CAL INSURANCE & ASSOCIATES, INC.

Computers are integral to most of our businesses. While this allows us to do business more efficiently it also comes with unique risk. Hackers, worms, and employee sabotage can literally shut down our businesses. We also have liabilities for private information getting out. This information includes social security numbers, credit card numbers, driver's license information and medical records that get released to the public.

Most all businesses rely heavily on computers. Most business now work solely by computers. Ask yourself these questions.

- Do you have a firewall?
- Do you require your information technology department or outsourced third party vendors/providers to adhere to software update process, including software patches and anti-virus software definition upgrades?
- Do you have a virus protection program that is used on internet-facing and internal mail servers, desktops and other mission critical servers?
- Do you restrict employee access to specific customer files, designated computers, or Personal Identifiable Information (PII) of employees to those with a business need-to-know basis?
- Are all employees periodically instructed or trained on their specific job responsibilities with respect to information security, such as the proper reporting of suspected security incidents?
- Do you have a process to review content or materials before they are published, broadcasted, distributed, or displayed on your website for defamation, right to privacy and copyright issues?
- Are the servers that hold sensitive data in a locked room? Are PCs that have sensitive data bolted or locked down physically?
- When you send sensitive data on the internet, is it encrypted?
- Do you have a written Security Plan and is there one person in your company responsible for implementing and updating the plan?
- Do you change your passwords and delete your web browsing history on a regular basis? Make sure your password is unique and delete your "cookies" often. These are the cyber footprints you leave behind on your computer that can track your previous computer usage. Consult your manual or IT person for more information.
- Does the company have a social media policy that prohibits unauthorized employees from posting on the company's Facebook page? Twitter account, etc? Many companies have Facebook pages, so stipulating who is authorized to post is essential.

Each company is different and these questions are meant to be a starting point. Please give me a call or an email if you have any questions.

Scott Hauge
President
CAL Insurance and Associates, Inc.
2311 Taraval Street
San Francisco, CA 94116
www.cal-insure.com
Phone: (415) 680-2109
Fax: (415) 680-2137