as to the value of different types of information, and where the sensitive or confidential information is, coupled to how it flows through an organization, ensures that data loss remains a board-level issue for organizations large and small. Without this understanding, it is difficult for organizations to put in place the appropriate security measures.

Advanced Persistent Threats

The next generation of malware is the APT or Advanced Persistent Threat. This is the 'replacement' for computer viruses of old, and while viruses are still a threat, these threats target specific companies and individuals with the aim of stealing information, including intellectual property, to sell for profit or disrupt commercial operations for political and competitive reasons. Viruses are usually detected using statistical analysis based on the fact they have been observed thousands or millions of times. The APT is most often a 'one-off' and so statistical analysis based on observation is not applicable.

Phishing and spear-phishing are the weapons of choice to begin the attack, and small- to medium-sized companies (those that tend to have less robust security policies in place) are particularly vulnerable. All information has a value to someone; not understanding where the business critical information is stored, makes it very difficult to adequately protect it. The rise of the APT has moved the focus for security away from systems, to the information they hold. Keeping the information secure, which leads to the reduction in risk, and the ability to track and trace its progress inside and across the organizational boundary, is critical for good governance and compliance.

[3] Ponemon Institute cost of data breach, http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher
[4] 2011 ITRC Breach Report, http://www.idtheftcenter.org/artman2/publish/headlines/Breaches_2011.shtml

Compliance

The issues surrounding data loss incidents, particularly those relating to Personally Identifiable Information (PII), healthcare (PHI) and financial information, for example credit cards (PCI), have resulted in increased legislation and compliance requirements for all businesses, including government bodies. The rules and regulations are expanding to include new guidelines on the reporting of security incidents, including those relating to Intellectual Property.[5] This increases the pressure on organizations to better understand not only where their information is, but also how it got there and who has access. The ramifications of non-compliance, including substantial financial penalties, can be ruinous.

Business is changing the way it operates, embracing new working practices and technologies. But these in turn have created a 'catch-22' situation. Information sharing is not being controlled or regulated, placing it at odds with the increased emphasis on compliance. The collaboration tools required to operate successfully in today's business environment create opportunities for APTs to strike at the heart of the business and steal information across organizational boundaries.

There is a renewed requirement for better understanding of, and clearer controls over, the information a business holds; a need for more comprehensive information governance.

What is Information Governance?

Information Governance, or IG, is an emerging term encompassing a set of policies, tools and controls that turn corporate information from a potential liability into a trusted, strategic asset. It is a relatively new concept, as yet there is no standard definition, but essentially IG ensures necessary safeguards for, and the appropriate use of, an organization's information. A significant consequence of the emergence of IG is the creation of new roles within an organization. The traditional role of CIO has been augmented with that of CISO (Chief Information Security Officer) and more recently DPO (Data Protection Officer). While closely allied to IT, these new roles tend to report to the Board through other business units, such as legal, audit and finance.
The decoupling of IT from the protection of information demonstrates the intrinsic value of information across all levels of an organization. Addressing every phase of the information life-cycle and information supply chain, IG enforces best practices for the creation, use, archiving and deletion of corporate data.

The Clearswift Aneesya Platform

The Clearswift Aneesya Platform (CAP) is a comprehensive solution addressing many of the information governance requirements faced by organizations today. By undertaking Deep Content Inspection (DCI) within data communication flows, such as email, web and social networking tools, as well as data at rest, CAP enables organizations to identify, manage and protect their critical information, whether it's stored within an organization's perimeter or within cloud applications and services. The CAP classifies and monitors data according to the organization's own classification rules. This in turn enables organizations to ensure compliance, protect information against data leaks, enforce data usage policies, identify data duplication and manage obsolete documents. Unlike other solutions, the Aneesya Platform can be implemented in an evolutionary manner allowing the customer to focus initially on the areas where they perceive the biggest risks to be.

