SOLUTION BRIEF
SECURE SOCIAL NETWORKING

Helping to Secure Social Networking with CA Data Protection

ca technologies

Executive Summary

Challenge

Just when organizations in both the private and public sectors were getting a handle on how to protect their sensitive data, the era of social networking arrived on the scene, bringing with it a slew of capabilities that could put sensitive data at risk. Despite the risk, there is tremendous value that these collaborative communication channels can bring to organizations across all industries. The demand to adopt these new tools has left many security professionals scratching their heads figuring out how to empower end users to properly access and leverage these important tools to do their jobs while also preventing inappropriate information from being shared.

Organizations appear to have only two options. One option is to open the flood gates to these sites (or to offer some semblance of selective access) and accept the risk of doing so. The other option is to block employees from accessing the sites entirely, possibly inhibiting the organization's ability to interact with the market and customers, thereby potentially creating dissatisfaction and competitive disadvantage.

Opportunity

Social networking can enhance customer relationships, increase customer service, reinforce marketing campaigns, deliver important market research input, enable employee collaboration, and impact a firm's brand or perception. Organizations need a strategy to allow their end users to make use of social networking tools while mitigating the associated risks of data loss. Effective Data Protection solutions can be the means for the security team to enable these important benefits while protecting the firm's critical information assets.

Benefits

Data Protection solutions can enable the opportunities listed above by helping to:

- Lower the risk of compliance violations by preventing the release of non-public data.
- Sustain competitive advantage by preventing the disclosure of trade secrets and product roadmaps.
- Minimize the IT burden associated with identifying, tracking and reviewing suspect social networking activities.
- Enhance employee productivity by minimizing non-business activity.
- Maintain consistency when social networking channels are used.

Section 1:

Introduction to Social Networking

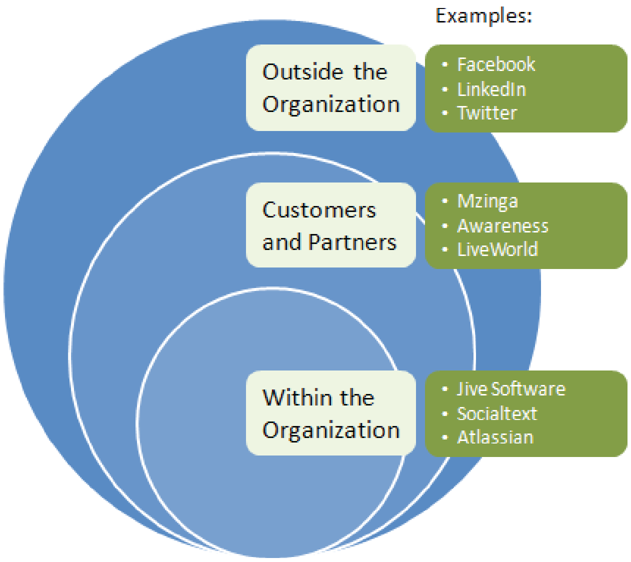
It is clear that social networking is not only a social tool, but has positive business benefits for many organizations. This transformation seemed to occur in real time. Organizations are now wondering when Facebook™ morphed from a website where students bragged about the escapades of their college lives to a multi-billion dollar entity that should be enabled and incorporated into their business processes.

Over the past few years, both the adoption rate of social networking tools and the age of the average user has increased significantly past the collegiate ranks. With global user communities of tens of millions on LinkedIn and hundreds of millions on Facebook, it's no surprise that organizations are debating if and how to support the use of such applications. Social networking could play a strategic role in corporate communication, marketing, and relationship management for employees, partners, and customers.

The social networking market no longer consists of only public websites such as Facebook, Twitter, and LinkedIn. Solution providers have begun to create social networking tools to aid organizations to serve their customers and constituents. Vendors such as Jive Software, Socialtext and Atlassian have led the march to create Facebook for business. These vendors have integrated their user-centric applications with content collaboration tools such as Microsoft® SharePoint®. Some solutions offer extended capabilities such as the ability to collaborate between customers and partners. Other vendors such as Mzinga, Awareness, LiveWorld, and Lithium are focusing more on bridging the communication gap between organizations and their customers and partners by offering user groups and forums.

Figure A.

The three social networking use cases.



As organizations expand the audience from internal to external users, the risks increase. Over the course of this paper, we will discuss these deployment methods, the pros and cons of each, and relevant security policies for protecting the data in each of these environments.

Section 2: Challenge

Why Are Organizations Struggling With Social Networking?

