

Planning Considerations for Wireless Phones (Part 2 of 2)



By [Leo Wrobel](#), [Sharon Wrobel](#)

Date: Jun 15, 2010

[Return to the article](#)

Leo A. Wrobel and Sharon M. Wrobel conclude this two-part series by considering the importance of addressing your wireless devices in your standards documents

Part 1 of this series discussed how to ensure that customers can reach you by phone despite an emergency. Wireless phones are becoming increasingly important, versatile, and useful in a disaster. But depending on your wireless phone could be a two-edged sword. The power and versatility of that device so useful in a disaster, could hurt you in other circumstances. For example, think about what would happen if your CEO loses his or her phone in an airport and it winds up in your competitor's hands.

Does your firm have security standards for wireless devices? If not, it's time to start putting standards in place. If you already have such standards, consider the tips in this article for improving your standards. Once these ideas become corporate policy by virtue of their adoption in a standards document, your recovery plan will flow much more smoothly.

Addressing Wireless Devices in Your Corporate Standards

In the context of a recovery plan, standards serve two purposes:

- **Standards can keep disasters from happening.** "Don't store paint thinner in a server closet. Keep a fire extinguisher handy. Make regular software and data backups.
- **Standards form the foundation to ensure that your disaster recovery plan will execute gracefully.** If your recovery plan says "Go to list A and call certain people back to work," the instructions assume two things:
 - List A exists.
 - List A is up to date.
- The *action* in the recovery *plan* (using the list) is supported by the *standard* (the list must exist), under pain of violating corporate policy. Got it?

By the way, are you thinking in terms of a *paper* list? Don't you have everyone's contact info in your BlackBerry or iPhone? If so, that device could be very helpful if your office burns down or you're otherwise cut off. But we can do even better. What if a corporate standard like the following could be devised?

- Everyone has the same (or compatible) wireless devices
- Everyone has the same emergency names, lists of recovery teams, and relevant documents.
- Everyone has sensitive info encrypted, just in case a device gets lost or stolen

Standards like these would keep everyone on the same page in a disaster. Some companies and vendors are moving in precisely this direction. Even better, systems are being developed to update your recovery plan *automatically*, and then broadcast changes and updates to your responders. All of these changes take place by virtue of the wireless devices that your responders will carry with them all the time.

Consider Tenet Mobile's [PINpoint](#) application for emergency management of BlackBerry phones. According to BlackBerry and Tenet, PINpoint automatically collects the most up-to-date document and contact information from a company's internal systems. It then "pushes" this information out to any number of phones, without the active involvement of the user of each device. This information is automatically stored on the BlackBerry so that it will be available and up to date when needed. Cool.

The Advantage of Automation

Tenet's PINpoint app cracks a most interesting nut for me (Leo). Over 30 years in this industry, I've found that keeping a recovery plan up to date has often been a laborious and time-consuming problem. When LANs started proliferating in 1987, I published about how files could be object-linked from servers to the recovery plan, in order to avoid having to assign someone to do manual updates. Indeed, identification of key databases (personnel phone numbers, equipment inventories, vendor numbers, email addresses, recovery procedure, chains of command, etc.) is half the battle in developing a plan. Now the wireless companies have developed a new angle:

- All this information now fits on your hip, in your purse, or in your pocket. I'd call that convenient
- After the heavy lifting is done in identifying key databases and repositories, the information is sent out to you automatically from time to time. Data fields are standardized to allow for easy export and import automatically. Documents or contact lists can be pushed out to users. Different content can be pushed out to different groups of people. Again, convenient.

According to BlackBerry, the system is managed centrally, and it allows an administrator to define what information will be delivered, by user, and when. With all the hype about cloud computing these days, wouldn't this be an interesting service to provide? The data would be stored offsite as well. (Then again, maybe I already is!)

Expanding Conversation to Communication

Complete and up-to-date documents and contact information are obviously very valuable in a disaster. However, remember that the BlackBerry is also a *phone*. Verbal communication is necessary to maintain command and control. These days, PDAs such as BlackBerry are more aptly considered to be *communications devices*, since they can do more than just make phone calls. Modes of communication such as email, instant messaging, SMS messaging, and even services as mundane as Twitter are all available if needed. The method used by the people conducting the recovery will vary, in part due to demographics and preference.

Let me digress for a moment.

One thing that 30 years in telecom gives to someone like me is a broader view by virtue of age. When I got started in this business, an "old salt" told me a story. He said that when he was a young telecom newbie, he actually had customers who didn't want telephones. They wanted to stay with the *telegraph*. Their reasoning? "It's quick. It's to the point. And I don't need all the b----- with talking to someone. I'd rather communicate graphically."

I laughed when I heard this story but consider the state of affairs today. "Just text it to me" is the norm now for many people, and for entirely the same reasons! In 60 years we've come full circle back to the telegraph at least its 21st century corollary. Wireless devices and PDAs let people communicate in familiar ways: voice, email, text, or whatever.

I just said that demographics also played a role. Consider

Baby boomers:

- Go to seminars.
- Like face-to-face contact.
- Talk on the phone

Generation X:

- Go to webinars.
- Do business via the Web.
- Send email.

Generation Y:

- Prefer texting.
- It had better be all about *them*.

Okay, I'm speaking a little tongue-in-cheek, but look around your office and see whether I'm not at least partly right.

Summary

Consider carefully the role that wireless devices play in your disaster recovery plan. More importantly, give some thought to implementing wireless devices as part of your organization's operations and security standards document. In this fashion, you should be able to create a comprehensive wireless strategy that not only bolsters your recovery plan, but also keeps a handle on wireless cost through greater standardization and economies of scale. Consider systems like the PINpoint, which automatically collects the latest documents and "people" information and then pushes the information out to devices that will be in the pockets of people you need to recover. Automatic updates are preferable to manual involvement by busy people.

We hope that you've found a few morsels in this series worthy of further thought and integration into your recovery plans and standards. Until next time, be well and happy planning.

Leo A. Wrobel has more than 30 years of experience with a host of firms engaged in banking, manufacturing, telecommunications services, and government. An active author and technical futurist, he has published 10 books and more than 400 trade articles on a wide variety of technical subjects. In 1986, Leo pioneered carrier collocation by placing the first computer disaster recovery center inside a telephone central office. Leo served 10 years as an elected mayor and city councilman (but says he is better now). A sought-after speaker, he has lectured throughout the United States and overseas and has appeared on several television news programs. Leo is presently CEO of Dallas-based [TelLawCom Labs Inc.](#) and [b4Ci, Inc.](#) Contact Leo at 214-888-1300 or email leo@b4ci.com.

*Sharon M. (Ford) Wrobel conducted extensive publishing and regulatory research for her former employer (a nationwide telephone company), a function she continues today as vice president of business development for [b4Ci, Inc.](#) Sharon was a major content contributor to Leo's book *Business Resumption Planning, Second Edition* (Auerback Publications, 2008), coauthored his book *Disaster Recovery for Communications and Critical Infrastructure* (Artech House Books, 2009), and has published dozens of trade articles under her own name. Sharon attended the University of Maryland and El Centro College in Dallas, where she trained as a registered nurse before joining Leo in his businesses. Sharon also served honorably as a public official, accepting appointments to the city's Planning and Zoning Commission and Historical Commission. She can be reached at sharon@b4ci.com.*
