

A Cyber-Attack on an American City

By Bruce Perens

Just after midnight on Thursday, April 9, unidentified attackers climbed down four manholes serving the Northern California city of Morgan Hill and cut eight fiber cables http://www.mercurynews.com/localnewsheadlines/ci_12106300 in what appears to have been an organized attack on the electronic infrastructure of an American city. Its implications, though startling, have gone almost un-reported.

That attack demonstrated a severe fault in American infrastructure: its centralization. The city of Morgan Hill and parts of three counties lost 911 service, cellular mobile telephone communications, land-line telephone, DSL internet and private networks, central station fire and burglar alarms, ATMs, credit card terminals, and monitoring of critical utilities. In addition, resources that should *not* have failed, like the local hospital's *internal* computer network, proved to be dependent on external resources, leaving the hospital with a "paper system" for the day.

In technical terms, the area was *partitioned* from the surrounding Internet. What was the attackers goal? Nothing has been revealed. Robbery? With wires cut, silent alarms were useless. Manipulation of the stock market? Companies, brokerages, and investors in the very wealthy community were cut off. Mayhem, murder, terrorism? But nothing like that seems to have happened. Some theorize unhappy communications workers, given the apparent knowledge of the community's infrastructure necessary for this attack. Or did the attackers simply want to teach us a lesson?

Although they are silent on the topic, I hope those responsible for emergency services, be they in business or government, *are* learning the lessons of Morgan Hill. The first lesson is what stayed up: stand-alone radio systems and not much else. Cell phones failed. Cellular towers can not, in general, connect phone calls on their own, even if both phones are near the same tower. They communicate with a central switching computer to operate, and when that system doesn't respond, they're useless. But police and fire authorities still had internal communications via two-way radio.

Realizing that they'd need more two-way radio, authorities dispatched police to wake up the emergency coordinator <http://www.arrl.org/news/stories/2009/04/15/10771/?nc=1> of the regional ham radio club, and escort him to the community hospital with his equipment. Area hams dispatched ambulances and doctors, arranged for essential supplies, and relayed emergency communications out of the area to those with working telephones.

That the hospital's local network failed is evidence of over-dependence on centralized services. The development of the Internet's communications protocols was sponsored by the U.S. Department of Defense, and they were designed to survive large failures. But it still takes local engineering skill to implement robust networking services. Most companies stop when something works, not considering whether or how it will work in an emergency.

Institutional networks, even those of emergency services providers, are rarely tested for operation while disconnected from the outside world. Many such networks depend on outside services to match host names to network addresses, and thus stop operating the moment they are disconnected from the Internet. Even when the internal network stays up, email is often hosted on some outside service, and thus becomes unavailable. Programs that depend on an Internet connection for license verification will fail, and this feature is often found in server software. Commercial VoIP telephone systems will stay up for internal use if properly engineered to be independent of outside resources, but consumer VoIP equipment will fail.

This should lead managers of critical services to reconsider their dependence on software-as-a-service rather than local servers. Having your email live at Google means you don't have to manage it, but you can count on it being unavailable if your facility loses its internet connection. The same is true for any web service. And that's not acceptable if you work at a hospital or other emergency services provider, and really shouldn't be accepted at any company that expects to provide services during an infrastructure failure. Email from others in your office should continue to operate.

What to do? Local infrastructure is the key. The services that you depend on, all critical web applications and email, should be based at *your* site. They need to be able to operate without access to databases elsewhere, and to resynchronize with the rest of your operation when the network comes back up. This takes professional IT engineering to implement, and will cost more to manage, but won't leave you sitting on your hands in an emergency.

Communications will be a problem during any emergency. Two-way radios have, to a great extent, been replaced by cellular "walkie-talkie" services that can *not* be relied upon to work during an infrastructure failure. *Real* two-way radios, stand-alone pager systems, and radio repeaters that enable regional communications are still available to the governments and businesses that endure the expense of planning, acquiring, maintaining, and testing them. Corporate disaster planners should look into such facilities. Municipalities, regardless of their size, should not consider abandoning such resources in favor of the less-robust cellular services.

Satellite telephones can be expected to keep operating, although they too depend on a land infrastructure. They are expensive, and they frequently fail in emergency situations simply because their users, administrative officials rather than technical staff, fail to keep them charged and have no back-up power resource once they are discharged.

A big plus for Morgan Hill was that emergency services had an well-practiced partnership with the local hams. Since you can never budget for all of the communications technicians you'll need in an emergency, using these volunteers is a must for any civil authority. They come with their own equipment, they run their own emergency drills and thus are ready to serve, and they are tinkerers able to improvise the communications system needed to meet a particular emergency.

Which brings us to the issue of testing. No disaster system can be expected to work without regular testing, not only of the physical infrastructure provided for an

emergency but of the *people* who are expected to use it, in its disaster mode. But such testing takes much time and work, and tends to trigger any lurking infrastructure problems, creating outages of its own. It's much better to work such things out as a result of testing than to meet them during a real disaster.

We should also consider whether it might be necessary to harden some of the local infrastructure of our communities. The old Bell System used to arrange cables in a *ring* around a city, so that a cut in any one location could be routed around. It's not clear how much modern telephone companies have continued that practice. It might not have helped in Morgan Hill, as the attackers apparently even disabled an unused cable that could have been used to recover from the broken connections.

Surprisingly, manholes don't usually have locks. They rely on the weight of the cover and general revulsion to keep people out. They are more likely to provide alarms for flooding than intrusion. Utility poles are similarly accessible. Much of our infrastructure isn't protected by anything so tough as a manhole cover. Underground cables are easily accessible in surface posts and "tombstones", boxes often located in residential neighborhoods. These can be wrecked with a screwdriver.

Most buried cable cuts are caused by operating a back-hoe without first using one of the "call before digging" services to mark out the location of all of the buried utilities. What's done accidentally can also be done deliberately, and the same services that help diggers avoid utilities might point them out to an attacker.

The most surprising news from Morgan Hill is that they survived reasonably unscathed. That they did so is a result of emergency planning in place for California's four seasons: fire, floods, earthquakes, and riots. Most communities don't practice disaster plans as intensively.

Will there be another Morgan Hill? Definitely. And the next time it might happen to a denser community that won't be so astonishingly able to sustain the trouble using its two-way radios and hams. The next time, it might be connected with some other event, be it crime or terrorism. Company and government officers take notice: the only way you'll fare well is if you start planning *now*.