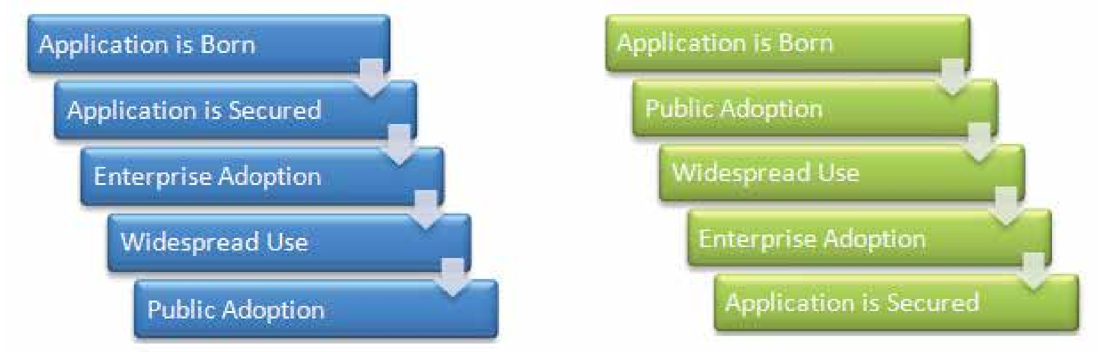
Organizations are forced to make a decision on how they manage social networking. By enabling their employees to use these communication channels, they are exposing themselves to security risks. Blocking employees from accessing the sites inhibits the business from taking advantage of new marketing channels, gaining market knowledge and communicating staff and corporate expertise to an interested community.

Organizations are experienced at securing “the known” such as business applications, employee and contractor identities, business processes and corporate networks. They incorporate industry best practices to protect and secure these assets while also working to meet various compliance and regulatory guidelines. Organizations leverage corporate security policies and processes to protect the assets that they actively manage, and can measure their success in doing so. Prior to purchasing and deploying a business application or other technology solution, IT performs thorough due diligence. The IT and security teams may execute a proof of concept, compatibility tests, and even run a full implementation in a test environment. Only once they are satisfied with performance and the ability to secure its use is an application deployed to the organization. The “unknown” is what puts a scare into security professionals because of the potential to compromise an organization’s security posture. Some examples include unknown application vulnerabilities, unmanaged users, new malware threats, and unreported data loss events.

An unfortunate reality of social networking applications is that they were not architected with the foresight to secure sensitive corporate data. Organizations have little to no control over both their use and the content posted to and shared on these sites. Unofficial or unregulated use of popular networks like LinkedIn, Facebook, and Twitter for business purposes and industry networking is pressuring organizations to formally adopt and govern their use.

Figure B.

Adoption lifecycle differences.



The adoption lifecycle is generally dramatically different between traditional applications and social networking tools.

Security teams are caught in a difficult situation. If they succumb to pressure from the business and allow users to utilize social networking tools, they will have few programmatic controls in place to mitigate the risk of sensitive data loss and disclosure. If internal security blocks the use of social networking tools, the business will likely give them an earful as that action could be responsible for inhibiting strategic business activity and hurting competitiveness.

Section 3: Opportunity

How Do Firms Leverage Social Networking Tools?

The use of Social Networks varies from one organization to another. Organizations are using them to communicate with their customers or partners, show leadership, create brand awareness, execute viral marketing campaigns, and foster collaboration among their employees. Considering these goals, social networking tools could be used in the following ways:

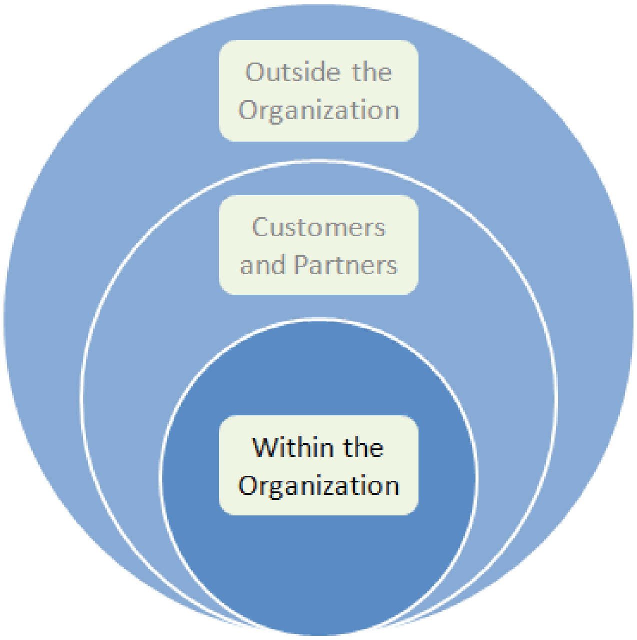
- Social networking within the organization
- Social networking with partners and customers
- Social networking outside the organization

