Commercial Insurance Update

Topics Concerning Buyers of Commercial Insurance

MSP C 04/2010 – "Social Media and Its Risk Implication" April 2010
Commercial Insurance Update Newsletter

Social Media
and Its Risk Implications

By Don Phin, Esq., President of Employers Advisors Network, Inc.

Social Media includes such programs as FaceBook, MySpace, Twitter, LinkedIn, Yelp and YouTube. Each one of these Web sites has users numbering in the tens of millions, including employees that may work for you.

As with any communication technology, these new media forms bring with them considerable risks. Just as telegraph transmissions, phone calls, and e-mails carried with them unique liability exposures, so too does social media. Although the nature of those risks hasn't changed all that much, the environment in which they are incubated has changed considerably.

Social Media — a Whole New Game

Social media has exploded on the scene because it is:

1. Inexpensive
2. Accessible to all
3. Easy to use
4. Has a broad reach, and
5. Allows for instant feedback

It has been hailed as a social liberator (witness the "tweets" related to the Iranian elections), yet at the same time, a contributor to the "dummying down" of America. A writer in an April 2009 ***New York Times*** piece concluded that those most interested in social media represent the poorest among us. Perhaps it's because social media is dominated by gossip rather than by a discussion of significant events or ideas.

Social Media Is Everywhere — Yet Still Has Room to Grow

Despite its ubiquitous presence, social media is still a relatively new phenomenon. According to statistics generated by Deloitte's 2009 Ethics and Workplace Survey, as expected, most employers felt they had the right to access any information that is publicly displayed on their employees' social media pages. Conversely, most employees felt that such information was none of their employer's business. Big surprise there!

Most business executives I know and interviewed, shy away from spending time on social media, just like they don't waste time watching TV. From the gazillions

Social Media *(continued on page 2)*

In this issue...

Social Media *(continued from page 1)*

of articles I've read on this subject, my guess is less than one-third of executives actively use social media tools. That means as many as two out of three executives really don't know what this exploding phenomena is really all about, nor have they fully grasped the risks that accompany it!

The Risks as I See Them

An Enormous Waste of Employee Time Spent on Nonsense

Perhaps this is the biggest risk of all. Case-in-point: I saw one social networking site advertising a coffee mug that stated, "Social Notworking." I often speak and write about non-productivity being one of the greatest risks faced by any organization.

For example, assume you have 250 employees, $10 million in payroll, and that your workforce spends only 2% of its week using social media (of course, all of it for personal reasons). The bottom line impact to the company is at least $200,000 ($800 per employee), in wasted productivity — and that does not account for the return on investment (ROI) expected on that payroll.

In a time of recession and layoffs can any of our organizations afford to surrender this much of its profit margin in today's hyper-competitive economy?

Privacy Violations

A company that digs too deeply into someone's personal, social media activities can expose itself to privacy violation claims; almost a kind of "cyber stalking!" These claims may relate to the disclosure of medical information or a disability (thereby invoking the Americans With Disabilities Act, Health Insurance Portability and Accountability Act, and a host of other laws), to laws involving discrimination on the basis of marital status, sexual orientation, and so forth.

Clearly, a company that relies on information obtained from social media sites to make decisions in the hiring process, or uses it to manage its employees on a post-hire basis, can set itself up for breach of privacy type claims.

Sexual Harassment and Discrimination Claims

I remember when e-mail first came out how stupidly it was used, and the number of times evidence of sexual harassment had been preserved for eventual use in trial—even where the wrongdoing

Social Media *(continued on page 3)*

Risk Management Seminars

2010 Series

450 B Tower, 450 B Street, Suite 1800, San Diego, CA 92101-8005

- 7 Steps to Avoid Costly Employee Lawsuits
  Friday, May 21, 2010 7:30-10:00 am
- Sexual Harassment Prevention Training
  AB 1825 Compliant
  Friday, June 4, 2010 7:30-10:00 am
- Mid-Year Legal HR Update
  Friday, June 18, 2010 7:30-10:00 am
- OSHA 10-Hour Training
  Friday, July 16, 2010 7:00 am-5:00 pm
- Navigating the Leaves of Absence Minefield
  Friday, August 20, 2010 7:30-10:00 am

For more information about upcoming seminars

Click here to view our seminar list and individual flyers

To sign up for upcoming seminars

Contact **Darcee Nichols** at **dnichols@cavignac.com** or **619-744-0596**.

