Source Callé

September 25, 2015

Via www.sec.gov/cgi-bin/ruling-comments
Ms. Mary Jo White
Chair
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

RE: Cybersecurity Roundtable, File No. 4-673

Dear Chair White:

The following comments are intended to supplement the cybersecurity roundtable discussion hosted by the SEC in Washington, D.C. on March 26, 2014. I was impressed by the backgrounds of your panelists and the quality of the dialog that was captured in the transcript posted on your website. I want to offer specific recommendations to help the SEC address cybersecurity issues and challenges faced by market participants and public companies.

Source Callé LLC is a consulting firm that helps Boards of Directors, as well as Chief Financial Officers (CFOs), Chief Information Officers (CIOs), Generals Counsel, and their teams, to strengthen the internal controls and improve the ROI on their technology. My cybersecurity practice employs leading edge diagnostic and prescriptive approaches to help companies reduce risk and realize opportunity.

Explicitly Link Sarbanes-Oxley §404 and §302 Certification to Technology Controls

The growing number and expanding scope of data breaches plaguing SEC registrants as well as virtually every organization today highlight the need for stronger technology controls and a much more proactive approach to the effective prevention, detection and remediation of data breaches. Greater transparency of data breach incidents and more consistently applied standards for disclosure would help too. A data breach is evidence of weak controls around data as an asset and, for many companies, those assets are among the most valuable in the company.

Data security at most companies tends to be the responsibility of the CIO. Explicitly linking the §404 and §302 certification requirements under the Sarbanes-Oxley Act of 2002, with its focus on internal controls over financial reporting (ICFR), to technology controls would further motivate the CFO to help close the cybersecurity gap that exists at most companies today.

Holding the CFO (and CEO) accountable for technology controls through the certification process will reinforce a necessary behavior change. Of course every CFO, like every company, is unique. However, there are some representative characteristics of CFOs that I have observed. CFOs tend not to have a good understanding of how technology is procured, provisioned and managed. In the budget process, they might expect an increase in next year's revenue of 5%, but ask the IT department to find a way to operate with a budget of 5% less to force productivity gains and fuel operating margin expansion. They might be inclined to outsource responsibility for information technology to firms that make promises that cannot be delivered. They may feel like

cybersecurity risk is something that can simply be transferred with insurance. However, CFOs are well positioned to own data as an asset, and to safeguard it and help to generate value from it. They are strategically positioned to unify the many other departments that have a stake in information governance, control, risk management, and monetization.

It was appropriate, if not about time, that the Committee of Sponsoring Organizations of the Treadway Commission (COSO) placed an emphasis on technology controls when it updated its Internal Control – Integrated Framework in May 2013. Technology has become embedded in virtually every aspect of business activity, and many companies have outsourced important technology management functions to third parties. CFOs and the auditing profession are now obliged to take a much deeper and more comprehensive view of technology controls.

Principles 11 and 13 of the 17 principles in the COSO update reference management's responsibility to implement strong controls over technology.

- Principle 11 (Control Activity): "The organization selects and develops general control activities over technology to support the achievement of objectives."

- Principle 13 (Information and Communication): "The organization obtains or generates and uses relevant, quality information to support the functioning of internal control."

The COSO framework update has an effective date of December 15, 2014, so we are beginning to develop insights on how management teams and their auditors are reacting. The framework's emphasis on technology controls is broad and comprehensive, and a much needed step in the right direction. Within this framework, it is clear that a data breach would be evidence of a weakness in ***controls over an operating system***.

Data is an asset that is recorded in financial statements as part of goodwill. When data gets breached, there can be a diminution in the value of goodwill attributable to damaged reputation or brand integrity, and vital data such as intellectual property or other operating data can be altered, stolen or destroyed.

Today, it can be implied, but it is not explicitly stated, that data breaches are evidence of weak ***controls that affect a company's financial reporting.*** COSO and the SEC should explicitly state that data breaches are evidence of weak controls over financial reporting, clarifying that §404 and §302 of Sarbanes-Oxley are applicable. Considering the penalties associated with false representations under §404 and §302, the Audit Committee, CEOs, CFOs, as well as internal and external auditors, an explicit connection would have a dramatically stronger motivation to improve a company's cybersecurity posture.

