

Laptop Security

By: Will Fleenor, CPA.CITP, Ph.D.

Member, K2 Enterprises

Laptop theft appears to be a cottage industry in the US. Consider these facts: according to Safeware Insurance Agency, more than 750,000 laptops are stolen every year. This translates into more than \$1 billion in lost property and, according to the study, more than a \$5 billion loss of proprietary information. According to the FBI, a whopping 97% to 98% of stolen computers never return to their rightful owner.

From 2005 to 2006, there was an 81% increase in the number of companies reporting stolen laptops containing sensitive information (2006 Annual Study: The Cost of Data Breach. Ponemon Institute, LLC, 2007). The average business loses about 5% of its laptop inventory to theft. Even top law enforcement agencies aren't immune. The FBI reportedly experiences three to four laptop thefts a month. More than half of the stolen laptops are stolen out of offices, so almost no one is immune to the risk of having their laptop disappear. 90% of laptop theft is committed by insiders.

Clearly, people with confidential information on their laptops need to take measures to make sure that the thieves will not be able to access this confidential information. Regulations like Gramm-Leach-Bliley, HIPAA, Canada's PIPEDA, the EU Data Directive, Sarbanes-Oxley, and state security breach notification laws, can impose criminal penalties for those who compromise another's confidential information.

The Microsoft® Security Intelligence Report, for the 2nd half of 2007, provides insight into just how serious a security issue laptop theft and loss is. According to their research, 57% of the security breaches publicly disclosed involved lost or stolen equipment in 2007. With 45 states currently having security breach notification laws, companies that fail to have some type of policy are probably negligent and exposing their companies and firms to serious legal and financial risk.

[Editors Note: Will Fleenor will be one of the presenters at the 2008 Heartland Technology Conference, December 18-19, at the Doubletree Hotel in Overland Park. For more information or to register for this program, visit www.kscpa.org/conted.cfm.]

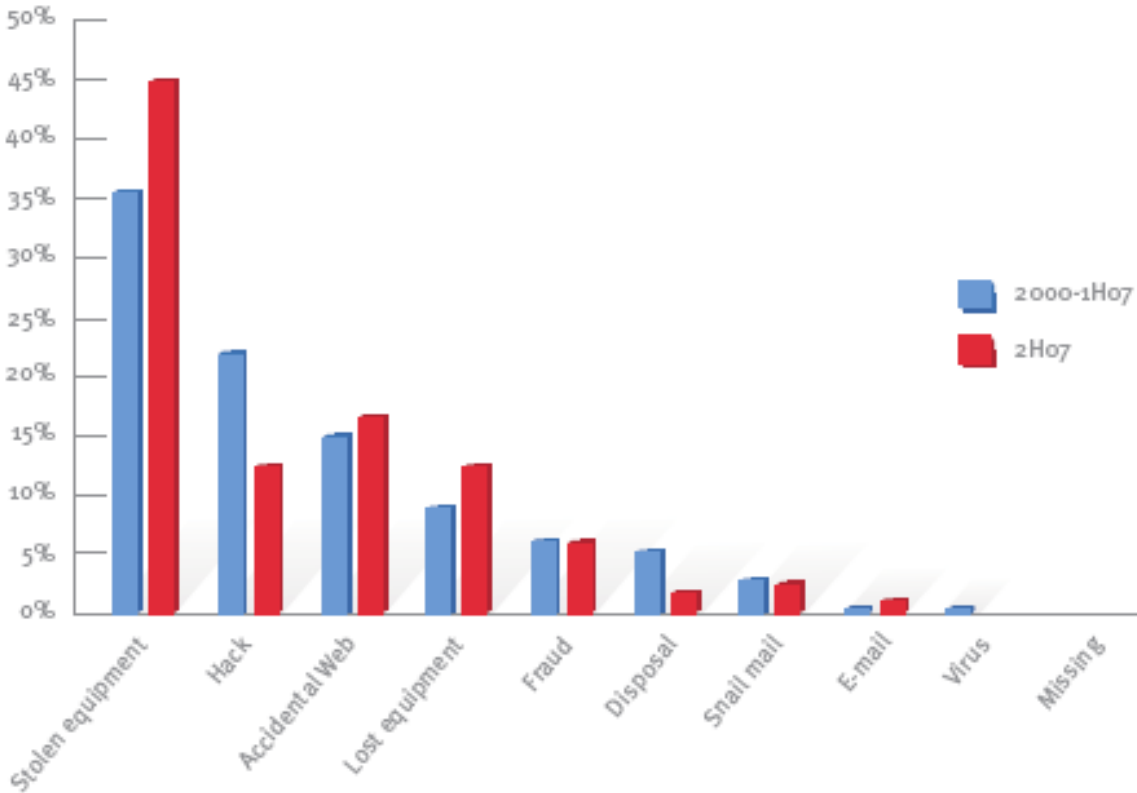


Figure 1

Source: The Microsoft® Security Intelligence Report for the 2nd half of 2007

Whole disk encryption is certainly a solution people with confidential information on their laptop should consider. Whole disk encryption can be used with Vista. Whole disk encryption for computers is also available for almost all other operating systems, including the Apple Leopard OS. For example, the latest release to the PGP Encryption Platform, PGP Whole Disk Encryption 9.9, adds pre-boot authentication to PGP Corporation data encryption technology for Intel-based Mac OS X systems “Tiger” and “Leopard”, providing protection for data on desktops, laptops, and removable media. Whole disk encryption solutions are widely available and some are even free, including high profile tools like TrueCrypt, free open-source disk encryption software for Windows Vista/XP, Mac OS X, and Linux.

While protecting confidential data is certainly a concern with laptop theft, it is not the only concern. Following is a more complete list of common concerns with lost business laptops:

- The possibility that confidential information will be compromised
- The financial and other business costs (loss of goodwill and clients) of having company, employee, customer, or vendor data compromised as a result of your actions
- Lost productivity

- Gaining assurance that the data was destroyed and was not accessed before being destroyed (LDD – Lost Data Destruction)
- Dollars to replace hardware and reconfigure software
- Lost data that was not backed up and, therefore, is permanently lost
- Attorney fees to make sure the legal issues are being dealt with properly

If you conclude, after understanding all the potential costs, that a comprehensive whole disk encryption solution meets your needs, you have choices. The following is a short sampling from a very big market with lots of good choices, many of which are not included in this list:

- PGP Desktop Professional – The Gold Standard
- BitLocker – Microsoft’s Entrant and a Strong Player
- TrueCrypt – Open source, free, highly respected, more complex interface, for support you must rely on the community of users
- Beachhead Solutions – Most Comprehensive Approach
- McAfee Endpoint Encryption – Strong Consumer and Small Business Player

If you conclude that you need more than whole disk encryption (for example, Lost Data Destruction, or centrally managed laptop tracking and recovery tools), there are other tools and services that will provide these features at a reasonable cost.

Consider attending the Kansas Heartland Technology Conference on December 18th & 19th for more solutions on laptop security issues currently faced by CPAs.