

Presented:

37th Annual Corporate Counsel Institute

April 16-17, 2015
Houston, Texas

May 7-8, 2015
Dallas/Addison, Texas

An Insurance and Risk Management Primer for Corporations

**Tracy H. Bowden
Sandra Cockran Liser**

Author contact information:
Sandra Liser, Partner
Naman Howell Smith & Lee, PLLC
Fort Worth Club Building
306 W. 7th Street, Suite 405
Fort Worth, TX 76102-4911
sliser@namanhowell.com
817-509-2035

INSURANCE AND RISK MANAGEMENT – A PRIMER FOR CORPORATE COUNSEL

Sandra Liser - Naman Howell Smith & Lee

March 24, 2015

As the general counsel or in-house counsel for a company, you are likely asked questions on a variety of topics every single day. You are not afforded the luxury of specializing, but instead must be a “jack of all trades” in order to represent your employer and client. Some of the most significant questions you will face in every company come annually at the time to renew your insurance policies:

“What insurance policies do we need to buy and which ones can we forego?”

“How can we save money on our insurance premiums?”

“A claim is being made against our company – does our insurance cover that?”

We have divided this paper into three major sections. First, we will identify the major types of insurance all companies should consider purchasing, depending upon their business. Second, we will identify several types of losses or claims your company may face and whether you want or should purchase insurance to cover those losses or if those losses are covered by the policies you have already purchased. Lastly, we will address how you and your company can analyze your risk tolerance and how you can minimize your risk and reduce your dependency on insurance.

I. Significant Insurance Coverages All Companies Should Have or Consider

A. Cyber Policies:¹

With the increase in the amount of information that is stored digitally, it has become vitally important for companies to find a way to protect their businesses when a cyber attack occurs. There are many areas where a company is vulnerable (hardware, software, human error,

¹ The cyber policies portion of the paper is inspired by an article appearing in the Winter 2015 edition of the Journal of Texas Insurance Law titled, “Anatomy of a Data Breach—What Cyber Policies Should Cover” by Jes Alexander, deputy general counsel at Dickey’s Barbecue Restaurants, Inc.

etc.) and an attacker need only find one to infiltrate a company's computer system and wreak havoc.

Cyber attacks include such dreaded activities as blackmailing a small business by holding its computer system hostage, posting employees' confidential information online, stealing payment information, and espionage. As sophisticated as some security systems may be, it is merely a matter of time before a hacker or digital pirate finds a way to infiltrate the system. We have seen this occur with Target, Sony, Michaels, Neiman Marcus, T.J. Maxx, The Home Depot, Staples, P.F. Chang's, and Jimmy John's.

We may not be able to prevent the news headline saying, "(Insert Your Company Name) is the Latest Victim of Data Breach," but there are steps that every company can and should take to protect their interests if such an attack happens. The first, most important, thing that a company should do is make sure they have coverage for any losses associated with a cyber attack by having a carefully structured cyber liability policy.

Very little coverage exists for liabilities resulting from data breaches under a standard commercial general liability policy ("CGL"). Many CGL policies are beginning to include new cyber exclusion ISO endorsements approved by regulators that leave little room for doubt that most data breach claims are not covered. A company that relies solely upon CGL or other general policies does so at its own risk. Such risks include having no coverage for the business interruption that results from a breach, the lawsuits from customers and employees whose confidential information is leaked, the cost of paying an attacker who is holding a company's computer system hostage for ransom, and the cost of complying with government regulations after a breach.

Unfortunately, no standard policy form exists yet for cyber insurance because the market is still relatively new. The risks that are covered under cyber liability policies vary depending on the insurers. Thus, a company must analyze their individual risks areas and acquire a cyber policy to cover those risks. Attention to detail is key.

Consider the recent security breach of Sony Pictures Entertainment ("Sony") when Sony was the victim of cyber attack for its decision to make a movie involving the assassination of the