

## Security or Insecurity - You Choose?

By Leo Bletnitsky  
LBA Networking  
[LEOB@LBAnetwork.com](mailto:LEOB@LBAnetwork.com)

One of the responses I often get from small business owners when I point out their lack of network and wireless security is, “We don’t have anything to steal”. Unfortunately that answer displays a serious lack of understanding of what the standard threat can mean to a small business.

The numbers of scenarios with poor outcomes is plentiful. Hackers can be professional criminals, unscrupulous competitors, or bored individuals anywhere in the world with an Internet connected computer. They can do immature things like defacing your web site, or more serious actions like deleting your company’s data or stealing customer credit card numbers or your employee’s personnel files.

Let’s look at a worst case nightmare scenario. Imagine there is a bored and twisted but tech savvy employee of another company in one of the offices in your building named Bob. He brings his personal laptop and begins browsing for unsecured or poorly secured wireless access points in the area.

“Well look at this!” he says, “XYZ Company’s network is wide open, time for some fun!”

Unfortunately for you, in addition to being an amateur hacker, Bob is also addicted to child pornography. Bob connects to your office PC and creates a hidden directory where he uploads gigabytes of illegal pornography for his viewing pleasure, and maybe even to share with others.

What Bob does not realize is that since now your hard drive is very full, you begin to experience poor computing performance and call a consultant out to investigate. Bob’s bad luck is yours as well; your consultant who happens to be a member of HTCIA (High Technology Crime Investigative Association) finds the hidden directory and calls the police.

You find yourself under arrest for possession of Child Pornography, and your home computer is also seized for analysis. Your once very supportive and loving wife changes the locks and gets a restraining order against you to protect the children. Your business partner says he believes in your innocence, but seems much more formal than ever before. Let’s not even think about how the fallout of your arrest will effect your employee and client relationships.

After the police conduct their investigation, you may or may not be prosecuted, may or may not be convicted. In either case, the chances of getting your old life back are pretty slim!

I agree, this was a worst case scenario, however the steps needed to prevent this and many other serious and less serious problems are fairly minor and inexpensive compared to even the minor potential consequences.

To sum it up, businesses and even home users should take some basic precautions to safeguard the CIA (Confidentiality, Integrity, and Availability) of their computer systems. You should at a minimum have a Firewall, Secure Wireless (if you have wireless access), Current Anti-Virus Software, a Daily Backup and regular spyware scanning.

While the above does not guarantee your security, most bad guys will go on to easier targets. This is not different than residential or commercial alarm systems. An alarm system can be circumvented, but if you're the only guy on the block without one, you're the likely next victim!

For more information the Federal Government has a helpful website:  
<http://www.onguardonline.gov>