

# Is Your Customer Information Safe?

By Tommy Bowden

Recently, an unfortunate Ernst & Young employee had his laptop computer stolen. Unfortunately for 243,000 Hotels.com customers, the stolen laptop contained their credit card information. Earlier this year, the U.S. Department of Veterans Affairs revealed that data on up to 26 million veterans had been compromised. Before that it was ChoicePoint, an Atlanta-based company, disclosing that thousands of individuals had their personal data, including their names, addresses, Social Security numbers, and credit reports, stolen by scammers. And the list goes on...

As a small business owner, what steps are you taking to protect your customer information from these kinds of assaults? The first step for any small business owner is to take an inventory of all data assets, especially customer data and other sensitive information, and determine what might happen if that data were to be stolen. If the results of this inventory check reveals that someone could maliciously benefit from the conversion of this information (internally or externally), you should take immediate action.

**Guarding your information from local threats...** Protecting your customer information from your own employees should not be overlooked. Not all of the “bad guys” are on the Internet. Simple steps

that you can take to safeguard your information at the local level include:

- Use computer login passwords that are hard to guess and password protect sensitive files and/or applications.
- Use screensaver locks that are password protected.
- Shut down your system when you are away for extended periods.
- Do not store backup data files in an accessible location.
- Don't overlook the “hard copies.” Lock them up.
- Never discard a computer that contains a hard drive. Old hard drives should be removed and destroyed.

**Guarding your information from remote threats...** Steps that you should take to safeguard your information from “cyber attacks” include:

- Install virus-scanning software and keep it updated.
- Install operating system software “patches” when they become available.
- Be wary of opening unexpected e-mail file attachments or embedded web links in e-mail messages.
- Do not connect your computer directly to a broadband modem. Always use a router between the computer and the modem (even if you do not need to share a connection).

- Utilize “data encryption” methods (SSL, HTTPS, VPN) when communicating sensitive information with other computers over the Internet.

Fortunately, the vast majority of small businesses are rarely targeted for major cyber assaults. The “bad guys” tend to go after bigger targets that have a higher reward potential...but it can and does happen. In reality, small businesses lose more data by accident (user error, hard drive crash, etc.) than by theft...which brings up this question:

**When did you perform your last full data backup?**



Tommy Bowden is an assistant director with the Georgia SBDC Network. To find the office located near you, go to [www.sbdc.uga.edu](http://www.sbdc.uga.edu) or phone 706-542-2762.

Funded in part through a cooperative agreement with the U.S. Small Business Administration. All opinions, conclusions, or recommendations expressed are those of the author and do not necessarily reflect the views of the SBA.