GLOBAL riskupdate
The quarterly independent risk review for banks and financial institutions worldwide
JUNE 2014

2014
A Year of Challenge for the Banking Industry

Also in this issue

- Global Banking Standards: A Long and Stoney Road Ahead
- How Auditors Can Overcome the Strategic Challenges Posed by Basel III
- Debt: Does It Continue To Be There?
- Banking in Emerging Markets – Female Entrepreneurs and Financial Literacy
- Managing the Risks of Social Media
- Star Trek Banking – When Disaster Strikes!
- The Bank for International Settlements and Large Exposures

Managing the Risks of Social Media

Jeremy Swinfen Green is a Principal Consultant of Social Media Risk Consulting Ltd. He contributes the article with the intention of explaining that, as well as offering many opportunities, social media present all organisations with substantial risks but that these risks can be managed effectively.

Social media? Where's the risk in that?[1] After all, the great majority of organisations use social media for marketing. There are some very obvious benefits, not least "free" advertising and the deeper engagement with consumers that companies can create through platforms like Facebook, YouTube and Twitter.

But there are also some very real risks that are attached to social media. These risks exist whether or not your organisation is using social media proactively for marketing or PR. And they are not just IT risks – because most concern people rather than technology. As a result, normal digital risk management, which tends to focus on cyber-security, is often insufficient protection.

What is social media risk?

Most social media risk concerns the potential for people to say something inappropriate on public social media platforms. This can result in problems with financial or communication compliance. Saying the wrong thing can have damaging effects on brand and on sales. And it can even cause HR and recruitment problems.

Why is social media risk such a problem? This is simply because it exists on the internet, which gives rise to a number of issues:

- Social media content is potentially permanent. Say something online and your words will be recorded on a server somewhere, and the chances are that someone will be able to find them in the future. Yet many people think of it as being ephemeral But even with Snapchat, the handy app that allows you to send pictures that self-destruct after a few seconds, supposedly ephemeral images can be recorded using screen capture
- Many people think of social media content as being private, when in reality it is often highly public. You can choose your Facebook privacy settings but you can't prevent people you link to (who may well not be genuine friends) sharing your content with other people if they want to
- Many people think of social media as being somehow "unofficial" and outside the law, failing to realise that any words can have a legal implication in the right (or wrong) context
- Social media content is, by definition, easy to share, and as a result content can be circulated across the whole globe very rapidly, especially when that content gets picked up and amplified by more established media platforms such as newspapers
- It is relatively easy to remain anonymous when you use social media, allowing people to say things that are essentially unaccountable

Personal or professional?

For most organisations though there is another factor that increases the difficulty of managing social media risk: the fact that corporate, personal and professional spaces tend to blur in social media.

Only a small minority of employees are likely to be active on "corporate" social media accounts, contributing to a company-owned discussion board perhaps or writing a blog piece for their employer.

However, most people of working age have "personal" social media accounts such as a Facebook page. And as often as not something to do with their working life will creep into their private social media activity, even if it just a comment about the company Christmas Party or an expression of frustration with a client.

As well as their own "private" Facebook accounts, many people also have "professional" accounts, perhaps on Twitter or LinkedIn, which they use for personal PR and to advance their careers, and where they may well be talking about their employer.

This is the danger. Any organisation should be able to manage content on their corporate accounts (although there are plenty of examples where this hasn't happened). The content on the personal and professional accounts is far harder to manage. But it can still have an effect on the organisation.

The IBM Social Computing Guidelines put it like this: "The lines between public and private, personal and professional are blurred in online social networks. By virtue of identifying yourself as an IBMer within a social network, you are now connected to your

[1] *Eagle-eyed sticklers after grammatical exactitude should note that I sometimes use "social media" as a singular noun representing a type of internet application that allows people to create and share content and to participate in online networking.*

colleagues, managers and even IBM's clients. You should ensure that content associated with you is consistent with your work at IBM."

Size of the risk

The effect of adverse social media content can be massive. In April 2013 an organisation called the Syrian Electronic Army was widely reported as having hacked into the Twitter Account of Associated Press where it sent a potentially disastrous tweet, falsely reporting two explosions at the White House and injury to the President.

