



## **Laptop Security for Accounting Professionals**

*By William C. (Will) Fleenor, CPA.CITP, Ph.D.*

*Member, K2 Enterprises, LLC*

*will@k2e.com*

Laptop security is a serious business risk that accountants should address directly with specific written policies and procedures. These policies and procedures are essential for regulatory compliance, reducing stolen laptop costs, and preventing data breaches. Regulations mandating privacy and confidentiality of sensitive personal information include Gramm-Leach-Bliley, HIPAA, Canada's PIPEDA, and the EU Data Directive. Sarbanes-Oxley also mandates strong "internal controls" for financial data.

At least 34 states (including Washington) have passed security breach notification laws. The Washington state law states that: *"Any person or business that conducts business in this state and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."* Can you imagine how many people would have to be notified if, for example, you are CPA in public practice and you lose a laptop with several client QuickBooks files and numerous client tax returns on the computer? All the employees whose information is contained in those QuickBooks files would be part of the list of people to be notified. Accountants in industry and government typically also have lots of confidential information on their computers.

In addition to regulatory requirements there are other costs associated with the loss of confidential information. Loss of productivity, damage to client and customer relations, damage to your reputation, loss of you job, and dollars spent to recover are some of the other costs. Clearly this is not a pretty picture.

The following is a list of the unique security issues laptop users must deal with:

1. Your laptop could be lost or stolen much more easily than your desktop computer
2. Your laptop is more likely to be hacked because it is not behind the protection of your business firewall
3. Your laptop is more likely to be hacked because you may be connecting to unsecure public networks
4. Your laptop could be compromised because you are not connected to the corporate network and therefore it is more difficult for your company to centrally manage the computer

Consider these facts:

- According to Safeware Insurance Agency ([www.safeware.com](http://www.safeware.com)), more than 600,000 laptops are stolen every year, which translates into an estimated \$5.4 billion loss of proprietary information.
- According to the FBI, a whopping 97% 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. Top law enforcement agencies aren't even immune. The FBI reportedly experiences three to four laptop thefts a month.

Once someone gets your laptop they can boot it with a CD and use programs like pwdump2 to extract user names and encrypted passwords. Then they can use free, open source cracking tools like "John the Ripper" to crack your passwords. From this point on they not only have access to the confidential information on your computer, they have access to your email server, and possibly even remote access to your business servers. With your Windows password they can use your computer to host illegal activities, launch malware, and/or send out SPAM thorough your businesses email server. Once again, not a pretty picture.

Fortunately, there are solutions that provide reasonable assurance that these things will not happen to you.

- Create and enforce a written security policy regarding portable computers and removable media.
- Use whole disk encryption for laptops containing confidential data.
- Use "track and trace" software to be able to recover lost or stolen laptops and to delete confidential data once a laptop is lost or stolen.
- In larger organizations that have full time IT staff consider centrally managed software solutions for protecting information on laptops.
- Require those who access your business servers remotely using their laptops to use two factor authentication.
- Windows laptops with highly sensitive information should be running the Vista operating system.
- Never leave access numbers or passwords in your laptop carrying case.
- Treat your laptop like cash. Never leave it in a hotel room or on the seat of a car.
- Disable wireless connection devices that are not in use (ex. Infrared Port, Bluetooth, and WiFi).
- Educate your laptop users about the security risks associated with portable computers.

## Creating a Written Security Policy

For small business a formal, written security policy may seem like overkill but it is clearly a necessary step. Creating written security policy forces business managers to understand and think through the issues. The process will result in both a change in how sensitive data is managed on laptops and in the implementation of new technologies to help protect the data. For example, adopting a policy that all laptops with sensitive information to use full drive encryption will probably cause some people to just be more careful about what they keep on their laptops. SANS.org, the international association of computer security professionals, has sample policies and is a good place to start (<http://www.sans.org/resources/policies/>). You may not like their sample policies but it is a lot better than starting with a blank sheet of paper.