For many organizations the sequence which the implementation occurs is based around the risks that have been defined. While there is no single 'correct' order, the most frequent approach is:

1. External email (as information moves across the organizational boundary)
2. Internet traffic (as files are uploaded and downloaded, including to web sites, cloud collaboration platforms, internet based email and social networking sites)
3. Internal email (as information moves around the organization)
4. At the endpoint (where information is created and stored)
5. Internal collaboration and file sharing sites
6. Custom applications

[5] SEC, CF Disclosure Guidance, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

A Platform Approach

The CAP is an open platform and therefore is apposite for technology partners and customers to extend. Current Clearswift gateways are excellent at capturing the information flows in and out of the organization, but in order to be comprehensive, the internal information also needs to be taken into account. An API/SDK is available to enable third parties to integrate with the IG Server and the platform overall.

While the initial release focuses on integration through the Clearswift Gateways, subsequent releases will see other major sources of information, for example SharePoint, being integrated into the Aneesya Platform. With the API, there is no reason why any application cannot be included, including cloud based and proprietary solutions developed in-house or by system integrators and technology partners.

Information Discovery and Tracking

The explosion of information within an organization today, coupled with myriad of different devices that it can be accessed and stored on, makes it increasingly difficult to answer the most basic of questions: where is my information? Who has access to it? And how did it get here? The CAP monitors information as it flows through and across an organization and supports new methods of detecting critical information. This equips businesses with greater understanding of their information flows, while the new detection methods support improved accuracy and reduced false positives when detecting critical information. The CAP supports the use of full and partial document matching techniques, enabling snippets of information to be detected across various document formats, as well as legacy keyword based and regular expression content detection.

Users are able to register sensitive documents either manually or automatically, based on rules, in order to indicate their sensitivity. If a registered document, or any fragment, is detected being communicated in a manner that breaks policy - for example in an email or a tweet – an action, or series of actions, will be carried out according to the defined policy and the security event logged. Fundamentally, the potentially damaging data loss will be prevented. See Figure 2: A Clearswift Aneesya Platform example, where CAP automatically prevented damaging data loss through its deep content inspection and associated policies.

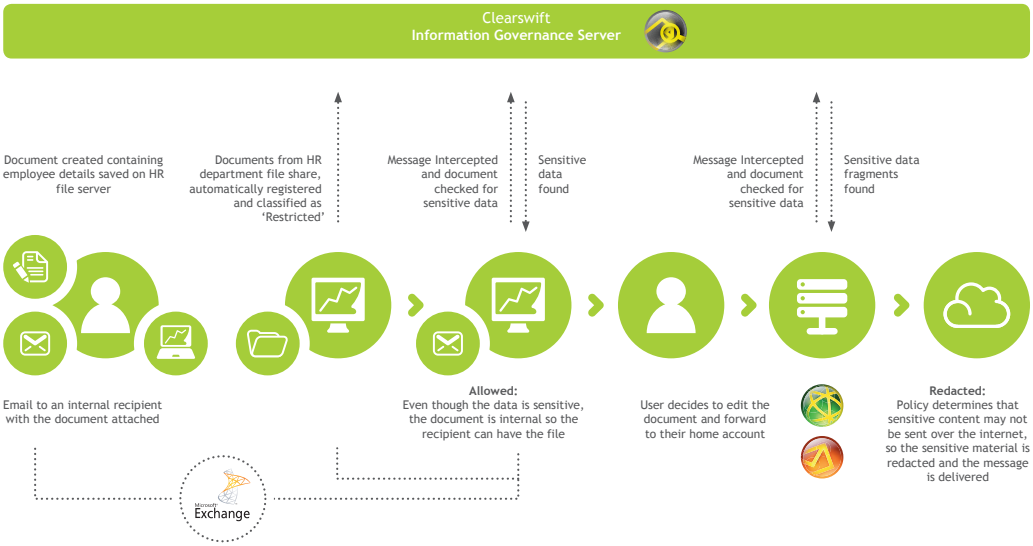

Figure 2: An example Clearswift Aneesya Platform deployment configuration

The initial release of the CAP includes support for the Clearswift SECURE Gateway suite of products, including the SECURE Exchange Gateway that integrates with Microsoft Exchange for internal email.