The initial response was panic on Wall Street with the Dow Jones dropping 100 points and $140 billion being wiped of the S&P500 index for a short period.

Of course most of the time social media doesn't represent anything like such a large risk. In fact often any damage caused is limited to people in the marketing community laughing at a brand. But nonetheless the risk can be substantial: Directors have been fired for irregular financial disclosure (US retailer Fransesca), brokers have been fined for inappropriate marketing (Jenny Quyen Ta), and client accounts lost for rogue employee tweets (consultancy New Media Strategies which lost Chrysler).

There are bigger stories too. Take Kryptonite Locks: one of their bike locks was "outed" as being easy to pick in an online forum; the post went viral, leading to massive reputational dame and costs alleged to be around $10million. And some people have linked a 10% drop in the value of United Airlines in July 2009 to a video posted on line by musician Dave Carroll singing about how "United Breaks Guitars". Of course you don't need social media to destroy your business (remember Gerald Ratner?) but it helps.

Across the board

The negative effects of social media can be felt right across an organisation and they are not all to do with organisational reputation, as some people assume. Many risk area are concerned with profits, while others stem from laws and regulations, and there are considerable risks in the HR area as well.

Because of the widespread nature of social media risks it will rarely be appropriate to have social media managed by a single organisational function, such as marketing. Ideally there will be a cross-functional team (marketing, legal, IT, finance, HR, operations) overseeing the risks with an experienced executive in charge of "triaging" any incidents to the appropriate members of the team.

Types of risk

Risks to profits include:

- Entering into or altering contracts accidentally
- Losing Patent protection
- Being sued for stealing 3rd party IP
- Being sued by a client for disclosing confidential information
- Loss of control of social media assets

Risks to brand reputation include

- Rogue employee tweets offending customers
- Discovery of obsolete marketing content
- Customer complaints escalating into a full scale PR crisis

Risks to employee management include

- Bullying by colleagues
- Intrusions on staff privacy
- Employees being put in physical danger
- Damage to organisation's reputation as an employer

Risks from legislation include

- Publishing illegal content e.g. incitement to hate
- Inappropriate disclosure of financial information
- Libel suits
- Fines for illegal marketing from industry regulators

How is risk triggered?

Risk events can be triggered by a variety of factors, both internal to an organisation and external.

The Board

Internally, risks start with the Board. If there is insufficient oversight, if executives are not held to account, then social media risks will increase. And while many Board members will use social media in their own personal lives they may well be naïve about the implications for business.

There are a number of implications that relate to corporate governance. At the simplest level it is easy to disclose financial information inappropriately through social media. Even a social media post along the lines of "Board meeting: didn't we do well!" could fall foul of the regulators.

In the USA, the SEC has extensive and sensible guidelines for social media. In the UK the FCA says that the old FSA guidlines still stand and that these guidlines are platform agnostic. These include somewhat vague statements like "Twitter…may be insufficient to provide balanced & sufficient information" which don't address the difference between "static" content like website articles and "interactive" content like forums and online chat.

At this stage Boards in the UK probably need to second guess what might upset regulators in the future and play it safe.

The Board also has a responsibility to ensure appropriate processes are implemented and managed properly by ensuring:

- social media management and training is in place
- security protocols for corporate social media are adequate
- adequate social media records are kept
- advertising standards are complied with

Board members (and indeed other prominent employees) have another responsibility: to ensure that their own personal or professional use of social media is appropriate and secure. There have been a few cases of senior employees having their Twitter accounts hacked. It probably doesn't matter too much if Jamie Oliver's Twitter account is hacked and sends out tweets promoting diet plans. But if the Twitter account of a High Street Bank's Chief Exec was suddenly to send out messages saying the bank was in trouble it could have a massive effect on share price and even cause a run on the bank. No, it hasn't happened yet…

Employees

Employees also represent a very significant source of risk by talking about their business, colleagues or industry inappropriately. The problem is generally caused by naivety about social media and what it is inappropriate to say or do.
This isn't a hard problem to solve. All organisations should have in place a formal social media policy that gives employees guidelines about their use of social media. All too often though there are problems caused by:

- The lack of a formal social media policy
- An insufficient social media policy
- A failure to explain the social media policy (and the sanctions that attach to it) to employees

It is not sufficient to have a few lines about social media in the employee handbook. The social media policy should be a key strategic document, customised for each organisation.

