



New Cybersecurity Disclosure Guidance for Public Companies: *Focusing attention, raising questions*

The SEC's Division of Corporation Finance has issued guidelines for the disclosure of cybersecurity risks and cyber incidents in SEC filings. The Guidelines are intended to help reporting companies determine whether they need to disclose the risks they face in protecting their electronic data, as well as the costs they have incurred or could incur because of cybersecurity breaches.

Increased corporate reliance on computer networks and electronic data has brought a corresponding increase in risks associated with breaches of their security. Such breaches have become more frequent and severe. With these Guidelines, the Division has indicated that public companies and their advisors should focus greater attention on how disclosure obligations under the federal securities laws may be affected by the potential financial and operational impact of cybersecurity breaches.

The Guidelines note that cybersecurity breaches (generically referred to as *cyber incidents*) can be malicious (*cyber-attacks*) or unintentional. The Guidelines provide something of a rogue's gallery of cyber malice: the gaining of unauthorized access to steal or corrupt sensitive data or to disrupt operations, denial of service attacks, sophisticated electronic circumvention of network security, and social engineering techniques such as phishing to extract passwords or other information that will enable the gaining of access.

The Guidelines mention both intentional and unintentional breaches of cybersecurity, but mostly focus on deliberate attacks. They note that such attacks may involve money or other financial assets, intellectual property, or other sensitive information belonging to a company, its customers or its business partners. The Guidelines list some of the many adverse consequences of successful cybersecurity attacks, including:

- Remediation expenses, such as the cost of providing notice of breach, credit monitoring and call center services;
- Increased cybersecurity protection costs such as the hiring of additional personnel and third-party experts and consultants, and the purchase of additional protective technologies;
- Lost revenues resulting from unauthorized use of stolen proprietary information or the failure to retain or attract customers following an attack;
- Litigation; and;
- Reputational damage adversely affecting customer or investor confidence.

The federal securities laws are designed to provide disclosure about “*timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision.*” The Guidelines state that the potential consequences cited above may in particular cases be sufficiently material, because of the nature of a company’s business or the magnitude of a cyber incident, to require disclosure. The bulk of the Guidelines describe the principal places in federal securities filings that such disclosures should be considered.

The Guidelines remind companies to consider, on an ongoing basis, whether they must disclose the nature and extent of their particular cybersecurity risks. Some early commentary has referred to the Guidelines as rules or regulations. That they are characterizing the guidelines as nonbinding suggestions likely understates their importance.

Each company determines what it must disclose by applying the rules to its own business and circumstances. When important new developments arise, it can be difficult for companies to know how these developments affect their disclosure obligations under rules that don’t appear to address them. So the Division of Corporation Finance periodically issues guidelines explaining how it believes the existing disclosure rules should be interpreted with respect to these new developments. This happened with Y2K, with climate change — and now with cybersecurity. The Guidelines say that they are intended to be “consistent with the relevant disclosure considerations that arise in connection with any business risk.” Guidelines are not intended to break new ground; they represent what the Division thinks the existing disclosure rules already require.

In other words, the Division’s position is that the current disclosure rules already require registrants to consider cybersecurity risks and to disclose them as necessary to provide “timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision.”

The Guidelines cite several places in public filings where such *disclosure may be required*. Here’s a summary of the key provisions:

Risk Factors

Each public company must disclose the most significant factors that make investment in it speculative or risky. Companies assessing the need for a risk factors disclosure should consider the probability of cyber incidents and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. Generic risk factor disclosure should be avoided; the rules are intended to elicit information about the material risks affecting the particular company making the disclosure, not a listing of risks that can affect any company.

According to the Guidelines, appropriate disclosure may include the following:

- 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.

Management’s Discussion and Analysis of Financial Condition and Results of Operations (MD&A)

Companies need to disclose cybersecurity risks and past incidents “if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant’s results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.” The theft of key corporate intellectual property is cited as the kind of cyber incident that might materially affect future revenues and/or cybersecurity protection expenditures and therefore should be disclosed.

Description of Business

A company must disclose in the ‘Description of Business’ section of its SEC filings if cybersecurity incidents materially affect its products, services, relationships with customers or suppliers, or competitive conditions.

Legal Proceedings

If a company is involved in legal proceedings involving a cyber incident, it may need to make disclosures about the proceedings. The Guidelines give the example of the theft of a material amount of customer information that result in litigation.

Financial Statement Disclosures

Cybersecurity incidents and risks may materially affect a company’s financial statements in ways that must be disclosed. The Guidelines provide various examples, such as payments to customers as incentive to maintain business relationships, losses from asserted and unasserted claims related to warranties, breach of contract, product recall and replacement, and indemnification obligations.

Disclosure Controls and Procedures

Companies are required to assess and disclose the adequacy their disclosure controls and procedures. Companies must disclose if cyber incidents and risks may compromise their ability to record, process, summarize, and report information in SEC filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective. For example, if information might not be recorded properly because a cyber incident has affected a company’s information systems, a company may conclude — and have to disclose — that its disclosure controls and procedures are ineffective.

