

The Buzz Around Town

U.S. Public Safety Events

Vol: 1, Issue 1, May 2009

NENA 2009: 9-1-1 Conference and Trade Show

June 6-11, 2009, Fort Worth Texas <http://www.nena.org/conference2009>

APCO

August 16-20, 2009, Las Vegas, Nevada <http://www.apco2009.org>

In This Issue:

Text To Landline—Does Your PSAP Know What To Do With These Calls? [Read more...](#)

Is Your PSAP Really Secure? [Read more...](#)

Thinking Outside of The Box—Problem Solving.
[Read more...](#)

Input Solicited for Study. [Read more...](#)

This newsletter has been designed to provide you with updates and information on issues that affect the unique world of public safety. Our aim is to provide timely and accurate information that assists you in making decisions today and down the road.

If you have ideas for stories or content or would like to contribute an article, please contact us, we would love to hear from you.

[Contact Us](#)

Input Solicited for Study

The Barkwell Holland Group is currently working on a study of how to optimize the process for writing and issuing proposals within the public safety sector. We are soliciting participation from public safety agencies and municipalities for the study. To participate, simply fill in and submit a questionnaire.

Purpose:

- To define and articulate the processes of organizing and drafting a proposal document.
- Determine what areas of the process can be made more efficient.

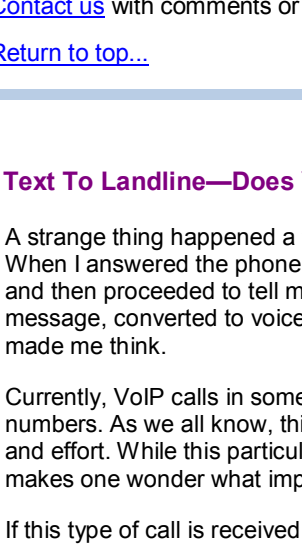
Results:

- Maximize return and minimize costs to agencies engaged in writing and issuing proposals.

The study will result in a white paper which will be made available to all participants of the study.

Please visit www.bhgroup.ca to download a copy of the survey

[Return to top...](#)



The Barkwell Holland Group Provides a wide range of project management, documentation and financial consulting services to Public Safety Agencies, Municipalities and Technology Vendors

To remove your name from our mailing list, please [click here](#)

[Contact us](#) with comments or questions or call (905) 852—1064.

[Return to top...](#)

Text To Landline—Does Your PSAP Know What To Do With These Calls?

A strange thing happened a few weeks ago. I received a phone call in my office with a bit of a twist. When I answered the phone, an automated voice identified itself as a particular cellular provider and then proceeded to tell me that it was delivering a text message from a cell phone. The message, converted to voice, then followed. As it turns out it was actually a wrong number, but it made me think.

Currently, VoIP calls in some areas are still being redirected to 10 digit administrative PSAP numbers. As we all know, this is not acceptable, but encouraging the industry to change takes time and effort. While this particular issue (VoIP to admin line) has more or less been addressed, it makes one wonder what impact this new text to voice service will have in the PSAP.

If this type of call is received by your PSAP, do you have a Standard Operating Procedure in place to deal with it? The call that I personally received did not provide a call back number and if it did, I am sure that it would have been the number for the service provider, not the original caller.

There is also a push from the hard of hearing community in the United States to allow something similar to this kind of service for mobile devices so that they can communicate with 911.

If you have received any of these calls, I would be very interested in knowing how it was handled and what operational procedures you have put into place to deal with them.

[Return to top...](#)

Is Your PSAP Really Secure?

When organizations think of system security, they immediately turn to the computer network and the software that keeps it safe from outside attack. Rarely do IT people consider the idea that compromising a secure network can be accomplished using other methods. Contrary to what one might expect, gaining access to sensitive data is often a rather simple process. Most IT personnel expect that an attack will occur over the internet and expend most resources and energy setting up firewalls, creating tight access rules and locking down any unnecessary ports of entry.

While from an IT point of view this is a comprehensive and logical strategy, many times access to sensitive data is gained by an outsider using a more straight forward approach; the thief simply walks in the front door. Below is a list of questions to consider when thinking about this potential threat .

- Does anyone actually check the credentials of telephone, radio or network technicians before granting them access? Once external technicians have gained access to a facility, few organizations actually monitor their whereabouts within the building.
- Does your facility locate service (communications) access points or hubs near or in the room that houses most of the sensitive computer equipment for the PSAP? Once a criminal has access to that room, the entire organization is at risk.
- How many of your network servers have post-it notes stuck to the screen with passwords written on them? Once someone has access to your network, the sky is the limit, particularly if they have administrative rights. They can simply create an administrative account for themselves and do the rest from home. They only need access for a couple of minutes to do this. By the time the breach is noticed it is often too late because the damage has been done.
- How often do employees leave post-it notes stuck to their own workstation monitors with passwords or other access information written on them, or in their desk drawer? No more than a few seconds is required to read a post-it note. Employees should be encouraged to secure their work areas during off hours
- How often do employees lock their workstation when they are not at their desk Someone with malicious intent can gain access to information that will lead them further into the system at a later date from any user's terminal. It does not have to have administrator access.
- Do employees prop open external exit doors to move furniture or equipment, or do they block them open while on breaks? These types of lapses can be an easy entry point for an intruder when someone's back is turned even for just a moment. Alternatively they may simply walk in with a group of people.

These questions are designed to help you think outside of the box regarding network security and to take into account the obvious threats rather than focusing solely on software attacks.

[Return to top...](#)

Thinking Outside of the Box—Problem Solving

To get your creative thinking cap working, here are a couple of problems to solve. Seeing things only for what they were meant to be used for and not seeing things for what they can be used for is called *functional fixedness*. A book is meant for reading, a waste basket for waste, and a hair dryer for drying hair. But a book can be used for a weight or a booster seat, a wastebasket for a flowerpot, and a hair-dryer for drying paint. Try to transcend functional fixedness to solve the two problems below:

Problem 1: Two strings about four feet long are suspended from an eight foot ceiling at opposite points in a room. Each string is about three feet from the nearest wall. Your task is to tie them together. Although the strings are long enough to meet in the middle, holding on to one of them prevents you from grasping the other, which is just two feet out of your reach. Nearby, and within reach as you hang onto one string, is a desk with some tools on it: a hammer, a pair of pliers, a screwdriver, and a penknife. What do you do?

Problem 2: On a table is a full box of kitchen matches, a candle, and some tacks. Your task is to attach the candle to the wall in a way that wax will not drip on the floor. What do you do?

Reproduced from Critical Thinking, Second Edition, by Gary R. Kirby and Jeffery R. Goodpaster.
Copyright © 1999 by Prentice-Hall, Inc.

[Return to top...](#)