There is a special sort of employee who can also cause problems: marketers. When marketers get it wrong their errors may well, because of the nature of what they are trying to do, be amplified by other marketing channels. Of course there are plenty of excellent marketers with experience of social media. But where social media is left to an ambitious but inexperienced junior then you can expect problems (or at the least, wasted investment) to happen.

Ex-employees can also be a problem as they sometimes still have the "keys" to social media accounts. Access to company email and files on servers are disabled as a standard but if there is a lack of control over who can use corporate social media accounts then all too easily an ex-employee can retain access to them. There is a potential for "revenge" posts if the ex-employee is unhappy; at if they have moved to a competitor company then there is the potential for confidential data to leak out.

The public

Managing the public through social media is a skilled and difficult task. It is

one that it is almost impossible to get right 100% of the time: there will always be some people who are offended by something.

The skill is in deciding what represents a crisis and what doesn't. Some complaints are probably worth ignoring. Most should be responded to positively and helpfully – after all complaints represent a source of competitive advantage, if acted on appropriately. (They tell you how to improve your service.)

But sometimes you will be faced with a crisis that spreads beyond one or two unhappy customers. This is why preparing for the possibility of a social media crisis is important. You can never know exactly what might happen. But you can make some educated guesses. The CEO might leave unexpectedly. A new product may fail to perform properly. An employee might be caught out lying to a customer… A review of problems that have previously happened in your industry will give you some pointers.

Once you have identified likely problems you can think about how you would want to manage those problems. What initial holding statements would you issue? Who would be your main spokesperson? Who would be in the crisis team and how much freedom of action would they have?

It is important to prepare well. But as well as preparing it is important to practice by setting up a simulated social media crisis. Having a dry run will test your crisis management system (for instance, does your escalation process work; do people understand the guidelines within which they have to operate?) And it will give people a realistic experience of what it is like to handle a crisis. (It can be very stressful and sometimes personally hurtful so giving people some experience of what it is like is invaluable.)

Managing social media risks

Social media risks are like any risks. While you can't prepare for every eventuality, a rigorous and structured approach will minimise the likelihood of major disaster and enable most difficulties to be managed effectively.

- **Audit:** The first thing to do is to **audit your risk profile** and create a comprehensive register of the risks that apply across the whole of your organisation, and proposals for mitigating those risks
- **Listen:** Next you need to **implement appropriate "social listening" tools** so that you are aware of any relevant social media activity that might represent a risk. The chances are that your marketing department may already be using a listening tool but this needs to be rolled out across your organisation with a single person responsible for identifying problems and notifying the appropriate people
- **Educate:** Then you will need to **ensure you have a sufficient social media policy** in place; importantly employees (most especially senior employees) will need to be trained in its use and made aware of sanctions for failing to use it
- **Manage:** You will need to **manage your social media risk activities;** monitoring them to judge whether they are being followed and whether they are effective
- **Archive:** Most organisations, but especially those in regulated industries, will need to **archive all social media conversations** so that there is a sufficient record of them should that be needed
- **Prepare:** And you will need to **prepare to meet and manage problems** by creating temporary holding statements, generic responses, guidelines for managing a crisis, and practising your actions

None of this is particularly difficult. But it does take attention to detail as well as a willingness to take these risks seriously. It is unlikely that the worst will happen: but it is very likely that some of the risks you identify will come to pass and without due preparation their effects will be far worse than need have been the case.

The author invites your comments via email to JK@riskrewardlimited.com

For further information please contact:

Dennis Cox – CEO
telephone: +44 (0)20 7638 5558
email: DWC@riskrewardlimited.com

Lisette Mermod – New York
telephone: 1-917-310-1334
email: LM@riskrewardlimited.com

Joanna Kraska – Public Relations
telephone: +44 (0)20 7638 5558
email: JK@riskrewardlimited.com