SAN FRANCISCO
Daily Journal
www.dailyjournal.com
FRIDAY, APRIL 5, 2013

PERSPECTIVE

SEC takes hard line on 'cyber incidents'

By Michael Mugmon and Joel Fleming

The nightmare starts with an innocuous-looking, early-morning email. A groggy employee sees a bland subject line and a familiar name in the "From" field. He opens the attachment. That small mistake is all it takes.

Weeks later, the organization realizes that it has been the victim of a cyberattack. Instantly, it's plunged into crisis mode. IT professionals work around the clock to fix the vulnerability and establish the scope of the security breach. Executives scramble to determine the impact on customers, suppliers, employees and other stakeholders.

In responding to this sort of challenge, corporations usually focus on operational issues, such as securing their networks, preserving data and repairing any damage done. Recently, however, the Securities and Exchange Commission has signaled that it wants companies to focus on one more thing: promptly disclosing cyberattacks to investors.

In October 2011, the SEC released guidance — "CF Disclosure Guidance: Topic No. 2" — emphasizing that registrants may need to disclose cybersecurity risks as well as "known … cyber incidents." According to the SEC, if a company experienced a "material" cyberattack in which malware was embedded in its systems and customer data was compromised, it "likely would not be sufficient" merely to mention the risk of such attacks in its disclosures. Rather, the registrant may need to "discuss the occurrence of the specific attack and its known and potential costs and other consequences."

As the New York Times recently pointed out, such guidance was historically at odds with the practices of some American corporations — which "treat[ed] online attacks as a dirty secret best kept from customers, shareholders and competitors, lest the disclosure sink their stock price and tarnish them as hapless." Indeed, one executive quoted by the paper said, "There are an awful lot of lawyers out there trying to keep companies from exposing that these breaches are happening."

But as the SEC's guidance shows, that hush-hush view is giving way as cyberattacks have become bolder, more frequent and more disastrous. In early February, President Barack Obama issued an executive order directing federal agencies to improve their sharing of cyberthreat information with the private sector and seeking to create a voluntary program to encourage enhanced cybersecurity for U.S. firms. One week later, the computer security firm Mandiant reported that, since 2006, a cyberespionage group linked to the Chinese military had "systematically stolen hundreds of terabytes of data" from at least "141 companies spanning 20 major industries." And in early March, in testimony before the Senate Intelligence Committee, the director of national intelligence listed cyberattacks as the most dangerous immediate threat to the U.S. — even ahead of the threat posed by global terrorism.

For its part, the SEC has followed its guidance with a number of comment letters pushing companies to disclose specific cyberattacks. In April 2012, the SEC directed one large online merchant to disclose that its subsidiary had experienced a cyberattack earlier that year. Half a dozen other companies have received comment letters from the SEC directing them to disclose specific cyberattacks that they'd suffered.

What is also interesting is that the SEC seems to be reading "material" out of its guidance — and thus expecting disclosure of even minor cyberattacks. On one hand, the SEC guidance requires disclosure of "material" cyberattacks — which could be interpreted to mean only attacks that have a material effect on operations. On the other hand, the SEC has also rejected several attempts by companies to resist disclosure on grounds of materiality. In one comment letter, the commission rejected an online merchant's argument that the attack on its subsidiary was not material and demanded disclosure. In another comment letter, the commission rejected the same argument from another company and explicitly instructed it to disclose "any" attack. This suggests that the commission may view most attacks as material because they reveal an underlying vulnerability, even if the actual financial effect of a specific attack was minimal.

> Perhaps sensing that shift, four of the country's largest financial institutions recently chose to disclose cyberattacks that they had experienced in their Form 10-Ks filed at the end of February or in early March.

Obviously, every case is different. The SEC can't possibly require disclosure of each and every attack, and there is no one-size-fits-all solution.

But any company that has suffered a cyberattack needs to know that the SEC is taking an increasingly hard line on what must be disclosed. Thus far, the SEC has restricted itself to comment letters and hasn't brought any enforcement actions for failures to disclose cyberattacks. But the recent revelations of the Mandiant report and President Obama's executive order may have changed the political landscape.