Supplement the October 2011 Disclosure Guidance on Cybersecurity

The SEC's disclosure guidance on cybersecurity dated October 13, 2011 is well reasoned and offers numerous avenues for management to put risk into perspective, but it can be improved upon.

If management and the Board are not measuring a variable, they are unlikely to be managing it to achieve a desired outcome. The SEC can help improve the level of accountability by requiring management to report the following information in their reports on Form 10-Q, covering incidences that have been appropriately evaluated on a forensic level.

- The number of individual records that were compromised.
- The type of data that was compromised (e.g., individual names, addresses and phone numbers, credit card numbers, social security numbers, health records, intellectual property, other sensitive information, including that which egresses, is altered or has been destroyed, etc.).
- Indicate whether the breach was deemed to be intentional (e.g., initiated by an external bad actor or employee acting maliciously) or unintentional (e.g., the result of negligence, as is the case when an employee or contractor laptop containing sensitive data is lost or stolen).

There is other information relating to an incident that would be of interest to certain parties but should not be required to be disclosed periodically because it would impose too great a burden on management to prepare or would compromise a registrant's cybersecurity.

Public dissemination of the information outlined above would have the beneficial effect of focusing the Board and C-level executives on an appropriate set of metrics that represent an indication of management's skill in exercising effective controls over technology. Such dissemination also would offer reasonable transparency for shareholders, customers, partners and other constituents who care about the state of a registrant's cyber hygiene.

Management must be afforded the opportunity to exercise judgment in the disclosure of data breaches as they occur in real time, and between 10-Q release dates. Such disclosure could be more expansive than the three items listed above. Management would take into consideration several factors, including the materiality of the breach, the potential effects of alerting perpetrators regarding the investigation, and the quality of the information about the incident at hand, among other factors. No two breaches are exactly alike, so it is not feasible to impose rigid, numerous or impractical disclosure requirements. In general, management teams and their Boards are cognizant of the virtues of operating in an open and transparent manner, and the penalties of operating otherwise, and know they will be judged by the quality of their disclosure practices.

Codify Disparate State and Local Disclosure Requirements into a National Standard

Immediately following a data breach, management must quickly identify and comply with all of the local and state level security breach disclosure laws. The National Conference of State Legislatures points out that security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc.); definitions of personal information (e.g., name combined with social security number, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information). The result is a patchwork of disclosure requirements. Registrants would be well served by an exercise, led by the SEC, to assemble appropriate industry and government participants to review these various requirements and attempt to codify them into a national standard.

Prepare to Exercise Oversight of NRSROs Focused Exclusively on Cybersecurity Risk

The SEC exercises exclusive authority over the registration and qualification of Nationally Recognized Statistical Rating Organizations (NRSROs) that assess the creditworthiness of issuers. The SEC will need to consider the registration and qualification of firms that can provide a rating of a company's cybersecurity risk. I welcome the opportunity to share my research of this

emerging class of entities that can objectively measure a company's cybersecurity practices and the resultant level of hygiene on a continuous basis. Considering the vulnerabilities inherent in any company's reliance on third party vendors to securely link to their networks (as was widely reported in the Target breach), it is good public policy to have much more transparency when it comes to a company's cybersecurity posture.

Organize More Frequent Roundtables on Cybersecurity

My views are informed by a consulting practice that appeals to a senior level audience that wants to prevent, detect and remediate cybersecurity incidences. Cybersecurity is a contact sport, requiring continuous attention, and it carries serious consequences. There is much more that organizations need to do to operate securely and to realize the great potential offered by technological innovation.

My practice currently is especially oriented to the large, growing, and remarkably under-addressed attack surfaces that originate from employee use of cloud-based services such as SaaS apps and cloud hosts, as well as the vulnerabilities associated with network connections to third party vendors. By organizing more frequent roundtables on cybersecurity, and including a more diverse set of practitioners, the SEC can help promote best practices and improve the integrity of the technology controls that govern its registrants.

Sincerely,

Craig Callé
CEO, Source Callé LLC
Philadelphia
www.sourcecalle.com
ccalle@sourcecalle.com

cc: Robert B. Hirth, Jr. (via email)
Chairman, Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Office of the Secretary
Public Company Accounting Oversight Board (PCAOB)
1666 K Street NW
Washington, DC 20006-2803