# Social Media for Engineering Firms – Benefits and Risks

ACEC Risk Management Committee, October 2016

## INTRODUCTION

Social media technology is used every day by individuals and organizations to stay in touch, share experiences, promote causes, and rally people to action. ACEC member firms vary in the degree to which they embrace social media. They might use social media to help market their firm's services, but wonder about the associated value and have concerns about potential risks. While social media benefits may include enhanced business successes through increased communication and promotion, the potential risks are real.

This white paper is intended to provide ACEC member firms with a basic understanding of risks associated with the use of social media. Suggestions for mitigating those risks include developing social media policies that set parameters for employer and employee engagement of these powerful tools, and implementing terms of use governing third-party posts to a firm's social media pages.

## DO YOU TWEET?

### *How Social Media Might Benefit Your Business*

Social media technology allows users to easily create and disseminate content through social networks using the Internet. The use of social media is ubiquitous today and has drastically changed the way we communicate. Social media creates a sense of intimacy and immediacy in our communications with colleagues and clients. But what business value can social media such as Twitter and Facebook bring to your engineering firm? And, if you're challenged just managing your email, how do you get on board (or do you need to get on board)?

In a May 2010 paper,[1] ISACA (a global information services education, auditing, and control standards organization) opined that businesses can no longer try to keep social media usage out of the enterprise: "Social media use is no longer the exception for businesses, but rather the rule." Businesses are realizing the potential for utilizing social media tools to stimulate interaction and innovation among their employees, assist in human resource actions, create brand recognition, and improve client contact.

However, all the possibilities and hype around social media may overwhelm and paralyze business owners, who are uncertain how to implement these technologies to benefit their companies.[2] Firms must select the platform(s) that feel most comfortable and best fit the company's goals and communication style. But before diving head-first into social media, you should know how each platform can be used and whether it's useful for your business.[3] The following is a primer on the platforms commonly used by United States businesses today (although we note that it's a rapidly expanding field, this list may not contain your favorites, and there are a host of similar platforms in other countries).

**Facebook**. Launched in 2004, Facebook was reported to have 1.13 billion active daily users on average and 1.71 billion active monthly users as of June 2016.[4] Many businesses have Facebook pages, and a 2012 blog provided ten tips on using Facebook to boost business,

including integrating Facebook connect buttons into the company website, using Facebook as a "second website" with similar robust company information, and using a tool to measure the effectiveness of any Facebook campaign.[5]

**LinkedIn**. Its website touts LinkedIn as the world's largest professional network, and the best means to control your online identity. As of October 2016, LinkedIn had more than 450 million members in over 200 countries and territories, with 28.9% of their members in the United States.[6] It claims that LinkedIn profiles rise to the top of search results, letting you control the first impression people get when searching for you online. One purpose of the site is to allow registered users to maintain a list of contacts with whom they have some sort of relationship, called "Connections." A contact network is built up consisting of a person's direct connections, the connections of each of their connections (termed *second-degree connections*) and also the connections of second-degree connections (termed *third-degree connections*). This network can be used to gain an introduction to someone through a mutual contact. The site also includes various job search features, as well as professional groups that individuals can join for specific interests and blogs.

**Twitter**. Twitter is an online social networking and microblogging service that enables its users to send and read text-based posts of up to 140 characters, known as "tweets." It was created in March 2006, and averaged 313 million monthly active users as of October 2016.[7] Unregistered users can read the tweets, while registered users can post tweets through the website interface. A 2009 study of 2000 tweets by Pear Analytics, a firm specializing in marketing analytics, insights and intelligence, opined that almost 80% of the posts fell into the two categories of "pointless babble" or "conversational."[8] Only about 6% of tweets were in the "self-promotion" category, i.e., corporate tweets about products and services. However, corporate Twitter use has likely increased; in 2013, 377 of the Fortune 500 companies reported having a corporate Twitter account.[9]

**Yammer**. Launched in 2008 and sold to Microsoft in 2012, Yammer is similar to Facebook in its sharing and news posting capabilities. However, Yammer differs from Facebook in its use for private communication within organizations, or between organizations and pre-designated groups. Access to a Yammer network is determined by a user's internet domain, so only those with appropriate email addresses may join their respective networks. Yammer boasted a customer base of 8 million users by 2013,[10] and has reported that 85% of Fortune 500 companies use it for collaboration.[11]

**YouTube**. Created in 2005, YouTube is now the world's most popular video-sharing website. Most of the content is uploaded by individuals. Unregistered users can watch videos, while registered users can upload an unlimited number of videos. Businesses may use YouTube to build brand awareness through the use of video, and to use YouTube's embedding script to easily add videos to their own websites. YouTube offers free analytical tools that are simple to use, providing a quick snapshot of the number of views, demographics of viewers, and how people found the video.