All information submitted to the CAP, regardless of the communication channel, undergoes Deep Content Inspection (DCI) in order to create information fingerprints – not just at the file level, but also at the sub-file level. These, coupled with metadata are extracted and stored in the IGS database. It is this data that is used to track the information flows as well as driving policy-based actions.

One of the CAP's key features is its ability, through the Clearswift Gateways, to transform information to meet policy. We call this process Adaptive Redaction. For most organizations, protecting their information is of paramount importance and so DLP solutions are used. However, standard DLP solutions suffer from a 'stop and block' behavior which when coupled with 'false positives' means that they are seldom fully deployed as these actions cause business disruption and commercial negativity. Adaptive Redaction offers an alternative to 'stop-and-block' by removing only the piece of information that breaks policy and letting the remainder continue to the recipient unhindered, encourging a secure continuance of collaboration.

A Platform Approach

Adaptive Redaction is the removal or transformation of data according to policy (rules), to ensure that information complies with corporate information security policies before it is sent to the recipient (person or system). By employing adaptive redaction, organizations can enable safer, more effective collaboration – in the cloud, external to the organization. Traditional DLP solutions are a simple 'yes' or 'no' to sending information. Adaptive Redaction removes this barrier by modifying the information according to policy to ensure only the acceptable levels of information is shared, and that critical information remains safe at all times.

Adaptive Redaction consists of multiple functions[6]. These include:

Text Redaction	The automatic removal of keywords or phrases. For example, the removal of sensitive project references in a document attachment sent within an email or via cloud storage outside of the organization. Or the removal of expletives from social network pages that enter the user's browser. Specific pieces of information, tokens, can be detected and removed via text redaction, such as credit card numbers. For example, sharing an order with a supplier becomes a seamless process when the CAP removes an overlooked credit card number from the original purchase form.
Document Sanitization	For many organizations, the existence of meta-data and history information in documents is a potential source of data leaks. The CAP detects and removes or modifies meta-data, revision history and selected properties associated with multiple document types.
Structural Sanitization	The automated removal of content that could contain malware, viruses or critical information including objects such as macros, scripts, embedded executables and other active content items.
Encryption	The SECURE Email Gateway also supports encryption. This is fully automated and ensures that critical information is encrypted, based on policy, before it leaves the organization. Encryption can be carried out in several ways, from the transport layer (TLS) through to PKI, application of certificate-based encryption, ad hoc password encryption and even portal based encryption.

The key to any information security policy is the automatic, consistent application of the policy. The Adaptive Redaction and encryption options enable this to happen – with complete transparency to the user.

Further enhancements to the CAP will see enhanced control of critical information when it is outside an organization's locus of control.

[6] Adaptive redaction features are licensable options.

Reporting

As well as the ability to carry out proactive real-time policies based on deep content inspection, including Adaptive Redaction, another key feature is reporting. Flexible reporting within the CAP enables delivery of the solution with a number of pre-prepared reports and the ability for customers and/or professional services to easily create customized reports.

Out-of-the box, pre-defined reports are available, for example information analytics reports can be used in post-event security analysis. One example is to show information provenance to help the organization's Compliance Officer or Data Protection Officer to understand which pieces of information are being communicated most frequently and to whom. This answers the questions, "how did this information get here", "where did it come from and go to" and who else has seen it".

The open platform has a well-documented database schema enabling customers to use their own reporting tools. This enables CAP to be readily used as part of a compliance program as well as in response to data breaches.

