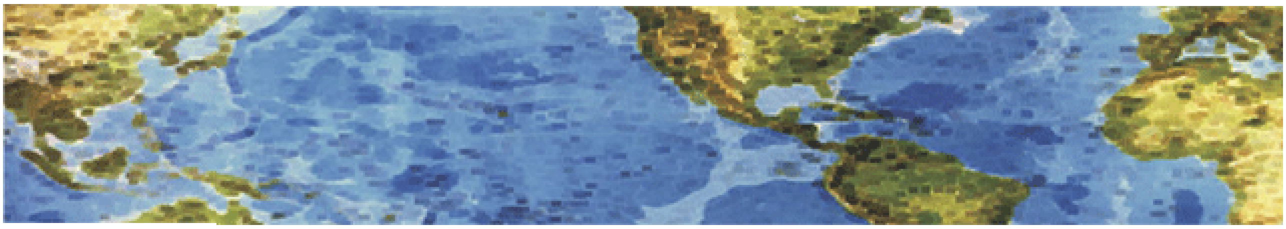
# HALL ASSOCIATES



# Risk-Based Decision Making Commentary
# 12 May 2013 Newsletter

## 7 Ways to Protect Your Small Business (or any business) from Fraud and Cybercrime

How secure are your small business assets from fraud, identity theft and cybercrime?
According to the Association of Certified Fraud Examiners (ACFE), **companies with less than 100 employees lose approximately $155,000 as a result of fraud each year.** Small businesses also have a higher fraud rate than larger companies and non-business owners. One of the most frequent sources of fraud is credit card abuse – largely due to the fact that few business owners actually take the time to go through every line item on their bill or choose to mingle business and personal accounts. Other sources of fraud stem from an overall lack of security across the business – such as inadequate network and computer security and a lack of background checks when hiring employees.
Don't be a victim! Here are some tips you can take to better protect your business from some common forms of fraud and cybercrime.

### Protect Your Credit Cards and Bank Accounts

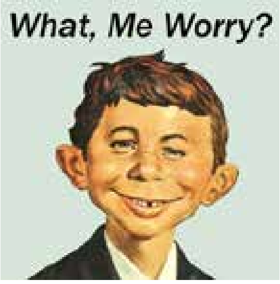
Since this is a common area of fraud for everyone from sole proprietors to employee-based firms, this one goes at the top of the list. Start by separating your personal banking and credit cards from your business accounts – this will ensure fraudsters don't get their hands on ALL your money. Separating your accounts will also make it easier to track your business expenses and report deductions on your tax return. Be sure to check your online banking every day for suspicious activity.

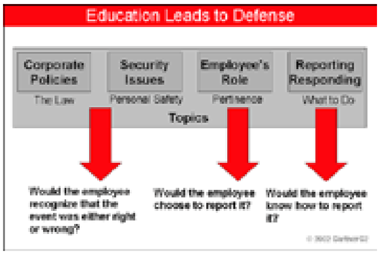
### Secure Your IT Infrastructure

Every business owner should invest in a firewall as well as anti-virus, malware and spyware detection software. Backing-up is also a must and will make it a lot easier for you to continue working in the event of a cyber attack.

### Use a Dedicated Computer for Banking

Use a dedicated computer for all your online financial transactions and, ideally, make sure it's one that isn't used for other online activity such as social media, email and web-surfing which can open up the machine to vulnerabilities. Avoid mobile banking if you can.





Education Leads to Defense

Corporate Policies — The Law
Security Issues — Personal Safety
Employee's Role — Pertinence
Reporting Responding — What to Do

Topics

Would the employee recognize that the event was either right or wrong?

Would the employee choose to report it?

Would the employee know how to report it?

## Have a Password Policy

Another easy step you can take to protect your IT systems is to institute a password policy.
Make sure you and your employees change them regularly (every 60 to 90 days is good rule)
Set rules that ensure passwords are complex (i.e. contain one upper case letter, one number and must be a minimum of eight characters). Use different passwords for different online and system accounts.

## Educate Your Staff

**Employees are perhaps your biggest point of vulnerability when it comes to fraud**, but they are also your first line of defense. **Hold regular training sessions on basic security threats** (online and off) and prevention measures – both for new hires and seasoned staff. Enforce the training by instituting policies that guide employees on the proper use and handling of company confidential information, including financial data, personnel and customer information.
For ideas on what to include in your training, check out the resources offered by small business groups like your local Small Business Development Center or Women's Business Center (find one near you here), you could also look out for free online webinars from security organizations and businesses.

## Consider Employee Background Checks

One of the first steps to preventing fraudulent employee behavior is to make the right hiring decision. Basic pre-employment background checks are a good business practice for any employer, especially for those employees who will be handling cash, high-value merchandise, or have access to sensitive customer or financial data. This blog offers tips on which background checks you can legally pursue and some tips for doing your own detective work: Conducting Employee Background Checks – Why Do It and What the Law Allows.

## Insure Your Business

Fraud and cybercrime does happen; however, you can still seek to cover your damages by purchasing an insurance policy that protects you against any losses that you may incur from crime or fraud. Remember, your normal Errors and Omissions and Liability insurance DOES NOT cover cybercrimes, breaches and identity theft. You need special cyber insurance for that. Likewise, find out what your bank is willing to do to help you out if your credit card or business account is compromised.

**http://www.sba.gov/community/blogs/7-ways-protect-your-small-business-fraud-and-cybercrime**