



ThinkFriday is a weekly posting, every Friday afternoon, of items of interest to the media, technology and network security insurance community. Some weeks, *ThinkFriday* might contain a summary of an interesting (or frightening) new claims example; other weeks, a discussion of an obscure coverage issue; others, it might simply be a rant on some esoteric insurance issue that we think might be useful or entertaining. If you would like to subscribe to *ThinkFriday* and have these weekly items emailed directly to your Inbox, please visit <http://www.ThinkRisk.com> to subscribe.

Even the SEC Sees the Value of Data Security Insurance

February 3, 2012 – It is often the seemingly small references in relatively obscure regulations that end up having a huge impact on the insurance industry. Just look at the recent flurry of activity surrounding The Beverly-Song Act and collection of ZIP codes from credit card holders, as reported in our [ThinkFriday](#) piece in July of last year. It appears we have found just such a reference in a recent cyber security disclosure guidance issued by the Corporate Finance Division of the SEC (the "Guidance"). The Guidance, quietly issued in October of 2011, indicates that publicly traded companies are required to disclose cyber security risks and cyber incidents when those risks and incidents would be considered important to a reasonable investor's investment decision. As you might imagine, that is almost always the case. (Follow this [link](#) for the full text of the Guidance.)

The Guidance could almost serve as a marketing piece for data security insurance. It cites the recent increase in cyber attacks as the catalyst for heightened attention to cyber security and goes on to list the substantial costs and other negative consequences that could result from such attacks. These include remediation costs, lost revenues, litigation and reputational damage, all the costs potentially covered, in part or full, by a good data security insurance policy. The Guidance then discusses the risk factors that a company may be required to disclose in its filings. These risk factors are exactly what an experienced cyber underwriter would use to assess a cyber risk, including the following:

- a description of the company's operations that give rise to cyber security risks and the potential costs and consequences of an attack on those operations;

- the nature of security measures in place to protect against cyber attacks;
- any outsourced functions that have a cyber security risk and how the company has addressed those risks;
- a description of any cyber incidents experienced by the company, the costs and consequences thereof; and (drum roll please)
- **a description of relevant insurance coverage.**

As you can see, the SEC has saved the best for last, but at least they did not ignore this very important aspect of cyber security. By placing an insurance component in the company's required disclosure of risk factors, the SEC has implied that relevant insurance coverage is an integral part of a business's data security. This reference also gives agents and brokers an invaluable tool when advising applicant's on the need for data security insurance. Namely, companies that must disclose that they have no relevant insurance coverage may be viewed as riskier investments and may be asking for D&O claims should a data breach occur. In fact, it may be prudent, when presenting a quote for data security insurance to a publicly traded company, to include a copy of the SEC's cyber security disclosure guidance, appropriately highlighted, so that this obscure but important requirement is taken into consideration when determining the need for such insurance.