All training sessions available to our clients

Reserve early / seating is limited! *

* **NOTE:** Due to the popularity of our seminars and limited seating, we regret **we cannot provide refunds or credits with less than 72 hours advance notice of cancellation**.

Published by

Cavignac & Associates

INSURANCE BROKERS

License No. 0A99520

450 B Street, Suite 1800 San Diego, CA 92101-8005

Phone 619-234-6848 Fax 619-234-8601

Web Site www.cavignac.com

manager or employee thought it had been erased. As is the case with e-mail, social media has a never-ending shelf life to it.

Employees can also complain on their social media site that an employer or manager acts in a manner that violates discrimination laws. Once posted, it's too late to eradicate.

Wrongful Termination Claims

Employees who are disciplined or even terminated for their social media-based activities can claim that the termination constituted a violation of public policy (i.e., infringement on privacy rights, First Amendment rights, whistleblower rights, or they can make a claim on some other grounds).

National Labor Relations Act (NLRA)

The NLRA, which is enforced by the NLRB, prohibits an employer from interfering with employee discussions surrounding their work conditions (wages, vacations, hours, etc.) Employees are also protected in their "concerted activities," meaning their efforts to organize.

Lastly, it has issued guidelines that warn employers against e-mail policies that would infringe on their work-related communications. To learn more, go to www.nlrb.gov.

The Impact of Disgruntled Employees, Clients, Customers

Upset, vindictive, and scheming employees can cause considerable damage to former employers. Their negative postings can cause possible new-hire applicants to think twice about joining the firm, not to mention souring clients and competitors on the organization.

Disgruntled workers can also disclose confidential or proprietary information. Just as the guy who says too much at a trade show can undermine your efforts to maintain trade secrets, so too can the employee who says too much on his personal or company blog site.

Headhunters and Recruiters

Pretty soon everyone can know most everything about your employees. Headhunters, recruiters and the like love social media and actively use it to pursue candidates. Potential employees will look at it to determine if they want to work with your company, or even with specific employees.

So, how are your HR folks using social media? Because there is much disclosure of personal info (i.e., age, race, national origin, possible disabilities, etc.), many companies prohibit mangers from viewing these sites in the hiring process. Other companies say that is nonsense, and want to know everything they can about a potential employee. They have every right to look at a candidate's public site – and should.

The point is to not make decisions based on what you see that violates the law (such as age, race, etc.), but if applicants are stupid enough to post how many beer bongs they did last night or defame a former employer – you should think twice!

Sabotage of a Company's Reputation

Customers and clients can cause considerable damage to a company's reputation. A Bay Area restaurant was "attacked" by negative reviews on Yelp, a site that encourages reviews of a restaurant, shopping and other experiences. Rather than fight it, they decided to have their waiters wear shirts with the negative reviews printed on them.

Unfortunately it was reported that a Bay Area bookstore owner couldn't take the online criticism, and ended up in a physical altercation with the negative "Yelper."

Social Media technologies are ripe for such abuse. Fortunately, efforts at sabotage are usually apparent to most consumers. This is one reason why we suggest that you constantly monitor the Social Media sites to see if you or your company is mentioned.

Third Party Lawsuits

On the flip side, if you have employees who inappropriately place comments in social media that relate to clients, customers, other employees, competitors or other third parties, they can provoke lawsuits against you.

For example, the worker who talks about a client they hated or an employee who betrayed him/her, or tries to bash a competitor's products, may invite lawsuits for slander, defamation, or interference with business relationships against the employer.

The Federal Trade Commission (FTC)

The FTC wants to make sure blogs, etc. are compliant with Fair Disclosure Requirements (for public companies). It also doesn't want postings to go stale as they may cause confusion. Lastly, the FTC is

Social Media *(continued on page 4)*

Social Media *(continued from page 3)*

very much against anonymous postings that should really not be anonymous.

Finally, the FTC recently issued guidelines restricting the ability to use testimonials on blogs and other sites. Simply following a testimonial up with the phase "results not typical" won't cut it anymore. You must also reveal if you are paying, or being paid, for any endorsements (the "mommy blogger" rule). To learn more about these guidelines, go to www.FTC.gov.

The Permanence Factor

The evidence simply never goes away. Once it's out there, it's too late. No matter how swift and decisive are the measures taken to stop and eradicate false and slanderous material posted on social media, its effects linger on.

In fact, companies that actually try to alter Wiki pages, blogs and the like and attempt to remove unfavorable information or erase negative comments will get slammed by online communities that carefully monitor Web and social media manipulation.

