Recent SEC Guidance on Cybersecurity Disclosure Obligations

Considering Potential Environmental Impacts and Insurance Coverage Issues

This article first appeared in *Bloomberg Law Reports,* January 3, 2012.

by Vincent E. Morgan and Kathryn D. Pavlovsky

Vince Morgan
Insurance Recovery & Advisory
+1.713.276.7625
vince.morgan@pillsburylaw.com

Vince Morgan is a Partner at Pillsbury Winthrop Shaw Pittman LLP where he focuses on assisting corporate policyholders with insurance issues, beginning with legal advice concerning the placement of coverage as well as involvement in the claims process and, if necessary, litigation and arbitration against insurers when coverage disputes arise. He also advises clients on risk management issues from a legal standpoint.

Kathryn D. Pavlovsky
Deloitte Financial Advisory Services LLP
+1.713.982.4358
kpavlovsky@deloitte.com

Katie Pavlovsky is a Principal at Deloitte Financial Advisory Services LLP where she leads the Environmental and Sustainability Consulting Services practice. In this role, she focuses on environmental risk management where she conducts risk, exposure and damages assessments, leads analyses for environmental litigation and insurance disputes, conducts investigations of environmental claims, and analyzes environmental liabilities for financial reporting and transactions purposes.

Deloitte.

In response to stakeholder petitions and Congressional requests seeking improvements in corporate risk disclosures, the Securities and Exchange Commission (SEC) has been active in issuing guidance to enhance disclosure obligations. The SEC has entered into new areas with the issuance of its Climate Change Disclosure Guidance in 2010[1] and the more recent proposals drafted in conjunction with the Dodd-Frank Act[2] that would require disclosure of certain health and safety compliance violations. Inadequate disclosures of environmental, health, and safety and "sustainability" risks have been used as examples by investors in complaints to the SEC as they are perceived to be a tangible reflection of company management; mis-management results in direct impact not only to investors but also to the public at large. Specifically, the SEC Climate Change Disclosure Guidance was followed by formal petitions to the SEC during the period of 2007 to 2009 to clarify the climate change disclosure requirements of public companies submitted by state attorneys general, institutional investors, and environmental groups.

Cybersecurity events have similar exposure, visibility, and reach. In addition, some of these events have either resulted from or have themselves caused environmental issues. The SEC's Division of Corporate Finance (Division) recently issued guidance that responds to concerns regarding how organizations are getting ahead of the evolving technology and these threats.[3] The guidance draws upon existing disclosure obligations for support.[4] Accordingly, this latest development is a continuation of the recent evolution of disclosure requirements designed to encourage companies to address their vulnerability and readiness to respond to business risks that are increasingly difficult to anticipate and manage given trends in globalization, technological innovation, and stakeholder expectations for performance.

High-profile data breach events have hastened stakeholder focus on the ways in which sensitive data is housed and whether management is taking a holistic and comprehensive approach to protecting the data. The magnitude and impact of these breaches have intensified, garnering media attention globally and highlighting gaps in international policy, protocols and legal frameworks for sharing information, collaborating on incident response, or pursuing illicit actors across borders. This is compounded by a rapidly evolving cyber-environment that consists of new technologies, networks, smart devices, and cloud computing which do not yet have worldwide standards for security.

Cybersecurity risk is typically associated with misappropriation of personal information and in certain instances data corruption. However, as evidenced by recent events, the effects of cyber incidents may be far broader in scope and impact including issues such as misappropriation of assets, operational disruption, and financial exposures associated with lost revenues or the onset of new litigation. Organizational leaders are challenged to anticipate, prevent, manage, and address the threats and potential implications given the range of exposures that have been caused by both internal and external actors, ranging from cyber accidents to cyber attacks.

The guidance directs registrants to undertake an ongoing review of the adequacy of their disclosures related to cybersecurity risks and incidents by addressing potential disclosure issues in the context of a company's management discussion and analysis (MD&A), business description, legal proceedings, financial reporting, and disclosure controls and procedures.

This article addresses three topics. We begin with a brief discussion of the recent guidance. Next, we offer recommendations to companies on how to incorporate this guidance into their disclosure controls and procedures by exploring examples of cybersecurity risks through the lens of potential environmental incidents. Finally, we use that framework to analyze the implications of the Division's reference to insurance as an appropriate subject of disclosure concerning cybersecurity risks.