Social networking within the organization

In this use case, an organization deploys a social networking application only for internal use. This stretches beyond the scope of traditional collaboration tools such as Microsoft SharePoint by focusing more on the user rather than the content in the system. Each user can create a profile, share information and create relationships with other users within the organization. These tools can integrate with other internal applications and corporate processes. Examples of these tools are Jive Software, Socialtext, and Atlassian.

Figure C.

Use Case 1: Within the Enterprise



The use of these tools is growing in large organizations where "subject matter experts" need to be quickly identified, contacted and engaged. Global Systems Integrators are good examples of these types of organizations. If a consultant encounters an issue at a customer site, the consultant could leverage their internal social network to find a colleague with the required level of expertise to resolve the issue. These tools also provide a social dimension by helping to build relationships between co-workers with common interests such as sports, literature, and travel.

Primary drivers:

- Organizations desire to enable the collaboration and productivity benefits of social networks. However, they are not comfortable exposing the organization to "public" tools, such as Facebook, due to the potential for data loss and other security violations.
- Publicly available tools lack organization business features such as the ability to tailor user profiles to promote skill sets, control access and content, and integrate with other internal systems and processes including organization collaboration tools and user store.

Pros	Cons
▪ Low-risk approach to initiating a "social networking" strategy for the firm.	▪ Customers and partners are not included.
▪ Realize the benefits of social networking within the firm with no related security risks.	▪ The need to provide secure access to LinkedIn, Facebook, and Twitter is not addressed.
▪ Deploying a private "social network" enables a firm to familiarize itself with the nature of the application.	▪ ROI can be difficult to articulate.
▪ This approach can often be extended to include partners and even customers.	▪ Deployment and user education costs can be significant.

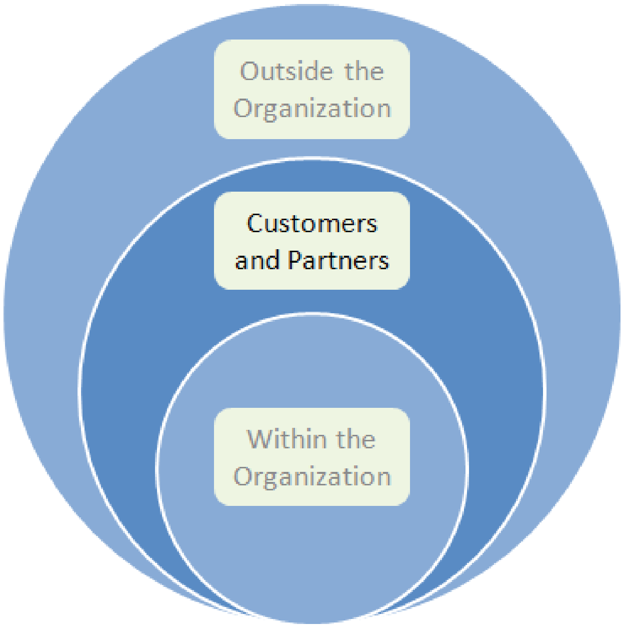
Recommended security policies to protect social networks used within the organization:

- **Privileged and legal content.** Protect the firm by identifying questions or topics concerning the legality of content posted to social networking sites. When this kind of content is identified, the appropriate legal representative should be alerted.
- **Termination or layoff discussions.** Restrict communications concerning potential and pending terminations and layoffs.
- **Confidential projects.** Teams within an organization may need to share materials that are proprietary to their team. This content should be protected from leakage to other employees.
- **Merger and acquisition plans (a type of non-public information).** Protecting data pertaining to pending or proposed merger and acquisition transactions is often a regulatory requirement and, if breached, could lead to substantial sanctions and fines.
- **Inappropriate or otherwise harassing language.** Enforce policies and standards as defined by Human Resources.

Also, when used within the organization, security teams should use an Internet access management solution to closely control authentication and access to social networking tools as well as other Web applications and portals.

Figure D.