What Can A Company to Do to Reduce Its Risks?

Now that I've discussed the nature and scope of social media risks, here is a list of action steps that a company can and should take to minimize these exposures today.

1. Grab as many Social Media sites with your company name as soon as possible.

   Note: In an attempt to shift corporate responsibilities, a number of larger companies report placing their blogs and community sites under separate business entities. We'll have to see if that approach actually works.

2. If you are not already doing so, monitor your own social media Web sites by using Google Alerts, Technorati, and other tools.

   Accordingly, companies should be concerned with comments and track-backs which are back links to their site from an external media site. Make sure you respond to negative comments (see "The Employee Viewpoint," opposite column).

3. Consider using employee monitoring software. According to the Gartner Group, spending on security software rose by close to 19% (to over $13 billion) in 2008. Again, one of the fastest growing areas is forensic software, which can record and replay everything that has happened on the employee's computer screen.

   As always, whenever you use any type of employee monitoring, make sure to inform your employees, identify the legitimate business purpose, and then enforce any policies uniformly.

4. Create a Social Media Policy and communicate it. Get employees involved in the process. Don't let them play victim on you in this area — give them a part in formulating the policy.

   Make sure your employees acknowledge receiving the policy in writing, and then verify that they comply with it. According to a Robert Haft technology survey published in October 2009:

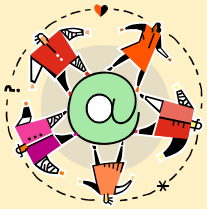
   - 54% of the companies polled ban all workday social media use
   - 19% allow it for business purposes
   - 16% allow limited personal use
   - 10% all full access

5. Have a plan or process for managing and responding to problems. As with any type of risk management planning, think of some possible case scenarios for your business, and then develop a plan for managing them.

Social Media *(continued on page 5)*

The Employee Viewpoint

I have scoured the Internet to see what types of comments employees post about their employers' efforts to restrict their access. What follows is a fairly representative sample of the overall comments:



- "Judge us on outcomes, not activities."
- "It's 'creepy.'"
- "Don't you trust us?"
- "It's so old school."
- "All my friends get to do it."
- "It's how we get to communicate."
- "Zappos does it, why can't we?"
- "All games should be blocked."
- "I don't know why anyone would waste their time doing it anyway."
- "If you have to worry about it, maybe you're hiring the wrong people."
- "I need the release every once in awhile."

For example, draft an entire response protocol to manage negative or inappropriate blog postings about your company.

6. Educate employees on social media in general. Help them understand how it works and the distinction with public and private settings.

Survey your employees on their social media use and concerns, and then get them involved in formulating a reasonable company policy.

Creating a Social Media Policy that Makes Sense

- **Definitions –** What is meant by Social Media? Exactly what do you consider to be a private, employee-based communication versus a company-based one?
- **Use of Company Equipment –** Are you going to let employees use company tools for personal reasons? If so, which ones? When? Why? With what limits? What about company issued cell phones?
- **Monitoring –** Who's watching what? What disclosures must be made? In almost any privacy case, a court will require the defendant to show that less intrusive alternative means were not reasonably available to do the monitoring.

  Furthermore, even if the intrusion is proper, once an employer delves into matters not related to its business, it must stop on a dime. The court also reminded us that privacy is not wholly lacking simply because the occupants of an office can see one another, or because colleagues, supervisors, visitors, and security and maintenance personnel have varying degrees of access.
- **Accuracy of Information –** Any post should be factual, timely, and within the employee's scope of expertise. Logging in under false identity is known on the online world as being a "sock puppet."

  Similarly, setting up fake blogs, known as "flogs," is something for which Sony was ridiculed when it created a blog, allegedly written by a kid, asking his parents for a Sony game console. The company and its employees should also stay away from using any "parody" sites.
- **Personal Use –** Since most employee use of social media is for personal reasons, its use should generally be restricted to personal time.
- **Training Requirements –** Don't assume most employees automatically "get" any of this — so make sure they do. Devote segments for discussing social media risks in both harassment training and computer security training. Discuss it in marketing meetings, as well as during the orientation process.
- **Create a FAQ –** Many companies will also include a Frequently Asked Questions document, to accompany their social media policy. Include the following among the questions that could be asked and answered:
  - What right does an employee have to access their MySpace, FaceBook, and other social media sites while on company time?
  - Can the company read personal messages sent by friends or relatives who are unaware of the policy?
  - What are employees allowed to say about their workplace on my MySpace or FaceBook page? They may have a First Amendment right to disagree with certain company actions, but that doesn't mean you have to keep them employed.
  - If an employee is sincerely interested in promoting the company, what is the best way to do so?
  - What types of postings would the company deem to be inappropriate, so an employee can avoid them?
  - What are some specific examples of appropriate and inappropriate postings?
  - Identify the "Go To" team. Who is in charge when there is a problem? IT? Legal? HR? Marketing?