**Blogs**. A blog is a discussion or information site published on the web consisting of discrete entries, typically displayed with the most recent post appearing first. There are many online blogs. Businesses may have an internal blog, used to enhance communication and culture, and/or an external blog, used for marketing, branding, or public relations.

## UNDERSTANDING THE ISSUES

### *Identifying the Risks Associated with Social Media*

All social media platforms have potential risks, with the degree of risk dependent on how they are used, who is using them, and the type of safeguards and controls your company has in place. To tap the benefits of social media, engineering firms need to know how to use it effectively while minimizing the risks. Risks can be categorized in three broad areas: reputational, legal, and operational/financial:

1. **Reputational**: How do you promote your firm but still safeguard its reputation? The greatest risk to company reputation arises from the inability to control the content and quality of external communications, potentially leading to serious brand/reputational damage. These issues can arise from the inability to control staff personal use, being drawn into debates on public issues (via staff postings), and the release of sensitive or embargoed information. There is also the risk that someone outside your organization can use social media to attack your company's reputation.

2. **Legal**: What are the legal risks of social media use? One of the chief issues relates to its use in the hiring process. Other employment-related issues include those related to employee access to inappropriate/illegal content on social media sites and the Internet, privacy violations, and cyber bullying.

   The ease of information posting and dissemination may be a benefit, but it also increases the likelihood that content may be posted (accidentally or deliberately) without being subject to an internal quality control review. Moreover, firms must ensure compliance with applicable laws when posting advertisements or other promotional information on its social media pages. With respect to external legal threats, content posted by third-party users could lead to civil liability for defamation or other torts, copyright and/or trademark infringement, or antitrust violations.

3. **Operational/Financial**: How do you take advantage of social media's efficient communication and marketing tools, while limiting productivity losses? How do firms ensure their social media decisions are strategic? Issues include ensuring staff use of social media during business hours is for professional purposes, differentiating between valuable discussion and needless chatter, determining who does or does not have access to social media platforms, and whether the information disseminated trivializes the core message of the organization. Technical issues such as increased risk of viruses and malware entering the organization's network, and costs of training may also arise.

Contemplating these risks may make business executives shy away from social media engagement. But, in these times, not having a distinct presence on social media sites could have a negative impact on your staff and clients. It is highly likely that organizations will miss opportunities to fully engage with all their stakeholders and to increase their firm's visibility and market share. Not engaging social media can become a risk in itself.[12,13] It's best to understand the risks and develop strong internal policies to guide your use of social media and your response to both internal and external risks.

## I HEARD IT THROUGH THE GRAPEVINE

### *Mitigating Potential Damage to Your Firm's Reputation*

Reputation damage resulting from social media falls into two basic types: (1) damage that is self-inflicted, and (2) damage that comes externally from others. There are almost limitless ways that companies can look bad publicly, and the speed with which social media disseminates information ensures that mistakes can't be easily hidden. William Cunningham and Jeff Hunt report that, because of social media, nearly any risk – a product liability allegation, a poorly handled natural disaster, a financial problem, you name it - can hurt a company's reputation.[14] Citing examples of corporate *faux-pas* by AT&T and Dell, the authors opine that, rather than hunkering down in a defensive crouch, companies do better if they adopt guidelines that carefully balance the risks and rewards of engagement. If valid criticism is directed at you, it might be better to look at it as an opportunity to right a wrong, or give your side of the story with respectful candor.[15] Such a response must be done in a timely manner.

