The
Broadcasters' Desktop Resource
www.theBDR.net ... edited by Barry Mishkind – the Eclectic Engineer

Site Management

Site Security FLAP: P is for Presence

By Kevin Kidd, CSRE/AMD

[December 2014] Our series on site security comes to an end with this installment from Kevin Kidd. As we publish this, Comex Copper is still close to $3.00 per pound, with scrap continuing to sell for double what new copper cost just a few years ago.

As readers of this series know, I use an acronym for site security, **FLAP**, to focus on positive things broadcasters can do to prevent or minimize losses to vandals.

Thus far we have looked at **F for Fences**, **L for Lighting** and **A for Alarms**. This article will point out some easy to implement strategies that are all too often ignored in what is probably the simplest of our site security preparations.

P IS FOR PRESENCE

The problem that needs to be solved, in many cases, is actually the *lack* of presence. Or, site maintenance. Or, *just the mere appearance that anyone cares.*

This might have been the reason that several Kennewick, WA stations were knocked off the air in mid-November. The site, just behind a high school, appears to have had a number of graffiti incidents, which might have allowed some to think no one was around.

I have been told by several law enforcement officers that, when caught, the vandals told them that the site was abandoned and did not think anyone would care if they helped "clean it up."

MOW AND MAINTAIN THE GROUNDS

Your site does not have to look just like a golf course but you must to put forth the image that someone cares.

Somewhere back in there is a 3-tower array

We have worked on many more vandalized sites that were overgrown and appeared to be abandoned than nicely kept sites.

The number one method to make a site look like it is inhabited is to do what should be done for the best operation of the site anyway: keep it clean.

Nevertheless, that is not, on its own, the whole solution. Many sites sport good fences, good gates, acceptable lighting, a nice mowed ground field – and still the vandals come to visit.

A major difference in solving many vandalism cases, if not preventing them in the first place, is human presence – or at least maintaining the appearance thereof.

VANDALISM TIMING

Only one vandalism case that we have been involved in appeared to have been perpetrated by *one* person on *one* trip on *one* date.

The damage at that site was pretty extensive but the actual amount of materials he stole was relativity small. That vandal spent more time cutting and tearing than loading his loot, and for some reason never came back for the rest of it.

Nevertheless, the ground system was seriously compromised and required several thousand dollars of remediation work to restore normal operations.

Far more often, we find most vandalism incidents are obviously the result of several people on several trips over several different dates.

One site in particular (mentioned several times in my previous articles as an example as what not to do) in South Carolina probably was ignored for *months.* There were weeds growing through destroyed HVAC units, and grass growing where ground screen, weed block fabric and strap should have been.

This station had no regular engineering support. No one from the station had even visited the site in *months.* Even basic transmitter readings probably had not been taken for months – and it seemed to these eyes that the DA *probably* had not been changed to night mode in *months.*

NOT THE BEST WAY TO FIND OUT

In this case, the thieves got greedy and decided to strip wiring from the transmitter room rack. Finally, they cut enough audio wiring to take the station off.

That finally got someone to go out to see what was wrong. They discovered the transmitter building doors standing open and with obvious damage to everything copper (including numerous HVAC units, phone lines, building wiring, DA feed and sample lines, ground system, audio wiring, etc, etc).

This particular station has since been sold to a more responsible owner and has been re-licensed as an ND2 instead of its original DA-N.

Ironically, the main thief's father turned him in when he heard about the destroyed radio station.

A GENERAL PRESENCE

Someone should go to the site a couple of times *every* week, even if they are non-technical staffers. This really is cheap, easy security, but for some reason the bean-counter mentality often derails such good practices.

That does not mean pull up, say "yep it's still here" and leave. They should enter the site and building, check for vandalism, burglary attempts, fence damage, lighting damage, unusual tracks in grass or mud, unexplained trash (cups, cans, etc), etc. Then document anything that has changed since the last visit.

It only takes about 15 minutes for someone to do a quick drive around and inspection. Of course, this duty would probably be more effective if the inspector has a stake in the optimum operation of that particular site.

FIX THE EYESORES QUICKLY

The station described above in South Carolina had a paved parking lot within easy view of breached doors, broken light fixtures, piles of shredded wire/pipe insulation, obvious excavations and broken gates around all three towers.

There was no excuse for that situation to have continued to its unfortunate conclusion.

More recently we have been involved in rehabbing a couple of sites (one AM, one FM) that were severely vandalized. Fortunately, both were discovered (transmitter off, DA out of tolerance, etc) very quickly as the vandalism progressed. In both cases Authorities were able to locate the copper at recyclers *and make arrests.*

On the other hand, vandalism that is discovered <u>cold</u> – long after the bad guys got away – often does not result in arrests.