Summary of the Recent Guidance

The Division articulated its rationale for issuing the guidance by noting that federal securities laws are at least partially designed to elicit disclosure of timely, comprehensive and accurate information about matters that a reasonable investor would consider important to an investment decision. It noted that no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, but other disclosure requirements may impose an obligation to disclose such matters, either directly or to avoid making other required disclosures misleading. Therefore, 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.[5]

Similar to other recent SEC issuances, the guidance is high level and provides reference to existing rules. However, it contains specific guidance related to controls and companies should consider whether cyber incidents create or reveal deficiencies that would impair the ability to accurately record, process, summarize or report information that is required to be disclosed.[6]

In determining whether disclosure is warranted, the guidance suggests companies consider the following risk factors including but not limited to:

- prior cyber incidents and the severity and frequency of those incidents;
- the probability of cyber incidents occurring;
- threatened attacks of which they are aware;
- the quantitative and qualitative magnitude of those risks, including potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption; and
- the adequacy of preventative actions taken to reduce cyber-related risks in the context of the industry in which they operate and risks to that security.[7]

Finally, where risk factors suggest that disclosure is appropriate, the guidance suggests the following subjects to consider regarding content of the 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 it 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.[8]

A company need not, however, reveal so much detail that the disclosure itself creates an increased vulnerability.

Recommended Steps for Incorporating the Guidance

The recent issuance of the SEC's guidance provides registrants with an opportunity to review the adequacy of their controls in terms of identifying, measuring, reporting, and disclosing cybersecurity risks. Companies should consider the SEC's new guidance and their disclosures to shareholders as they prepare their filings, particularly if they have been impacted by prior cyber events that have ongoing consequences or a likely potential for future consequences.

Leading companies are taking a renewed focus on what this changing paradigm means for their organizational policies, processes and systems that require collaboration across departments to protect their people, programs and mission. To do this, they are asking key questions in order to evaluate:

- How the organization is thinking about and managing risks;
- The adequacy of risk intelligence frameworks;
- Crisis management capabilities;
- Unintended consequences of business priorities, such as the effect cost reduction initiatives might have on cybersecurity capabilities.

Companies can learn from past events where the control and risk management environments for cybersecurity have failed. Lessons from those events include:

- The importance of a robust governance infrastructure that may consist of:
  - Roles, responsibilities, and expertise in Finance, Accounting, Legal, Risk Management, and Operations to support the evaluation of the risks that may be further supported by subject-matter specialists as needed.
  - A framework that is clear with respect to the risk management objectives and implementation expectations.
  - Data protection systems, identity verification, and access management frameworks.
  - Predictive tools and forensic analytic procedures to support threat intelligence, to assess vulnerability to asset exploitation, and to determine whether a breach has occurred or is at risk of occurring.
- Establishing a risk-based strategy for understanding and managing the environment along with potential threats, which includes treating data as a target. A 360 degree view of organizational risks can help all functions make better decisions, set priorities, manage investments, and achieve more favorable results. Such information should be considered in conjunction with the manner in which it may be accessed, destroyed, or otherwise exploited for competitive, monetary, or adversarial advantage by sophisticated cyber attacks.

Risks should also be evaluated based on the value of the company's assets and the potential for disruption that could arise out of a cyber attack. Consider how utilities-related assets such as water or power may be targeted by terrorist initiatives or how environmental exposures that are broad in reach and impact may result in long-term implications to (1) human health, (2) the environment, and (3) the price and availability of natural resources. For example, water resource systems have long been recognized as being potentially vulnerable to cyber attacks of various types and attacks on these systems would pose risks in the form of threats to public health, the environment, and the economy.

Companies should also consider how cybersecurity risks may be created or magnified by adverse events unrelated to information technology vulnerabilities. For example, catastrophic events resulting in contamination often require massive response efforts involving coordinated activity between the companies involved, government agencies and service providers contracted to help address the clean up and resulting damages claims. It is not unusual for the coordination of multiple agencies and providers to be enabled through the use of "war rooms" or "command centers" where outside parties are granted access to networks containing critical systems and sensitive data.

The governance infrastructure and risk management systems should be flexible enough to address evolving alliances, joint ventures, and contracting relationships where the flow of information is followed inside and outside the organization's four walls. These systems should allow for identification of vulnerabilities as well as opportunities to strengthen every link in the chain. This approach applies even in the absence of a catastrophic event. Further, changes in the way business is done,

such as the development of supply-chain trends and non-traditional collaboration with governments, academic institutions and even competitors, should be considered to address infrastructure constraints that impede the progress of cybersecurity initiatives.

Insurance Coverage Implications for 2012 and Beyond

One likely result from the enhanced focus on disclosing cybersecurity risks is a similarly increased focus on a company's use of insurance as a risk mitigation device. This is especially true in light of the Division's specific reference to insurance coverage as an appropriate subject for disclosure. Insurance proceeds as a recovery asset have long been considered with respect to the disclosure of loss contingencies but could serve to result in an increase in coverage disputes if disclosures become more prescriptive with respect to coverage assertions. This section addresses current developments in the market for cyber-related insurance, considerations during the placement process, and scenarios where potential gaps might exist that insureds, brokers and insurers will need to address.

The starting point for analyzing a company's potential coverage for cybersecurity risks is its existing insurance placement, which may well provide some coverage for these kinds of events.

