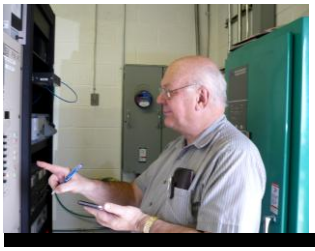

The
Broadcasters' Desktop Resource
www.theBDR.net ... edited by Barry Mishkind – the Eclectic Engineer

IT Connection

Managing Station-Owned Computers

By Chris Tarr

We live in a mobile society. In fact, radio has always prided itself in its mobility, from "News Cruisers" to play-by-play, radio has always been out and about in the community.

Meanwhile, from notepads and pencils, to recordings, to Marti's, and now notebook computers, the devices we use have become more advanced and expensive. Notebooks now are common at station remotes, especially in conjunction with wireless Internet connections.

As the use of notebooks increases, the importance of protecting and managing these devices becomes critical. By nature small and portable – they make easy targets for thieves inside and outside the building, and can also be subject to quite a bit of abuse.

HANDING THEM OUT

It is not unusual for a radio station to issue notebook computers to many different staffers these days.

The most important item when dealing with these computers is to have a detailed and easily accessed policy on the use of company-owned computers, as well as clear expectations on its use and handling.

For example, if I issue a company notebook, I make it very clear that it is to be used for business purposes only, and just like a company-owned desktop, the company retains the right to take it and inspect it at any time. There is no expectation of privacy at all with the computer.

Additionally, if they bring the computer home (which I allow) they must bring it back with them when they are at work. The computer is to remain in their care and custody at all times, and if the computer gets lost, they are responsible for purchasing a replacement.

KEEPING THINGS SECURE

Another important aspect is data security. You need to remember that the minute that computer leaves the building, you lose control over the contents.

Since company-owned notebooks can generally access our networks and can contain proprietary information, I require at the very least a login password for the operating system, and in some cases a boot password, which is a password that it needed for the computer to boot up.

You can also add "lo-jack" type software that can help you track down a stolen computer by checking in every so often with a central server. Information is then passed to the Police to help with the investigation. A caution: savvy thieves now are aware of this type of software, and will often replace the hard-drive before they turn the computer on thus making this method ineffective.

If you have very sensitive data, you will want to look into encrypting the data on the hard drive. There are several ways to do this, but it is beyond the scope of this article.

POOL COMPUTERS

What about "common" computers, like ones used at remotes? Well, with these computers, the concern is not about data, it is about the physical computer.

Again, I recommend a "checkout" system where the person taking the computer is responsible for it is security and use. That will go a long way in preventing problems.

In most cases a simple notebook computer lock will be sufficient. These are much like bicycle locks in that you wind the chain around a fixed object and slip the lock into the computer. Almost all current model notebooks have a slot for this type of lock.

KEEPING THE SOFTWARE "CLEAN"

I often find that these "common" computers take a lot of abuse and the operating system gets easily corrupted.

I use a program like Norton Ghost to make a baseline image of these machines after I set them up the first time. That way when they come back to me with problems, I can just simply re-image the hard drive and it is ready to go. It is quite a timesaver!

HAVE A POLICY

There are many other tricks that you can use in the care and handling of these computers.

I have found that 99% of potential problems can be prevented by simply having a thorough and complete policy regarding the use of notebook computers - and by making sure that the users of those computers completely understand and accept that policy.

If you emphasize the importance of what is contained in that policy, chances are the users will see the importance as well.

- - -

Chris "Doc" Tarr, CBRE, CBNT, is the Director of Engineering for Entercom in Milwaukee and Madison, WI. You can contact Chris at ctarr@entercom.com

Return to The BDR Menu