How your employees behave can have a big impact on your company's social media reputation. For companies that are actively involved with social media, setting expectations, creating policies for employee behavior, and providing training are the best ways to ensure that they help your reputation, not hurt it. Your guidelines may also need to extend to your employees' use of social media away from the office. What about the situation where a junior engineer's personal Facebook page reports something disparaging about a job site he visited that day, or about a client interaction? Such exposure could breach the client confidentiality agreement and, should it come to your client's attention, severely damage your firm's credibility. For this reason, it is crucial that employees understand their responsibilities with respect to confidentiality. Confidential matters should never be discussed on Twitter or Facebook, for example. Other providers, such as Yammer, could provide more security and corporate control. In order to ensure that no confidential client information is misused or used in a way that damages client relationships, you may want to bar employees from discussing clients, projects, or fellow employees online without written permission.

Companies allowing third-party posts to their website also need to be alert for reputational threats. Posts by third-party users can be abusive, offensive, intimidating, obscene, profane, discriminatory or otherwise inappropriate. Companies that do not monitor posts may fail to promptly remove inappropriate content and thereby appear to tacitly support inappropriate posts. A perceived endorsement of offensive or inappropriate content may harm a firm's reputation.

For a 2011 paper on social media and its associated risks, Grant Thornton LLP and the Financial Executives Research Foundation, Inc., conducted a survey and in-depth interviews with a range of business executives consisting of 141 respondents from public and private companies.[16] "Negative comments about the company" was ranked as the second highest social media risk by the participants. You may not be able to prevent online ranting, but companies have found some relief in court if the statements involve libel.[17] Firms can remove negative comments from their own websites, but controlling other unwanted posts is difficult. Demanding removal or retraction of negative reviews or other online writing could result in an escalation of efforts to defame your business's reputation. And, while the instinct might be to tell your side of the story, posting a response could increase the visibility of the negative post.

Managing your online reputation could include using a monitoring tool to keep on top of information about you on the internet.[18] For example, the Yahoo! Marketing Dashboard allows

entities to monitor thousands of sites from one platform. Google Alerts is another option for monitoring information being created about your company, as it can be set up to notify you when new content from news, the web, blogs, and/or discussion groups mentions your firm. Several companies offer assistance in social media crisis response. Risk Management Monitor suggests developing a Social Media Crisis Response Plan, and offers an easy-to-read flow chart from one such company, Social Media Influence, to help guide decision-making if the worst occurs.[19] Companies may want to create several positive social media posts to hold in reserve in order to immediately counter a negative post.

## WILL YOU BE MY FRIEND?

### *Legal Issues Related to Social Media Use*

One of the most common areas of discussion on the legal implications of social media is around hiring and disciplining employees. Some companies are not only checking out potential employees on Facebook, but are also asking for passwords so they can look at personal information on private areas of a potential employee's site.[20] Other companies are reported to stop just short of asking for passwords but ask applicants to "friend" human resource managers, giving the company access to the applicant's entire online profile. While prospective employees may "volunteer" to provide access or passwords, it could be considered coercion given the inequitable relationship between prospective employee and employer. In addition, handing out Facebook login information is a violation of the social network's terms of service.

Four states – California, Illinois, Maryland, and Michigan - enacted legislation in 2012 prohibiting employers from requesting or requiring an employee or applicant to disclose a user name or password for a personal social media account. The National Conference of State Legislatures reports that, as of 2015, forty-six states introduced legislation to restrict employers from requesting access to social networking usernames and passwords of applicants, students, or employees.[21]

Apart from asking for passwords, even viewing the social media pages of job applicants can lead to various problems, including exposing yourself to a discrimination lawsuit. Instead of finding red flags, such as drug use or criminal activity, the employer is more likely to discover previously unknown information on the applicant's race, age, religion, sexual orientation or disability.[22] Because this type of data is readily available online, your decision to not hire the screened applicant may be questioned, especially if the applicant knows your company screens possible hires.

What about monitoring the online activities of your existing employees? Other exposures may come from information that could be used in a discrimination suit regarding wrongful termination or passing over an employee for a promotion or bonus. Certainly, if you are going to monitor your employees' social media use, it must be conducted uniformly for all employees.

