

Protecting Your Confidential Information

By Emery J. Kohut

Recently there has been a tremendous amount of publicity on confidential or personal information lost or stolen in the weekly news reports. The Veterans Administration, IRS, and Beaumont Hospital Home Care were seriously affected. The latter case was caused when a nurse's car was stolen and a business laptop was in the car! How many people have been affected? In the case concerning the VA, over 30,000 and in the case of Beaumont Hospital Home care, over 28,000 people were affected. How and why does this happen? Couldn't more care have been taken with personal information?

Everybody loses something at some point in time. A friend recently purchased a USB memory stick and found a woman's entire medical history, social security number, birthday, and other important personal documentation on it. She had returned it to a store because it was "defective." Fortunately for her, it came to a responsible person and her confidential data was destroyed.

Things like this happen every day. In fact, in the first half of 2005, in London, over 5,000 laptops, 6,000 pocket PCs, and 63,000 mobile phones were left in cabs. There is no count of how many memory sticks, also called "jump drives," have been lost in Britain. Imagine what this would be like in the United States. In 2001, as reported in Time Magazine, 519,000 laptops were lost or stolen. These numbers are staggering and considering what most people store on these pieces of hardware, frightening. Millions of dollars of lost proprietary information is out there some where. Everyday more information is lost because people are in a hurry and leave valuable information lying around in plain view. It is also stolen because we are not carefully monitoring our surroundings or our bags, briefcases, purses, etc.

How do we protect this information? We need to make sure that we keep track of everything we have and that our laptops, pocket PCs, cell phones, and memory sticks are secured. When something is lost or stolen, then what do we do? There is a way to protect your information stored on many of these devices.

The first step is to make sure that a password or security code is used to access laptops, pocket PCs and cell phones. Most thieves will not spend the time to try and unlock them. If you use long and complex, but easily remembered passwords or security codes, this will slow them down considerably and may even frustrate them enough to stop trying.

The second thing that can be done on most of these pieces of hardware is to encrypt the data with a secondary password that is not the same as your password to access the device. Encryption is an age old method of making sure everything is secure. It may sound complicated, but it is not. There are software solutions that solve this problem and you can install and use them very quickly. The great thing about these solutions is that they protect our information even if it falls into the wrong hands

If the lady from the above description had encrypted her data, the likelihood of anyone getting to it would have been very slim. Keep your information safe; encrypt it even on your workstation. Keep your private matters, and those of others, safe.

Word Count: 547