The SEC Staff's "Cybersecurity Disclosure" Guidance: Will It Help Investors or Cyber-thieves More?

Sarah Jane Hughes  
*Indiana University Maurer School of Law, sjhughes@indiana.edu*

Roland L. Trope  
*Trope and Schramm*

Follow this and additional works at: [https://www.repository.law.indiana.edu/facpub](https://www.repository.law.indiana.edu/facpub)

Part of the Business Organizations Law Commons, Corporate Finance Commons, and the National Security Law Commons

**Recommended Citation**

[https://www.repository.law.indiana.edu/facpub/2558](https://www.repository.law.indiana.edu/facpub/2558)

This Article is brought to you for free and open access by the Faculty Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Articles by Maurer Faculty by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact rvbaughan@indiana.edu.
On October 13, 2011, the SEC’s Division of Corporate Finance quietly issued new guidance (Guidance) describing disclosures of cybersecurity incidents and attacks and the prevention and remediation measures that public companies (Registrants) have suffered or may suffer, and of the prevention and remediation expenses they have expended or may expend (CF Disclosure Guidance: Topic No. 2—Cybersecurity). This Guidance is not a rule or regulation or a commission interpretation. It did not appear in the Federal Register for comment or otherwise. Its issuance is likely to cause substantial amounts of work among Registrants and legal professionals who represent them. At the very least, the Guidance brings new attention to cybersecurity issues in Registrants’ operations and disclosures.

This Guidance appears to result from an exchange of letters between Senator John D. Rockefeller IV and SEC Chairman Mary Schapiro. Senator Rockefeller’s May 11, 2011, letter noted the “growing threat and the national security and economic ramifications of successful attacks against American businesses,” declared it “essential” that corporate executives “know their responsibility for managing and disclosing information security risk,” and requested the SEC to issue guidance “regarding the disclosure of information security risk, including material network breaches.” Chairman Schapiro responded on June 6, 2011, reciting a number of disclosure requirements imposed on Registrants under the federal securities laws and pointing out that certain of these requirements might obligate a Registrant to make cybersecurity disclosures:

For example, Item 503(c) of Regulation S-K may require risk factor disclosure regarding a prior cyber attack, a potential cyber attack, or the effects of a cyber attack. . . . Thus, a company should consider whether cyber attacks and vulnerabilities present specific and material risks and should avoid generic risk factor disclosure that could apply to any company.

Chairman Schapiro explained, however, that she had asked the commission staff to provide her with a briefing on “current disclosure practices” and to advise her on “whether additional guidance is needed to make sure investors have access to the information they need when making their investment decisions.”

The resulting Guidance lays out six aspects of disclosures that may be affected by cyber attacks and prevention and remediation expenses. However, it gives only passing attention to the trade-off inherent in making Registrants’ cybersecurity risks and prevention measures more transparent. The trade-off can be summarized as follows: The more revealing a Registrant’s cybersecurity disclosures become, the greater the likelihood that they will provide information useful to hackers and competitors (Adversaries). Specifically, a Registrant’s cybersecurity disclosures, which the longstanding SEC interpretations require be specific to the Registrant rather than generic, will be understood far better by a cyber Adversary, than by a potential investor, and, accordingly, more valuable to Adversaries.

The goal of this article is to arm Business Law Today readers with the basics about the Guidance so that they can have conversations with clients who are or are about to be Registrants, about what this new Guidance requires in responsive disclosures and revisions to disclosure controls and procedures. The article also expresses concerns that, notwithstanding the SEC’s staff’s expressed intentions to the contrary, the greater transparency in Registrants’ post-Guidance disclosures may provide roadmaps for cyber attacks and thefts.

Reinterpreting Existing Rules
The Guidance acknowledges that “no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents,” but then advises that “a number of disclosure requirements may impose an obligation on Registrants to disclose such risks and incidents.” The Guidance further notes that disclosure of cybersecurity risks and cyber incidents might be required in order to “make other required disclosures . . . not misleading” when made. SEC staff also cautions that “Registrants should
review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents.” The obligations thus created pose potentially burdensome tasks for Registrants.

