WHITE PAPER

The Risks of Social Media and What Can be Done to Manage Them

An Osterman Research White Paper

Published June 2011

SPONSORED BY

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

Executive Summary

Social media, when used in a corporate setting, represents a balancing act of rewards and risks for IT, business and senior management in virtually any organization or industry:

- **Rewards** in the context of new business opportunities that can be created, the competitive differentiation that a company can enjoy from intelligent use of social media, the ability to build customer loyalty, and the new channels of communications that open up with current and prospective customers.

- **Risks** from the inappropriate content that can be posted on social media sites, the malware that can enter a network through short URLs or phishing attacks, and the failure to retain important business records posted on social media.

In short, although social media is a relatively new communication and information management channel relative to more traditional tools like email or instant messaging, the same fundamental management requirements apply: social media must be monitored for malware and inappropriate content, and relevant business records sent through social media must be retained and easily accessible for as long as necessary.

KEY TAKEAWAYS

There are four important points made in this white paper:

- Social media management – by virtue of the sheer numbers of social media users and the importance of the applications for which the technology is used – cannot be ignored by corporate decision makers.

- Social media creates a number of potential risks for firms of any size and across all industries. These risks are focused primarily on a) the ingress of malware that could wreak financial or other havoc in an organization; b) the potential for employees to post content that could harm their employer; and c) not retaining business records that must be preserved to satisfy legal, regulatory or other obligations.

- Any organization – whether or not it sanctions the use of social media – must develop detailed policies focused on how and when social media can and cannot be used.

- The technologies exist to monitor and archive social media content in a way that can minimize corporate risk – every organization should evaluate and deploy technologies that will meet their requirements.

ABOUT THIS WHITE PAPER

This white paper was sponsored by CommVault and McAfee and is an adjunct to a Webinar that was delivered by these companies and Osterman Research on June 1, 2011. A replay of this Webinar is available by clicking here. Information on both sponsors is provided at the end of this document.

The Growing Use of Social Media

USE OF SOCIAL MEDIA, OTHER WEB 2.0 APPS IS GROWING RAPIDLY

There are many social media sites in use around the globe, although the "Big Three" in North America – Facebook, Twitter and LinkedIn – receive much of the press attention because of the huge following they have among business users. For example, the combined subscribership of these three social media properties currently exceeds 800 million users:

- **Facebook** had 687.1 million users in June 2011, up 1.7% from 675.4 million in May 2011[i].

- In March 2011, **LinkedIn** had 79.2 million unique visitors worldwide, up 65.3% from a year earlier; 35.4 million of these visitors were in North America, representing an increase of 36.7% from a year earlier[ii].

- **Twitter**'s numbers are bit harder to come by, but an interesting analysis of Twitter's 175 million accounts reveals that, as of February 2011, 119 million of these accounts followed one or more other accounts and 85 million Twitter accounts had at least one follower. The analysis also discovered that 56 million accounts follow at least eight other accounts, but just 12 million accounts follow 64 or more Twitter accounts[iii].

In addition to these social media tools, there are more than 1,000 social media sites in use outside of North America, including Hong Kong's Sina Weibo (140 million users as of mid-2011, expected to reach 200 million by year-end 2011[iv]), Google's Orkut (37 million accounts[v]), and South Korea's Cyworld (more than 20 million users as of late 2010[vi]).

SOCIAL MEDIA OFFERS A NUMBER OF IMPORTANT BENEFITS

The use of social media provides a number of important benefits for both users and organizations that use the technology properly:

- Users benefit from the use of social media by having a ready source of current information, being able to share articles and viewpoints, and partnering with like-minded individuals inside and outside their organization.

- Companies benefit by creating and building a following among current and prospective customers, sharing information in ways that would not otherwise be possible using normal communication channels, and by gaining competitive advantage through being perceived as thought leaders in their market space. Moreover, the proper use of social media strengthens client and prospect relationships with real time, authentic dialogue in a way that other media cannot.

BUT IT ALSO INCREASES THE LEVEL OF CORPORATE RISK

Although social media offers a number of benefits and can create competitive differentiation for any organization, it is risky from a behavioral standpoint in three important ways:

- Users might leak business records, confidential information or other sensitive information mistakenly or intentionally. This can include seemingly innocuous types of posts or tweets, such as "off to Bentonville again" or "another meeting in Redmond this week", which might let others know about possible negotiations with Wal-Mart or Microsoft, respectively.