Direction Agnostic

Information flows through and across organizations via multiple communication channels. It's equally important to protect and track information flowing into and around an organization as information flowing out. While the policies associated with the direction flow may be different, the CAP utilizes the same deep content inspection technologies and analysis to assess the data and apply appropriate content aware policies.

For many organizations these days, having a blanket policy to remove active content (aka Structural Sanitization) from incoming documents is crucial to preventing infection by APTs. Similarly, a blanket policy to remove document meta-data and revision history on all documents leaving the organization is also frequently used to prevent inadvertent data leaks.

CAP is not just about email, it also protects the organization from information sent or received through the Internet, including via social networking and cloud collaboration sites.

Deploying the Clearswift Aneesya Platform

The Aneesya Platform is a combination of products and solutions. The key to its operation is the **Clearswift Information Governance Server** (IGS). This acts as the central repository for registered items, and stores the metadata from the various information sources including those relating to tracking the information. As with other Clearswift products, IGS integrates with an LDAP service, such as Microsoft Active Directory, to enable users and roles to be set up in a granular manner. Polices for access to the system as well as those defining actions on detected security events are also configured within the IGS solution.

The Aneesya Platform requires information sources to feed data into IGS and to carry out policy actions. Clearswift provides several compatible products:

- **Clearswift SECURE Email Gateway**: For track, trace and control of critical information through email across the organization boundary.
- **Clearswift SECURE Exchange Gateway**: For track, trace and control of critical information through email inside an organization.
- **Clearswift SECURE Web Gateway**: For track, trace and control of critical information through the Internet across the organization boundary.
- **Clearswift SECURE ICAP Gateway**: For track, trace and control of critical information through ICAP enabled boundary devices.

For existing Clearswift customers with SECURE Gateway solutions already deployed in their environment, it is only a case of installing and configuring the Clearswift Information Governance Server and then a license key can then be provided to the existing products in order for them to connect to IGS.

For further information on the IGS API / SDK and the ability to integrate other applications into the Aneesya Platform please contact Clearswift.

Use Case: Intelligent Information Protection

The Clearswift Gateways are capable of detecting specific content, whether it's in email or web traffic, and blocking it. However, the addition of the CAP facilitates a more intelligent approach to sharing information outside the organization. A simple change to the data can make it acceptable to share, enabling information to flow more freely. Based on the organization's information security policies, this may involve selectively removing a document from a zip file in an email attachment. Or it could be that a document contains sensitive information that needs to be removed before the document can be shared. In this scenario, the CAP would be able to perform some adaptive redaction on the words to remove them.

For example, an order needs to be shared with a supplier, but the credit card information has to be removed for PCI compliance. DCI would detect the credit card information, and the CAP would remove it before it was sent to the supplier.