Although companies may have policies stating that all activities conducted on company computers may be monitored, such policies are limited in their reach. The fact that an employee has accessed Facebook from work, for example, does not mean that the employer can log onto that account and poke around.[21] And other privacy considerations, such as attorney-client privilege, are not overridden by the employer's monitoring policy. Companies should obtain

employee acknowledgement of policies dictating the extent of monitoring activities. Having set these boundaries, you must not deviate from them, even if there is implied consent. And keep in mind that what you find out by investigating an employee's online activity may also trigger further legal obligations. If an employee uses company computers for unlawful activity, such as child pornography or cyber-bullying, you may be liable if you know and don't intervene.

Can you punish an employee for posting negative comments about your company? The answer is . . . it depends. The National Labor Relations Board (NLRB) has been inundated with complaints regarding employer disciplinary actions arising out of Facebook and other social media communications. Section 7 of the National Labor Relations Act (NLRA) gives employees the right to self-organization, and to engage in concerted activities for the purpose of mutual aid or protection, i.e., regarding wages, benefits, or terms or conditions of employment. The NLRB has ruled against many employers who disciplined employees for online grumbling about work terms, holding that the online forum is similar to the water cooler/break room activity protected under Section 7. Other types of negative comments, however, may not be protected under the NLRA.

There are also legal issues around the use of published content.[23] Grant Thornton's survey on social media risks found that "disclosure of proprietary information" was ranked as the highest social media risk by the participants. Liability can also arise in the areas of: intellectual property violations, such as copyright and trademark infringement; defamation though publishing false facts about a person or corporate entity; false advertising through exaggerated claims about products or services; and insufficient online disclosures of conflicts of interest related to products or services discussed.

A failure to register and appropriately label company copyrights and trademarks located on social media pages may lead to infringement by third parties. A company could also be held liable for infringing another's copyrights, although the Digital Millennium Copyright Act (DMCA) may provide immunity for third party postings. Similarly, a company could be held liable for defamation, invasion of privacy, or infringement of publicity rights unless the claim is subject to the available statutory immunity under the Communications Decency Act. No similar statutory immunity exists for trademark infringement claims.

Finally, social networking sites can make it easy for members of trade and professional associations to let their guard down and share information or engage in online discussions that could lead to violations of federal and state antitrust laws or loss of confidentiality (and trade secret status). Clearly, company risk managers must be aware of the information their company is posting online, and check for these types of issues.

## STRATEGIC CONSIDERATIONS

### *Operational/Financial Issues Related to Social Media Use*

In the Grant Thornton survey, many executives reported that the explosion in growth of social media outpaced their ability to comprehend the new technology and adjust their strategies. But, as with any business decision, the choice to use social media must be strategic. Is your online content enhancing or trivializing the core message of your organization? Has your company conducted a risk assessment to evaluate which sites you will use, and what the risks and rewards may be? Is there an established policy (and supporting standards) that addresses social media use? How will you measure the effectiveness of your social media strategy? These issues should be addressed before a company actively engages in social media usage.

Several interviewees in the Grant Thornton survey expressed concern that the use of social media on the job may negatively impact productivity. Many wrestle with the tradeoff between the benefits and the potential for lost productivity due to abuse by employees. And how do you ensure that the information your employees are putting out there is valuable and not a waste of their time (and your money)? A good social media policy, laying out expected behavior around work time social media engagement, will help employees understand the limits.

Grant Thornton opines that, as the use of social media continues to grow, so too does the risk of fraud involving social media. Risks include identity theft or other scams, incidences of imposter accounts at third-party social media websites, or email hacking to gain access to your sensitive data. If your staff tweets about their project working for water authorities or a government agency, could it alert someone with bad intentions who might hack into your system to obtain plans for an embassy or a water treatment plant?

A timely response to any fraud or breach is essential, but prevention and early detection are also critical. Management and employees must learn how to identify and respond to fraudulent activities. Does your IT department have a strategy and supporting capabilities to manage technical risks presented by social media? More than half of Grant Thornton's surveyed companies did not have a plan in place for dealing with instances of fraud and/or privacy breaches related to social media. More than half the executives interviewed were not confident that sensitive, confidential information is adequately protected in their social media platform. The massive and very public security breach at LinkedIn in 2012, involving the hacking of more than six millions passwords, occurred in part because the company failed to use best practices for encrypting passwords.[24] Is your company vulnerable?

Training that is required for appropriate and safe use of social media can be a financial drain. However, training is essential, and effective training is required for all users. Users should also receive regular awareness communications reminding them of policies and risks.

