

Laptop Theft: What are the implications and how can you protect your data?

By Ricky Crow, CISSP

Theft of laptops and the data contained on them is becoming an increasingly significant and costly problem. Annual theft statistics figures range from 400,000 to more than 1,500,000 laptops stolen per year. This does not take into account the fact that many people do not take the time to report a stolen laptop to law enforcement officials.

More individuals and organizations are taking advantage of the convenience and mobility provided by laptop computers. In many cases, laptops are replacing standard desktop platforms. Increased mobility introduces new threats to information security not prevalent with standard desktop platforms. Recently, several high profile cases have been in the media spotlight relating instances in which laptops containing sensitive information including personal employee and customer data were stolen. This trend of laptop theft is growing year after year.

There are precautions users can take to ensure their laptops remain secure, but there is no way to guarantee a laptop will not end up lost or stolen. Multiple sources indicate that approximately 10% of all laptops end up lost or stolen at some point, with only 3% of those stolen laptops recovered. Businesses and individuals should assume that one day an unauthorized user will take possession of their laptop. People should take proactive measures needed to ensure sensitive information is not lost or disclosed when that day ultimately arrives.

Many laptop vendors now provide built-in system BIOS features that render the hardware inoperative, in the event it is reported stolen. However, is this enough? If a thief removes the disk drive from the disabled laptop and installs it in another device, the data will likely still be retrievable.

Encryption methodologies used to protect information have been around for centuries. Modern encryption technologies simply scramble data using a key or passphrase so that it is not readable without specific knowledge; in most cases the decryption key, passphrase, or in the case of a two-factor encryption, a combination of a physical electronic key and a passphrase is required. One of the leading reasons why encryption has not been widely used historically is due to the level of effort required to encrypt specific individual files.

A simple cost-effective solution is to employ the use of whole-disk encryption to protect this data from unauthorized individuals. While this will not prevent the loss of the device itself, it is a good step to ensure sensitive data does not end up in the wrong hands. By combining whole-disk encryption with a secure method of backup storage kept in a different physical location, the loss resulting from the missing laptop will not be much more than the cost of the device plus the lost productivity. This is a small price to pay when compared to company secrets or confidential customer data disclosure, regulatory compliance fines for executives and the institution, or malicious individuals taking advantage of identity theft.

Today, many individuals and companies choose to encrypt only specific files designated as confidential. By selecting only specific files or specific file types, the risk still exists that certain files not meeting the pre-defined encryption selection criteria will not be encrypted or a user may inadvertently forget to encrypt an important file. While there is a system performance cost to use whole-disk encryption, today's portable computers with fast hard drives and powerful processors can handle the additional load with little impact on daily tasks.

To use a system with whole disk encryption, one typically inserts an electronic key into a USB port at system start up. The system then prompts for the users pass phrase to unlock the data on the drive for the specific boot session. The USB token (what you have) and the pass phrase (what you know) provide dual-layer protection for every file on the system, not just those the user

deemed important. Without both items at boot time, all of the data on the drive will be inaccessible. This eliminates the possibility of skipping over or omitting the encryption of a file that actually is important and/or confidential.

In addition to implementing appropriate physical security and technical controls, proper security awareness training is essential to a complete security program. There is a marked reduction in data loss resulting from theft when users are aware of the risks facing the organization and understand how to minimize these risks. Common sense, simple ways to prevent your laptop, and the data stored on it, from “growing legs” include:

- When working in the office, use a cable lock or similar mechanism to prevent the removal of the laptop from your desk.
- If using a laptop in a conference room or any other location outside your office, never leave the laptop unattended.
- When transporting the laptop in a vehicle, never leave the laptop in the vehicle while the vehicle is parked and unattended. “Smash and grab” laptop theft from vehicles is very common.
- Take your laptop home with you at the end of the day to eliminate the temptation that might cause other employees or after-hours maintenance and cleaning crews to steal equipment.
- If you absolutely need to leave your laptop at your office overnight, place it in a locked cabinet and take the keys with you.
- Most importantly, ensure you have an effective backup system that is tested regularly for proper function in the event the above measures do not prevent the loss of portable computer equipment.

It may be impossible to eliminate all risks related to information or equipment loss, but dedicating a little effort to provide a secure environment and use of judicious behavior when transporting your computer equipment will go a long way toward preventing you from being the next victim of laptop theft.