Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Disclosing Cyberattacks: How To Follow SEC Guidance

By John Reed Stark

Law360, New York (November 01, 2011, 12:32 PM ET) -- On Oct. 13, 2011, the U.S. Securities and Exchange Commission released its first ever staff guidance pertaining exclusively to the cybersecurity-related disclosure obligations of public companies. The guidance serves as a wake-up call for many of today's public companies.

This new and unique SEC guidance covers a public company's reporting responsibilities both just after a cyberattack as a "material" event, and even before as a "risk factor." From the SEC's perspective, the requirements outlined in the guidance introduce nothing new but, instead, merely clarify the SEC's long-standing requirement that public companies report "material" events to their shareholders, i.e., important developments or events that "a reasonable investor would consider important to an investment decision."

What precisely renders an event material has plagued securities lawyers for years and has been the subject of countless judicial decisions, SEC enforcement actions, law review articles, law firm guidance and the like. Now, as of the date of this new guidance, the SEC has officially (and quite noticeably) added cybersecurity into the mix of disclosure by putting every public company on notice that cyberattacks and cybersecurity vulnerability fall squarely within a public company's reporting responsibilities.

The Guidance

With respect to the aftermath of a cyberattack, the SEC discusses the myriad of ways a cyberattack can impact the operations of a public company and then sets forth the various reporting sections of typical SEC filings that may warrant mention of the cyberattack, including Risk Factors, Management's Discussion and Analysis of Financial Condition and Results of Operations, Description of Business, Legal Proceedings, Financial Statement Disclosures, and Disclosure Controls and Procedures.

With respect to the mere possibility of a cyberattack, the guidance goes so far as stating that companies should also "consider the probability of cyber incidents occurring 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."

As to the particularity of the disclosure, the SEC seems to want to have its cake and eat it too. On the one hand, the guidance appears to allow for a lack of specifics so as not to compromise a company's

security. On the other hand, the guidance cautions companies not to use any sort of generic "boilerplate" type of language in its disclosures. The guidance navigates between these challenges, stating somewhat opaquely:

> While registrants should provide disclosure tailored to their particular circumstances and avoid generic "boilerplate" disclosure, we reiterate that the federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity. Instead, registrants should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular registrant in a manner that would not have that consequence.

Even though the SEC might view this guidance as simply a reiteration of previously existing requirements, there remains little doubt that these new guidelines impose an arguably unprecedented and certainly significant obligation upon public companies. As a result of this guidance, companies would be wise to considerably step up both their processes for defending themselves against corporate attack, and their plans for incident response.

Of course, it is not a matter of "if" a company will experience a cyberattack, but "when" — so it is not surprising that the SEC has taken the unusual step of issuing interpretive guidance in this area. Indeed, cybersecurity attacks have become a significant concern to public corporations and their shareholders.

Yet not everyone understands just how progressively more complex and sophisticated cyberattacks have become over the past few years. These are no longer just teenager delinquents in their basements engaging in some "cyber-joyriding." Today's attacks are organized, sophisticated, intricate — and costly.

Handling disclosure obligations relating to a cyberattack is a far cry from the usual triggering events that prompt reporting obligations of today's public companies. Merely understanding the nature and impact of a cyberattack can quickly evolve into a tremendous challenge within itself, and knowing how to disclose the nature of the incident in a timely, complete, and accurate manner is often a Herculean task.

Moreover, the reality is that assessing and solving any cybercrime can necessitate a significant level of expertise that many public corporations simply might not have on hand. In fact, there may very well be public companies that experience a cyber-related incident and genuinely want to meet their obligations under the relevant securities regulations but regrettably remain essentially paralyzed until they can adequately determine precisely what happened.

Yet the SEC in its guidance has sent a strong message, in clear and uncertain terms, that the staff's expectation is exactly that — a timely, accurate and, albeit somewhat generalized, but complete, disclosure of cyberattacks (no matter how delicate and difficult the undertaking).

The Guidance and the Whistleblower

This new guidance (unfortunately for public companies) dovetails with the recent whistleblower provisions enacted within The Dodd–Frank Wall Street Reform and Consumer Protection Act, which rewards informants who provide certain types of information leading to successful securities actions, including failure to disclose actions, with between 10 and 30 percent of any recovery over $1 million.

Thus, public companies, which might have previously believed they could fly under the radar and keep

their cyberattacks secret, now run an even higher risk than ever before of getting caught — because the SEC guidance has issued the equivalent of an all-points bulletin to potential whistleblowers for the chance to take home a hefty bounty.

With an effortless (and even an anonymous) email to the SEC whistleblower mailbox, a disgruntled employee who learns about a cyberattack before a company opts to disclose that attack to the public, can instantaneously notify the SEC about the issue. What will then inevitably follow is the unwanted attention of an empowered SEC enforcement staff seeking to identify the first violator of the new SEC guidance — not only costing a company significant legal expenses and possible lost revenue but also, and most importantly, potentially causing a company immeasurable reputational damage.

