October 31, 2018

Mitigating the Risk of Cyber Attacks to Your Employee Benefit Plan

CYBERSECURITY, ERISA
BY SCHNEIDER DOWNS PROFESSIONAL

From Target to Equifax to the federal government, it seems that a new cybersecurity breach makes headlines on an almost daily basis. With all these breeches, an attack on your employee benefit plan seems inevitable.

Cybersecurity risks, such as phishing techniques, malware and ransomware attacks, facing employee benefit plans are no different than those facing corporations, and in fact, may be even more significant. Why is this you may ask? Well the answer is two-fold.

First, in addition to the plan assets being susceptible to theft, there are two potentially far more valuable pieces of data that hackers may be after; personally identifiable information (PII) and electronic protected health information (EPHI).

With PII and EPHI, hackers may be able to, among other things, open accounts, falsify insurance claims, file fraudulent tax returns and even create new identifies. Unlike credit cards, this information may be used over longer periods of time and can even be sold to other criminals.

Secondly, the nature of how employee benefit plans operate, that is, in an almost completely electronic environment, make them more susceptible to cyberattacks. The electronic environment, along with significant use of outside third-party service providers, who may have varying degrees of controls in place to address cyber risks, and the fact that often employee benefit plans fall outside of the corporation's cybersecurity plan can be a recipe for disaster.

As a plan sponsor and those charged with governance, you have a responsibility with respect to management and oversight of the plan, including understanding risks to the plan, even risks of cyberattacks.

Thinking that all is lost? Fear not, the Department of Labor in its Advisory Council Cybersecurity Report identified four areas of effective practices.

- Data management – protect and control data; and ensure that your employee benefit plans fall under the organization's cybersecurity policies
- Technology management – maintain up-to-date technology and perform routine scans for potential vulnerabilities
- Service provider management – understand the data security controls at your third-party service providers as well as their procedures in the event of a breach

- People management – properly train and manage your employees

Think you don't have the time to address these risks or that the cost is too much or that it couldn't happen to your plan? Consider the consequences of a cyberattack: significant costs to detect, investigate and remediate; theft of PII and/or online access resulting in monetary losses to participants, beneficiaries and the plan sponsor; loss of reputation and trust of employees; and potential fines and penalties resulting from HIPAA violations. According to a study performed by the Poneman Institute, the average cost of a malware attack is $2.4 million.

If you have concerns about cybersecurity for your employee benefit plan, remember that our firm houses the premier employee benefit plan audit practice in the region as well as one of the largest cybersecurity practices in Pittsburgh. Schneider Downs is well positioned to answer your questions and meet your organization's needs.

You've heard our thoughts… We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.