Adding to “Business Risk Disclosure” Requirements
Cyber risks and costs fall within the “risks and events” that may affect the accuracy, timeliness and completeness of required disclosures. The Guidance cites obligations to keep shelf registration statements up to date, the over-arching responsibility to disclose material information (pursuant to Securities Act Rule 408, Exchange Act Rule 12b-20, and Exchange Act Rule 14a-9), and the antifraud provisions of Securities Act Section 17(a), Exchange Act Section 10(b), and Exchange Act Rule 10b-5, in support of responsibilities to review and disclose cyber risks and incidents so that their disclosures are not misleading to investors.

Articulating Six Key Duties
The new Guidance sets forth six aspects of Registrants’ disclosure duties under the Securities Act of 1933 and the Exchange Act of 1934 and related SEC rules:

Risk Factors
To the extent that they are “among the most significant factors that make an investment in the [registrant] speculative or risky,” the Guidance requires disclosure of the risk of cyber incidents affecting the registrant. It recommends that Registrants, in determining “whether risk factor disclosure is required,” assess their own cybersecurity risks considering all “relevant information, including prior incidents, the severity and frequency of those incidents” from quantitative and qualitative perspectives, and the “costs and consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption.” Registrants also should “consider the adequacy of preventative actions taken to reduce cybersecurity risks” from the perspective of the industry in which the registrant operates, including “threatened attacks of which [the individual registrant] is cognizant.”

Risk factor disclosures should cover the nature of “material risks” and should describe how specific risks might affect the registrant as contextually as possible, avoiding risks and effects that are generic (as SEC Regulation S-K requires). The Guidance suggests “appropriate [risk factor] disclosures” as follows:

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

Management’s Discussion and Analysis
Risks and incidents should be disclosed (pursuant to SEC Regulation S-K and Form 20-F, respectively) if costs and consequences of known or potential cyber incidents would constitute “a material event, trend, or uncertainty that is reasonably likely to have a material effect on results of operations, liquidity or financial condition” or to cause reports not necessarily to indicate future operating results or financial condition. Examples include: disclosure of how a theft of intellectual property would affect the registrant’s stated results of operations, or reduce revenues, or, in the absence of a loss of intellectual property, of how an event would cause a material increase in cybersecurity prevention or remediation costs, including litigation costs.

Description of Business
Registrants must disclose (again pursuant to Regulation S-K and Form 20-F, respectively) the effect of one or more cyber incidents on its products, services, relationships with customers or suppliers, or on competitive conditions if any would materially affect any reportable segment(s) of their businesses. The staff’s example concerns knowledge of a cyber event that could affect materially a forthcoming product’s future viability.

Legal Proceedings
If a Registrant or any subsidiary has a pending legal proceeding pertaining to a cyber incident whose outcome would affect its prospects, it should disclose the proceeding(s) pursuant to Regulation S-K. For example, if a “significant amount of customer information” had been stolen, the Registrant should disclose the court, the date the action commenced, the principal parties to the action, the factual basis for the action, and relief sought.

Financial Statement Disclosures
The nature and potential severity of cyber incidents a Registrant may have can affect its financial statements in material ways according to standards adopted by Financial Accounting Standards Board (FASB). The SEC staff’s Guidance suggests a time-bifurcated analysis and disclosure:

Prior to an Incident. The FASB Accounting Standards Codification (ASC) on Internal-Use Software requires capitalization costs for cyber prevention to be disclosed.

During and Following an Incident.
Disclosures during and following a cyber incident fall into four categories regulated by specific FASB guidance:

• Customer Payments and Incentive requires “appropriate recognition, measurement, and classification of these payments used to mitigate cyber-incident damages.”

