The New York Times
NYTIMES.COM
"All the News That's Fit to Print" Monday, March 5, 2018 Reprinted With Permission

ANOTHER VIEW | BY CRAIG A. NEWMAN

When to Report a Cyberattack? For Companies, That's Still a Dilemma

It has been seven years since the Securities and Exchange Commission first advised public companies to tell investors if they had suffered a cyberattack deemed to be material. But even with the rising number of severe hacks, only a few companies report incidents each year to the S.E.C.

Now the S.E.C. has issued updated cybersecurity guidance. Again, it warned public companies to make "timely" disclosure, recognizing the "grave threat" that cybercrime poses to investors and the capital markets.

Yet, the S.E.C.'s new guidance doesn't confront the practical quandary facing public companies victimized by a cyberattack: Going public with news of a cyberattack isn't always an easy call. Doing so can risk tipping off the bad guys and imperil investigations. Law enforcement often encourages, or even demands, that the incident not be disclosed. At the same time, companies know they have a duty to their investors to provide prompt information about any real risks to their businesses.

This tension between the need for discreet cooperation with law enforcement and the obligation to inform investors and the markets creates a dilemma for public companies. Unfortunately, the commission's updated guidance provides little direction to corporate leaders confronting these conflicting demands. While the guidance acknowledges that it will often take time to "discern the implications" of a breach and that it "may be necessary to cooperate" with law enforcement, it concludes that an active investigation would not "on its own" be a reason to avoid disclosure of a material cybersecurity incident.

Perhaps this dilemma explains why so few public companies report breaches. In 2017, only 24 companies reported breaches to the S.E.C., according to Audit Analytics, a firm that tracks securities law filings. Since 2011, when the S.E.C. issued its initial cyber guidance, only 106 companies have reported incidents to the S.E.C.

But during that same period, there were 4,732 cyberattacks on American businesses, researchers for the Privacy Rights Clearinghouse found. While a proportion of those were private companies, it's unlikely that public companies suffered only 106 breaches that were material in that time.

The S.E.C. has investigated tardy data breach disclosures but has yet to bring an enforcement action against a company that failed to disclose an incident. The agency is investigating Yahoo's two data breaches in 2013 and 2014, which the company did not disclose until 2016 even though information on three billion users was compromised. Equifax, too, has acknowledged that the S.E.C. is looking into the theft of Social Security numbers, license numbers, addresses and dates of birth for nearly 145.5 million Americans. The breach was detected in July but not disclosed to the S.E.C. and investors until September.

Where does that leave public companies that have been hacked?

The solution is not simple. Some say the S.E.C. should adopt a regulation giving companies a "pass" from public disclosure obligations if they refer the matter to law enforcement. But such a rule could easily be abused by corporations that have a big incentive to hush up attacks. They could easily make a halfhearted referral to law enforcement and then use it as a smoke screen to avoid a potentially devastating disclosure.

Even companies trying to do the right thing are stuck. They might report an attack to law enforcement, and then hear nothing for weeks or months, in part because there is not enough staff to investigate all of these hacks. At some point, a company will have to conclude that its duty to investors overrides its responsibility as a good corporate citizen to comply with requests for discretion.

Even when a breach is disclosed, it's difficult for companies to support the needs of law enforcement. Companies face irate money managers and investment advisers, who are duty-bound to ask tough questions about their investments. Without getting straight and candid answers to those tough questions, they lose the ability to monitor their investments and, indeed, risk watching their investments lose critical value without visibility into what actually happened.

Perhaps this conflict is fundamentally irreconcilable. But with stakes so important given the increasingly sophisticated threats posed by cybercrime to corporate America, we should view the S.E.C.'s new guidance as a starting point and collective opportunity to figure this out.