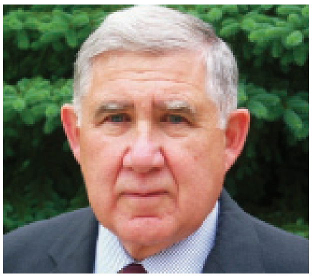
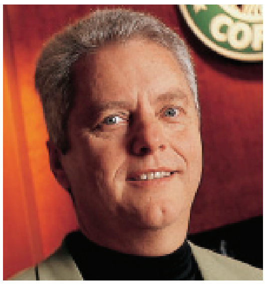


Rad Jones, *academic specialist in the School of Criminal Justice, Michigan State University; former international security manager, Ford Motor Company*

Kathleen Kotwica, *executive vice president and chief knowledge strategist, Security Executive Council*



Francis D'Addario, *emeritus faculty, Security Executive Council; former vice president of Partner and Asset Protection, the Starbucks Coffee Company*

Chuck Eudy, *principal at Chuck Eudy Corporate Communications Inc.:*

How might I respond to a Web-based incident that causes significant brand damage?

Crisis management helps to protect four types of assets: people, property, information, and reputation. When I talk to a company about crisis response, I emphasize the importance of a crisis management team that includes key executives from human resources, marketing, legal, operations, security and other key functions.

The same processes used to prepare for a fire, an explosion or severe business disruption are also helpful in preparing for a Web-based threat to the company's reputation. What is the damage to the product? What is the marketing and sales recovery strategy? What are the legal options/concerns? Are there proprietary information issues? What is the financial impact?

The crisis management team process brings everyone to the table to discuss how to respond. Tabletop exercises prior to an incident will help the team respond during an event.

You don't have to decide things under fire if you have already considered critical incidents in a relaxed and thoughtful atmosphere.

If there is already significant brand damage, it is too late to ask the question. The most important activity surrounding brand damage incidents, whether or not in the Web world, is to have a brand reputation crisis strategy.

First, assess the possible risks based on your company or industry. Based on that exercise, craft a response plan to include process scenarios, roles and responsibilities.

Brand damage on the Web can happen fast, so the corporate response must be equally fast and should use the same channels in which the offending information surfaced. If a company is not prepared, a quick response could backfire because it's not appropriate to the Web 2.0 audience's concerns (e.g., corporate double-speak).

Key for this audience are transparency of corporate reaction and being able to communicate a response quickly, even if it is only an assurance the company is assessing the issue and/or that appropriate action is imminent.

It may be more valuable to ask: "How do I influence the nimble and relevant response required to preclude or mitigate brand damage from a Web-enhanced incident?" The incidents range from alleged, fictitious or fraudulent claims, to true, newsworthy events that shake consumer or investor confidence. Compliance-related threats to public safety typically broaden stakeholder concerns as government agencies enter the fray.

Depending on the incident allegation, oversight can include local, state, or federal, health or law enforcement agencies. Brand messaging must be relevantly directed to any engaged audience.

Brand cross-functional emergency preparedness or crisis teams (Communications, Operations, Quality Assurance, Legal, Security, etc.) are well advised to anticipate all-hazards risk on a pre-event basis, to draft priority messaging, to enumerate persuasive mitigations, to transparently acknowledge the gravity of the allegation, and to demonstrate conduct that stakeholders expect of a world-class brand.

Always keep audiences informed of developments via Web sites and consumer and investor channels.

In today's technology-for-all world, anyone with a $30 video phone or an entertaining opinion blog can unintentionally or deliberately destroy your sales trajectory. They can say or show things about your company or its products that are not true and that are vastly different from the image you have invested scores of years and millions of dollars to establish.

Preparing for such an incident should be mission-critical for any consumer-dependent business. You should have the processes and tools in place to identify potential Web-based incidents before they spread and to harness the power of Web-based discussion channels to minimize or prevent damage. Know the menu of social media and related cyber-arenas available to them and you.

Know and understand Facebook, Twitter, YouTube, Digg, media-based blogs and the trailing reader commentary. And use them thoughtfully — even entertainingly, if you have to — to address the misinformation, and do it on an attitude level consistent with each channel's users.

Next Month's Question: What can I do to combat a lack of management confidence in Security?

For more information about the Security Executive Council, please visit www.securityexecutivecouncil.com/?sourceCode=std.
The information in this article is copyrighted by the SEC and reprinted with permission. All rights reserved.