

Data Leak Control

By TOM GOLL
www.AdvanSysUSA.com
Nashua, NH August 2008

One of the largest openings for serious data leakage within a network is due to the oversight of mobile memory devices. You only need to stop a moment to realize just how many of these devices are around you, including the one on your key chain. Cell phones commonly carry 1 or 2 Gig SD cards, USB Flash Sticks or what ever name you call them are owned by many. Think of all the small remote hard drives around today with 120+ Gigs including the popular IPod. Now consider the availability of fast connection methods like Bluetooth and now the ever growing use of IrDA. How much easier can it become to take information? Data files most likely to be copied to a personal flash drives includes customer records (25%), financial information (17%), business plans (15%), employee records (13%), marketing plans (13%).* Not all information removed from your network causes concern but the open opportunity to remove or copy sensitive data remains a serious threat. Not everyone connecting their memory device is out to get you. Maybe they just want to listen to music or show a friend some pictures from home. But the network manager can not be sure that these devices don't carry malware of one type or another. This is why it is recommended that memory device use policies be put in place. Part of that policy should state that only company issued memory devices be allowed on a network. A recent study found

...AARP study** reports that close to 50% of identity theft comes from educational institutions ...

that 77% corporate end-users surveyed have admitted to using personal flash drives for work-related purposes. However, when asked to estimate what percentage of the workforce uses personal flash drives, corporate IT respondents said only 35% percent. This shows a major gap between what management thinks is happening and what actually is, as it relates to a possible threat from memory devices.

Why is it important to but proper control in place? We are of the opinion that it is highly important giving reason to why Advanced Systems International USB Lock products were designed for easy installation and robust security features. The thing I hear most from network managers and IT technicians is that the products are clean and fit without issue into their current plans and policies. They look for a product that will take the least time to put in place and easiest to work and live with. Originally designed for small company's that don't have professional IT technicians on staff the larger company's have found the USB Lock ST & RP to be everything they need to control their end point security at a low cost and providing robust end point protection.

* Reported by ScanDisk April 2008

** Neal Walters, AARP Public Policy Institute July 2006