

Avoiding Telecom Sabotage, Part 2 of 2



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

Date: Jun 22, 2009

[Return to the article](#)

Leo A. Wrobel and Sharon M. Wrobel, specialists in disaster recovery and business resumption planning, conclude their series on avoiding the hazards of deliberate telephone sabotage with some suggestions about other communications options (some of them free!) that you should include in your First Alert procedures.

In part 1 of this series, we explained how on April 9, 2009 someone deliberately cut underground fiber-optic cables in south San Jose, California, throwing the area into chaos and causing untold misery millions. Other than pursuing the perpetrators (AT&T is offering a \$250,000 reward), what can you do to mitigate the impact of such disasters on your home, your business, your community, yourself?

We ended part 1 with the beginning of a funny story. It seems that Twitter survived the AT&T outage. Not only did Twitter survive, but AT&T used Twitter to broadcast updates about the outage, and has continued using the service to provide AT&T updates to the community.

If Twitter could survive a telecom sabotage incident, you might think that other technologies could also survive and you'd be correct! In this article, we'll examine some of those technologies.

Tweeting About Phone Sabotage

Following the fiber-optic sabotage, millions of people in Silicon Valley and San Francisco were without broadband phone, and wireless service for most of that day. Twitter was used by communication giant AT&T to reach out and update its customers on April 9, as AT&T began "tweeting" about the sabotage in California around 7 a.m. PDT: "CA customers: We are aware of a cable cut situation impacting services in Santa Clara and San Jose areas."

Better than nothing, particularly when you can't pick up your phone and call people about the situation. From that point onward, AT&T sent more "tweets" (messages) to keep its customers up to date on the outage:

- Informing customers that technicians had been on the scene
- Indicating that service would be restored as quickly as possible
- Apologizing for the outage.
- Reporting that the outage was caused by vandals who had cut the fiber cable
- Offering a reward for anyone with information. ("AT&T offering \$100,000 reward for info leading to arrest/conviction of those responsible for CA vandalism. Call 408-947-STOP.")

How did customers respond? One source [quoted](#) Janine Popick, CEO of VerticalResponse, a company affected by the outage, who stated that the only way she had stayed on top of the situation was via Twitter: "All of my real time updates have been coming from the AT&T Twitter feed." Thousands of people kept tabs on the situation via AT&T's Twitter feed.

How does a vehicle designed for social networking help in a disaster? In part, Twitter survived due to the kind of Internet Protocol (IP) technology it employs. This is described in more detail later in this article. Since this technology survived, it could be used to coordinate and communicate connections.

NOTE

Similarly, when the Twin Towers were destroyed on 9/11, one company affected by this disaster survived by using AOL instant messaging, for many of the same technological reasons we describe in this article.

Twitter is a Web-based social-networking service that lets people send messages of 140 characters or less to a

group of followers. I (Leo) never took Twitter very seriously although Sharon and the kids live and die by the thing, as well as by their MySpace accounts. (Leo's forays into the world of Facebook were less successful. After garnering hundreds of dubious email messages from Ukrainian women looking for husbands, he gave up and moved his profile to LinkedIn.)

Any technology that helps someone communicate can be very valuable when disaster strikes. This point wasn't lost on AT&T, which commonly uses Twitter to keep customers (and anyone else interested in the company) informed in real time. In serious moments like the sabotage incident, Twitter could be used to communicate about a crisis.

Reportedly, Sprint Nextel, whose wireless customers also experienced interruption, did not provide official updates via Twitter, though a company spokesperson updated customers and reporters via her personal Twitter feed: "Assessing fiber cut issue in CA w/ network + emergency response team. We're all in this together folks. Let's have a day of peace in telecom."

Kind of makes you feel warm all over, doesn't it?

Let's not forget our friends at Verizon. Their spokesman sent updates with links to news stories about the outage. He even sent a message to AT&T's media relations representatives: "Understand spokesperson has been tough for reporters to reach at AT&T on Silicon Valley outage. Who should they call for info?"

This thing is starting to sound useful! But a lot more technology is available than just Twitter for people who plan ahead. Read on for more.

It's All About Communications for Command and Control

When telecom sabotage occurs, not only the well-being of your organization is at stake, but often the lives and livelihoods of employees, families, and customers as well. Therefore, it makes sense to organize and write "First Alert" procedures with the intention of getting your response into gear, regardless of which technology survives the event, and in the shortest time possible. The U.S. military has long recognized that command and control is key to any response. This makes sense, since most of their mission involves responding to catastrophic, unexpected, and potentially deadly situations. As we have pointed out in previous articles, the military has a suitable acronym, "4Ci," which refers to the major areas of concern in a disaster:

- Command
- Control
- Communications
- Computers
- Intelligence

What was so bad about the latest incident in California is that it *knocked out 4Ci*, not only for AT&T but for thousands of its customers.

Today, businesses need to be more like the military, prepared to coordinate their response to any situation, no matter what happens. Part of that process is deciding issues like who would need to come to work immediately in a disaster, and who should stay home. Who needs to change the way they work, such as telecommuting or, as in previous examples, by driving from house to house conducting "wellness checks"?

