7

Crisis Communication Plan in Action: Social Media

Keywords: **legacy media, social media, digital media, blogs, YouTube, Flickr, Twitter, Facebook, citizen journalist, micro-communities, social media monitoring, reputation management, search engine optimization, RSS feeds, tag cloud, hardball, take-downs, NGOs, Risk IT, COBIT, SMART team**

Whatever your experience relating successfully with traditional media – newspapers, magazine, television, and radio – the challenges and the opportunities of the new media are rapidly eclipsing the reporting and predictability of legacy media behaviors. Readiness today requires that current crisis management plans include a good working knowledge of the new media, functioning digital communication platforms, including dashboards, as well as applying time-tested media tactics.

This chapter will help you to:

- ➢ Understand how social media can supersede media relations.
- ➢ Assess your “web readiness.”
- ➢ See the growing influence of the “citizen journalist.”
- ➢ Monitor social media, assess its impact.
- ➢ Consider the ways in which you could use social media to help your company’s business.
- ➢ Identify the ways in which social media could be used to attack your company’s reputation.

7.1 What Makes Social Media Different From Legacy Media

Two distinct categories of media have now evolved – traditional or legacy media (see Chapter 4 of this book) and social media. What makes social media differ from traditional media is that the social media employ readily available web-based technologies, such as popular networking sites, to allow ordinary users, acting independently, to generate content, to share content with other users, to integrate content across networking sites, and to disseminate the content to a large audience almost instantly. Social media have injected new intensity, urgency, and effectiveness into the media relations equation:

- The emergence of the "citizen journalist."
- Instant, sometimes astoundingly broad distribution of "news."
- Direct reporting from individuals to local, national, and sometimes international audiences through iReports and web portals at all national networks. Most TV station news websites allow direct uploading of video content from citizen contributors who have produced video reports, which are aired virtually as they are submitted. In 2011, 22% of video on CNN came from citizen-submitted content through ireport.cnn.com.
- Elimination of the professional journalist, along with the entire time-consuming news editing and vetting process.
- Permanent shattering of the journalist/legacy media trust relationship with audiences, especially newspapers.

7.1.1 Changing Trends in How People Get the News

Newspapers everywhere are failing or struggling to survive, literally coast to coast. The same condition is true for many weekly and monthly news magazines. Recent Pew research monitoring the relationship between the American public and the news media appears to indicate that the American public no longer depends on newspapers as it did in the past. With the exception of National Public Radio (NPR), reliance on radio as a source of news is in full decline. While radio news still remains a staple at drive times, it is mostly "rip and read" services using the Associated Press and other news services. National Public Radio seems to be the only truly functioning news radio network in America today, but it is reducing the "news hole" in favor of music and arts features, and its Federal funding by the US Congress remains an issue. Still, the statistics indicate that, on the whole, the public tends to rate radio as more valuable than newspapers (Pew, 2010).

Television, which used to be first to serve the news, is now a poor second to social media. Nevertheless, respondents in a Pew study rated television significantly ahead of radio as a reliable and trusted news source (Pew, 2010). The decline in reliance on television news reflects the real-time information source competition from social media, talk channels, other Internet sources, and the rise of smart phones and smart communication tools.

The big surprise to the journalism community in this study is the public response to social media. The two major trends identified by the Pew study are 1) social media, and 2) mobile connectivity. Pew statistics reflect extraordinary levels of public trust and interest in social media as a source of information (Pew, 2010).

The report states, "Beyond the chatter about news that takes place in email exchanges, a notable number of Internet users are beginning to treat news organizations, particular journalists, and other news mavens as nodes in their social networks. In this survey we found that 57% of online Americans use social networking sites such as Facebook, MySpace or LinkedIn – and 97% of them are online news consumers. Some 51% of the social networking users who are in the online-news population say that on a typical day they get news from people they follow on sites like Facebook. That amounts to 28% of all internet users who get news via social networking with friends" (Pew 2010).

The broad acceptance of new media has raised questions and issues about this news coverage:

- Who is a journalist?
- What is journalism? Does this matter anymore?
- Who answers these kinds of questions?
- How important is a journalistic approach when so many of their social media sources seem to be untrustworthy, uninteresting, or unnamed?

Whatever the current state of flux of media relations, communication in a crisis now has new strategic and valuable channels.

Whatever the current state of flux of media relations, communication in a crisis has new channels that are strategically valuable. The challenge for the communicator is to use both new and old channels strategically in order to effectively, promptly, and credibly get information out.

7.1.2 Coping With Crises in a New Media Environment

Digital and social media have changed the way we communicate, redefining the meaning of "crisis response." By the time a crisis winds down, how promptly and directly an organization has responded can determine both its reputation and its future viability. The problem is how to respond in the digital and social media age. When news "reporting" is instantaneous, anyone can take on and easily embarrass a major corporation, politician or organization, and every misstep is magnified.