The Bottom Line

By following the recommendations above, you can help prevent these Social Media risks. If you are interested in a basic Social Media policy, please contact me at don@hrthatworks.com.

*Don Phin is President of Employer Advisors Network, Inc., and author of the **HR That Works** series of compliance and management products. For more information, visit*

http://www.hrthatworks.net/index.aspx

Articles courtesy of Cavignac & Associates Employee Benefits Department

LIVE WELL, WORK WELL

IRS Scams Increase

Protect yourself from online identity theft and other scams that increase during and just after the filing season. Such scams have been known to impersonate the logo, names and design of the IRS or U.S. Department of Treasury to mislead taxpayers into believing the scam is legitimate.

The "Refund Scam" is the most common IRS-impersonation scam during the filing season. A bogus e-mail claiming to come from the IRS says that the recipient is eligible for a tax refund of a specified amount. To claim the refund, the recipient must fill out a claim form requiring the entry of personal and financial information. Use extreme caution, as this scam claims to be sent by the Exempt Organizations area of the IRS or from a genuine or made-up name of an IRS executive.

Watch for E-Mails that:

- Request personal and financial information. The IRS does not send unsolicited e-mails to taxpayers. It does not discuss tax account information with taxpayers via e-mail, or use e-mail to solicit sensitive financial and personal information from taxpayers.
- Threaten a consequence for not responding to the e-mail, such as additional taxes or withholding the refund.

If you are sent a suspicious e-mail, visit www.irs.gov and use the "Where's My Refund?" tool, not the e-mail, to determine your refund amount. Then forward the e-mail to the IRS and delete it from your inbox.

Dangers of Driving Drowsy

We all know that driving while sleepy isn't smart, but just how dangerous is it? Studies show that driving while sleep-deprived can be just as hazardous as driving while intoxicated. Both result in decreased alertness, which will impair your reaction time.

Keep the following tips in mind to make it safely to your destination:

- Avoid driving between midnight and 6 am, if possible.
- Pull over and stop if you feel sleepy. Even a 20 minute nap can make a difference in your alertness.
- Caffeine may keep you alert, but it is only a temporary solution.
- Avoid making long drives after you've lost sleep.
- Above all, call for a ride if you're too sleepy to drive.

Community Bulletin Board

"Neighbors helping neighbors in San Diego"

Monarch Schools

- Volunteer
- Web Site

San Diego Humane Society and SPCA

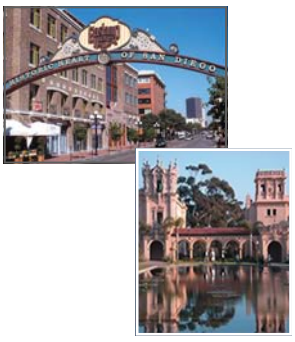
- Walk for Animals
- Web Site

Downtown YMCA

500 West Broadway, Ste. B, San Diego 92101 619-232-7451

- Web Site
- Newsletter
- Questions? Contact **Alicia Gettys** by phone at **619-232-7451** or e-mail **agettys@ymca.org**

SDAF San Diego Architectural Foundation



- Web Site
- Questions? E-mail **info@SDArchitecture.org**

Senior Community Centers

Mission:

To provide quality and compassionate services for the survival, health and independence of seniors living in poverty

- Impact Areas
- Web Site

San Diego Police Foundation

The San Diego Police Foundation supports the men and women who "protect and serve" by raising community awareness of important unbudgeted or "discretionary" needs that will improve crime-prevention and law enforcement efficiency. The Foundation puts your tax-deductible contributions to measureable work in local communities.

- Web Site
- Ask the Chief
- For more information, contact **info@sdpolicefoundation.org**

Society for Design Administration

An Affiliate of the American Institute of Architects

Mission:

The Society for Design Administration advances management and administrative professionals in the A/E/C industry through education, networking and resources.

- Become an SDA Member
- Web Site
- For more information, e-mail **vicepresident@sdasandiego.org**