

A PROZAC MOMENT IN PRIVACY AND MARKETING

Stephen Cobb is the author of "Privacy for Business: Web Sites and e-mail" (www.privacyforbusiness.com). Together with his wife, Chey, who is also a Certified Information System Security Professional, Stephen advises companies on matters of privacy and security and teaches graduate courses in Information Assurance at Norwich University, Vermont. The Cobb's weekly column on security can be read at Newsscan.com. Stephen can be reached at scobb@cobb.com.

A few years ago, when someone broke into the Western Union Web site and compromised about 15,000 credit cards, including one of mine, it was described by the press as a "security incident." A couple of months ago, when the press reported that 8 million credit cards had been compromised, it was called a "privacy incident." This subtle shift in language underlines a major shift in consumer perception. When incidents occur that result in the exposure of personally identifiable information-known in privacy circles as PII-the media will pounce, the public will take notice, and any individuals who feel they suffered as a result of the exposure will find the lawyers lining up to take their case.

This shift in perception is unfortunate for many reasons, not least of which is the fact that many of these incidents could be avoided if companies would pay closer attention to time-honored business practices. For example, using disciplined software development methods and quality assurance controls can go a long way to ensuring the protection of customer PII. Indeed, the first really big privacy incident of this century, the so-called "Eli Lilly Prozac e-mail Incident" was a case of software development and quality assurance gone wrong (I know because I assisted the Federal Trade Commission with its investigation of, and ensuing settlement with, Eli Lilly; however, nothing in this article is privileged information-it is all there in the public documents at www.ftc.gov).

Some readers may be familiar with this particular incident, but a surprising number of people are not. For example, a few weeks ago my company presented a series of privacy seminars for a different but equally large pharmaceutical company. To our surprise, less than a third of those attending were aware of the facts of this case, so they obviously bear repeating. Here they are, in the words of the FTC (the term "respondent" refers to Eli Lilly, and "Medi-messenger" is an e-mail reminder service that the company promoted at Prozac.com):

"On June 27, 2001, at respondent's direction, an Eli Lilly employee sent an e-mail message to Medi-messenger subscribers announcing the termination of the Medi-messenger service. To do this, the employee created a new computer program to access subscribers' e-mail addresses and send them the e-mail. The June 27th e-mail disclosed the e-mail addresses of all 669 Medi-messenger subscribers to each individual subscriber by including all of the recipients' e-mail addresses within the "To:" line of the message. By including the e-mail addresses of all Medi-messenger subscribers within the June 27th e-mail message, respondent unintentionally disclosed personal information provided to it by consumers in connection with their use of the Prozac.com Web site."

You might wonder how this could happen. Surely a company like Eli Lilly has a comprehensive set of information security policies, proper software development procedures and a software quality assurance program. In fact, Eli Lilly had all of these. For example, there was a policy that said no code was to be put into production without adequate testing and supervisor approval. But here's the rub, something you will see in a lot of other companies: those rules were applied mainly to the IT department, the folks who grew out of the mainframe, in-house data processing departments of yore. Those rules had not been applied consistently to the Internet team, the fast-moving, fleet-footed, code-for-the-moment folks who brought you the corporate Web site. And who manages e-mail? In many companies, it's those same Internet folks, who may not be

accustomed to, or feel bound by, standard IT safeguards and protocols. Here is more of what the FTC said:

"The June 27th disclosure of personal information resulted from respondent's failure to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information. For example, respondent failed to provide appropriate training for its employees regarding consumer privacy and information security; failed to provide appropriate oversight and assistance for the employee who sent out the e-mail, who had no prior experience in creating, testing, or implementing the computer program used; and failed to implement appropriate checks and controls on the process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the e-mail. Respondent's failure to implement appropriate measures also violated certain of its own written policies."

There are numerous lessons to learned here, especially if your company wants to avoid hefty fines and 20 years of government oversight (which were the consequences for Eli Lilly). First of all, companies need to make sure that there are strict rules for software development and that everyone doing software development is playing by them (simply having rules was not a defense as far as the FTC was concerned).

The second lesson is that all employees need to be made aware of the company's privacy policies (assuming you have these properly documented). Today's smart companies are making sure that every employee who deals with customer PII, even the folks in IT, whom you might not think of as "customer" people, are aware of just what a big deal it is to breach the privacy promises that the company has made to its customers. Any transgressions that come to the attention of management should be addressed (this may not mean firing people-but if you don't enforce a policy it is legally useless in your defense).

The third lesson, from this and other recent incidents, is that bad news can have a cumulative effect. For example, less than six months after Eli Lilly reached a settlement with the FTC over the prozac.com privacy problem, the company was accused of another Prozac-related privacy violation. This second case involved samples of Prozac which were mailed to people in Florida, through a marketing deal involving-allegedly-the recipient's physician, the recipient's pharmacist and Eli Lilly sales reps. Reporters writing about this incident took the opportunity to remind people of the company's troubles with the FTC over the earlier Prozac-related privacy incident.

The fourth lesson is that marketing is probably the "hot spot" for privacy of customer information. Both Lilly incidents were related to marketing efforts, as was the Ziff Davis Media case, which cost the company six figures in fines last year. The potential for marketing via the Internet is so enormous, and the perceived cost-of-entry so low, it is understandably difficult for marketing folks to resist the urge to rush out and put up a Web site or send out a zillion e-mails. But if something goes wrong, your company could be paying hundreds of thousands of dollars to fix it, money that would have been far better spent doing it right the first time.

Copyright Stephen Cobb, 2003.

Right of first electronic publication granted to MRA Newsletter.

All other rights reserved.