- Users can send racially or sexually offensive content using social media tools in violation of the law, legal best practice or corporate policies. Even a casual search of Twitter, for example, will reveal an enormous number of offensive jokes, derogatory terms and other content that, if posted by an employee, could land his or her employer in serious trouble.

- Some social media content constitutes business records that must be preserved in compliance with corporate, legal and regulatory retention requirements, but that might not be archived appropriately.

SOCIAL MEDIA IS A SOURCE OF MALWARE

Moreover, social media can introduce various types of malware into an organization. For example, there are numerous types of malware that can be introduced into an organization through the unfettered use of social media:

- **Koobface**
  This worm targets primarily Facebook, but also Twitter, MySpace and other social media sites. Its goal is to gather login information for purposes of building a peer-to-peer botnet.

- **Boonana**
  Written in Java and first reported in late October 2010, Boonana targets Macs and operates much like Koobface.

- **Bugat**
  Related to the infamous keystroke-logging malware Zeus, Bugat has been delivered in a large-scale phishing attack against LinkedIn.

Social Media is Too Important to Ignore

DECISION MAKERS CAN NO LONGER IGNORE SOCIAL MEDIA MANAGEMENT

The inappropriate use of social media can create enormous liabilities, embarrassment and other problems for an organization. For example:

- The president of The Redner Group, the (now former) public relations firm for 2K Games' Duke Nukem Forever tweeted in June 2011 "Too many went too far with their reviews … we are reviewing who gets games next time and who doesn't based on today's venom", publicly threatening to blacklist those who negatively reviewed the game[vii].

- Employees at the Tri-City Medical Center in Oceanside, California posted patient information on Facebook[viii].

- In 2009, authorities investigated a situation in which exit poll results for three German states were leaked on Twitter prior to the polls closing[ix].

- Also in 2009, an employee of Ketchum, a public relations firm, used Twitter to post insulting comments about the city of Memphis shortly before presenting to the worldwide communications group at FedEx – Memphis' largest employer. An employee of FedEx

discovered the tweet, responded to the tweeter, and then copied FedEx's senior managers, the management of FedEx's communication department and the management of Ketchum[x].

- A hospital employee in Hawaii with access to patients' medical records illegally accessed another person's records and posted on MySpace that the individual had HIV[xi].

- A West Allis, Wisconsin employee was fired for a post she made on her Facebook page claiming that she was addicted to alcohol and various prescription and illegal drugs, although the employee claimed that her comments were made in jest[xii].

- The case of *Blakely v. Continental Airlines* [164 N.J. 38 (2000)], although decided by the New Jersey Supreme Court prior to the advent of social media, established the precedent that employers are liable for what their employees post online.

It is also important to monitor content based on regulatory guidelines. For example:

- Various rules issued by the Financial Industry Regulatory Authority (FINRA) require supervision of communications by registered financial services representatives. For example, FINRA Regulatory Notice 10-06 states that ""Every firm that intends to communicate, or permit its associated persons to communicate, through social media sites must first ensure that it can retain records of those communications as required by Rules 17a-3 and 17a-4 under the Securities Exchange Act of 1934 and NASD Rule 3110."

- Federal Energy Regulatory Commission (FERC) Order No. 717 requires monitoring and archiving of communications between the marketing and transmission operations of vertically integrated electricity and natural gas companies.

Various US government agencies have also issued guidance on the retention and management of social media content. For example:

- The National Archives and Record Administration (NARA) continues to refine policy regarding the retention of social media communication. An October 2010 NARA bulletin explains that "Open and transparent government increasingly relies on the use of these [Web 2.0] technologies, and as agencies adopt these tools, they must comply with all records management laws, regulations, and policies. The principles for analyzing, scheduling, and managing records are based on content and are independent of the medium; where and how an agency creates, uses, or stores information does not affect how agencies identify Federal records.[xiii]"

- The US State Department's official policy, *Using Social Media*, requires a site sponsor to be the record keeper for content that must be preserved long term, requiring that records "be maintained with related records or managed through an acceptable records management application."

- The Environmental Protection Agency has published *Interim Guidance for EPA Employees who are Representing EPA Online Using Social Media*, requiring that "agency records created or received using social media tools must be printed to paper and managed according to the applicable records schedule in a recordkeeping system."

