Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Employee Benefit Plan Cybersecurity
Are you doing enough?

John F. Matte, CPA Andrew J. Reading CPA May 2021

Published May 24, 2021 - Recently issued guidance from the Department of Labor and the AICPA provide best practices for plan management and plan fiduciaries to mitigate exposure to risk from an information security incident. In this recap, we've provided a summary of actions you should take immediately.

To watch our companion video presentation, please click here or visit www.dopkins.com/videos.

In April 2021, the Employee Benefits Security Administration of the U.S. Department of Labor (DOL) issued guidance on best practices for ERISA-covered plans - Cybersecurity Program Best Practices (dol.gov). The DOL begins that release by informing readers that "Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks". The DOL has acknowledged that this is an underserved area of cybersecurity, albeit one with tremendous risk due to large asset balances and personally-identifiable information that are inherent in this space. Along with that acknowledgement, there has been a noticeable increase in incidents, regulatory enforcement, claims and litigation, prompting the DOL and the American Institute of Certified Public Accountants (AICPA) to continue to issue guidance on the topic. Generally, they are finding plan sponsors do not have sufficient entity-wide programs or such programs omit certain pertinent aspects impacting employee benefit plans.

The AICPA has developed an entity-level "Cybersecurity Risk Management Framework" for the purpose of effectively documenting and communicating information regarding an entity's cybersecurity risk management program. Consistent with the messaging and timing of guidance released by the DOL, the AICPA recently recommended plan management consider utilizing this framework to assist in developing, designing, and/or documenting the plan sponsor's Cybersecurity Risk Management Program. Utilizing this framework is expected to:

a. Help plan management identify where the plan's cybersecurity processes and controls may need to be shored up;
b. Communicate information regarding the plan's Cybersecurity Risk Management Program to stakeholders, including plan fiduciaries and participants; and,
c. Document the actions and efforts undertaken by the plan sponsor in an effort to fulfill its fiduciary duty under ERISA. In short, the AICPA framework, if utilized properly, can meet the guidance and best practices recommended by the DOL.

KEY TAKEAWAYS: WHAT YOU SHOULD DO NOW

All plans and plan sponsors should consider working with professionals in the proper fields to build a cybersecurity program that fits their needs and their plan – attorneys, CPAs and cybersecurity experts. All

plans should have an understanding of where plan data is stored, who has access to it and how it is transferred. According to the DOL, plan sponsors should also have a "formal, well documented cybersecurity program" that identifies internal and external cybersecurity risks. If you, as plan management or a plan fiduciary, step back and ask yourself, "what am I doing in this space?" and the answer is difficult to come by, you are likely not doing enough, exposing plan participants, the plan sponsor and yourself to risk.

For more information, please contact:

John F. Matte, CPA
jmatte@dopkins.com

Andrew J. Reading, CPA
areading@dopkins.com