Three Ways to Stay Ahead of the SEC Cyberthreat Disclosure Mandate

by Joshua Gold

For senior management, directors and officers (D&O) insurance understandably has an importance like no other policy in the company's portfolio. Given the staggering number of data security breaches revealed in recent months, that self-protective instinct must also include ensuring that management is covered against cyberthreats. No company is immune-even computer security firms and government agencies working on top secret projects have been hit.

The SEC has stepped up to mandate that related disclosures must be made in securities filings. Now, every company under the watchful eye of the agency must disclose its analysis of exposure to a data breach or attack, discussion of material cyber-incidents, description of related legal proceedings and the implications for the firm's financials.

The SEC has thus elevated cyberthreats from risk management, legal and IT to the corporate suite. This will entail far greater scrutiny from investors to what is disclosed and the quality of the disclosure-all of which will be judged with 20/20 hindsight after a breach occurs. D&O underwriters will accordingly find new interest in their customers' cybersecurity awareness and preventive measures, and will likely add new or more tailored questions concerning both past cyber-incidents and present plans for curtailing or preventing data breaches. And they will expect answers.

As with any insurance application, it is imperative to answer these applications carefully. Policyholders should be aware that some insurance applications are purposefully designed to ask overly broad questions that end up as nothing more than a snare and potential coverage fight. Policyholders should therefore prepare for negotiation over the terms of the insurance application.

It is critical to ensure that D&O coverage will be available should a cyber-related lawsuit target management. This will help defray the defense and indemnity costs involved. And added care must go into reviewing all D&O insurance policy terms and endorsements (including those contained in the primary, excess layer and Side A policy forms). It is likely that some insurance companies will try to insert exclusions into D&O policies akin to those inserted into many specialty internet policies. Many of these terms are vague and may lead to disagreements over their effect on the scope of insurance coverage for a cyber-related claim.

There are three steps that will help any company lower its exposure.

1. Beyond D&O insurance issues, companies should also have an overall cyber risk management game plan that draws from a wide range of departments including treasury, risk management, legal, IT and at least some senior managers. One key step is to build a computer infrastructure with up-to-date security to guard against hackers, malware and viruses. Plaintiffs, regulators and insurance companies often seize on accusations that a business used obsolete or ineffectual security measures to guard against unauthorized data access events.

2. To the extent that a business entrusts data management or hosting to a vendor (e.g., via cloud computing), the business should disclose this fact to its customers, partners, suppliers and other parties with which it may transmit or share data. While such disclosures may not be mandatory, they can go a long way toward nullifying certain legal accusations. Also, companies should undertake - and document - due diligence measures regarding the security employed by the company that is providing the data hosting or management. Demonstrate and make a record that your business has been judicious in its entrustment of data to an offsite business.

3. When cloud computing firms are utilized, make sure that the contractual agreements expressly set forth the level of indemnity and "hold harmless" protection that the cloud company will provide should the entrusted data be hacked. Insist also on representations and warranties regarding the level of security employed by the cloud firm to protect the entrusted data against hacks from outsiders, other cloud customers and even improper internal access of data from within other segments of the cloud computing firm.

Advance planning and analysis will ease the burden of navigating the SEC's new pronouncements on data security threats. It will also prepare the company, should a hacking incident occur, to cope with state notice laws, shareholder litigation and inquiries, and potential lawsuits from government authorities including the SEC, FTC and state attorney generals. ■

Joshua Gold *is a shareholder in the New York office of the law firm of Anderson Kill & Olick, P.C. and regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property insurance coverage issues.*