## RISK MITIGATION

### *Developing a social media policy*

While most executives in the 2011 Grant Thornton survey acknowledged the risks associated with social media, many felt that the risks could be mitigated or are outweighed by the benefits. However, more than three-quarters of respondent companies did not have a clearly defined social media policy. While many companies have policies regarding email communication and technology use, very few companies have policies that specifically address social media governance and risks. More than half of respondents indicated their organizations do not have an incident management plan to help them deal with instances of fraud and/or privacy breaches. When Grant Thornton inquired why companies do not have social media policies, two points were repeated by nearly all interviewers: the speed of social media growth and the generation gap.

A stand-alone social media policy may not be necessary if companies have an electronic communications policy that can be amended to address the use of social media. Many companies already have an electronics communication policy that guides appropriate use of the company's computer system, reduces employee expectations of privacy, and reduces the company's risk. Regardless of which approach is taken, the policy must be consistent and integrated with other company policies.

This paper does not offer a “standard” or “sample” social media policy because every firm uses social media differently, and every firm has a different level of risk tolerance with regard to social media use. Policies should be specifically tailored to the unique circumstances and policies of a given firm after thorough consideration of relevant factors. A generic or sample policy may not be appropriate to your firm. The following, however, provides general considerations that should help inform a firm in the development of its own social media policy.

Establishing social media programs and policies should include the principles of leading by example; building policies around job performance rather than fuzzy concerns about productivity; encouraging responsible use; granting equal access; providing training; and beginning from a position of trust.[25] Include people who will be leading your social media charge in developing your policy, and develop policies that will extend to other new and emerging communications technologies. Once published, distribute guidelines widely.[26]

Policies should establish the parameters of employee behavior online. As social media breaks through the boundaries of personal privacy, a good social media policy can help separate business and personal social media activity, and control what information is available to your subordinates, supervisors, colleagues and clients. Establish a protocol for who can post what information about the firm, and on what social media platform(s). Every company may have a different threshold and arrive at different policies. Companies should designate a lead person in charge of all social media activities.

Policies that have legal implications, such as those prohibiting illegal activity or posting of copyrighting material, must be clear and unequivocal. If you have a legal department, include them in the process or have legal review of your final policy document.

In addition, it is imperative that companies identify when a communication or posting to its social media pages is published or edited. Controls should be established to ensure an appropriate editorial role and to monitor company social media pages for problematic postings, so that timely and responsive action can be taken when needed. In addition to regular monitoring, companies should post clearly written terms of use that describe appropriate content, disclaim responsibility for user-generated content, and provide for removal of inappropriate content.

## CONCLUSION

The use of social media offers the potential for increased visibility and more efficient communications for engineering firms. But, the risks are many and real, and must be managed. Risks can result from the broad categories of reputation, legal, and operational/financial issues. Firms must develop rigorous policies and practices to mitigate the risks, so that they can enjoy the rewards of their social media engagement.

## CITATIONS

1 *Social Media: Business Benefits and Security, Governance and Assurance Perspectives*, ISACA, May 2010. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Social-Media-Business-Benefits-and-Security-Governance-and-Assurance-Perspectives.aspx.

2 *How to Calm Your Social Media Anxiety*, Barry Moltz, American Express Open Forum Blog, July 2, 2012. www.openforum.com/articles/how-to-calm-your-social-media-anxiety

3 *Choosing the Best Social Media*, Christine Erickson, American Express Open Forum Blog, May 8, 2012. www.openforum.com/articles/choosing-the-best-social-media

4 *Facebook Newsroom*: accessed October 2016. http://newsroom.fb.com/company-info/

5 *10 Tips on using Facebook to Boost Business*, Angela Stringfellow, American Express Open Forum: April 18, 2012. www.openforum.com/articles/10-tips-on-using-facebook-to-boost-business

6 *About us*, LinkedIn Press Center: accessed October 2016. http://press.linkedin.com/about

7 *It's What's Happening:* accessed October 2016. https://about.twitter.com/company

8 Twitter Study, Pear Analytics, August 2009. http://www.pearanalytics.com/blog/2009/twitter-study-reveals-interesting-results-40-percent-pointless-babble/

9 *DMR* Digital Marketing Stats/Strategy/Gadgets: accessed October 2016. http://expandedramblings.com/index.php/twitter-stats-for-businesses/