- The US Department of Defense has provided formal guidance on the use of Web 2.0 tools, which includes guidance that "all users of these Internet-based capabilities must be aware of the potential record value of their content, including content that may originate outside the agency."

POLICIES FOCUSED ON SOCIAL MEDIA ARE LACKING

Osterman Research has found that relatively few organizations have detailed and thorough corporate policies focused on social media. For example, in a large survey of mid-sized and large organizations conducted during February 2011, we discovered that fewer than one in five organizations has such as policy for various leading social media tools, while more than two in five have no policy whatsoever.

Development of Policies for Various Tools

Issue	Detailed and Thorough Policy	Basic Policy, But Not Detailed	Do Not Have a Policy
Employees use of Twitter	18%	38%	44%
Employees use of Facebook	18%	41%	41%
Employees use of blogs	18%	41%	41%
Employees use of LinkedIn	16%	38%	46%

The lack of sufficiently detailed policies exposes an organization to two serious problems in the context of their social media usage:

- Organizations that lack corporate policies for social media are unlikely to deploy technology that will mitigate the risk. Simply put, there is relatively little justification for a technology to support a policy that does not exist.

- The absence of any corporate policies focused on social media puts employers at greater risk for inappropriate content their employees post. For example, if an employee posts racially or sexually offensive content via Twitter or on the company's Facebook page – and there is no policy that explicitly prevents such behavior – an employer will find it more difficult to justify firing that employee and, if they do, they will have a more difficult time defending themselves against a claim of wrongful termination.

THE THREE FUNDAMENTAL THINGS THAT ALL ORGANIZATIONS MUST DO

As a result, every organization must do three things:

- **Develop social media policies**
  First, develop detailed and thorough policies that are focused on establishing acceptable use of social media. These policies should clearly indicate the tools that are acceptable, those that are unacceptable, which functions and features are permitted and not permitted, etc. More on this is provided in the next section.

- **Monitor content**
  Second, deploy technologies that will:

  - Monitor social media content for inbound malware and, preferably, integrate these capabilities with other security systems already in use in the organization.

  - Monitor social media for potentially libelous comments that are sent externally, as well as trade secrets that might be referenced in social media posts, potential regulatory violations, breaches of ethical walls, etc.

  - Monitor social media content for sexually harassing, racist or other inappropriate content that might be sent internally.

- **Archive social media content**
  Finally, determine the extent to which business records are being sent and received via social networking tools with regard to official and unofficial communications. Official business records in social media would include information posted on a corporate Facebook page or tweets from the social media manager. Unofficial communications would essentially include every other type of communication that might include a business record or some other content that should be preserved.

  With regard to the latter type of communication, consider the following actual tweets posted on April 6, 2011:

  > *Last week got talked to at work because several months ago someone lied and told HR that I was announcing I was bisexual.*
  >
  > *One reason this client website has been like pulling teeth is because I think their entire business model is STUPID.*

  Clearly, these types of communications might be actionable at some point in the future and so must be retained in the event of litigation or potential violations of the law. For example, in the case of *EEOC v. Simply Storage Management LLC, et al.*[xiv], the Court ordered that relevant (but not all) information for two plaintiffs in a sexual harassment case had to be produced from their Facebook and MySpace accounts, including their relevant password-protected and friends-only content.

A Multi-Stage Plan for Managing Social Media

UNDERSTAND HOW AND WHY SOCIAL MEDIA IS USED

Business units and the IT department should conduct a thorough evaluation of how social media is used by various functions, which tools are used and why they are used. This audit should also include a focus on how these tools might be used in the future, how competing firms are employing these tools, and any new capabilities that might be required in the future. In short, an organization should determine if it could obtain competitive advantage through the use of social media instead of making a knee-jerk decision not to use it because of security or other risks it might pose.

This evaluation might reveal that there is a major disconnect between what IT, security or compliance perceives as a legitimate application of social media and what individual users or business units perceive to be legitimate. The goal, of course, is to balance the competing interests of both groups and derive the greatest benefit from the use of social media while still remaining compliant with corporate policies and security requirements. This might include:

- Corporate users, such as Human Resources and legal staff who need to research new hires and investigate shared content.

- Marketing, communications, PR teams and spokespeople who want the ability to post commentary, create events and utilize the full functionality of social media.

- Employees who utilize social media to prospect for business, network with customers and partners and collaborate with suppliers.