Perhaps sensing that shift, four of the country's largest financial institutions recently chose to disclose cyberattacks that they had experienced in their Form 10-Ks filed at the end of February or in early March. Two of those institutions made disclosures despite also stating that the cyber-attacks they had experienced did not have any material impact on their operations or financial results. So, it seems that nondisclosure is becoming an increasingly risky proposition.

Obviously, there are also risks associated with making a disclosure. Every company operates in a unique environment and should think carefully about the particular risks that it might face in disclosing an attack. But with careful drafting, many of the most common concerns associated with disclosure can be minimized. And, in our judgment, those concerns are often outweighed by the dangers of remaining silent for three key reasons.

First, companies don't need to disclose sensitive operational details that would further compromise cybersecurity or encourage other hackers to exploit the vulnerability. Indeed, the SEC's guidance emphasized that "the federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity."

For instance, one technology company disclosed that it "regularly face[s] attempts by others to gain unauthorized access through the Internet to [its] information technology systems" and that "[t]hese attempts … are sometimes successful. One recent and sophisticated incident occurred in January 2010 around the same time as the recently publicized security incident reported by [another company]." It provided no further specific details about how the attack was accomplished.

In another case, after receiving a comment letter directing it to disclose past attacks, a large Silicon Valley company discussed the risks of cyberattacks generally and disclosed, specifically, that it experienced "cyberattacks of varying degrees on a regular basis, and as a result, unauthorized parties have obtained, and may in the future obtain, access to [its] data or [its] users' or customers' data." Tellingly, it did not say when the cyberattacks occurred or share the breadth of the data that was compromised.

Additionally, the online merchant referenced above disclosed a past attack by stating that "[s]ome subsidiaries had past security breaches, and, although they did not have a material adverse effect on our operating results, there can be no assurance of a similar result in the future."

Disclosures such as these — which merely note that a breach occurred — aren't telling sophisticated hackers anything that they don't already know. Indeed, in 2011, Dmitri Alperovitch, then-Vice President of McAfee, wrote that the entire set of Fortune Global 2,000 firms could be divided into two categories: "those that know they've been compromised and those that don't yet know."

Of course, before filing any disclosures, registrants should ask their top IT professionals to review the proposed language to confirm that the disclosures do not inadvertently reveal information that could lead to further breaches.

Second, nervous executives should be reassured that, although the business risks of experiencing a cyberattack may be increasing, the business risks of disclosing an attack are decreasing. The stigma of being a cyberattack victim is rapidly fading. Some of the most sophisticated organizations in the world — in every industry — have seen their systems compromised in recent years. Companies that disclose a cybersecurity failure are not admitting incompetence. They are joining distinguished — albeit, unfortunate — company. Moreover, the risks of a future attack should increasingly be built-in to the share price of all companies, including those that have not yet disclosed a breach.

Third, and perhaps most significant, it is highly likely the SEC will soon be looking to set a precedent that will encourage others to disclose cyberattacks, even potentially small ones. Any company disinclined to serve as a cautionary tale would be wise consult closely with securities lawyers about not only how to disclose the risks of future cyberattacks, but also whether and how to tell investors about and the occurrence and effects of known attacks — significant or otherwise.

Michael Mugmon *is a partner in WilmerHale's Palo Alto office, and one of the Daily Journal's "Top 20 Under 40."* **Joel Fleming** *is an associate in WilmerHale's Boston office. Both are members of the firm's Securities Department. Their practices focus on complex commercial litigation, securities litigation, government enforcement actions, and investigations. Mr. Mugmon may be reached at (650) 858-6103 or Michael.Mugmon@WilmerHale.com. Mr. Fleming may be reached at (617) 526-6929 or Joel.Fleming@WilmerHale.com.*


MICHAEL MUGMON
WilmerHale


JOEL FLEMING
WilmerHale