Check Your Public Face: Carry Out Routine Internal Audits of Communications

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Everyone has received robocalls and hang-up calls (call abandonment), right? You are in the middle of dinner with the family, the phone rings, you pick it up, and – nothing. Sometimes you actually do hear a recorded message, sometimes you get a harried telemarketer trying to get you to give a donation to some cause or to spend money on some item, but sometimes you just hear a click as the call is dropped.

Michael Cooney wrote about the problem in a column back in August 2008<http://www.networkworld.com/community/node/31211> where he reported that the Federal Trade Commission was adjusting its Telemarketing Sales Rule to (a) stop unsolicited commercial robocalls and (b) mandate a 97% completion rates on all calls placed using predictive dialing (Cooney explained, “Predictive dialers place calls in anticipation that a salesperson will become available by the time one of the numbers called is answered.”)

In the days before I wrote this article, I started getting several calls from a non-profit educational institution I have supported for many years. Each call was a hang-up, so, out of concern for their reputation, I called their main number to report the problem. I listened to their menu options and pressed 7 to reach the Public Relations department so I could let them know that hanging up on donors is not cool and not likely to increase or even maintain their level of donations.

To my astonishment, the line to which “7” directed me had the following response message: “This is ------. As of December 31, 2008, I will no longer be working at the ------. Please call ---- at extension 307.”

Good heavens! This respected institution has an inappropriate phone message over 18 months old on its Public Relations line??

The incident reminded me of some of the principles I teach in consulting and in academic courses. Just as we should routinely check our security measures using vulnerability assessment tools and methods, we must check all aspects of our public face to ensure that we are presenting precisely what we want to present to visitors, customers, potential customers, and donors.

Here are some ideas for what you can start checking today at your place of business:

1. Web site
   a. Run a broken link analysis. Web design tools such as Dreamweaver <http://www.adobe.com/products/dreamweaver/> all provide automatic tools for scanning all the source files in the Web site repository for broken internal links; most also provide checks for broken external links. You can also use the excellent Link Sleuth<http://home.snafu.de/tilman/xenulink.html> from Xenu for checking link integrity.
2. E-mail system
   a. Does everyone who is currently working at the organization have a proper e-mail address?
   b. Are all the e-mail addresses currently on the system actually assigned to current employees or other authorized, intended users?
   c. Are there any automatic forwarding instructions on the system that violate corporate policy (e.g., forbidding corporate e-mail to be forwarded to private e-mail addresses)?
   d. Are all the distribution lists (i) complete and (ii) correct? Specifically, are there any addresses in the lists which are out of date by referring to staff members who have changed their roles and are no longer appropriate for that particular list? Are there any ectopic addresses such as those of outsiders who should not be receiving confidential information at all?

3. Telephone system
   a. Is the message that an outside caller receives correct, professional and up to date?
   b. Does the list of menu choices reflect known statistics about the frequency of calls to specific functions (the most frequently called services should be earlier in the list)?
   c. Do the phone numbers associated with each of the menu items match the current roles and responsibilities of the people fielding those calls?
   d. Are there measures in place to handle absences? For example, do people know how to forward their phone calls automatically to their backups so that callers immediately reach the appropriate employee when calling in from the outside?
   e. Are the answer messages on every extension (a) clear and professional; (b) friendly; (c) useful for the caller; (d) up to date?
   f. If robocalls are in use, is there a specific team assigned to monitor the frequency of hang-up calls? Does the team monitor repeat hang-ups to specific numbers to stop the robocalls to those numbers after a defined limit?

4. Fax lines
   a. Are the fax headers complete on all outgoing faxes? Do they include the correct contact information and organization name?
   b. Are the fax systems identifying themselves correctly to inbound callers?

5. Letterhead and envelopes
   a. Is the information such as addresses, divisions and so on correct on letterhead, notes, and envelopes?
   b. Are the brand names, and trademarks correct on all paper products?

We should all be scheduling routine internal audits of these issues as a matter of course.

Boring, but better to fix the problems before they become embarrassing.

* * *


Copyright © 2010 M. E. Kabay. All rights reserved.
Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.