Aside from traditional coverage placements, the past few years have seen rapid growth in the market for cybersecurity policies. These policies are being sold with various names such as "network security insurance" and "cyber-security insurance." Though risks associated with data privacy breaches are often a driving force in this market, information technology (IT) systems have much broader importance to modern business and, consequently, they present much broader risks. As a result, these policies can provide first – and third-party coverage for losses associated with cybersecurity incidents, such as data restoration costs, crisis response costs, privacy notification costs, investigation costs, defense and indemnification against lawsuits arising out of cyber incidents, and loss of revenue for business interruption caused by a data security breach.

Past experience suggests that the first few years of a new line of insurance coverage often results in an uptick of coverage litigation as disputes involving new policy language arise and the scope of coverage gets tested in courts across the country. As this market is still maturing, the policy forms in use from insurer to insurer still contain significant variances and currently lack the standardization seen in other coverages that results from years of market forces and guidance from numerous legal precedents. Although any policy should be carefully studied prior to placement, this is particularly true here until more uniformity develops. In addition to the recommendations provided above, some suggestions for companies considering the purchase of cybersecurity insurance are as follows:

- Pay close attention to limits and sub-limits. Are they sufficient to fully respond to predictable cyber incidents that the company is trying to insure against?
- Consider whether it covers acts of a company's vendors or customers. If the company provides confidential data to a third party, or allows contractors to access its systems, then the insuring agreement should be broad enough to encompass losses caused by such third parties.[9]
- Similarly, do the company's vendors or customers have appropriate coverage? If so, is the company covered as an additional insured on their insurance policies?
- Is coverage provided if data is simply destroyed but not used or disclosed?
- Does the insured have the right to select counsel? This right may be more important for cybersecurity matters than in other areas. For example, the company's regular counsel may already be familiar with the company's IT capabilities, personnel, and related procedures. It may also make sense to retain counsel with specialized expertise in cybersecurity issues.

Potential gaps in coverage deserve special attention. For example, one possible gap that may be particularly problematic results from the potential for convergence of two historical trends in the insurance market that could form a unique obstacle for the kinds of environmental claims arising from cybersecurity risks such as the ones that were discussed in the previous section. First, insurers have long been inserting computer-related

exclusions in a variety of commercial policies. Similarly, environmental liabilities of the past few decades led to the near-universal practice of inserting pollution exclusions in liability policies, resulting in pollution coverage being limited and sometimes confined to specialized insurance markets and policy forms.

Specific pollution coverage should be examined to determine whether an IT-related exclusion is present. For example, the 2003 version of Insurance Services Office's "Pollution Liability Limited Coverage Form" excludes coverage for:

> [d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.[10]

"Electronic data" is defined to include not only stored information but also programs, software and "any other media which are used with electronically controlled equipment."[11] Accordingly, a potential environmental incident "arising out of" the excluded IT perils may not be covered under a policy with a similar provision.

Similarly, many cyber insurance policies contain pollution exclusions. One fairly typical example negates coverage for losses or claims "alleging, arising out of, based upon or attributable to" the presence of pollutants, the actual or threatened discharge, release or escape of pollutants, or clean-up and response activities involving pollutants.

For these reasons, when environmental and cybersecurity events have a sufficient causal nexus to each other, it may be possible that neither event is covered under a company's liability, pollution coverage or cybersecurity policies. How these issues might play out depends on a number of variables such as the specific facts of a given loss, the policy language at issue, and applicable law, but they are worth further study.

To the extent gaps such as these exist, companies may not be fully protected against cybersecurity risks. Only careful thought regarding potential coverage scenarios and a detailed review of a company's existing or contemplated coverages can identify these gaps, and only then can they begin to be addressed. Consequently, experienced risk management professionals, brokers and coverage counsel should be engaged to assist in this process. Given the Division's inclusion of insurance as an appropriate subject of disclosure, undertaking this kind of rigorous analysis should become a priority.

Conclusion

The recent guidance on disclosures concerning cybersecurity risks presents both a cost and an opportunity. Companies that aggressively respond to this initiative may better understand their cybersecurity risks and insurance coverage, which in turn provides an opportunity to consider whether enhanced insurance protection is necessary to respond to them.

Endnotes

1. U.S. Securities and Exchange Comm'n, Commission Guidance Regarding Disclosure Related to Climate Change (Feb. 2, 2010).
2. Pub. L. 111-203 (2010).
3. U.S. Securities and Exchange Comm'n, CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011).
4. "Although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents." *Id.*
5. *Id.* at 2.
6. *Id.* at 5.
7. *Id.* at 3.
8. *Id.*
9. This concern works in reverse as well. If a company provides such services to others, then it also needs insurance for potential liabilities related to those services.
10. ISO form CG 00 40 12 04, at p. 3 of 9.
11. *Id.*

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | 1.877.323.4171

Pillsbury Winthrop Shaw Pittman LLP