jmb INSURANCE

Cyber Exposure Notice

During the past several months, “cyber” breaches have become front page news. Major national retailers including Target and Neiman Marcus have been victimized by computer hackers. The view among many technology industry leaders is that these attacks will continue, the results being significant additional expense and big headaches!

This is not only a large company problem. Medium and small businesses are considered easy targets. A cyber criminal is less concerned about the size of the target than the ease of a target. Further, a company is also at risk when sensitive data is outsourced to a third-party. Processing transactions and payments and cloud servers may seem removed, but often the liability remains with the company. A 2012 DHS Cyber Security Report shows that third party service providers, such as cloud computing hosts, are responsible for approximately one-third of cyber incidents.

As someone with responsibility for managing your company’s risk, we want to assist you in ascertaining your cyber exposure. Following is a brief checklist to determine cyber exposure. Please take a minute to respond to the questions with a Yes or No answer:

1.	Does your business accept credit cards?	Yes	No
2.	Do your employees use mobile devices or laptops for work?	Yes	No
3.	Does your business engage in ecommerce?	Yes	No
4.	Have you evaluated and vetted the security infrastructure of your vendors?	Yes	No
5.	Have you reviewed the vulnerabilities of your company’s IT infrastructure?	Yes	No
6.	Does your business have procedures in place to prevent a rogue employee from causing harm?	Yes	No
7.	Does your company collect and maintain human resources data?	Yes	No
8.	Are you in an industry that collects a large amount of personally identifiable information which is subject to any form of regulation?	Yes	No

If you answered yes to any of these questions, our view is that you have Cyber exposure and your business could be at risk.

Now that you have a sense of your risk, what do you do? We have compiled recommended actions for you to take:

1. Password Protection - Company devices, including mobile and laptops, and files should be encrypted and password protected;

2. Privacy Policy - Implementation of an attorney-approved Privacy Policy for employees and vendors to sign;

3. Mobile Device Policy - Mobile device access and distribution should be on an as-needed basis. Companies should have processes to perform remote wipes of device content. Encryption, password protection and employee education should be mandatory;

4. Data Analysis - It is important to identify and protect critical information that could have the greatest impact on your company's financial well-being. It is advisable to do an internal analysis of how many records your company stores, where they are being stored, who has access, as well as their contents and importance;

5. Employee Transitioning Security Procedures - For employees that have transitioned, a standardized policy should be in place to rapidly eliminate company access;

6. Third Party Contract Review - Properly evaluate vendors to understand how secure your critical information is on their network and servers. It's best to review the contracts with your vendors and customers to ensure that your company doesn't assume unnecessary liability;

7. Security Leader - Every business should appoint an individual to be responsible for network security. Their responsibilities should include implementation of company procedures while also holding employees accountable for violating security policies.

8. Risk Transfer: Consider the advantages of transferring their risks through insurance. This coverage is commonly referred to as cyber liability and is designed to cover the costs for defense, notification, credit monitoring, regulatory fines and penalties, forensics, public relations, business interruption, cyber extortion, and network damage. It also **provides reimbursement for the costs associated with a compromise of personally identifiable information (PII). PII includes financial data, social security numbers, medical records, driver's license numbers, e-mail addresses, mailing addresses and the like.**

It is our sincere hope that you never face a cyber attack or a data breach. Unfortunately the risk is greater than any of us would like. Our goal is to offer you some insight on this growing issue, actions to take, and risk mitigation for better results. JMBI's expertise in this area has grown out of our clients' necessity. Let's talk if you would like to learn more.