How might the Guidelines affect securities claims?

Guidelines are not entitled to formal deference by courts in disclosure cases, but judges give varying degrees of informal deference to Division guidance when they adjudicate disclosure cases. Plaintiffs will likely point to the Guidelines when arguing that defendant companies haven’t complied with the disclosure rules. On the other hand, companies often try to use Division guidelines defensively, asserting that in following the guidelines they have satisfied the disclosure rules.

How will the Guidelines affect disclosure and risk management and insurance?

Some early commentary suggests the Guidelines will not significantly change disclosure practices. Public companies will certainly take the Guidelines seriously and more fully describe their material cybersecurity exposures -- without providing a roadmap for exploiting any security weaknesses. Some companies will try to inoculate themselves from securities claims by providing the kind of broad, generic statements often seen in the Risk Factors section of SEC filings. The Guidelines will lead many companies to confront the nature and extent of their cybersecurity risks more forcefully than they have in the past. In order to assess the materiality of their cybersecurity risks, companies will have to quantify them — and quantifying risks unmask previously vague or fuzzy judgments about them. Corporate executives will have more useful information about their cybersecurity risks, which may in turn lead to increased efforts to forestall the operational and financial disruption that breaches cause. Companies will almost certainly review and strengthen their cybersecurity risk management practices.

After being forced to quantify the potential financial impact of cybersecurity breaches, many companies will also reassess the adequacy of their insurance protection. That is rarely a simple task. Among many other things, it requires an in-depth and nuanced understanding of what various types of insurance policies do and do not cover with respect to cybersecurity breaches.

Here are a few of the issues that companies and their advisors will have to consider as they determine how to respond to the Guidelines:

How should a company quantify cybersecurity risks? Cybersecurity breaches can have wide-ranging consequences. A company will probably spend large sums on matters such as forensic investigation into the cause and extent of the breach, legal fees, notice to affected individuals, credit monitoring, identity theft and call center services where appropriate, public relations and communications, government and PCI DSS fines and penalties, and indemnification to corporate clients and others if their proprietary information is compromised. The company may also incur business interruption expenses, the loss of customers, management distraction, opportunity costs, discounts and other customer retention costs, and many other direct and indirect costs. Some of these exposures will be relatively easy to estimate based on currently available data, while others will be extremely difficult to gauge. How should a company estimate these exposures in assessing the materiality of cybersecurity breaches? Will widely cited studies into the costs of data breaches (such as the Ponemon Institute's annual study) become the de facto standard for estimating exposure? How should a company weigh the many potential indirect costs of a data breach in determining the materiality of cybersecurity risks?

Which policies may provide at least some coverage for cybersecurity-related breaches? A company may have several different types of insurance policies -- some commonly considered "cyber" policies, others not -- that could provide coverage for at least some of the costs it would incur after a breach. The company will have to determine which policies might provide any coverage and which wouldn't; which cybersecurity exposures each policy addresses and which it doesn't; and whether and to what extent various policies can be aggregated to provide additional protection. And as the insurance coverage dispute in the Sony PlayStation breach matter demonstrates [See blog post here <http://wp.me/pFoTv-LU>], the availability of coverage under non-cyber policies is far from clear.

How should a company that accepts payment cards (such as credit cards) address the special bundle of risks that are related to the evolving Payment Card Industry Data Security Standards and the rules imposed by the payment card brands? It can be expected that over time there will develop fairly standard ways of disclosing payment card-related risks, but it may be a rocky road.

What will be the impact of more extensive disclosure on the availability and cost of insurance to indemnify cybersecurity losses? Insurers routinely review a public company's SEC filings as part of the underwriting process. Many stipulate that a company's SEC filings constitute part of the application for insurance (usually a negotiable issue to some degree). At least two adverse possibilities come to mind: (1) that extensive descriptions of cybersecurity risks and incidents, crafted by lawyers to overcome allegations of inadequate disclosure, will scare insurers into curtailing coverage and/or charging higher prices, and (2) that some insurers will use these disclosures to try and deny coverage in subsequent claims, on the grounds that a disclosure later shown to be inadequate constitutes a breached warranty that therefore voids coverage. The D&O (Directors and Officers) insurance sector has dealt with this issue for a long time and seems to have largely worked things out. The cyber insurance sector will probably get to a similar equilibrium, although it may take a while and cause some pain in the process.

The new cybersecurity guidelines therefore may have raised as many questions as they answer, and they will certainly require careful and nuanced navigation by companies and their advisors. Companies will need to undertake a fresh and detailed analysis, with each SEC filing, to make sure that their disclosures adequately reflect the cybersecurity risks they face in their then-current business operations.



John Doernberg is a Vice President at WGA. He is responsible for developing relationships and serving as a resource for WGA clients, with a particular focus on privacy, information security and risk management issues. Before becoming an insurance broker in 1995, he practiced law for more than ten years at major firms.