actiance™

Information Governance for Social Business

Unleashing the Full Potential of Enterprise Social

Executive Summary

Social business platforms have exploded onto the scene the last few years. Also known as "social software," "enterprise social software," and "social collaboration software," these platforms are riding the social media wave. Essentially, these platforms are bringing the collaborative and engagement aspects of social media into the enterprise.

However, holding back much broader adoption of social business tools are regulatory and compliance concerns. Given the intense interest social media is generating, regulatory bodies and the courts are issuing more specific guidance pertaining to social media and social business. While collaboration platforms offer a wide range of capabilities, they lack critical governance capabilities not natively addressed by today's social business platforms.

This paper will address potential gaps in compliance, explain how organizations can minimize risk, and outline best practices for information governance in today's social business platforms.

- **Potential gaps:** Organizations that utilize collaboration technologies without taking into account regulatory, legal, and corporate mandates may expose themselves to significant and unnecessary risks.
- **Risk mitigation:** Organizations can lower their risk profile, which spans brand, reputational, and legal aspects, by deploying complementary technologies to address social business platforms' functional gaps.
- **Best practices:** Developing a set of best practices for information governance ensures that a template can be established for continued adherence to regulatory, legal, and corporate requirements.

Information management technologies, such as Actiance Vantage, enable organizations to meet their critical governance requirements and realize the full potential of enterprise social software.

The Emergence Of Social Business

Over the past decade, organizations have been shifting an increasing number of enterprise tasks and content over to collaboration platforms like Jive, SharePoint, Connections, Yammer, to name a few. Additionally, enterprises are now leveraging these platforms' social media capabilities, such as managing documents, posting relevant group updates and collaborating on projects in real time. (i.e., basically anything that facilitates collaboration and enhances employee productivity).

The growth of these platforms is reflected in the following data points:

- Enterprise Social Software space is expected to reach $2 billion by 2014 (Source: IDC)
- Among all of Microsoft's server offerings, SharePoint achieved $1 billion in annual revenue in the shortest amount of time.
- Microsoft acquired Yammer for $1.2 billion (June 2012)
- 61% reduction in time spent on compliance activities through the use of Traction software (Deloitte Center for the Edge Study, March 2011)

The bottom line is that many stakeholders have benefited from the growth of social business platforms.

Gaps Of Native Social Business Platforms

While social business software offers a broad swath of capabilities, there are a number of areas where the lack of native features creates risk for the organization:

- **Real-time information management**
  The inability to capture content in real-time creates recordkeeping gaps, which have regulatory, legal, and corporate governance implications.
- **Data leak prevention**
  The absence of content-inspection features exposes organizations to the potential loss of sensitive or confidential information.
- **Brand integrity**
  The lack of real-time alerts endangers the corporate brand and reputation should inappropriate content be posted.
- **ROI maximization**
  The absence of granular, contextual capture of social business content increases IT and operating costs by archiving too much content and prolonging eDiscovery efforts.

In short, even though social business software is a robust platform in its own right, there are still several information management requirements yet to be satisfied.

Information Management Considerations

Given the vast amount of corporate data stored in most collaboration environments, it should be clear that collaboration content must be treated in accordance with governance best practices. Corporate information must be managed properly for a variety of reasons, namely those pertaining to regulatory, legal, and records management concerns.

Corporate Governance

There is increased interest among organizations for exemplary corporate governance in light of new compliance regulations and statutes as well as some high-profile scandals over the past fifteen years (e.g., Enron). Consequently, organizations are paying more attention than ever before to developing sound corporate governance strategies, which must encompass a few key elements:

- **Records management—** having the appropriate policies in place regarding retention periods, litigation readiness, privacy, etc.
- **Information security—** ensuring that corporate records are in tamper-proof, easily accessible repositories
- **Data disposition—** ensuring the defensible disposition of data when it is beyond the retention period or is no longer worth keeping

Organizations are extremely protective of their intellectual property and have strict policies and systems in place to protect against this type of loss. Examples of policies that need to be enforced include restricting feature access to certain individuals, protecting against unauthorized external access, and outlining what can happen with sensitive material that is created, stored, or even removed.

Well-managed organizations also have corporate policies and systems in place to stop inappropriate content from being distributed, prevent the creation of certain types of content, and have an audit trail of all relevant activity. Ideally, notification of any breaches or posting of inappropriate content are dealt with in real-time in order to mitigate risk. Hence, corporate policies are instrumental in an organization meeting its governance requirements.

Legal Policies

Legal holds (aka "litigation holds") require organizations to preserve all data that may relate to a legal action involving the company. Legal holds are designed to ensure that all data in question will be available for the discovery process prior to litigation. It is thus critical to capture original content as well as any deletions or alterations to it. Furthermore, the content must be stored in a tamper-proof environment.