- Regulatory compliance teams who must not only maintain records of shared content and activities, but also approve and moderate subject matter.

UNDERSTAND THE RISKS YOU FACE FROM MISMANAGEMENT

The next step is to understand the problems that can arise when social media is not managed properly, when business records in social media posts are not retained, and so forth. It would be appropriate at this phase of the evaluation process to understand the potential consequences associated with not managing social media use adequately. For example:

- Employees that want to discuss work conditions or complain about their benefits cannot be prevented from doing so according to rules codified in the National Labor Relations Act. This means that employers must tread a fine line between monitoring and blocking social media for inappropriate use or sharing of content in an inappropriate way and preserving the rights of employees to share information. Further complicating the issue is the need for multinational organizations to satisfy the diverse requirements of each territory in which it operates.

- Business records or other important content that are sent using social media tools must be retained. A management decision to purge this content could be seen as spoliation of evidence in a lawsuit. For example, if management decides not to preserve sexually harassing direct messages sent using Twitter, a party offended by this content that takes legal action may be entitled to access the archives of these posts as part of an e-discovery exercise and could claim spoliation in their absence.

  The ramifications of spoliation can be substantial and include fines and sanctions imposed by the court, the requirement to pay the prevailing party's legal fees, attorneys' costs for additional motions, and other serious consequences.

- Another issue is to prevent the use of certain functions within social media. For firms in the financial services industry, for example, investment advisers cannot be the beneficiary of a testimonial or recommendation on LinkedIn because that might violate Rule 206(4) of the Investment Advisers Act of 1940[xv]. This rule makes it illegal for an investment adviser to

publish or benefit from an advertisement or testimonial that deals with their conduct as an adviser.

Similarly, registered financial services representatives are subject to scrutiny when they post content on social media sites, including monitoring of their posts and retention of their communications.

IMPLEMENT POLICES FOCUSED ON APPROPRIATE USE OF SOCIAL MEDIA

Next is to implement policies that will focus on striking the appropriate balance between employee freedom to communicate via social media tools, the business benefits that will be derived from the use of these tools, compliance with industry regulations, and advice from legal counsel. Considerations for these policies should include:

- Policies about the use of social media tools should be part of an overall messaging and communication policy that covers the use of corporate email, personal Webmail, instant messaging, collaboration workspaces, cloud-based storage tools and any venue through which individuals might share corporate information.

- Sufficient granularity should be included so that differing roles within the organization are clearly subject to different policies. For example, energy and securities traders may be subject to different rules about their use of social media than clerical staff, senior managers should be subject to different policies when communicating with external auditors than when they communicate with employees, formal communications that represent a company position should be subject to different scrutiny than personal communications, and so on.

- Policies should also include a detailed discussion about appropriate use of social media tools, including requirements not to post sexually or racially offensive comments or images, not to include links to inappropriate Web sites, not to defame or slander others, not to post content that could run afoul of copyright laws, not to post personnel records or other sensitive information, and the like.

- The specific tools that can and cannot be used should be specified clearly, preferably along with a rationale for the decision. This includes the social media sites themselves, as well as the platforms on which these sites are accessed – home computers, smartphones, desktop computers at work, etc.

- Policies should clearly spell out that management reserves the right to monitor employee communication via social media, when it has the right to act on this information, and that content may be retained for an indefinite period.

- Where appropriate and if at all possible, disclaimers should be included for communications like Facebook posts or blogs. Clearly, disclaimers will not be practical for tweets and other space-limited communication tools (unless, possibly, a short URL is included that points to a corporate disclaimer).

- Succession planning should also be a part of social media policies. For example, when an employee leaves the organization, the corporate policy should include provisions about

"ownership" of the followers or friends of that employee: do they belong to the individual or the company?

- Policies should also spell out the corporate reaction to a data breach and the consequences of a policy violation.

DEPLOY THE RIGHT TECHNOLOGIES

Ultimately, every organization should deploy technologies that will do a variety of things:

- **Monitor communications**
  Monitor employee posts on every social media protocol that might be used. This monitoring may be after the fact, such as sampling employee posts to check for inappropriate content; or it might be in real time to monitor posts before they leave the organization.

- **Block malware**
  It is also vitally important to block threats that can enter an organization through social media. This is particularly important given a) the widespread use of short URLs that offer the user no visual cues about the veracity of the link, and b) the fact that many social media tools can display content provided by individuals to whom users have not given permission to display posts.

