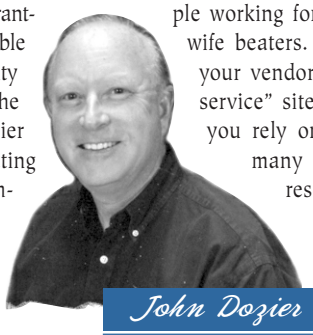
# The Online Business Cyber-Attack: DEFAMATION

It is said that the worst lies are told behind your back. That may be true. Until recently, rumors about businesses have generally been oral, fleeting in nature, and (hopefully) not given much credence. Unfortunately, the dynamics of the rumor mill are changing. Just about everything on the Web, including the good, the bad and the outright lies, are now indexed by search engines.

## That leads to problems.

In the online world, rumors or outright lies are receiving unprecedented publicity primarily because Congress granted service providers (those not involved in, or responsible for, the content of a Web site) immunity from liability as publishers of defamatory content. Coupled with the anonymity of the Web, damaging lies are now easier to tell, and it is easier to tell them without getting caught. But these lies don't just come across to others as baseless rumors. They now have credibility, because they are right there on the Internet to see! And, sometimes, others will appear to have posted similar false claims about the company, giving the appearance of independent validation.



John Dozier

The source of the defamation seems to come from four types of online information purveyors: Weblogs, industry forums or boards, commercial Web sites, and self-proclaimed "consumer protection" sites.

The rule of thumb in identifying the author of defamatory statements when your company is attacked on the Web is to "follow the money." There is almost always a direct economic motivation by the author. Perhaps the responsible party is an affiliate or supplier of a competitor, or the competitor itself. Consider that, recently, an online industry forum was providing customer satisfaction ratings in a seemingly objective manner. It became quickly apparent, however, that the revenue from the site was exclusively banner advertising, and those companies not advertising on the site were getting horribly negative "customer ratings."

Of particular interest right now are the "spam" sites that label a company a "spammer" because they use a definition of spam that includes even those companies actually complying with our federal CANSPAM Act. The site owner is reportedly selling email software in competition with many of those reported as "spammers" on its own site. Follow the money, because that is often the motivating factor for the publication of online defamation.

It is not surprising, then, that the most prevalent platforms for defamation are chat boards or forums on which competitors, acting like customers, offer up damaging "testimonials" about how your company ripped them off. Of course, the author, purely for the benefit of public consumption and protection, helpfully points out that all of the people working for your company are crooks, or felons, or wife beaters. The general public, your customers and your vendors often view these comments on "public service" sites as unbiased and, therefore, truthful. If you rely on the Web to drive business sales, how many unknown prospects went elsewhere after researching your company?

Unfortunately, these are complex matters to solve. Search engines, Web sites, chat boards, "public service" sites, rating sites and the like generally won't agree to remove a defamatory post without a court order. After all, Congress gave them immunity from liability. There are ways, however, to deal with online lies without litigation.

Sometimes the site publishing the statements is not a "service provider" since it actually influences content, and therefore is not immune. The realization of possible litigation tends to get the attention of the site proprietor if a convincing theory of liability is put forth.

Sometimes the poster can be tracked down and identified through research. An author facing a lawsuit can often be motivated to remove the offending postings. An employee's actions are often imputed to a company, so that legal notice to a business that is a suspected source can reap dividends.

In the end, though, if litigation does become necessary to identify the author and to seek damages and an injunction, the anonymity of the Web often dissolves. The chance of identifying the author is high if you move quickly. Remember that most Web sites and ISPs keep log files and access records for between 30 and 90 days, so time is of the essence. Having your lawyer send a standard cease-and-desist form is usually ill-advised; you may find it posted as support for newly alleged extortion, intimidation and harassment. All demand letters, such as the aforementioned cease-and-desist letter, must be exacting, detailed, tactful yet direct, and have interspersed within the body of the letter allegations support-

> The rule of thumb in identifying the author of defamatory statements when your company is attacked on the Web is to "follow the money."

John Dozier is President of Dozier Internet Law, PC, a law firm representing small and mid-size online businesses.

ed by facts that the recipient would not want to post.

## Going forward, then, there are steps your company can take to manage the damage caused by this type of cyber attack:

- First, monitor the search engines. I strongly recommend the "Google Alert" feature that sends out a report of indexed results based upon your keywords (consider using company, business, product, officer and key employee names). While you are at it, consider adding your key competitors to the alert for business intelligence!
- Second, designate a person to search the top engines (Google, Yahoo!, MSN, AOL, Dogpile) to look at the results for your keywords on a regular basis.
- Third, do your best to determine what your customers, and prospective customers, are hearing about you.

There are ways to prevent search engine spiders from indexing a Web site, and even the most devious competitor can post lies, providing a "confidential" link to selected parties.

I guess it is true...the worst lies are told behind your back.