10 *Microsoft Reveals Eight Million Yammer Users on First Anniversary,* Dan Worth, V3, June 25, 2013. http://www.v3.co.uk/v3-uk/news/2277279/microsoft-reveals-eight-million-yammer-users-on-first-anniversary

11 *Yammer website:* accessed October 2016. https://about.yammer.com/why-yammer/

12 *Managing Your Company's Social Media Risk*, Matt McGonegle, Sustainable Business Forum, March 22, 2011. http://www.sustainablebusinessforum.com/matt-mcgonegle/50619/managing-your-company-s-social-media-risk

[13] *What are the Risks Associated with Social Media?*, Robert MacKenzie, Business Edge Network Limited, February 21, 2011. http://www.freshbusinessthinking.com/articles_print.php?CID=&AID=8404

[14] *Online, You Are Your Reputation*, William H. Cunningham & Jeff Hunt, Risk Management Magazine, Volume 57, October 1, 2010. http://www.rmmag.com/MGTemplate.cfm?Section=RMMagazine&NavMenuID=128&template=/Magazine/DisplayMagazines.cfm&MGPreview=1&IssueID=349&AID=4177&Volume=57&ShowArticle=1

[15] The Risks of Social Media: Self-Inflicted Reputation Damage, Jared Wade, Risk Management Monitor, April 23, 2010. http://www.riskmanagementmonitor.com/the-risks-of-social-media-self-inflicted-reputation-damage

[16] *Social Media and its Associated Risks*, Grant Thornton LLP and the Financial Executives Research Foundation, November 2011. http://www.grantthornton.com/staticfiles/GTCom/Advisory/GRC/Social%20media%20and%20risk/social%20media_whitepaper%20-%20FINAL.PDF

[17] *What Can You Do About Online Ranters*, Courtney Rubin, American Express Open Forum: May 18, 2012. www.openforum.com/articles/what-can-you-do-about-online-ranters?

[18] *Four Steps to Managing Your Online Reputation*, Carol Roth, Huffington Post Small Business, May 22, 2012. http://www.huffingtonpost.com/carol-roth/4-steps-to-managing-your-_b_1532639.html

[19] *The Risks of Social Media: Developing a Social Media Crisis Response Plan*, Jared Wade, Risk Management Monitor, January 31, 2012. http://www.riskmanagementmonitor.com/the-risks-of-social-media-developing-a-social-media-crisis-response-plan/

[20] *Job Seekers Getting Asked for Facebook Passwords*, Shannon Mcfarland, Associated Press, March 21, 2012. http://www.usatoday.com/tech/news/story/2012-03-20/job-applicants-facebook/53665606/1

[21] *Employer Access to Social Media Usernames and Passwords (Summary of Legislative Efforts – 2012 - 2015)*, National Conference of State Legislatures, June 4, 2015. http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx

[22] Employee Monitoring and Pre-Employment Screening, Jon Vegosen, Risk Management Magazine, October 1, 2010. http://www.rmmag.com/MGTemplate.cfm?Section=RMMagazine&NavMenuID=128&template=/Magazine/DisplayMagazines.cfm&MGPreview=1&Volume=57&IssueID=349&AID=4180&ShowArticle=1

[23] Legal Liability for Published Content, Damon E. Dunn, Risk Management Magazine, October 1, 2010. http://www.rmmag.com/MGTemplate.cfm?Section=RMMagazine&NavMenuID=128&template=/Magazine/DisplayMagazines.cfm&MGPreview=1&Volume=57&IssueID=349&AID=4179&ShowArticle=1

[24] What You Can Learn From the LinkedIn Security Breach, Courtney Rubin, American Express Open Forum: June 8, 2012. www.openforum.com/articles/what-you-can-learn-from-the-linkedin-security-breach

[25] A Corporate Guide for Social Media, Joshua-Michele Ross, Forbes, June 30, 2009. http://www.forbes.com/2009/06/30/social-media-guidelines-intelligent-technology-oreilly.html

[26] Best Practices for Developing & Implementing a Social Media Policy, Society for New Communications Research, March 2007. http://sncr.org/sites/default/files/documents/tip%20sheets/SNCR_Social_Media_Policy_Best_Practices.pdf