

Data Security Is the Rule of Thumb

November 2008



How many times have you seen this scene? A very nervous individual is at an airport's lost and found asking if anyone had turned in a thumb drive. When asked what it looks like he replies, "I think it was blue and the size of my thumb. The person behind the counter just regretfully shakes his or her head. Or possibly worse, the person pulls out a box of drives that all look the same. The number of scenarios for disaster here are almost endless.

Mobile media, like thumb drives, are convenient, easy to use and inexpensive. They also can carry a huge amount of data – up to 64 GB in commercially available drives. The amount of data they can carry would have required a bulky hard drive not that long ago.

The attributes that make these drives so popular are also their greatest vulnerability. Because of their size, they can be easily lost or stolen. The news is filled with stories about people leaving entire computers on a plane. If it is that easy to forget about a laptop, how hard would it be to forget about a thumb drive? In addition, because they are so small it could be hours, even days, before you realized it was gone. Think about how many times you have searched frantically through pockets, briefcases or handbags looking for a two-inch piece of plastic and metal that holds entire databases of potentially critical information. Develop a security habit and routine in the handling, storage, and accountability of removable devices used in travel and data transportation. Always right click and scan for viruses when you plug in a thumb drive or other data storage device.

It's not just the highly sensitive information that requires care. People who are normally very good about securing classified data often relax when transporting or storing unclassified data like personally identifying data or the last update to the planned briefing at your destination. No matter what information you carry on mobile media, you should treat it as if it is the security codes of a top secret military facility. While it may seem easier and less likely to be lost, placing that recent update and the associated spreadsheets on your iPOD™ or other mobile device is unauthorized. The risk of theft of these devices is greater than that of a media device alone.

The best way to prevent data loss through misplaced drives starts with the basics. Don't use these drives to carry or store sensitive information unless absolutely necessary. When you do carry mobile media, put them in a secure place, preferably on your person. Make it a standard part of every shut down and logout routine to remove mobile media and store it securely.

Also, when you must use mobile media for transporting information make sure you follow these rules of thumb.

- Use only government provided drives to transport government information.
- Never use free, found, vendor-provided, or "conference-ware" drives for any government work, and never connect these drives to a government system while on travel.
- Make use of all appropriate encryption, password protection and biometric safeguards.
- Make sure your drive is labeled as to the kind of information it holds, Unclassified, Secret, Top Secret, etc, and safeguard it appropriately.
- Report lost devices.
- Don't use the same thumb drive for SIPRNet and NIPRNet. Once SIPR never NIPR!

In short, make sure you don't let your data at rest become data at risk.