## Use Whole Disk Encryption

Some people are under the misconception that using the Windows NTFS file system encrypts data and provides protection when a computer is stolen. This is wrong. If someone steals your Windows computer, the Windows operating system will prevent them from logging on without a valid username and password. However, it does not necessarily protect the files on the hard drive. Products like NTFS4DOS Private (<http://www.bootdisk.com/ntfs.htm>) allow you to boot most Windows computers using the DOS operating system and read the files off the hard drive. To patch this serious security hole you will need to encrypt the confidential files on your laptop. Windows does have the ability to encrypt files and folders but unless you are using Windows Vista Ultimate or Windows Vista Enterprise you do not have full disk encryption (i.e. BitLocker). Since Windows caches files and creates temporary working files when files are being used and printed, encrypting only files or folders may not cover up every trace of confidential information. There are lots of third party products like PGP Desktop, SafeBoot Device Encryption, and XTool Encrypted Disk that will perform whole disk encryption.

## Use “Track and Trace” Software to Recover Missing Laptops

This is great software for people who have laptops with lots of confidential information and for companies who are losing lots of laptops. It works by loading software on your laptop that uses an Internet connection to tell you where it is after it is stolen. There are lots of these products (ex. Computrace LoJack, XTool Laptop Tracker, and CyberAngel) and some are loaded at the bios level so they still work even if the hard drive is reformatted. One of the products, XTool Tracker can even detect a laptop camera, take a still photo of the thief and relay it back to you for evidence in a criminal trial. This company has a staff of security professionals who work with the local police to get search warrants and find the physical location. All you have to do is call them and file a police report. While the FBI reports that only 2% to 3% of stolen computers are ever recovered, users of “track and trace” software have an over 70% recovery rate.

## Consider Centrally Managed Software Solutions

Companies like Entrust (<http://www.entrust.com/laptop-security/>) and CheckPoint (<http://www.checkpoint.com/>) have products that can be loaded on laptops but still centrally managed by the IT staff. These computers “check in” when connected to the internet and the centrally managed software will not let them connect to the businesses network unless they meet certain criteria. These products work very well in larger organizations where it is difficult to get everyone on the same page and where regulatory compliance is a must. Some of these products take advantage of the TPM (Trusted Platform Module) chip that is built into many new laptops and the Intel vPro technology which is built into some of the Centrino Pro mobile processors (<http://www.intel.com/business/vpro/>).

## Require Laptop Users to use Two Factor Authentication for Remote Access

Two factor authentication involves the use of “something you know” (ex. username and password) and “something you have” (ex. a token you must plug into a USB port). Since the 2<sup>nd</sup> factor is a physical device the thief would have to steal both the computer and the token to be able to gain remote access to your servers using a stolen computer. Two factor authentication has become very common. If you just ask around in your next CPA society meeting I am sure you will find several of your colleagues that are already using it. Remember, when someone steals your laptop and cracks your passwords they potentially gain access to a whole lot more than just the information on your laptop.

## Use Vista on Laptops with Serious Security Needs

The Windows Vista operating system made very significant improvements to laptop security. Just a few of the important improvements are:

- Support for TPM chips in laptops
- Improved support for Smart cards and biometric authentication devices
- User account control
- Windows Service Hardening
- Address Space Layout Randomizer (Microsoft estimates that 99% of remote attacks will fail due to this new feature. This is important when you are connected to a network outside your office.)

## Conclusion

Laptop security is clearly an issue that accountants should take seriously and devote significant resources to. Failure to address this issue adequately can result in serious business risk, criminal penalties, loss of employment, and even business failure. In this brief article we have discussed the key business risks that are unique to laptops. We have also talked briefly about the available solutions. Finding and implementing these solutions will require some significant additional effort in developing written policies and procedures and also in researching the technology solutions. The good news is that there are lots of good solutions and your choices are getting better every day.

## References:

Washington State Security Breach Notification Law

<http://privacy-law.blogspot.com/2005/05/washington-enacts-security-breach.html>

Laptop-tracking technology rarely used among SMBs

[http://searchcio-midmarket.techtarget.com/news/article/0,289142,sid183\\_gci1251758,00.html](http://searchcio-midmarket.techtarget.com/news/article/0,289142,sid183_gci1251758,00.html)

Using the Windows Operating System to Encrypt Files and Folders

<http://www.microsoft.com/windowsxp/using/security/learnmore/encryptdata.mspx>