THE ENGINEERING PRESENCE

This is part and parcel of the General Presence mentioned above. The engineer should know what is happening at each site for which he is responsible.

Do I and all of my engineering clients check all the sites for which we are responsible several times every week?

Ah. Hummm. Well. No.

Although I try to visit all of my steady clients' sites regularly, it easily can be several weeks between visits. Most of my other clients (probably like your station(s)) are doing their best to keep operating and mostly call me only when they are having problems.

Transmitter and DA readings should be taken regularly and investigated if different from normal / licensed. Regularly does not mean every few weeks. It means regularly. Every few hours. Know what your transmitter site is doing, regularly, at least twice a day.

Not only does the FCC demand parameters be kept in licensed tolerance but transmitter and DA readings departing from normal – but remaining legal – will not only signal impending technical problems but will usually give an indication if vandals are at work. Do you see the readings changing? Is it a cap going bad, a feed line sucking water, a leaking sample loop or a local crackhead stealing something to pay for his daily fix. It does not matter. Check it out.

Even better, with most modern transmitters and/or remote control systems, this can be automated, with an alarm for out of tolerance situations. This way you will know for sure. I can hear all those GMs squealing about paying for this, but it really is cheap insurance.

SITE KEY HOLDERS

The engineer ***<u>should not</u>*** be the only person with site keys. There should be at least four sets of keys for each site – and make sure that keys are updated as sites evolve.

- An original set of keys should be secured in a locked safe or fire proof cabinet, not used by any. (Copies of copies of copies usually do not work very well.)
- The engineer(s) should obviously have a set.
- The station owner / GM / PD should also have a set each.
- There should be at least one set hidden but accessible (with directions) to anyone needing them. ("Over door of Engineering office with big green #1 tag" or "in equipment room behind HVAC unit on ring marked 4th floor men's room"). You decide where; just make it identifiable.
- Keyed-alike locks and programmable combination locks are really handy but pose their own security problems if a key or com-

bination is lost. We use many of the settable combination locks and have never had one defeated although there are many examples of them being "picked" on YouTube.

Here is why keys are important: in my 30+ years of engineering I can count at least ten times when I was called to a non-client station in the absence of their regular engineer and had to physically break into the transmitter building.

Interestingly, a couple of those calls resulted in my driving two hours to a site, defeating a simple door lockset, resetting a breaker, and driving two hours back home. They did not need an engineer. What they really needed was a technically-orientated burglar.

In neither case were the vacationing engineers the only key holders for the sites. The owners and/or management had keys but could not find them. There was no designated key repository nor were there hidden keys. Properly planned access arrangements would have saved a lot of hassle and money.

DO NOT DAWDLE ON RECOVERY

In 2007, vandalism was discovered at a site in Cincinnati by a third party engineer doing some before-work due diligence measurements on a nearby cell tower (as required by 22.371, 27.63, 73.1692). The site had just been rebuilt and re-licensed in mid-2006.

That engineer discovered some of the station's monitor points were well out of tolerance and others were very low. The stations consulting / contract engineer was called for the first time in months to check it out and he discovered damage to two of the five *new* ground systems.

Due to the station's financial status (bankruptcy) and other factors, we were asked for an estimate in January 2007 but were not contracted to do the repairs until June 2007. During those six months, this station had no site security other than the mandated locked chain-link fences around the towers. Most, but not all, of the damage occurred outside of the tower fences on open, unprotected property.

Meanwhile the vandals returned.

When we returned in June to make the quoted repairs, we discovered even more extensive damage, now on three towers and around the transmitter building. Judging by the vegetation regrowth, this second round of damage probably occurred during the early spring that year.

As far as we could ascertain, no one had visited the site nor been taking readings since it had been commissioned a year earlier. Do you see a pattern developing here?

At the time of the repair work, no arrests had been made. Further action is unlikely.

PRESENCE IS PART OF FLAP

Perhaps all this makes the care why it is important not to let your sites to appear abandoned or go unmonitored. Strong indications of regular presence will deter many potential bad guys.

Of course, that is not to say that merely maintaining that presence will give 100% security. The F, A, and L are just as important as the P. And even then, a determined thief still can cause damage. But the result of applying the **FLAP** method will dramatically reduce the chances of a thief successfully getting away with vandalizing your site and gear.

As you **FLAP** away, please send me a note to let me know how it works out for you.

- - -

Kevin C. Kidd, CSRE/AMD is the proprietor of AM Ground Systems Company and KK Broadcast Engineering.

More information on ground systems and security systems can be obtained by calling Kevin at 1-877-766-2999 or visiting his web site at: www.amgroundsystems.com

- - -

Do articles like this help you to do your job? You are invited to subscribe to our one-time-a-week BDR Newsletter. Please take 30 seconds to sign up here. We will not ever flood your email box.

Return to The BDR Menu