• Loss Contingencies requires determination—and recognition of—liabilities from asserted and un-asserted claims such as related to warranties, breach of contract, recalls and replacement, and counter-party indemnification of remediation expenses. If these expenses and claims are probable and reason-

Published in Business Law Today, December 2011. © 2011 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.
ably estimable. Registrants should disclose them. Additionally, the SEC Staff Guidance requires Registrants to disclose losses that are “at least reasonably possible.”

- **Risks and Uncertainties.** requires disclosures of effects of cyber incidents that would diminish future cash flows because of impairment of intangible assets such as goodwill and other customer-related intangibles including allowances for product returns, trademarks, patents, etc. Post-event estimates and subsequent reassessments enable a Registrant to explain risks or uncertainties of “a reasonably possible change” in near-term estimates that could be material to its financial statements.

- **Subsequent Events** may require disclosures if incidents, recognized or non-recognized, occur or are discovered after a balance sheet date but before the associated financial statements are issued. Financial statements should disclose “material non-recognized subsequent” events in terms of their nature and an estimate of their “financial effect, or a statement that such an estimate cannot be made.”

**Disclosure Controls and Procedures**
The SEC staff Guidance also requires Registrants to disclose the effectiveness of their Disclosure Controls and Procedures to the extent that they affect the Registrant’s ability to “record, process, summarize, and report” information that they should disclose in SEC filings. In addition, Registrants should evaluate and disclose deficiencies in controls and procedures if a cyber incident would cause information not to be recorded “properly” and, therefore, would render disclosures to be “ineffective.” (SEC Regulation S-K and Form 20-F.)

**What Would Cybersecurity Specialists Say about this Guidance?**
Cybersecurity specialists acknowledge a simple truth: attackers need to find only one gap in an enterprise’s defenses. Registrants, in contrast, must plug and seal every gap to remain protected. As a result, cybersecurity specialists would have five concerns about the Guidance:

1. Registrants may begin complying with the Guidance cautiously, adding cyber risks to pre-existing lists of risks and describing them in terms that are too minimal and vague to be of much use to potential investors.

The Guidance creates new burdens for Registrants, the most significant of which will probably be to craft disclosures to enable a Registrant to comply with the Guidance without revealing any information of use to an Adversary. It may help Registrants to recall that division staff admits that they are mindful that “detailed disclosures could compromise cybersecurity efforts” and that “disclosures of that nature are not required under the federal securities laws.” If the staff notifies Registrants of deficiencies in their cybersecurity disclosures, many Registrants may respond by defending the deficiency as avoiding the kind of disclosure that could compromise cybersecurity and justify it further by reminding the Staff of their position that such disclosures are “not required” by federal securities laws.

2. Cautious, minimal and vague disclosures, as noted above, are likely to help Registrants’ adversaries before they will become useful for investors.

The Guidance likely will have the unintended consequence of encouraging increased investment in obtaining legal advice on finding the words to express cybersecurity disclosures that will satisfy the staff without informing the Adversary. If a Registrant has to choose between complying with the Guidance and sapping cybersecurity, the choice is clear: It will avoid compromising the enterprise. The division should not have put Registrants into the bind of having to make such choices, and should not be surprised when Registrants choose to make less informative disclosures. The Staff can then object, and a Registrant can point out to the staff their comments may well have overlooked or underestimated.

3. The Guidance calls for certain kinds of information to be disclosed that, if disclosed in detail or with any significant detail or specificity, would likely undermine cyber security.

A closer look at the bullet point list of “risk factor” disclosures reveals a tension between the Guidance’s aims and its disclosure requirements, some of which, as explained above, would provide potentially valuable intelligence to a Registrant’s Adversary. A Registrant that, as directed, disclosed “risks related to cyber incidents that may remain undetected for an extended period” could identify itself as a vulnerable target to Adversaries. To explain such risks without highlighting them for an Adversary would appear impossible except through use of obscure and ambiguously phrased disclosures. Similar problems would arise for a Registrant trying to discuss aspects of its operations that “give rise to material cybersecurity risks.” The staff may have seriously underestimated the skills of Adversaries.

