

# Top 5 Internet-Related Crisis Management Tips

**Any organization that wants to effectively prevent and manage crises absolutely must take these steps.**

---

The following are the top 5 Internet-related actions any organization must take, in my opinion, to effectively prevent and/or manage crises:

## 1. Be Prepared to Manage Crises 24/7

I have had more than a few clients whose culture assumes that work is done during daylight hours on weekdays. The Internet, on the other hand, never sleeps - and neither do the newshounds who feed it. Virtually every media outlet has a website, in addition to its print or broadcast operation, and some media are strictly online operations. The hunger for news is not restricted to their time zones or even to their countries of origin. Recently, for example, a situation that would have only been news in Canada, if it had happened 10 or even 5 years ago, quickly appeared in a Russian publication. How do I know that? Because I collect intelligence - in real time - related to my clients. Your crisis management team members, especially anyone responsible for communication, must be available 24/7.

## 2. Collect Intelligence

I've said before that the Internet is much like the famous song "Alice's Restaurant," where you can get anything you want (except online you could also probably get Alice, I'm afraid). Your critics, competitors and (if you come into the public eye) the media can and will read everything they can find about you, NONE of which should come as any surprise to you because you should already have read it and be prepared to answer questions about anything that would raise eyebrows. If you don't know how to do such expert research, then hire a geek who can. Heck, often you can find an intern who will be happy to do the job for minimum wage. Remember, though, I'm not just talking about news clippings, but ANYTHING that might be in the public record (e.g., court records, regulatory agencies). Ensure that any news clipping service you use is capable of delivering you results almost the moment they appear online.

## 3. Search Engine Optimization (SEO)

Don't leave your organization vulnerable to critics who can launch an anti-(name of your organization) site in minutes. Make sure your own sites - multiple sites if possible - are highly ranked under your own name and under the terms by which you want to be found. It's not only dangerous, but highly embarrassing, to be outranked by your critics! Effective SEO also produces more business (95 percent of my new business, for example) and makes you visible to media so that you can become expert sources in your respective fields.

## 4. Allocate the Budget Necessary to Maintain Information Security

There are few situations more embarrassing and, often, more damaging than a breach of confidentiality resulting from compromise of your computer system, whether it be a single computer or a corporate server. Additionally, almost all organizations outside of third-world countries are highly dependent on functional computer systems to operate, so anything which takes those systems down immediately

creates a potential crisis. At the same time, corporate leadership often makes the assumption that someone qualified to work in your IT department, or as an IT consultant, is also fully qualified to ensure that your information remains secure and your systems uncompromised. **THAT IS OFTEN A FALSE ASSUMPTION.** There are specialists within the IT world just as within the legal or PR fields. You may well be best served by an IT "generalist" on a day-to-day basis, but that individual, and his/her CEO, needs to know what they don't know and be humble and practical enough to call in experts who can optimize system security. If you have the luxury of such expertise in-house, you are the rare exception, in my experience.

#### 5. Have Multiple Means of Accessing the Internet

Ensure that you have Internet access no matter where you are, which is essential for crisis management in this century. A common flaw I have found in the connectivity plans of larger organizations is too much dependence on their own server's "up time" and an inability to function when it's down. In particular, there is a lack of planning, by small and large organizations, for how to operate if you can't use your primary server and/or computer system for an extended period of time - e.g., following a major earthquake or hurricane. This is another of those usually under-funded crisis preparedness activities that come back to haunt you later.

### Comments

[Sign in to write a comment](#)