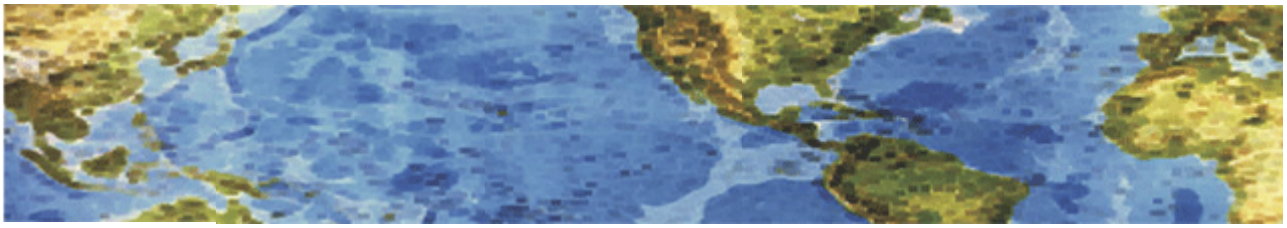
HALL ASSOCIATES



Risk-Based Decision Making Commentary
July 2012 Newsletter

Why Should Small Businesses Use Risk Management?

Risk is a part of being in business. Risks can be managed and bad outcomes can be controlled in large part. The greatest challenge for small businesses is to find the proper balance between peace of mind and profitability. Trying to eliminate (or ignore) risk from your business is unrealistic and can be prohibitively expensive or cause you to be so risk averse that your business never grows. And the risk environment you face as a small business is constantly changing.

What is the main challenge? For most businesses it is to determine what risks pertain to them and to use a repeatable, effective and minimal cost process to identify, assess, control and monitor risk without interrupting their business activities. This series of newsletters will discuss what can affect you and how you should respond to protect your business, your employees and yourself. If you have any questions or comments, let me know at halld105048@yahoo.com.

One major example of a rapidly changing risk environment is that of Information Technology and Cyberspace use. Your business increasingly works with and through the Internet and IT systems, making the risks inherent in IT systems and cyberspace far more visible and significant than ever. There are more and different threats "in the wild" every few months, making use of the Internet and cyberspace increasingly more problematic. It's not a case of **IF**, but **WHEN** you will be troubled by one or more of these threats. IT and cyberspace risks, when they occur, can cause business losses - lost revenue, lost customers, lost reputation, lost personnel effectiveness, lost productivity. And if you don't know what risks you face in your business, you will not be prepared for them.

So what is an IT or cyberspace risk? Basically they are any threat to your information, data, critical systems and business processes. Why should you be concerned about them? Because anyone in a business, especially management, has a responsibility to identify areas of risk and respond in a timely fashion by improving processes, augmenting controls and requiring testing to ensure that the business is properly identifying and responding to risks. Failure to identify, assess, control and monitor risk sets the business up for serious problems and significant financial losses now and in the not-so-distant future.

HALL ASSOCIATES

Latest Cyberspace Recommendations

We had a question at my last presentation about "Is PayPal safe to use?". PayPal is as secure as any other online credit account, but no such account is entirely safe, especially from the user side. Following are some recommendations I have found that should enable you to minimize (not eliminate) potential risks when using such sites. Note, however, that these are only recommendations and you should determine exactly what you need to do depending on your specific circumstances.

1. Don't link your PayPal account to your bank account or debit card account. If your PayPal account is compromised, it's money taken directly out of your bank account and by federal law (Regulation E) you only have two days to refute a fraudulent charge with your bank. . But if you link your PayPal account to your credit card and it's compromised, then you have 60 days to refute those charges with your credit card company. However, I did find a note that stated "A spokeswoman for Access Communications, acting as PayPal's representative, has said that PayPal's protection from unauthorized transactions gives the user 60 days to dispute the charges, no matter what the funding source".
2. Don't click on links in the body of emails from PayPal. Those emails might not really be from PayPal. Rather, they may be phishing e-mails from scammers designed to get you to enter your credentials. Instead, manually type in the PayPal address into your browser, log in to your account and see if there are any communications for you from PayPal. Remember, **NO** organization, be it PayPal, a credit card system, a bank, a commercial firm or the Federal Government, will **EVER** ask for your account information or personal information via e-mail.
3. Keep your PC, Cell Phone, I-Pad, etc. security up-to-date. Make sure you have installed the latest critical security patches to your operating system, as well as the latest browser patches and have updated antivirus/internet security software. If whatever you use to connect to a site is compromised with spyware or malicious software when you're using a financial site like PayPal, then others have access to your computer, phone, I-Pad, etc. and can access your user names and passwords. And that is not PayPal's fault.
4. Never log in to PayPal from a public PC or someone else's computer, phone or I-Pad. Each of these is only as secure as the person who logged in before you. Someone could easily have installed spyware or malicious software that will log all your keystrokes.
5. Maintain good records for all Internet commerce. It's a good idea to download and print final pages so that you have backups for purchases made and products bought and sold.
6. Treat your PayPal account like you treat your online banking account. You need to ensure that you have authorized any transactions, large or small. Typically, someone will start draining your account using a series of small withdrawals, hoping you won't notice. So you need to refute those charges as soon as possible and let PayPal know that your account may have been compromised.