4. If a cyber attack should follow a compliant disclosure, what is the likelihood that a shareholder’s derivative suit against officers and directors would succeed?

Registrants should not be pushed by a disclosure requirement to decide between compliance with a staff interpretation and facilitating an attack on themselves that could expose not only the enterprise’s assets to damage or loss, but that could expose officers and directors to costly and wasteful lawsuits.

5. The Guidance apparently marks the beginning, not the end, of the SEC’s efforts to influence Registrants’ cybersecurity. As revealed in testimony by Robert Cook, Director, Division of Trading and Markets (TM) before the Senate Committee on Banking, Housing and Urban Affairs Subcommittee on Securities, Insurance, and Investment, on November 16, 2011,

TM plans to enhance its ARP [Automation Review Policies] reviews, with a particular focus on whether registered entities have appropriate cybersecurity measures, and is preparing recommendations for the Commission to further strengthen the ARP standards.

(http://www.sec.gov/news/testimo-
ny/2011/ts1116rk.htm.)

The Guidance required disclosures that
have the result of making Registrants more accountable for cybersecurity lapses and failings. The TM plans would go further and apparently set standards for registered entities for “appropriate cybersecurity measures.” In light of the unintended consequences of the Staff’s Guidance, it seems premature and ill-advised for the SEC to be considering going even further and prescribing cybersecurity standards.

Conclusion
The new cybersecurity Guidance from the SEC’s Division of Corporate Finance recognizes the centrality of technology to Registrants’ operations and profitability, the risks that cyber-attacks present to both, and the resulting relevance of cybersecurity measures. As Deputy Secretary of Defense William J. Lynn observed in “Defending a New Domain,” Foreign Affairs (Sept./Oct. 2010):

Modern information technology also increases the risk of industrial espionage and the theft of commercial information. . . . Every year, an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government agencies.

The Guidance’s requirement that a Registrant disclose specific material information concerning their cybersecurity condition, preparedness, and experience with cyber attacks may create a Hobbesian choice for Registrants: If Registrants’ disclosures contain sufficient information to be meaningful for investors, disclosures almost certainly will have to contain information of value to Adversaries seeking reconnaissance data that will facilitate a breach or enhance its ability to exploit a cyber-vulnerability. As a result, Registrants may want to ensure that they avoid disclosures that would reveal information that prior to its release, Registrants had been reluctant to disclose, had not believed they were obligated to disclose, and, therefore, had refrained from disclosing. It also may be that, under the obligation to disclose such information, Registrants will be motivated to improve cybersecurity in order to avoid finding themselves in the position where their experience of a cyber attack obligates them, under the Guidance, to disclose information that would make them less attractive to investors. However close the Guidance comes to achieving such results, it also may put Registrants in a double-bind. As Tom Smedinghoff, partner in the Privacy & Data Protection practice at Edwards Wildman, observes:

If a Registrant conducts a risk assessment and finds cybersecurity deficiencies that are sufficiently material to require disclosure in its SEC filings, the registrant’s legal obligations to provide ‘reasonable’ or ‘appropriate’ data security under other applicable federal or state laws will likely also require that it take appropriate steps to address those deficiencies. Thus, in some cases, disclosing cybersecurity risks may prompt inquiry regarding compliance with applicable data security laws, and may increase the risk of potential liability for failure to provide legally required security. It may well be a ‘catch-22’ for the Registrant.

Registrants and their lawyers will not know, for a while at least, what the precise consequences of the new Guidance, intended and otherwise, will be. It also may take time for the SEC staff to discover how much value investors will gain from the required cybersecurity disclosures, or whether, as we fear, the earliest beneficiaries and the ones who stand the most to gain will be Adversaries, not investors. We hope that experience under the Guidance will not meet our most pessimistic predictions, but rather will motivate appropriate additional attention to cybersecurity.