Potential for Customer Data Breach Requires a Communications Plan Review

By Art Samansky and Eric Samansky

Reports in recent months about suspected break-ins to confidential and proprietary customer databases re-emphasizes the need for communications executives at corporations, educational institutions, and government at all levels to be sure their communications plans can adequately deal with this kind of threat.

Intrusions of these kinds eventually could happen almost anywhere. Regardless of safeguards, thieves, hackers, and con artists are always looking for new ways to break-in: there's potential quick money in the data kept on customers.

To be certain the communications team is ready to deal with this issue, communications executives should examine their plan well before a potential data-compromise is suspected.

Most critical among the planning steps is to determine the public announcement policy with senior management. Trying to do this on the fly, of course, is possible, and something professional public relations executives often must do: it's just that much harder depending upon availability of policymakers, and a host of other factors, from when communicators are informed of the issue to what other events or announcements are in process or about to be implemented.

Speedy, full, and accurate disclosure greatly outweighs waiting for a possible intrusion to be discovered outside the organization. Moreover, state notification laws may impact the decision. There also may be regulatory issues involved for publicly traded companies.

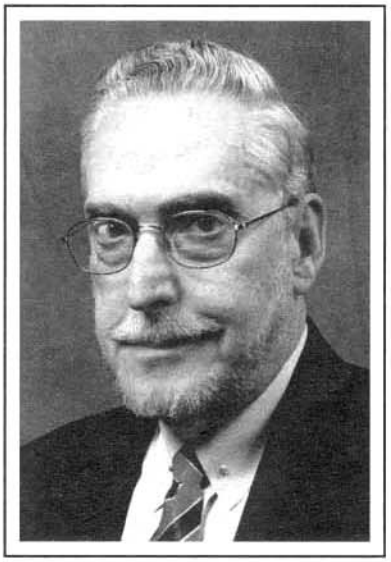
Central to public announcement, too, is the need to be sure the statements are focused upon informing customers so they can quickly take appropriate action, not scaring them about the potential consequences of the breach, whether by theft or otherwise.

These statements also must be carefully coordinated between those responsible for external and internal communications for message content and timing of dissemination. A glitch here can have a series of additional time-consuming, negative, and public ramifications.

A Communicator's Checklist

Further, depending upon the databases kept, and the geographical reach of the organization, communicators should determine if:

- the existing crisis communications plan has in it components across communications disciplines to deal with a potential exposure of client data on a global scale, as well as on a regional, or local scale;



Art Samansky

- the plan's components to deal with a database breach are up-to-date in terms of legal and regulatory opinion, among other items;
- a recent review has been made of the roles of the media relations, marketing, advertising, internal communications, and investor relations teams, and identifying the specific individuals charged with responsibility for coordination of communications on the subject within each team and company-wide;
- the "executive communications" group — those responsible for speechwriting and developing similar material — has been folded into the "team" effort and that there is a mechanism to quickly fill them in and keep them abreast of developments and the communications being distributed;

Speedy, full, and accurate disclosure greatly outweighs waiting for a possible intrusion to be discovered outside the organization.

- a mechanism exists to bring external communications consultants across disciplines into the process as necessary to use their skills and services, and to avoid implementation of preapproved programs which inadvertently may impact the "breach-communications" effort;
- a draft template of a letter/notice has been developed and approved, in concept, by the legal department for rapid dissemination by customer/client relation executives, and/or others charged with notifying clients of possible intrusion;
- consideration has been given to notifying clients, and the organization's staff, of the possible intrusion, and the steps they should take, by means other than standard letter, such as overnight mail, express mail, e-mail, and other methods;
- consideration has been given to re-enforcing, through inserts with monthly bills or statements, preventative measures individuals might take before a possible intrusion;
- internal staff, especially those dealing on the front line with customers, have been given adequate information about where to direct customer inquiries on the subject, or are adequately trained to provide answers;
- via coordination with the human resources group, there exists a formal training, or retraining, program for internal staff dealing with customers which takes into consideration current issues and conditions;
- an internal website FAQ dealing with the issue has been drafted, and can quickly be added to the site, and an e-memo has been drafted and quickly can be ready to be sent to staff to ensure they know of the FAQ;
- internal staff with access to customer data have been given adequate written reminders on how to safeguard such information;
- a draft "article" been prepared for the corporate external website, or other use, explaining the issue, the steps the company is taking to increase safeguards, and steps customers/clients (individual and corporate) might take to supplement the organization's actions; and,

There is a mechanism in place to coordinate these and related actions with government/regulatory authorities on all levels. PRQ

Eric Samansky

Art and Eric Samansky, *a father and son team, are the principals of The Samansky Group (www.samanskygroup.com), a public affairs consultancy. Prior to forming the firm in 2000, Art was a reporter and later an editor in New York City from 1961, and from 1970 served in several senior communications posts at major regulatory, trade, and corporate organizations. Eric has more than a decade of communications experience at New York City headquartered public relations/investor relations firms.*