Use Case 2: Customers and Partners



Social networking with partners and customers

In this use case, organizations wish to use social networking to communicate with customers and partners. This can be considered a logical progression for firms that have deployed social networking for internal use. Or, a firm may wish to create "Social Communities" to allow their customers to socialize their issues with other customers as well as with company delegates. Vendors who offer these types of social networking environments include Mzinga, Awareness and LiveWorld.

Primary drivers:

- Organizations need to promote their brand and reputation with partners in order to keep ahead of the competition. Partners appreciate tools that make communication easier and faster with their suppliers.
- Firms need to both attract and retain customers, in particular the ones who are technologically savvy. Easily accessible tools that are similar to popular public social networking communities can drive these goals.
- User forums can create tight relationships between a company and its customers by allowing customers to express concerns and to collaborate with other customers. These forums can also lead to greater levels of satisfaction and retention.
- Partners appreciate simple and easily accessible means to conduct business with their "suppliers." Social networking tools can provide partners a quick and secure way to share information.

Pros	Cons
▪ Improve relationships with customers and partners; improve satisfaction with specialized services.	▪ Access is closed to "outsiders." Collaboration and research is not possible for parties interested in participating, but who are not yet "members."
▪ Cost of doing business can decrease while speed increases.	▪ Customers could potentially discuss pricing and other customer-specific data.
▪ Ability to evangelize to customers via blogs, user forums and wikis.	▪ Inhibits marketing to new customers and partners.
▪ Organizations will be perceived as "innovative" by offering these tools.	▪ Does not allow prospective customers to interact with current customers.
▪ Security is not compromised as users and their access are controlled.	▪ Does not address the demand for the use of open sites like LinkedIn, Facebook and Twitter.
▪ Company can use such a tool as a competitive differentiator.	▪ Accidental sharing of sensitive data between customers and partners.

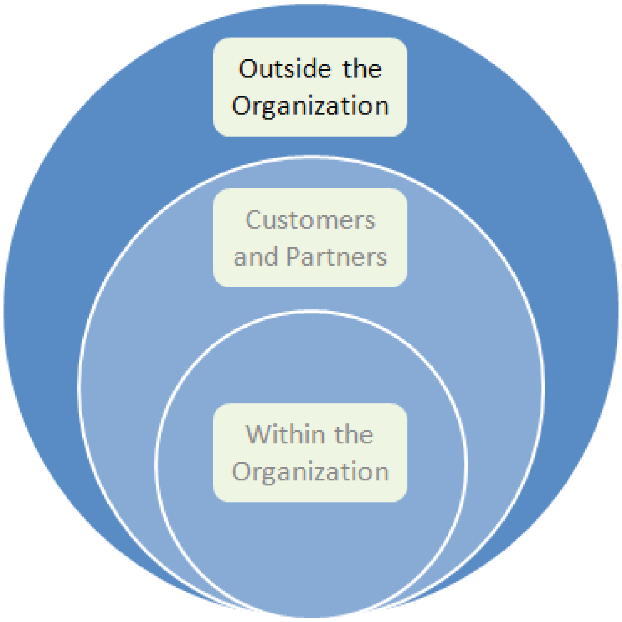
Recommended security policies to protect social networks among partners and customers:

- **Privileged and legal content (as defined above)**
- **Termination or layoff discussions (as defined above)**
- **Confidential projects (as defined above)**
- **Merger and acquisition plans (as defined above)**
- **Confidential trade data.** Organizations must protect various forms of confidential information including trade secrets, proprietary business processes and product designs and roadmaps so that this information is shared or made available only by parties who have the right permissions.
- **Inside information.** Organizations need to prevent non-public company information, such as management discussions and financial results, from being posted to and shared on social networks.
- **Guarantees and assurances.** Guarantees, though often considered a part of "fair and balanced" communication, carry with them legal, regulatory, and financial risks, as well as risks to a firm's reputation. This includes contract changes or promises related to contract terms. Organizations should detect unauthorized guarantees or assurances and prevent them from reaching customers.
- **Unprofessional customer interactions.** Organizations should analyze communications for indications that a company representative responded to a customer in an unprofessional or un-empathetic manner. This enables consistent interactions, a positive reputation, and high levels of customer satisfaction.

Also, when extended to partners or other known users outside the organization, security teams should leverage an Internet access management solution to control authentication and access to social networking and other Web applications.

Figure E.

Use Case 3: Outside the Organization



Social networking outside the organization

In this use case, organizations extend access to large public social networking sites. Here, employees could communicate with any users of these sites. The most successful public social networks are so popular that many business applications have built direct integrations to these platforms. For example, the very popular customer relationship management service provider Salesforce.com has extended its platform to communicate with communities in Facebook and Twitter through its ServiceCloud 2 service.