Organize your thoughts systematically and create a list like the following:

- Who will comprise your initial response teams?
- How will you contact them?
- How do you document call-out numbers?
- How do you keep call-out numbers up to date?
- Where are all your emergency numbers?
- Who do you call in case of injury or death?
- Who will be your spokesperson for the media?
- What will your customers hear when they call you after a disaster?

Considering a situation like the fiber-optic sabotage, an equally important part of the process should be deciding *how* to communicate with responders, based on which communication mediums survive.

Selecting the right technologies makes your First Alert procedures more powerful and yet more flexible in their ability to respond to changing situations, whether you're dealing with earthquakes or severed fiber-optic cables. For example, have you considered all of these potential communications options?

- Wireless phones
- Voice conference bridges
- Two-way radios
- BlackBerry units
- Laptop PCs
- Push-to-talk phones
- Broadcast fax machines
- Fax servers
- Offsite hosted email accounts
- Offsite hosted voicemail accounts
- Satellite phones
- "Black box" wireless-to-landline adapters
- VoIP phones

Let me give you a few examples of technologies that you can use to augment your First Alert procedures and some of these options are *free*:

- As the name implies, [Totally Free Conference Calls](#) is a conference bridge, and it's free. Imagine being able to publish a number that can host up to 99 conference participants after a disaster. This one small precaution could do wonders for maintaining 4Ci after a disaster.
- [Telecom Recovery's](#) product is surprisingly affordable and would have been of great help in the California fiber-cut. It stores your numbers in a place where they can be quickly redirected to any surviving technology (satellite, VoIP, etc.) after a disaster. It can easily be programmed with "update messages to customers from CEOs and others; it can also broadcast faxes, replace email accounts, host conference bridges, make outbound conference calls, and more.
- Don't rule out [Twitter](#) and [AOL instant messaging](#)! Even though some people consider them toys, they traverse a VoIP network that was specifically designed by the military in the 1960 to 1980s to survive disasters, even a nuclear strike. That's why they work in lesser disasters, such as telecom sabotage. Find out about these technologies and integrate them into your First Alert procedures. You might even be able to organize them using the Telecom Recovery product above or using other products such as the one offered by [TeleContinuity](#).
- To learn more about satellite communications, check out the [Global VSAT Forum](#). GVF is a nonprofit organization that can inform you about hundreds of good providers.
- If you have a large call center, ask [Telecom Recovery](#) about "PRI in the sky," a service in which they can literally drop a T1/PRI from the air to you *no matter what gets cut or sabotaged*. You redirect inbound numbers to your PRI in the sky, using the same vendor.
- [Rentsys Recovery Services](#) offers a similar satellite-based product. Building destroyed? That's no problem for Rentsys, which can roll an 18-wheeled building to you and then connect it by satellite!

Once you have organized the fundamentals in your head, seek out and use enabling technologies like those described above. They can help you to develop a level of reliability that rivals what the military uses, ensuring that you are never out of touch.

Summary

AT&T is still the omnipotent "Death Star" of telecom; so, logically speaking, its disasters will hurt the worst and affect the most people. Even though AT&T still controls just about everything, there is no reason for the serious contingency planner to be out of touch in a disaster. In fact, even if everything on the ground is wiped clean, such as in the 2004 Indian Ocean tsunami, satellite communications can be deployed quickly. Then those same numbers used to call you yesterday can stay in service via satellite if you plan ahead.

Even technology as mundane as laptops, BlackBerry devices, wireless phones, instant messaging, voicemail, broadcast fax, email blasts, low-power AM or FM radio stations, two-way radios, push-to-talk phones, and a host of other technologies add immeasurably to 4Ci, and ensure that your First Alert procedures execute perfectly. You never know which technology will survive, so factor them all into your plans. Many services, such as two-way paging, are

satellite-based, and therefore will survive disasters even worse than cutting a major fiber-optic cable. For example, select paging technology that does two-way text messaging, and you can "tweet" away over a satellite, no matter what happens.

The two most important things to remember are to a) understand and set your first alert objectives, and then b) enable them with a veritable plethora of available technology. We hope that these steps have helped you, and we wish you the best of luck in your contingency planning pursuit:

In addition to his work with his own two companies, TellAWCom Labs Inc. and b4Ci, Inc., Leo A. Wrobel is honored to have been elected president of the <http://www.naspa.com> (NaSPA) a not-for-profit company concentrating on the needs of tens of thousands of members since 1986. NaSPA specializes in career development, employment, information technology, and disaster recovery. Contact Leo at 214-888-1300 or email leo@b4ci.com.

Sharon M. (Ford) Wrobel served as corporate secretary and director of personnel for Premiere Network Services Inc. prior to joining b4Ci, Inc. in 2004. During that time, Sharon was instrumental in getting Premiere certified as the first CLEC to be certified in all 50 states, by aiding in filings and attending hearings. She also engaged in extensive research for Premiere, a function she continues with b4Ci as vice president of business development. Sharon was also president of the Ellis County Early Childhood PTA and the Ovilla Lions Club. She attended the University of Maryland and El Centro College in Dallas and received training as a registered nurse before joining Leo in business in the late 1990s. Sharon also served as a public official by accepting appointments to the local Planning and Zoning Commission and the Historical Commission.