Whether the SEC guidelines have simply restated a notion that securities lawyers all previously understood or have actually shifted the SEC disclosure paradigm is of no matter. The bottom line is that the SEC has launched a shot across the bow of public companies that this area of disclosure will henceforth be receiving the utmost attention from SEC staff.

The Need for a Technical Incident Response Team

To handle this new and daunting disclosure responsibility, if it has not done so already, a public company might want to consider forming a technical incident response team. The members of the team should include employees from all the relevant c-levels of a company's org chart, including from information technology, investor relations, public relations, legal and other important operational departments.

A company will also need to engage an independent outside expert to conduct the investigation of the attack, performing tasks such as data preservation, malware analysis, digital forensic analysis, network log analysis, reverse engineering remediation and other relevant investigative tasks.

An independent expert digital forensics team can surround the cyberattack scene with virtual "yellow police tape," which can prove valuable during the investigation and provide added credibility and neutrality to the ultimate disclosure of the event.

Moreover, leaving pristine in the short run any potential evidence left by a cyberattack until after the execution of a forensic identification, preservation and analysis can save time, money, and headaches in the long run. Cyberattack internal probes can be compromised, when, for instance critical logs, back-up tapes, hard drives or other data become corrupted or overwritten by nonexpert investigators.

Prepare, Preserve, Assess, Search and Notify/Disclose

Once a public company establishes its incident response team, its team should take five separate actions: prepare, preserve, assess, search and notify/disclose.

Prepare

Develop a response plan. Effective organizations do not determine how to respond to a data breach at the spur of the moment when one occurs; they plan ahead. An effective plan should include:

- Management endorsement — to underscore the mission

- Contact lists — for members of the response team
- Legal analysis and timeline — drawn from state or federal law
- Categories of adverse events — to prevent a constant fire drill
- "First steps" checklists — to identify priorities
- Facilities and equipment list — (e.g., cell phones, reserve servers, conference rooms) so that response can start immediately
- Outreach plan — Effective response to a data breach often involves more than just the company's managers and employees. As the National Institute of Standards and Technology has pointed out, effective incident response may involve software vendors, third-party Internet companies or ISPs, suppliers, law enforcement personnel and the media

Preserve

When a data breach occurs, a company often lurches between efforts to get back up and running and efforts to complete a full-blown breach assessment. In fact, the company's first reaction should involve preserving any evidence of the breach while swapping in clean machines. A company should:

- Assemble a team and distribute a list of responsibilities
- Unhook infected machines (leave power on)
- Call outside experts to forensically image infected machines
- Pull needed backup(s) out of rotation so they are not overwritten
- Insert clean and patched machines
- Save off log files (e.g., Web, firewall, intrusion detection system)
- Save keycard data and surveillance tapes
- Start real-time network packet capture
- Force administrator and user password change

Assess

Once data has been preserved, an assessment can begin. This involves several different types of coordinated action. The early goal should be to determine:

- If data has really been lost or compromised
- What type of data that has been compromised
- Time period of breach
- Initial volume estimate of data involved

Once hard drives and all relevant network and other communication logs have been preserved, begin an immediate digital forensic assessment:

- Analyze log files
- Review memory/virtual memory
- Analyze hard drives
- Analyze and reverse engineer malware code
- Review live traffic captures
- Run behavioral profiling

Search

Identify key, compromised data. Focus on intellectual property, trade secrets, unencrypted “personal information” or “personally identifiable information," or “protected health information" and other key compromised information.

Notify/Disclose

Multiple parties, not just the SEC, may require notice and reporting — including contracting parties, victims, credit reporting agencies, government agencies (e.g., the U.S. Department of Health and Human Services, attorney general offices), even the media.

Conclusion

Given the increasingly complex and thorny nature of recent cyberattacks, the SEC staff hopefully will allow public companies some latitude and give companies a chance to get their arms around a situation before mandating the filing of any sort of disclosure. Otherwise, rather than full and fair disclosure, the result of this new guidance will only be chaos and confusion, far from what investors need in today’s already volatile securities markets.

--By John Reed Stark, Stroz Friedberg, LLC

John Stark is managing director and deputy general counsel in charge of the Washington, D.C., office of Stroz Friedberg, a global digital risk management consulting firm. Formerly, Stark served for almost 20 years in the Enforcement Division of the Securities and Exchange Commission, the last 11 of which as chief of its Office of Internet Enforcement. He also has served for the past 15 years as an adjunct professor of law at the Georgetown University Law Center, where he taught a course on technology and the SEC and advanced securities regulation.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media, publisher of Law360. This article is for general information purposes and is not intended to be and should not be taken as legal advice.