

Theft from the Inside

By Tom Goll

Nashua, NH

www.AdvansysUSA.com

September 2008

This probably is one of the most uncomfortable employee relation issue a business owner or manager faces. Our human nature is to trust those that we work with especially since we spend so much of our daily time working together. We call our co-workers friends, we know their families and we rely on each other to produce quality results for the common good of the company. Why then should we as owners and managers need to protect our assets from our employees? As unpleasant as it may be, nearly \$40 billion of company assets from inventory to intellectual property and confidential information is stolen from small businesses across this country each year. As a small business owner or if you are in a position of responsibility for a company's assets, you know that this subject demands attention and needs to be on your radar. With the uncertainty of the economy, additional stresses placed on employees can add to these problems. As employees feel pressured from rising cost of living, threats warranted or not, of downsizing and job instability, have historically shown employee theft to increase.

Discovering a theft by an employee naturally leaves a small business owner feeling a deep sense of being violated. But do you have time to even notice? Reportedly 75% of all employee theft goes unnoticed. As a small business owner you don't have time to be a security guard, making it a must to have a complete security policy in place. Just as it is important to lock the door on your way out, it is important to know that your employees are following your company security policies. It is a breakdown in your security policy that commonly allows a theft to happen, making it necessary to have checks and balances in place. Quite often a misguided employee won't even look at some theft as actually stealing. This is why you need to remove the opportunity to steal. In the security industry we call this keeping the honest person honest. Once a theft is suspected, making an accusation toward an employee can permanently

damage relationships not only with that employee but also with those with whom the individual works with. Making sure you are on solid ground before you make your suspicions known or state any accusations is also very important. Putting in place adequate security tools that provide you with these controls and information needs to be in the forefront of your security policy.

In 2008 one of the most damaging theft opportunities comes from the theft of information. Almost everyone carries a memory storage device. They come in the form of cell phones, music players, USB Drives, SD Cards, CD, DVD writable disks and so on. They connect to your computers by hardwire, Blue Tooth or IrDA technology. They hold information in the 100's of Gigabytes and can do untold damage; just 1 Gigabyte is equal to 1024MBs. Just 27MB of data equals the volume of information commonly found in one 4 drawer office filing cabinet. On top of this, your honest employee could accidentally infect your computer system with malware simply by connecting their memory device to play music brought from home. Products like USB Lock ST or USB Lock RP are designed to provide the endpoint security necessary to allow you control of this potential problem and needs to be a part of your active computer security plan.

You don't need to be an IT professional to install and manage this type of security tool and the cost is not overwhelming. But it will allow you or your manager the administrative control over authorized and unauthorized use of memory storage devices. There are times when the use of these memory devices will be authorized so Advanced Systems Internationals, SAC products include tools that provide a log of files removed and another tool to protect your data while being transported on a memory device that is taken home or out on the road. If you didn't know that 77% of corporate end-users surveyed have admitted to using personal flash drives for work-related purposes, you're not the only one. A recent study indicated that corporate IT Directors thought that only 35% of the employees were doing this, indicating that it is a commonly overlooked problem with enormous potential to cause you and your company a financial and embarrassing negative situation.