Updates
February 01, 2022
2022 Cybersecurity Issues and Recommendations for ERISA Plan Fiduciaries

New cybersecurity developments and observations, including those relating to U.S. Department of Labor's (DOL) review of cybersecurity issues, warrant prompt consideration by plan sponsors and other fiduciaries of employee benefit plans subject to ERISA.

In our April 2021 update, we reported on the DOL's long-anticipated cybersecurity guidance applicable to both retirement and health and welfare plans. Though group health plan sponsors may be familiar with similar cybersecurity requirements imposed under HIPAA, the DOL's cybersecurity guidance (in the form of "best practices" and "tips") raise new considerations for retirement plans as well as welfare plans. These considerations are in addition to HIPAA data security requirements applicable to group health plans. Plan sponsors and fiduciaries should be attentive to the following concerns:

1. **The DOL's standard document request list for benefit plan reviews now includes a request for a cybersecurity policy.** It appears unlikely that a plan will receive a closing letter from the DOL without producing an existing or adopting a new cybersecurity policy. This has been our experience to date, even though plan sponsors and fiduciaries can take the position that the DOL's cybersecurity guidance is framed as an agency recommendation of best practices and that a cybersecurity policy is not required by ERISA.

   Recommendation: Consider adopting a cybersecurity policy applicable to all benefit plans subject to ERISA (i.e., within the purview of the DOL's investigative authority). This cybersecurity policy can take the form of a standalone policy document specific to the ERISA benefit plans or it may be addressed in existing corporate cybersecurity policies (noting that some revision may be needed to fully address the DOL's cybersecurity guidance).
2. **Benefit plans are increasingly being targeted by cyberattacks.** Benefit plans are increasingly viewed as lucrative targets for cyber criminals, given the almost $9.3 trillion in plan assets held in retirement accounts systemwide and the treasure trove of participant data maintained in online databases by plan sponsors, plan fiduciaries, third-party administrators, and recordkeepers for all plan types. Further,

increased electronic access to benefit portals by participants using internet-connected devices, including cell phones, laptops, and tablets, which suffer an average of 5,200 cyberattacks per month, makes it easier for bad actors to improperly access such benefit plan systems. Because it is a matter of not if—but when—a benefit plan will experience a cyberattack, plan sponsors and fiduciaries should be motivated to act promptly to implement the DOL's guidance despite its being framed as best practices.

Recommendation: Consider initiating a cybersecurity review and ongoing testing program to monitor their information and administrative systems and promptly remedy gaps that could lead to a cybersecurity breach if not addressed.

3. **Existing vendor services agreements may not sufficiently protect plan sponsors against the risk of cybersecurity issues.** Given the recency of the DOL's cybersecurity guidance, it is likely that many vendor services agreements entered into by plan sponsors with respect to their benefit plans do not adequately protect sponsors from DOL-specific cybersecurity risks. Except for those agreements specifically implicating HIPAA and specifically addressing cybersecurity issues in related Business Associate Agreements, vendor services agreements that do not specifically obligate vendors compliance with the DOL's cybersecurity guidance may limit liability and indemnity provisions, or related breach of contract claims, contained in the agreements in the event of a cybersecurity breach. Further, because vendor services agreements often carve out special and/or consequential damages, a general compliance with laws representation may not serve as a hook for indemnification purposes in the event of a cybersecurity breach, as breach-related damages are often considered special and/or consequential.

   Recommendation: Consider reviewing existing vendor services agreements and either renegotiate the terms of such agreements to include cybersecurity representations and other terms (specifically referencing the DOL's cybersecurity guidance) or, if the preference is to wait until an upcoming renewal, negotiate the addition of a data privacy and security addendum until appropriate cybersecurity terms can be incorporated into the main agreement as part of renewal negotiations.

4. **Existing cybersecurity liability insurance policies may not cover breaches involving benefit plans.** Plan sponsors often procure either standalone cybersecurity liability insurance policies or riders to broader commercial liability coverage. However, policies that list the plan sponsor as the insured party might not cover cybersecurity breaches affecting benefit plans or plan fiduciaries, even if the plan sponsor is financially responsible for related damages. Further, cybersecurity liability insurers may have another argument against covering damages arising out of a breach if the plan sponsor or fiduciary has failed to implement adequate controls and safeguards to protect benefit plan assets and participant data against common cybersecurity threats, or has failed to conduct required tabletop exercises ensuring such safeguards are adequate.

   Recommendation: Consider reviewing existing cybersecurity liability insurance policies to confirm whether their benefit plans and plan fiduciaries, in addition to plan sponsors, would be covered in the event of a breach, and review policy compliance requirements. If not, we recommend that plan sponsors considering procuring additional, appropriate cybersecurity liability coverage.

The above recommendations are general considerations for plan sponsors and fiduciaries, which will need to be weighed against existing cybersecurity programs and safeguards to arrive at appropriate responses. While strategy will vary, it is important that plan sponsors and fiduciaries evaluate and appropriately respond to the DOL's cybersecurity guidance and related issues proactively and not wait until applicable ERISA benefit plans become the victim of a cybersecurity breach or the subject of a DOL review.

Authors

Explore more in

Employee Benefits & Executive Compensation Labor & Employment Privacy & Security Corporate Governance Public Companies Capital Markets

Related insights

Update

The FY 2025 National Defense Authorization Act: What's New for Defense Contractors

Update

January Tip of the Month: Trump Executive Orders Challenge DEI Programs