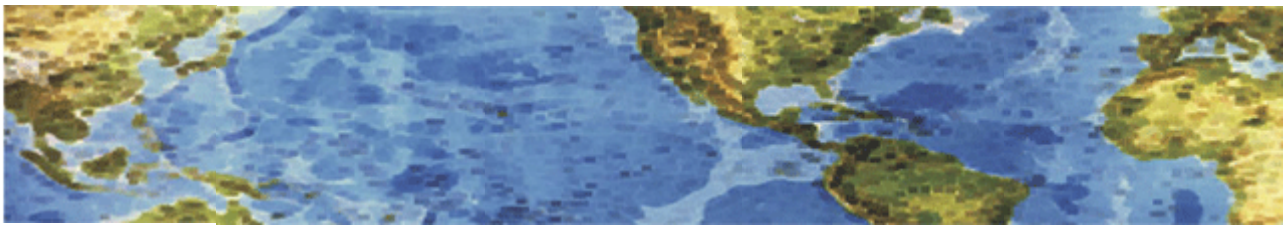
HALL ASSOCIATES



Risk-Based Decision Making Commentary
August 2012 Newsletter #2

Hackers Do Target Small Businesses

Small businesses are more at risk from identity theft than large companies. Large businesses can afford to hire IT professionals that focus solely on security while small businesses don't even know what vulnerabilities exist. While many small businesses think that their small size means that they are not on a Hacker's radar screen, the existence of holes in their systems is exactly what is attracting the criminals. Hackers use automated tools to search the internet and look for vulnerable sites and computers.

The main defense against this is making sure that your computer systems are safe and secure. Make sure that the software is updated and all patches are installed properly, have policies in place so that employees don't visit dubious web sites, click on e-mail links or inadvertently share information with the wrong person. Have strong passwords on all systems and make sure all your data is encrypted. Encryption is the simplest and most powerful security measure.

If you are infiltrated or breached, and personal customer data falls into the wrong hands, how you respond makes a world of difference. You should notify law enforcement about the breach immediately and notify customers/other businesses that are impacted to give them the chance to reduce potential misuse of their information.

This early notification demonstrates that you are taking the incident seriously and potentially could reduce your responsibility for future uses of the data. When notifying customers, it is necessary to look at the type of compromise, the information stolen, the chances of the information being misused and the potential damage.

HALL ASSOCIATES

Bogus Vendor Bills Bucket

Billing schemes come in all different shapes and sizes but small businesses are a primary target. Unlike larger businesses, small businesses rarely have segregation of duties and limited internal controls, making them more vulnerable to scammers. Small businesses rarely mandate payment compliance rules that employees have to abide by.

The current average cost of fraud for small businesses is $155,000 (2010). And once you have been the target of one scam artist, your information is shared with others on a list of easy prey. To protect yourself you first must know what to look for.

One popular scam is the phony grant scheme. A small business will get a call from a so-called grant writing service that promises government grants. However, first you must pay a processing fee of $3000 to $5000 and the grant company will get you into the waiting list. The “grant company” then disappears.

Another scam is the compliance scan. This scam targets SBs that are incorporated. They get an official looking letter stating that they are not in compliance with annual filing minutes and require a processing fee. Many simply assume that this is official and pay the fee.

In another scam, someone will offer you free samples of printing toner and send you the product even if you say no. Before long, you will be hit with a grossly overstated bill and the company won’t accept returns.

In another scam, a business will get a call supposedly from their phone company telling you that they want to check the line and to press 90#. Once that happens, the scam artist can place long distance phone calls and bill them to your business.

In another scam, someone will collect enough information about a business to make a phony bill look legitimate. The fake bills will be small enough not to raise a red flag and may even include past due of final notice notes to pressure the SB to pay quickly. When it comes to paying bills, be sure to read the fine print and never accept free products over the phone.

Be sure to educate all employees about the different scams so that they know what to look for. You need to know who you pay money to and need to follow the rules.