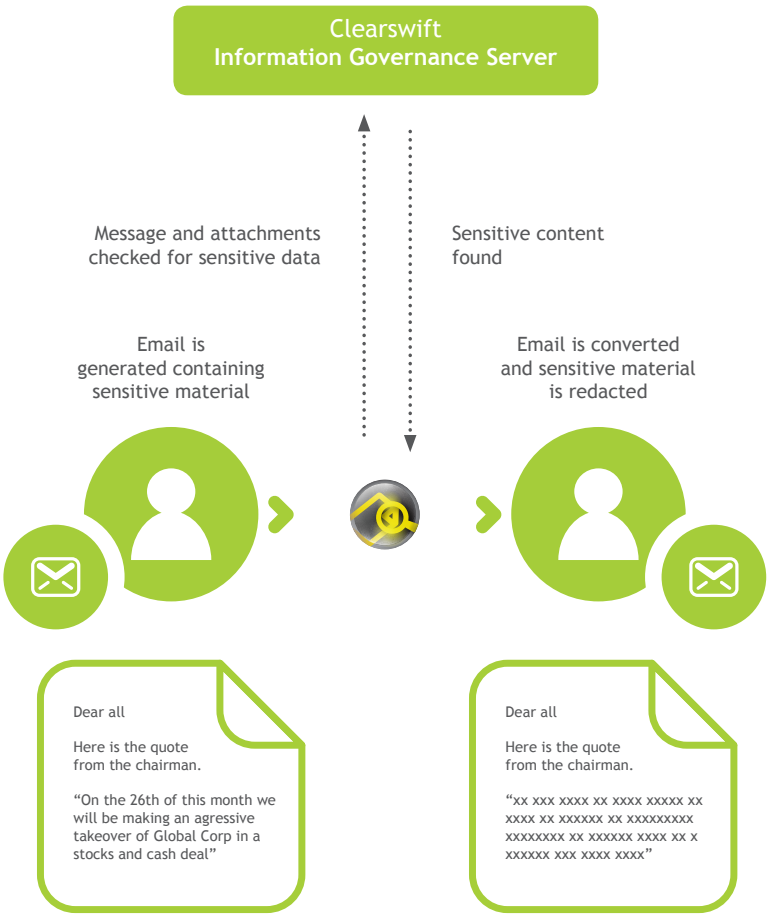

Figure 3: Adaptive redaction in practice

Use Case: Post-Event Information Forensics

By monitoring all the email entering, leaving and moving around the organization, all the browser traffic and even what gets created on file servers, the Clearswift Aneesya Platform enables an organization to develop a deep understanding of information flows.

In the event of a data leak, the Aneesya Platform would not only be able to show the flow of information around the company, but also who was involved, and when. Imagine the situation (see Figure 4: Information provenance analysis), where a file containing sensitive data is created by an employee, who then forwards it to two others, who each in turn edit the file and forward it on to several more. Some of these people then try to copy the data onto their Dropbox account or try sending part of the document in an external mail.

With the Aneesya Platform fully implemented, an organization can report on that original file and all of its derivatives, creating a report on the provenance of the information showing who had access to the data, when they had the data and most importantly what they did, or tried to do, with it.

Figure 4: Information provenance analysis

Summary

The Clearswift Aneesya Platform is a significant advance in delivering an Information Governance program. The platform is compatible with existing Clearswift products enabling existing customers to continue to utilize and augment their existing investments.

The ability to track, trace and control information across the enterprise as well as across the enterprise boundary, helps in both real-time detection of data breaches, as well as after-the-fact governance and compliance reporting.

By delivering the technology as a platform, Clearswift has enabled any organization the ability to integrate their specialist information sources into the platform.

About Clearswift

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Built on an innovative Deep Content Inspection engine, our unique Adaptive Redaction technology enables deploying a data loss prevention solution simply and easily, forming the foundation of an Information Governance vision, for organizations to have 100% visibility of their critical information 100% of the time.

Clearswift operates world-wide, having regional headquarters in Europe, Asia Pacific and the United States. Clearswift has a partner network of more than 900 resellers across the globe.

More information is available at **www.clearswift.com**

CLEARSWIFT
ADAPTIVE CYBER PROTECTION

UK - International HQ

Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire
RG7 4SA

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support:
+44 (0) 118 903 8200
Email: info@clearswift.com

Australia

Clearswift (Asia/Pacific) Pty Ltd
5th Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA

Tel: +61 2 9424 1200
Technical Support:
+61 2 9424 1210
Email: info@clearswift.com.au

Germany

Clearswift GmbH
Landsberger Straße 302
D-80 687 Munich
Germany

Tel: +49 (0)89 904 05 206
Technical Support:
+49 (0)800 1800556
Email: info@clearswift.de

Japan

Clearswift K.K
Shinjuku Park Tower
N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
Japan

Tel: +81 (3)5326 3470
Technical Support:
0066 33 812 501
Email: info.jp@clearswift.com

United States

Clearswift Corporation
309 Fellowship Road, Suite 200
Mount Laurel, NJ 08054
United States

Tel: +1 856-359-2360
Technical Support:
+1 856 359 2170
Email: info@us.clearswift.com