

By Donald Glazier

Over the last several years, the financial and healthcare industries have faced increasing exposure to privacy and data security breaches – both intentional and negligent. These exposures have also spurred increased governmental scrutiny and regulation to protect customers' and patients' sensitive financial and medical information. Now, the SEC, through a new set of corporate finance disclosure guidelines, requires all public companies, regardless of industry segment, to provide their investors with information on how they're dealing with cyber security.

Background

After last spring's huge computer hack involving Sony Corporation underlined the ever-increasing threats of cyber risks, the chairman of the Senate Commerce Committee sent a letter to the head of the SEC expressing the committee's concerns about the level of disclosure relating to data security risks. He wrote:

"Cyber risk management is a critical corporate responsibility. Federal securities law requires publicly traded companies to disclose "material" risks and events, including cyber risks and network breaches. A review of past disclosures suggests that a significant number of companies are failing to meet these requirements. The SEC has longstanding authority to publish "interpretive guidance" to clarify corporate responsibilities, protect investors, and promote fair and efficient markets."

The SEC's initial response in early summer was somewhat cool to the idea of increasing disclosure obligations for public companies, specifically in the area of data security. However, the new guidelines clearly show that the SEC has come around on this issue. Cybersecurity is not a onetime disclosure obligation anymore; it is now a standard SEC reporting requirement. The guidelines note that "as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents."

Also significant, the guidelines note that "material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the circumstances under which they are made, not misleading." The SEC included that language to remind companies that failing to adequately report cybersecurity issues could expose them and their directors and officers to liability under the antifraud provisions of federal securities laws, including Rule 10b-5. There is no doubt that if a reporting company should suffer a cyber breach that causes a financial loss, then a shareholder's attorney will look closely at the adequacy of disclosures in this area when assessing whether to pursue litigation.

Cyber Risk Exposure Guidelines

The SEC's guidelines provide cyber risk specific suggestions for disclosures to be used in a number of the sections contained in SEC form 10-K. The guidelines offer noteworthy suggestions for the 10-K, Risk Factors, and Management's Discussion & Analysis sections.

Risk Factors

In a filer's Risk Factor section, the SEC underscores that the "cybersecurity risk disclosure provided must adequately describe the nature of the material risks and specify how each risk affects the registrant." They go on to describe some areas of important disclosure:

- Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions, and how the registrant addresses those risks;
- Description of cyber-incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage.

MD&A

In the Management's Discussion and Analysis section, the guidelines require disclosure of cybersecurity risks if the costs or other consequences represent a material event or uncertainty that is reasonably likely to have a material effect on the registrant's results, liquidity, or financial results. The broad nature of the required disclosures coupled with those required in the Risk Factors section make those two sections areas of focus for potential claimants in the event of a financially serious cyber-breach or other incident.

Financial Statement Disclosures

In addition to the disclosures noted, the guidelines also require filing companies to provide information regarding the impact of cyber risks on their financial statements. This includes:

- Any substantial costs incurred to prevent cyber incidents.

- Losses from claims, stemming from a cyber-incident, for indemnification, breach of contract or warranties.
- Diminished cash flow and its impairment on tangible and intangible assets. In this area in particular, the SEC notes the challenge in adequately estimating the impact of the incident, but requires the registrant to provide subsequent reassessments of the assumptions underlying estimates and presumably change them in subsequent filings.

Insurance

As noted in the SEC's guidelines concerning Risk Factor disclosures, a registrant's appropriate disclosures might include a description of relevant insurance. In this regard, one area of insurance that may be particularly relevant is what has become known as cyber or data security and privacy insurance coverage.

Cyber insurance has developed parallel to the growing risks in connection with data security and privacy protection. A number of these risks, spelled out below from the SEC guidelines, are covered by cyber insurance. The policies often contains a blend of both 1st and 3rd party insurance coverages designed to protect against the various exposures arising from a data breach or other privacy situation.

The SEC identifies a number of substantial costs and other negative consequences associated with cyber attacks, including:

- Remediation costs that may include liability for stolen assets or information and repairing system damage that may have been caused.
- Increased cybersecurity protection costs that may include organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
- Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation;
- Reputational damage adversely affecting customer or investor confidence.

The insurance marketplace offers coverage for some of the risks noted by the SEC including cyber loss related business interruption, lawsuits by customers--individually or as a class, as well as governmental claims. Also, cyber insurance can pay for some parts of remediation costs in repairing computer systems. In addition, cyber-coverage will address the costs associated with notifying and providing credit monitoring to those parties affected by cyber breaches.

The insurance industry has developed and continues to develop risk tools to deal with this constantly changing risk. The SEC guidelines are only the most recent of

these developments. To assist in assessing the options available to deal with these risks, Integro offers a depth of expertise to help identify and mitigate these risks.

Donald Glazier, Esq. is a Principal with Integro's Management Risk Practice located in its Chicago Office. An attorney by background, he specializes in D&O and related professional liability issues. You can reach Don at (312) 780-8710 or Donald.Glazier@integrogrou.com

About Integro

Integro is an insurance brokerage and risk management firm dedicated to serving the insurance and risk management needs of complex institutional risks. Integro has offices across North America, as well as in Bermuda and London. Its headquarter office is located at 1State Street Plaza, 9th Floor, New York, NY 10004. 1-877-688-8701. www.integrogrou.com.

© Integro USA Inc. 2011