Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Protecting Employee Benefit Plans With Cyber Insurance

By **Laura Fischer** (July 18, 2018, 3:19 PM EDT)

Laura Fischer

Broadcast news and other media reports have been flooded with instances of cyberattacks, impacting thousands of people and costing millions of dollars.

Corporate employees have been inundated with training and alerts designed to help them identify and avoid email fraud, phishing attempts and myriad computer viruses. Some have even had the misfortune (and embarrassment) of clicking on that video link or responding to a plea to save a royal in need.

Hackers are in the business of stealing and selling confidential information. Malware and viruses are in the business of immobilizing computer systems, delivering a devastating blow to technology-dependent businesses, and individuals.

Cyberattacks have managed to invade all walks of life, and employee benefit plans are no exception.

Employee benefit plans rely on a variety of service providers to administer benefits. Those providers maintain a plethora of participant data and protect plan assets for the benefit of participants. When a plan is attacked, the fallout can be overwhelmingly expensive and burdensome to correct.

So what is a plan sponsor to do? Many are purchasing cyber liability insurance coverage to supplement their data security measures. Understanding those policies — and their exclusions — is important for sponsors who are exploring such coverage.

What's at Risk?

Because many plans maintain both personally identifiable information and protected health information, a cyber breach can impact employee and participant data, including social security numbers, dates of birth, dates of hire, compensation and level of benefits.

In the case of a health plan, a breach may involve information regarding medical coverage and claims. In the case of a retirement plan, plan account balances and account numbers may be impacted.

Because of this, cyber liability insurance can be an option to help avoid a costly payout in the unfortunate instance of a breach.

What Protection is Provided?

Typical cyber liability insurance policies may cover breach response costs (including notification requirements), regulatory fines and penalties, social engineering fraud, wire transfer fraud and various other types of liability.

Even when a plan has managed to mitigate and respond to a breach to the best of its ability, additional liability may exist in the form of regulatory penalties or participant lawsuits. In order to best protect the plan, it is important to secure a policy with both first-party and third-party coverage.

First-party coverage is typically triggered upon a data breach. It is designed to address response and recovery. This may include assistance with required notifications to affected participants as well as mitigation of damage following the breach and improper disclosure of confidential information.

Third-party coverage is triggered upon the filing of a lawsuit or similar claim against the plan. It may provide coverage for the cost of defense and the amount of any settlement or judgment, legal fees, forensic investigation and credit monitoring services.

Is it Worth the Cost?

Often, yes. Cyberattacks are increasing in volume, and security breaches are expensive.

The extent of the damage is often unknown until it is too late. Employee benefit plans are required by the Employee Retirement Income Security Act to use plan assets for the benefit of participants and various federal and state laws, including the Health Insurance Portability and Accountability Act, to protect and maintain the security and confidentiality of participants' information, require them. Therefore, it is generally appropriate for plan sponsors to purchase cyber liability coverage to protect plan assets and participant data.

Is it Duplicative?

Maybe. But, it is also likely that a plan sponsor's fiduciary liability insurance policy will not cover the types of claims addressed by a cyber liability policy. Similarly, a plan's third party vendors may have general liability coverage and errors and omissions policies, but without a specific cyber liability policy, claims for cyberattacks and data breaches might not be covered.

What's the Catch?

Notably, many policies vest the decision to retain legal counsel in the insurer, rather than the policyholder. Plan sponsors that prefer to utilize their own plan counsel in the event of a data breach or other cyber security incident should keep an eye out for provisions regarding the selection of counsel and consider whether that term is worth negotiating with the carrier.

Cyber liability policies also may have exclusions for certain types of claims, or exclusions for all claims where it can be shown that the plan failed to maintain appropriate firewalls and safeguards, update malware prevention and anti-virus software, impose strict requirements for passwords, and store and transmit data with appropriate encryption.

Review the policy terms carefully with the plan's legal counsel and plan professionals and be sure to

take all reasonable steps to ensure the safety and protection of the plan's data.

Best Practices

Plan sponsors should ensure that their employee benefit plans have as many levels of protection as possible, including fiduciary liability insurance, fidelity bonds and cyber liability insurance.

Work with the plan's professionals to determine the appropriate levels of coverage for each plan. Consider a cyber liability policy with both first- and third- party coverage.

In addition to securing the appropriate amount and level of cyber liability insurance, plan sponsors should adopt policies and procedures to protect participant information and plan assets and to mitigate the fallout in the event of a breach. These practices will also help to ensure the cyber liability policy will not exclude any claims.

Plan sponsors should also identify the plan's service providers who have access to PII and PHI and ensure that the plan's cyber liability policy covers those providers, or that those providers have their own cyber liability policies. Before contracting with a new service provider, inquire about the provider's level of coverage and whether they maintain a specific cyber liability policy.

Laura L. Fischer is a partner at Spencer Fane LLP.