

7 steps to effective social media risk management

Step 1: Assess the risks of what your bank is doing

By Raj Chaudhary and Erika Del Giudice, Crowe Horwath LLP. For more about the authors, see the conclusion of this article. For more about Crowe's social media advisory practice, [click here](#).

The power of social media channels such as Facebook (which reached one trillion page views in June), Twitter (with 100 million active users monthly), and LinkedIn (with 63% more visitors in June than it had a year earlier) cannot be denied. These channels provide an enormous opportunity for financial institutions to build employee and brand loyalty, communicate with customers, and increase their customer base. With this opportunity, however, comes increased risk.

Social media's most damaging potential impact is on reputation. Employees, customers, and vendors can be a bank's greatest ambassadors--or undermine its brand and public image. Realistically, no one can control or change what is said online, but banks can monitor comments and respond to them in a timely and appropriate manner.

Beyond reputational risks, social media exposes banks to legal and employment risks as well. Banks and other organizations are using social media not only for its marketing benefits but also for the networking opportunities it affords employees and employers alike.

As one might expect, regulators and courts are litigating and otherwise addressing new legal and employment issues. That these cases are being determined under laws that were designed before the age of Facebook--and therefore are outside the context of this relatively new and evolving technology--heightens the possibility of exposure.

In addition, technical attacks via social media expose banks to information security risks.

Keep up with bank social media ideas, trends, and warnings

Have you checked out our periodic blog, "Social Media: Banks' New Frontier"? Both staff authors and outside experts cover case studies, key trends, best practices, and ways to protect your bank and keep it in compliance. The blog is an online companion to periodic articles in ABA Banking Journal magazine.

Among the deceptive practices are "clickjacking" (getting a Web user to click on a seemingly innocuous button that takes control of the computer); link shortening; social engineering tactics, and the gathering of challenge question answers based on Facebook information.

Following are seven steps that provide guidance on mitigating existing risks--including reputation risks, risks of using social media for candidate screening and employee termination, the risk of virus attacks, and the risk of employees making company information public.

Mitigating the risks

None of the myriad risks associated with social media use can be eliminated completely. But taking a thoughtful and structured approach to understanding and assessing the risks and then developing and implementing a comprehensive plan will reduce a bank's susceptibility. To deploy an effective social media risk management strategy, we recommend banks take the following actions.

1. Engage a multidisciplinary team. Social media is not just an IT or marketing problem.

Since social media activity affects a wide range of functions, an effective strategy brings together senior representatives from Human Resources, Legal, Information Technology, Marketing, Risk Management, Public Relations, Compliance, and any other affected functions.

Assigning a project or program manager will help to track and maintain the team's progress.

2. Document current and intended social media use. The multidisciplinary team's first order of business should be to document how each department currently uses social media and how it intends to use it in the future.

It's up to the multidisciplinary team to use the bank's overall strategy as a guide to determine which types of social media use align with organizational objectives. The team then establishes how the bank--including its employees, recruiters, marketers, and IT department--will use and be affected by social media. Having multiple people involved in making these decisions can present a challenge, but having one person responsible for the execution of the social media strategy--and having the support of senior management--will move this process along more quickly.

3. Perform a risk assessment. Before the multidisciplinary team can even consider safeguards and controls, it must identify and quantify the various risks associated with social media use.

This risk assessment takes into account the likelihood and potential damage resulting from occurrences such as employee defamation of the bank, its products, or its leadership--as well as any other risks to which social media use exposes a bank. The risk assessment also involves identifying the controls that are already in place, which could be mitigating a portion of the risk. To help prioritize the most significant risks, a bank can determine the sufficiency of these controls and work them into an overall residual risk rating.

4. Expand current policies to include social media. Once risks have been identified, it should be apparent whether, and where, the bank's policy needs to be expanded in order to better address the risks.

A bank can choose to centralize social media guidelines by including them in a single policy. Or it could incorporate the guidelines into existing policies and add new content to cover social media risks. Whichever option a bank chooses, the policy needs to be easily accessible to employees and cover some basic topics: appropriate and inappropriate employee use of social media; human resources policies; information security policies; marketing and communications policies; and vendor management policies.

A 2011 survey by nCircle found that 68% of companies have social media policies--up from 58% in 2010. (How many employees follow them is a different question.)

5. Implement safeguards. A Proofpoint survey from August 2010 found that one in five U.S. companies had investigated a data leak that occurred via a posting on a social media site.

Social media is a channel unprotected by typical information security safeguards, which tend to focus on an organization's controlled network. As such, organizations must evaluate a new set of information security risks and mitigate them with information security policies and controls.

6. Provide social media training. Even the best policies will be ineffective if employees don't understand them.

It's critical for a bank to invest its time and resources into educating its workforce about the intricacies of its social media policy. Training should include examples of appropriate and inappropriate communications and actions, distinguishing between positive and negative use of the medium, and highlighting the constant threats present on these sites. In addition, training should not be a one-time occurrence, but, rather, an ongoing effort.

7. Monitor social media channels. Banks also need to consider how they will stay current on social media chatter that could have an impact on their objectives.

Social customer relationship management (CRM) tools, composed of software products and vendor services, can help banks monitor public channels for social media chatter that could affect the organization. How an organization responds to negative comments made via social media entails significant risks of its own.

Nestlé's Facebook page, for instance, was inundated with negative comments in March 2010 following a Greenpeace campaign against the company's use of palm oil. The company's attempt to restrict commentary drew more unwanted attention to the issue and created a public relations disaster.

Risks of doing nothing

So maybe you're thinking you can avoid altogether the many risks related to social media use. Simply eliminate its use in marketing, recruiting, and other bank departments, and ban employees from using it on company time or equipment.

However, failing to exploit the opportunities social media provides for building a brand, attracting new customers, and retaining current customers exposes banks to risks, too.

Banning any official participation in social media ignores the positive effects of using a powerful channel appropriately to build relationships with stakeholders, customers, potential employees, and other affiliates. Banks would give up the ability to use a potent communication tool and expand the reach of their products and services in a quick and cost-effective manner.

Face it: Social media channels have become part of the fabric of social interaction for an increasing segment of the population, and it's impossible to put the social media genie back in the bottle.

However, organizations that formally assess the risks of social media and implement guidelines that promote its responsible use will be better equipped to reap the benefits of these new tools.

About the authors

Raj Chaudhary, PE, CGEIT, CRISC, is a principal with Crowe Horwath LLP and is based in the firm's Chicago office. Reach him at raj.chaudhary@crowehorwath.com

Erika Del Giudice, CISA, CRISC, is with Crowe Horwath LLP and is based in the firm's Chicago office. Reach her at erika.delgiudice@crowehorwath.com

For more about Crowe's social media advisory practice, [click here](#).

This e-mail address is being protected from spam bots, you need JavaScript enabled to view it This e-mail address is being protected from spam bots, you need JavaScript enabled to view it