An organization must preserve records as soon as it learns of pending or imminent litigation or when litigation is reasonably anticipated. A legal hold prevents spoliation, which can have huge consequences for one or both parties. Legal holds not only apply to paper-based documents but also to all electronically stored information (ESI) that could be relevant to the case, no matter where it may be stored.

Therefore, once the legal hold order is issued, organizations must take the necessary steps to ensure that potentially relevant information not be deleted, even if it is scheduled for deletion in accordance with the company's records management policy. Moreover, companies are legally obligated to retain documents and records until otherwise notified.

A related aspect, **eDiscovery**, refers to any process in which ESI is sought, located, secured, and searched, with the intent of using it as evidence in a lawsuit.

The Federal Rules of Civil Procedure (FRCP) lays out two key rules that are at the heart of eDiscovery:

- **Rule 26—** Spells out the requirements for the discovery and production of documents, email messages, attachments, and other electronically stored information for civil litigation in federal court cases
- **Rule 34—** Mandates a timeframe for production of such information as well as specific provisions for privileged information

In litigation, an organization must comply with discovery requests from attorneys for documents (e.g., spreadsheets, slide decks), email messages, conversation threads, and other information that may shed light at what happened at some point in the past. Companies are given a set timeframe in which they must respond or risk getting sanctioned.

Because of the emphasis on tracing responsibility and establishing cause in litigation, a detailed audit log showing who created and accessed the various types of content is essential. To minimize the financial impact of eDiscovery, it is important that the appropriate amount of information be retained – not too much so as to drive up legal costs and not too little so as to raise suspicions of spoliation (i.e., destruction, alteration, or mutilation) of evidence. Moreover, information should be presented with associated data to give meaning and context to the findings.

Regulatory Compliance

Many organizations are subject to regulatory requirements, which mandate specific approaches for managing corporate data. The following is a sampling of the many regulations with governance implications:

- **Sarbanes-Oxley (SOX)** enumerates the various controls required for dealing with financial information.
- **The Health Insurance Portability and Accountability Act (HIPAA)** establishes various rules for handling and securing Protected Health Information (PHI). Ensuring privacy and confidentiality of patient health information is a primary focus of HIPAA but has been expanded in recent years to include a wide range of firms, including healthcare providers, benefits administrators, and others.
- **The Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA)** issued rules and guidelines for firms in the securities industry in order to prevent fraud and other financial wrongdoing. These standards encompass supervision, record keeping, and suitability issues, among others.
- **Data breach notification laws (e.g., PCI DSS)** require that government agencies, businesses, and individuals that store personal information on a computer system advise the affected entities if the data has been, or is believed to have been, accessed by unauthorized parties. A data breach is typically defined quite broadly, encompassing everything from a hacker's attack, in which information is stolen, to a missing backup tape that contains unencrypted information.

What's At Stake?

In light of the above considerations, it is clear that there are significant consequences for failing to manage social business content properly, including the following:

- **Brand and reputational damage** and the consequential drop in market valuation or business as customers, investors, and governments lower their perception of an organization's governance competence.
- **Legal exposure,** as customers or partners initiate litigation to shield themselves from the consequences of poor information management practices.
- **Regulatory penalties** for failing to comply with mandatory industry regulations.

Considerations for Managing Social Business

Investments in social business platforms can be maximized through the following features:

Secure, real-time capture

The ability to capture content such as Blogs, Discussion Boards, and Files in real-time ensures a full audit trail is maintained. Some technology solutions may only take point-in-time snapshots of content posted to social business platforms. However, what happens if someone posted a blog entry that contained confidential information then, upon realizing their mistake, removed the blog entry? If the point-in-time capture wasn't synchronized properly, it could've missed the uploading and deletion altogether. Hence, being able to capture content in real-time, including editing and version histories, is crucial for complete audit trails.

Granular capture of content

Policies for the capture of social business content must be flexible enough to allow for them to be applied at the global, group, or individual level. From a governance standpoint, granular policy setting and content capture is critical in order to satisfy the myriad regulatory and records management requirements of Sarbanes-Oxley, HIPAA, SEC, FINRA, FERC, and others. However, granular logging and archiving can also reduce storage costs by eliminating the capture of unnecessary content, expediting eDiscovery efforts by reducing the amount of reviewable content, and lowering corporate risk by retaining only relevant content.

Real-time alerts for potential policy violations

The ability to provide real-time alerts can prevent the publication and distribution of content that might be harmful to an organization, such as offensive language, confidential intellectual property, financial statements, draft policy documents, or other sensitive data. Furthermore, real-time alerts can protect the corporate reputation, prevent regulatory violations, and minimize legal exposure.

Contextual capture of content

Another core capability is the capture of information in its appropriate context, such as the presentation of related items in the same user interface. Contextual capture is invaluable for eDiscovery, early case assessments, or even informal management reviews of information. Moreover, contextual capture of information can substantially reduce litigation costs and limit the likelihood of sanctions arising from production delays. This feature is particularly important for eDiscovery and related requests, which often have tight response timeframes in many jurisdictions.