BP / Deepwater Horizon

On the evening of April 20, 2010, the Deepwater Horizon, a drilling platform in the Gulf of Mexico leased by British Petroleum (BP) exploded and caught fire. Eleven workers died, and survivors floated in the cold seas waiting to be rescued, watching the platform burn and sink into the mile-deep waters. As untold quantities of crude oil began bubbling up from the damaged well threatening the Gulf region from Texas to Florida, the story spread via digital and social media to millions. By the following morning, newspapers had caught up with the digital media and the 24/7 news cycle, which had been reporting on the catastrophe throughout the night.

At the outset of the crisis, how did BP respond to the crisis and the communications challenges? It is important to be aware that the U.S. Oil Pollution Act of 1990 promulgated in the aftermath of the Exxon Valdez oil spill, requires that drilling platforms must adhere to the same guidelines as a ship. First, the parties involved activated their crisis plans, issuing notifications and launching their unified command protocol, under which the U.S. Coast Guard acts as the central command for disaster response and as the central voice for the rescue mission and clean-up.

To ensure that it had controlled communications from the company's perspective throughout the response to the disaster, BP immediately launched several communication platforms. Hourly posts included links to images, videos, and news updates. The Houston-based crisis center was staffed by communications professionals flown in from BP's offices around the world. The company also hired a Washington, D.C.-based PR and public affairs agency to interface with the many federal regulatory agencies and the legislative and executive branches of government.

Web-based communications enable companies and individuals to communicate vast quantities of information to multiple audiences at the same time. To be sure that the facts going to the traditional media and new media were accurate, BP launched a micro site with the latest postings from the company and its suppliers. In addition to press releases, fact sheets and other bulletins, the company posted photos, maps, diagrams and videos. Thirty days into the crisis, millions of viewers, including the media, were watching the oil leak and kill attempts in real time from a video feed at BP's website. Of course, BP communicated through conventional channels, as well, issuing press releases, news conferences and providing interviews by phone and in person. But the heavy lifting was taking place on the web and in Facebook, Twitter and YouTube.

7.6 Digital and Social Media Crisis Management Recommendations

7.6.1 Establish a Useful, Helpful Social Media Policy to Moderate the Risks

Text and figures in Section 7.6.1 are reprinted in their entirety from ISACA (2010). *Social media: business benefits and security, governance and assurance perspectives* (Emerging Technology White Paper), 6-10. Used with permission.

Since enterprise use of social media tools usually requires no additional technology to implement, an enterprise social media presence does not always begin with a project plan and risk assessment. To effectively control social media usage by both the enterprise and employees, a documented strategy (and associated policies and standards) should be developed with the involvement of all relevant stakeholders, including business leadership, risk management professionals, and human resource and legal representation. This holistic approach to integrating emerging technologies into the enterprise helps to ensure that risks are being considered in the context of broader business goals and objectives.

While the use of social media presents an additional entry point for technology risks such as malware and viruses, these risks are elevated primarily because more employees may be using social media sites without understanding the threats that exist. Therefore, any strategy to address the risks of social media usage should first focus on user behavior through the development of policies and supporting training and awareness programs that cover:

- *Personal Use in the Workplace:*
  - ❒ Whether it is allowed
  - ❒ The nondisclosure/posting of work-related content
  - ❒ The discussion of workplace-related topics
  - ❒ Inappropriate sites, content or conversations
  - ❒ Alignment with/part of the acceptable use policy
- *Personal Use Outside The Workplace:*
  - ❒ The nondisclosure/posting of work-related content
  - ❒ Standard disclaimers if identifying the employer
  - ❒ The dangers of posting too much personal information
- *Business Use:*
  - ❒ Whether it is allowed

❒ The process to gain approval for use

❒ The scope of topics or information permitted to flow through this channel

❒ Disallowed activities (installation of applications, playing games, etc.)

❒ The escalation process for customer issues

Training should be conducted on a regular basis and should focus on the benefits and opportunities as well as on the dangers related to use of social media. Emphasis should be placed on the specific dangers and methods of social engineering, common exploits, and the threats to privacy that social media present. Training should also ensure full understanding of the rules governing acceptable use and behavior while on social media sites.

Technical controls that exist for other e-commerce opportunities will benefit the enterprise when embracing a social media strategy. Technology can assist in policy enforcement as well as in blocking, preventing or identifying potential incidents. This strategic component should utilize a combination of web content filtering, which can block all access, allow limited access, and in some cases provide protection against malware downloads and end-user system anti-malware, antivirus and operating system security to counter such attacks. As with most security technology strategies, a layered approach is optimal.