  One of the key problems with social media from a security perspective is that these tools are generally less well defended than more established tools like email. Given the rapid increase in the use of many of these tools, many IT departments are scrambling to keep up with the rapid growth of social media tools, leaving organizations vulnerable to malware infiltration. For example, an Osterman Research survey conducted during May 2010 revealed that 12% of mid-sized and large organizations in North America had been the victim of malware infiltration during the previous 12 months, while 9% of organizations had had sensitive or confidential information accidentally or maliciously leaked through a social media or Web 2.0 application[xvi].

- **Archive relevant content**
  Archive and log all relevant content that might constitute a business record and that might need to be retained. It is generally easier to simply archive or log all social media content than take the risk that some important content might slip through and not be retained, but this will depend to a large extent on the industry in which an organization operates and other factors. A key part of content logging is to ensure that the identity of the individuals who use social media tools is clear and that content can be tied back to their corporate identity.

  Most organizations will want to integrate their social media archive with their primary electronic content archive. This makes legal holds, as well as searching across all electronic content during early case assessment and e-discovery, much easier and less time-consuming.

Summary

Social media use in any organization can be boiled down to three basic points:

1. Use social media for marketing, thought leadership or other applications for which it might have utility. This is particularly important if a company is the first or the leading user of social media in its market.

2. Monitor social media content leaving and entering your organization so as to minimize the risks that it can create in the context of legal liability or regulatory violations.

3. Archive all relevant business content that is generated using social media for purposes of legal and regulatory compliance, as well as to comply with corporate best practice.

Sponsors of This White Paper

Officially, CommVault is a publicly traded data and information management software company headquartered in Oceanport, New Jersey. We first made our mark with the industry's leading backup software product. But, from the beginning—over a decade ago—our founders were passionately committed to going beyond backup, giving companies a better way to organize, protect and access business information.

Many of our 13,500+ customers started talking with us in search of a better alternative to their existing backup systems. But, ultimately, they were won over by CommVault's unique philosophy and ability to deliver complete solutions with infinite scalability and unprecedented control over data and costs.

CommVault
2 Crescent Place
Oceanport, NJ 07757

+1 888 746 3849
www.commvault.com

CommVault® Simpana® software provides an effective framework for the management of a range of information governance activities including efficient long term data retention, eDiscovery and compliance with industry-specific regulations. All this is achieved from a single platform, providing the most comprehensive, risk-adverse and cost managed records retention solution that exists today.

A wealth of accolades, and revenue growth greater than three times the software industry average further reflect the industry's burgeoning enthusiasm for CommVault's revolutionary approach to information management. More companies every day join those who have discovered the unparalleled efficiency, reliability, and control only CommVault can offer.

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.

McAfee
2821 Mission College Blvd.
Santa Clara, CA 95054

+1 888 847 8766
www.mcafee.com

---

[i] Source: Inside Facebook Gold
[ii] Source: comScore Media Metrix
[iii] http://www.businessinsider.com/chart-of-the-day-how-many-users-does-twitter-really-have-2011-3
[iv] http://www.clickz.com/clickz/news/2078304/sina-weibo-marketers-social-business
[v] http://www.orkut.com/About?page=keep
[vi] http://www.google.com/hostednews/afp/article/ALeqM5jTk-b8UadVNyPiEILD-tnjHIv34g?docId=CNG.fe1d0589886b23ad62bffe61357001df.21
[vii] http://www.zdnet.com/blog/gamification/twitter-tantrum-sinks-duke-nukem-forever-pr-agency/472
[viii] Source: Privacy Rights Clearinghouse (http://www.privacyrights.org/data-breach)
[ix] http://www.hollywoodreporter.com/news/germany-probes-twitter-election-data-88306
[x] http://shankman.com/be-careful-what-you-post/
[xi] Source: Privacy Rights Clearinghouse (http://www.privacyrights.org/data-breach)
[xii] http://www.courthousenews.com/2010/05/24/27513.htm
[xiii] NARA Bulletin 2011-02
[xiv] Case No. 1:09-cv-1223-WTL-DML
[xv] http://newrulesofinvesting.com/2009/03/22/adviser-use-of-linkedin-may-violate-sec-rules/
[xvi] Source: *Messaging and Web Security Market Trends, 2010-2013*; Osterman Research, Inc.