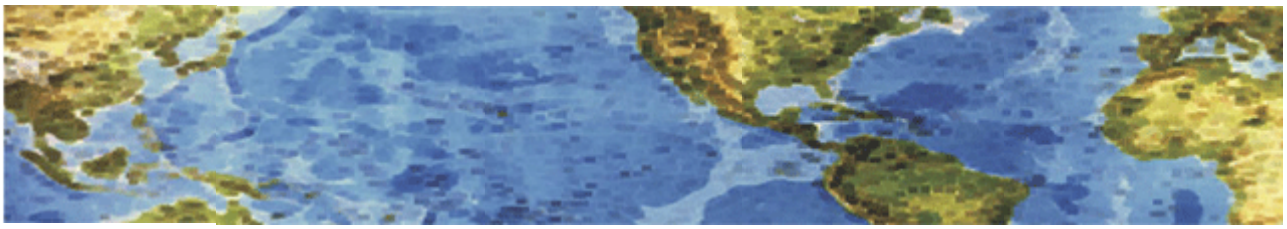
HALL ASSOCIATES



Risk-Based Decision Making Commentary
September 2012 Newsletter #1

New Media – Old Risks, Risks of Using Social Media

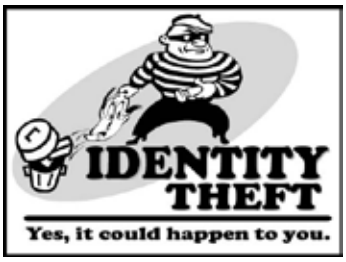
Social media is now a mainstream form of communication. You might not yet be using social media for your business, but some if not all of your employees are probably actively engaged on their own accounts. And your customers and prospects may well be posting about your products/services/ customer relations out there in the Cyberworld. With social media, everything gets around the entire world with the click of a mouse. That should be reason enough to address social media as part of your business risk management framework and establish social media policies.

A few social media risks a business should consider when developing a social media policy:

1. Negative comments posted by an employee (not during work hours) triggering claims of harassment by other employees.
2. Excessive use of social media during work hours, reducing productivity or affecting customer relations.
3. A disgruntled client/customer (or a cyber extortionist) posting negative comments across social media sites.
4. An employee posting confidential information (or Privacy act or HIPPA information) to a social media site either deliberately or inadvertently.
5. Giving in to the temptation to game the system by posting self-generated reviews and testimonials either anonymously or under false names in social media (prohibited by law in the US and most other countries).
6. Not using content created by others properly in promoting your business.
7. Not using “entirely” truthful descriptions when describing your products and services.
8. Blurring the line between business and personal social media communications.
9. Providing information that may be mistaken or is somehow misleading.

Using social media for business promotional purposes can be very beneficial, but can also lead to legal liabilities if a systematic approach is not applied. Social media is now very important and can be very useful to a business, but a healthy respect for the associated risks needs to be cultivated. The risks can lead to catastrophic problems if they are not managed proactively. Most of the social media risks can be handled by policies, but all policies (especially those pertaining to cyber) need to be supplemented with training of all employees. Most people cause problems accidentally because they don’t know any better.

HALL ASSOCIATES



College Student Identity Theft

Millions of Americans have their identities stolen each year as cybercriminals scour the internet for easy victims. College students are not immune. They make up about 25% of all identity theft victims according to the Better Business Bureau. College students need a strong understanding of how to protect their personal information and defend against identity theft. Following are ten recommendations to help college students defend against identity theft (it's impossible to totally protect against identity theft and everyone's situation is different):

1. Always check your bank statements and bills carefully – develop good habits and scrutinize each statement and bill for unexplained or unexpected withdrawals or charges.
2. Sign up for electronic statements – most college students don't shred paper documents with personal information on them, they just toss them out in the trash.
3. Monitor your credit rating – Cybercriminals really don't care about the $100 in your bank account, they are after SSN and credit histories that will allow them to open new accounts, take out loans or get new IDs.
4. Don't use unsecured Wi-Fi networks, computers or websites – Students regularly use unsecured wireless networks and public computers scattered around campus. When doing this, they should remember that anything being typed can be read by someone else. Don't log into a bank site or any site that requires a user name and password.
5. Use only secure connections when submitting important information – Always look for the https:// and the lock image on the website before submitting sensitive information and login credentials.
6. Don't let your personal computer or tablet or smartphone become a communal machine - Lock up your devices when not using them so that other people can't use them and NEVER let anyone use your device when you are logged in.
7. Use passwords and encryption – Always protect your devices with passwords (strong passwords!) and encrypt the data to prevent anyone else getting your data even if the device is lost or stolen.
8. NEVER share passwords – not even with roommates or your new (or old) BFF living down the hall.
9. Don't put too much information on social media sites – Don't fill out all the available fields on a social networking site and don't input personal information that could be used to establish an identity, set a password or used for a security question.
10. Bottom line – Don't trust anyone completely. Students are very trusting, but don't share passwords and PINS with friends and don't let someone look over your shoulder if you are entering passwords or PINs on a computer, phone or ATM. Secure your sensitive papers rather than leave them on your desk.