Primary drivers:

- Marketing, products, customer service and other internal divisions are pressuring organizations to open access to these sites and applications. If the organization does not provide this access, they may be hindering employees from being able to effectively do a portion of their jobs.
- An organization's brand can be consistently and positively reinforced with your customers, constituents, and other parties and communities of interest.
- Competition is likely already devising a strategy to selectively embrace social networking tools. In order to remain competitive, organizations need to have an active presence in these networks.

Pros	Cons
▪ Communication and marketing platforms can reach a huge user base across the world. ▪ Brand and reputation can be enhanced as embracing these applications is viewed as innovative and visionary. ▪ Employees can perform important research regarding market developments and competitor activity. ▪ Establish differentiation from (or, at least, parity) with the competition.	▪ Security and control risks related to data loss and other vulnerabilities are potentially exposed. ▪ As a potential distraction to employees, productivity could decrease while consumption of company resources increases, such as network bandwidth. ▪ Every employee or end user has the power to impact the perception and reputation of your business. ▪ Addressing control of these public networks with a manual approach can be time consuming and resource intensive.

- **Recommended security policies to protect social networks used outside the organization:**
- **Privileged and legal content (as defined above)**
- **Termination or layoff discussions (as defined above)**
- **Confidential projects (as defined above)**
- **Merger and acquisition plans (as defined above)**
- **Confidential trade data (as defined above)**
- **Inside information (as defined above)**
- **Guarantees and assurances (as defined above)**
- **Unprofessional customer interactions (as defined above)**
- **Wiki posting control.** Wiki sites allow users to post anonymously, creating an avenue for information disclosure. Organizations should prevent or allow certain users from accessing these sites to minimize the risk of exposure.
- **Access to blogging and other messaging sites.** Organizations should protect and control blogging and access to other message-posting sites where users are able to enter comments, post articles, and send messages.
- **Personal use of company messaging infrastructure.** This policy helps identify personal use and provides the necessary statistical information needed to define company policy in this area.

Section 4: Benefits

How Does CA Data Protection Help Secure Social Networking?

CA Data Protection is a robust data loss prevention solution designed to help customers better manage and control the use of internal and external social networking applications. CA Data Protection uses policies to detect various types of activity in order to help prevent the loss or inappropriate use of sensitive company data. CA Data Protection can also help IT to monitor that the tools are used for business purposes and not for personal tasks. Generally speaking, public and private organizations need to minimize the misuse or loss of sensitive data across the organization with minimal disruption to legitimate business activity. CA Data Protection leverages user identity, content coverage and pre-built policies to help control and secure the use of social networking for the organization. Additionally, CA Data Protection can provide basic metrics to help evaluate trends and overall usage of social network applications.

Identity-based control

Organizations may use a simple approach to controlling content posted to and shared on social networking sites by using a 'white list' to specify the users who are permitted access to these sites. In many organizations using this approach, users create service desk tickets to request access while the security groups maintain and administer the list. This approach is resource intensive and still does nothing to directly address the risk of data loss.

CA Data Protection takes a more intelligent and effective approach to helping secure the use of social networking sites. Not only does CA Data Protection inspect the content of a post, including content present in files or attachments, but the solution takes into account the role of the end user. CA Data Protection leverages identity to analyze end-user activity in real time and understand data with a higher level of precision. This can help organizations protect more types of sensitive information, more effectively. Using this approach, CA Data Protection can distinguish between an employee in marketing and an employee in finance using Twitter to post a message about a conference presentation. CA Data Protection could be configured to allow the marketing employee's action while blocking that of the finance employee.

Comprehensive coverage

CA Data Protection is designed to analyze and control sensitive information posted to social networking sites. This section discusses how CA Data Protection can be used to better protect an organization in connection with the posting and sharing of information on these sites.

- Updating status. This is one of the most popular features on sites like Twitter and Facebook. Users can change a status to provide somewhat short updates and instant opinions to one's network including friends, followers, and colleagues. There is a high potential for leaking improper content via status updates. Examples of this include the mention of an "important meeting with Company X" or a meeting at a specific location with certain people. Something as seemingly innocent as this could be divulging important insider information regarding an acquisition. Other examples include a short discussion of a company memo, details of a future product, and information on a new partnership. CA Data Protection can detect sensitive information, even in just a few phrases or sentences, and block it from being posted.

