CPA
Practice Advisor

From the December 2006 Issue

We’ve all heard or read the sensational stories: VA laptop stolen containing social security information of more than 26.5 million veterans; Laptop with credit card information for more than 243,000 customers stolen from auditor’s car; hard drives containing a treasure trove of confidential information recovered from machines “donated” to a worthy charity or fished out of a local landfill. On and on, the stories splash on our screens and evening news, each one a glowing example of breach in confidentiality — one of the “pillars” of IT security.

So with recent news events as a backdrop, I felt it would be especially worthwhile to begin a multi-part series that focuses on the topic of confidentiality — threats to maintaining the confidentiality of our most sensitive information — along with reasonable steps and measures we can take to safeguard this information. And as we explore confidentiality — threats and responses — you will quickly notice a number of factors that need to be considered since our data is susceptible across a number of fronts.

As a refresher, there are three primary goals (also known as the pillars) of IT security. They are as follows:

- **Confidentiality** — Information should only be available to authorized individuals.
- **Integrity** — Information should only be modified by those who are authorized to do so.
- **Availability** — Information should be accessible to those who need it, when they need it.

data, could spell disaster for an organization. Yet often, much of this information is distributed across a number of machines, in a number of locations, throughout an organization — many times with little or no thought given to security — with no clear corporate knowledge of what exists where.

PROTECT PHYSICAL ACCESS TO DATA

Once you’ve identified mission-critical data, the next order of business is to make certain it’s physically protected. This means that no one should be able to physically walk off with it. So to make that happen, all an organization needs to do is place network servers in a locked closet or server room, and the last person out at night locks the office doors … right? Well, not so quickly. With more and more organizations equipping their users with laptops, the reality is that increasing amounts of key data is walking out the door each and every day. In fact, as recent headlines point out, some of the most significant data breaches are the result of simple laptop theft (i.e., homes and cars broken into and laptops stolen). Our organization has experienced this first-hand when one of our staff consultants had her car broken into and machine stolen this past year.

So how should an organization respond? Well, in addition to some of the obvious measures, including placing all servers in locked closets as previously suggested, the following additional steps should also be considered:

- Train users regarding the importance of physically protecting company data, wherever it resides, including desktop machines, corporate laptops, backup media, USB drives, CD disks, etc.
- Caution users on the risk presented by portable USB thumb drives since large amounts of data can be quickly transferred to these devices from any accessible machine and because these devices can be easily lost, stolen or misplaced. Some

organizations have gone so far as to disable USB ports on user machines in order

BACK DATA UP

While we have explored this topic in depth in the past, it's important to note that a complete backup of both data and applications represents a crucial safety net, not only for restoring lost data, but for determining what data was lost or exposed in the event of a breach or theft. And just in case you missed my previous recommendation (you can read the full article in the November 2006 issue or access it online at www.CPATechAdvisor.com), it can be quickly summarized: backup, backup, backup!

PROTECT HARD DRIVES

With all this talk of lost or stolen machines, what steps can reasonably be taken to protect the data on the drive in the event it falls into the wrong hands or is unwittingly exposed to an unauthorized individual?

- **Logon password** — At the very least, every machine should require a user to logon prior to accessing the contents of the drive. This provides minimal protection, but should not be overlooked as a basic form of protection. If nothing else, it should prevent the casual user from accessing a machine.
- **Encryption** — A number of commercial products exist that allow the contents of selected folders, volumes or the entire hard drive contents to be encrypted. These products can provide excellent protection against unauthorized access. But one reminder is in order: Don't lose your password! In the event you do, you may never be able to access the contents of the drive again even via an outside data recovery service. Talk about protection!
- **Bit Locker** — Recognizing the importance of securing data on machine hard drives, Microsoft plans to include a new feature in the higher-end versions (Enterprise and Ultimate) of the soon-to-be-released Windows Vista operating system called Bit Locker. The Bit Locker utility is capable of encrypting the entire

hard drive contents, including the Windows volume, swap and hibernation files.

- Phone home — A number of tracking products also exist that are designed to e-mail you the exact location of your laptop in the event it’s lost or stolen. Many of these products also enable you to trigger a melt-down procedure that will completely wipe the drive, destroying the contents and making it completely unusable. Most of these products are available on an annual subscription basis.

On a similar note, if you plan to dispose of or donate an old machine, steps should be taken to ensure that your confidential information does not go along with it. If you would like to donate or dispose of the drive along with the machine, we recommend using some type of disk wiping utility to scrub the drive clean first. A number of freeware and commercial products are presently available that do an excellent job clearing a drive of all information, although a much easier method would be to simply remove the hard drive prior to disposing of the machine. The drive can then be physically destroyed to ensure the data can never be accessed again.

Next month, we will continue to look at ways users can safeguard their confidential data, especially when they are on the road. Until then, safe computing!

———————————————

David Cieslak is a Principal in Information Technology Group, Inc. (ITG), a computer consulting firm with offices in Simi Valley and Huntington Beach, Calif. He is currently an instructor for K2 Enterprises and a frequent speaker on technology issues. He also currently chairs the AICPA IT Executive Committee and serves on the Information Technology Alliance board of directors and CalCPA Council.

Technology