Flexibility for expansion

As the social business space is so dynamic, organizations can reasonably anticipate the emergence of new forms of social data that do not exist today. As a result, having an information management solution that can ingest content from any source system in real-time has compelling value for organizations with strict governance practices.

In summary, all organizations should consider the above when devising their information management strategies. Not doing so may subject the company to unnecessary regulatory or legal scrutiny.

Actiance Vantage

Vantage complements today's archiving systems by providing a level of granularity that ensures any information management strategy is executed seamlessly. Actiance's Collaboration Framework underpins the capture of this wealth of data, maintaining the context of conversations and posts and storing them natively. Additionally, the framework provides organizations the flexibility of conducting eDiscovery from the Actiance database (thus facilitating contextual review), the customer's own archive, or perhaps from a third-party archive.

Today's archiving solutions just grab all collaboration content without providing any real-time insight into the meaning of the data. Vantage's content-inspection technology features real-time alerts to detect potential loss or exposure of intellectual property and violations of corporate policy, such as the use of inappropriate language (e.g., inflammatory comments).

Benefits of Vantage

If policy management of collaboration is done effectively, significant benefits can be reaped:

- **Addresses functionality gaps** By augmenting the native functionality of today's social business platforms, Actiance ensures that organizations can safely and confidently meet their information management requirements.
- **Ensures compliance** Having the ability to do real-time, contextual capture of content greatly facilitates an organization's ability to comply with applicable regulatory, legal, and corporate policies.
- **Protects the organization** Through content inspection and real-time alerting mechanisms, organizations can ensure the integrity of their corporate brand, reputation, and sensitive information.
- **Enhances ROI** By integrating with existing archiving systems, organizations can minimize spending on additional storage and IT costs.

Best Practices

Organizations looking to establish a framework for managing their social business platform should start with these four steps.

Step 1: Assess The Risks

Corporate policies and technology selection should happen after a detailed analysis of the particular risks faced by an organization. While we have outlined some of the known risks in this white paper, most decision makers require specifics related to their organization, not generalizations. Which of the risks discussed apply to your unique situation? What rules or guidelines apply to your specific industry? How do these requirements change in light of new statutes and interpretations by regulators and the courts?

Step 2: Establish A Sound Information Management Policy

At a minimum, policies should include the rationale, the parameters, the stakeholders, and the consequences of breach. Be as detailed as possible as vaguely worded policies invite too much subjectivity.

Step 3: Enforce Policy Through Technology

Source and implement technology that enables the practical enforcement of information governance policies on a daily basis. Training and education are instrumental in making policies work, but these are insufficient without technical enforcement. Technology ensures that policies are applied consistently and even-handedly.

Step 4: Revisit And Revise Policy Frequently

Finally, new regulations, case law, or changes in company objectives will necessitate periodic revisions of an information governance policy. Making employees comply with policies that are no longer relevant or failing to make them comply with regulatory, legal, or corporate requirements altogether are reflective of poor corporate governance.

Conclusion

Enterprise social software is emerging as the dominant platform for information sharing, content management, collaboration, and social networking in enterprises today, enabling the sharing of information and collaboration across enterprise users, partners, suppliers, and customers. With this emerging role comes the responsibility to address the risks of using collaboration technologies for storing information that is likely to be subject to industry regulations, eDiscovery and legal hold demands, and records management policies.

Failure to undertake specific steps to manage this information properly is very risky, and while it saves money in the short term, is likely to result in severe costs and consequences in the future. Hence, understanding the risks, developing appropriate corporate policies, and implementing technology like Actiance Vantage to enforce those policies over time are vital to a sound governance strategy.

About Actiance

Actiance helps organizations manage, secure and ensure compliance across unified communications, collaboration and Web 2.0 applications such as blogs, wikis and social networks. Actiance's award-winning platforms are used by 9 of the top 10 US banks and 284 FINRA-regulated firms globally.

The Actiance platform allows organizations to gain visibility of applications in use, apply usage and content policies, ensure compliance, and gain valuable insights across the communications and collaboration channels in use. Actiance supports all leading social networks, unified communications, and collaboration providers, and IM platforms, including Facebook, LinkedIn, Twitter, Google, Yahoo!, AOL, Skype, Cisco, Microsoft, Jive, and IBM. Actiance is headquartered in Belmont, California. For more information, visit **www.actiance.com** or call **1-888-349-3223.**

actiance™

Worldwide Headquarters
1301 Shoreway, Suite 275
Belmont, CA 94002 USA
(650) 631-6300 phone
info@actiance.com

EMEA Headquarters
400 Thames Valley Park
Reading, Berkshire, RG6 1PT UK
+44 (0) 118 963 7469 phone
emea@actiance.com