- **Sending messages and the use of Instant Messaging.** Within most social networking tools, users can send full length email messages or shorter instant messages to other users. These mechanisms pose the same threat of data leakage as applications such as Microsoft Outlook/Exchange, Office Communicator, and Lotus Notes/Domino along with full-featured consumer webmail and instant messaging applications such as Yahoo!® Mail and Gmail. CA Data Protection is designed to analyze and intercept the full content in messages (including attachments), and detect and protect sensitive information from being shared or leaked in this manner.
- **Sharing media such as photos and videos.** Intellectual property (IP) can take the form of photos, videos, documents, and more. An example of IP that could damage a company's competitive advantage is a set of images of concept cars for an automobile manufacturer. Images of stock charts, models, and other non-public information can also be leaked, putting the firm at risk of violating regulatory or corporate mandates. CA Data Protection can help with these use cases by controlling the posting of pictures and other media files to social networking sites. CA Data Protection can disable any employee from sharing pictures and photos. Additionally, this control feature can help prevent employees from using social networking sites for personal or non-work purposes.

Highly accurate pre-built polices

CA Data Protection offers hundreds of pre-built policies designed to address the information risks related to data loss, regulatory compliance, and the protection of intellectual property and non-public information. CA Data Protection pre-built policies help reduce the need to design policies and rules from scratch, thereby accelerating the effort to deploy an information protection and control solution. Complementing pre-built or custom policies is the CA Data Protection Policy Refinement Methodology, a set of services and best practices designed to enable your policies to provide a higher level of detection accuracy.

In order to achieve a higher level of accuracy, CA Data Protection policies use powerful detection methods ranging from simple keywords and phrases to detecting patterned data, completely unstructured content, and other content and metadata elements. Accuracy helps drive Data Protection project success by helping you to find sensitive data exposure and to identify non-compliant end-user behavior.

Expanded control for blogs, wikis and other user forums

Subject-matter-experts need to be able to impart their knowledge to the blogosphere—including customers, partners, and other interested parties. Many organizations have guidelines dictating what employees can and cannot publish. The major disconnect tends to be the lack of a programmatic means to validate in real time the content that is being published.

This is a dilemma for security teams due to the volume of content that their end users post to these web-based forums. Users and experts can create a large amount of content because it's simple; they enjoy helping others; and they feel their constituents (customers, peers, partners) expect it of them. And, blog or user forum posts are expected to be current. If the posting process requires a week to obtain internal approvals, the content may very well be stale by the time it posts.

CA Data Protection is designed to address these issues by helping enforce data use policies as employees post content to a blog, wiki or user forum. This real-time content validation helps make sure that end users do not post inappropriate or sensitive information ranging from non-public information, to intellectual property, to content about customers. CA Data Protection also allows a company to determine who is allowed access to these types of sites based upon their roles.

Tracking social networking use

Although an organization may use 'white lists' to control who can access external social networking tools, there are still many who allow unfettered access to these sites. CA Data Protection provides basic usage metrics for social networking sites which include:

- The number of employees visiting a site.
- The name, IDs and other user information of those employees.
- The Data Protection policies that were violated while using the sites.

This information helps an organization to understand which policies to put in place in order to regulate the use of these sites. This information could then provide the justification for implementing a policy to only allow certain individuals or groups of employees to access the sites.

Section 5:

Conclusion

For the foreseeable future, social networking will become more entrenched in business. As this trend continues, the risk of data loss continues to increase. This is a great opportunity for organizations to evaluate their social networking strategic options. Things to keep in mind:

- Don't be fearful from a security perspective to embrace social networking. Be sure to keep security in mind while creating your strategy.
- There are many different approaches that can offer the right level of security control while enabling the business to thrive.
- Talk to your employees, customers, and partners to determine their needs, and then design a plan to keep data secure.
- Seek out solutions that are flexible, configurable, and modular.
- Leverage solutions that not only meet current needs, but can extend to meet future requirements

Effective data loss prevention is a necessary complement of any organization's strategy for enabling social networking. CA Data Protection was designed to provide the multiple layers of identity and content awareness, the sophistication of policy, and the variety of actions and interventions needed to help govern the proper use of social networking within the organization.

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.

This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. CA does not provide legal advice. Neither this document nor any CA software product referenced herein shall serve as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, policy, standard, guideline, measure, requirement, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. You should consult with competent legal counsel regarding any Laws referenced herein. To the extent permitted by applicable law, CA provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages.