Board iQ
A Financial Times Service

Opinion

How To Get Assurance on Cyber Insurance

January 30, 2018

Timothy Sullivan is asset management industry leader and Rob Yellen is D&O and fiduciary product leader at Willis Towers Watson.

The asset management industry is intensely focused on cyber security, an issue that has caught the attention of regulators and investors alike. With money and reputations on the line, these stakeholders are looking closely at steps senior management and fund directors can take to minimize harm from a data breach.

Rob Yellen and Timothy Sullivan

It's no wonder cyber security continues to be one of the top risk-management issues facing mutual fund boards today. Given that it is impossible to completely eliminate the risk of loss resulting from a cyber attack, directors must understand the relevant insurance policies that mutual fund boards can use to protect themselves.

There are typically two types of fund insurance policies that cover a cyber attack: cyber insurance, and policies that blend directors and officers and errors and omissions liability policies.

Below is a look at what fund boards should consider when reviewing each of these insurance programs.

Cyber Insurance

A comprehensive cyber insurance product includes both first-party and third-party coverages.

First-party coverage handles losses that the fund incurs when responding to a cyber attack. This may include costs of notifying affected individuals, the direct losses incurred because of the interruption of the computer system, or situations where attackers demand money in exchange for stolen data.

Third-party coverage applies to the liability that mutual funds and their boards may have resulting from a data breach. This would include, for example, claims brought by investors alleging they suffered a loss as a direct result of a data breach.

Mutual funds often seek cyber insurance coverage under the sponsoring investment adviser's policy. In these circumstances, the insurance policy may need to be amended so that the fund is fully, and expressly, covered without sacrificing its ability to bring a claim against the adviser.

When reviewing the cyber insurance coverage afforded to funds, directors should inquire about the breadth and scope of coverage available. Some questions include:

- Does the policy contain both first-party and third-party coverage?
- Are there any other policies that the fund currently holds that have overlapping coverage?
- Are the costs of responding to a data breach covered under the policy? Does the board have the flexibility to choose vendors?
- What are the key exclusions, notice provisions and coverage triggers?
- Is the fund required to be explicitly listed on the policy? If so, is the list updated at each renewal?

D&O/E&O Policies

Mutual funds typically maintain a liability policy that blends the two types. The D&O component of the policy is intended to respond to third-party management liability claims made against directors, officers and others (including some affiliated entities, employees and independent contractors).

The E&O component of the policy is intended to respond to third-party claims alleging errors and/or omissions in the performance of, or failure to perform, professional services.

A potential cyber-related D&O/E&O claim made against a mutual fund board could include allegations from investors that the board failed to conduct adequate IT or cyber-security cultural due diligence on, or supervision of, the fund's service providers.

Historically, D&O policies have handled exposures from cyber claims without much modification needed. However, war and terrorism exclusions can limit coverage for cyber attacks attributed to hacktivists, governments or quasi-governmental groups. Some insurance carriers are adding cyber exclusions. Others may plan to rely on exclusions relating to privacy or advertising.

When reviewing their D&O/E&O insurance coverage, fund directors should understand the implications of any exclusionary language relating to cyber security, terrorism or breaches of privacy. Ideally, the coverage should not have those exclusions at all. If the exclusion cannot be removed, directors should aim to ensure it is aligned with the coverage intended to be purchased. There may be an additional cost associated with the modification.

Some insurers are willing to include a specific cyber extension to their D&O/E&O policies. Such extensions, however, are more limited in scope than separate cyber policies that are available in the insurance market.

One Claim, Two Policies

It is possible that a cyber attack can be covered under both the cyber and D&O/E&O policies. For example, a data breach could cause the fund's computer systems to crash, resulting in a first-party loss under the cyber policy. The same event could then prompt harmed investors to bring claims against the fund board for failing to properly oversee its third-party service providers.

It is therefore important for boards to understand how such policies interact with each other and what steps can be taken to mitigate possible conflicts between both programs. For example, if two different insurers handle the cyber and D&O/E&O policies, would one firm be willing to cover both programs at a lower rate or with better terms? If so, this would mitigate the risk of potential finger pointing between two different insurers if one claim triggers both policies.

Understanding the interplay of these coverages is critical and will lessen the risk of confusion. Though not all encompassing, the steps outlined above should assist fund boards in navigating the ever-evolving cyber-risk landscape.