2022 Advisory Council on Employee Welfare and Pension Benefit Plans

Cybersecurity Insurance and Employee Benefit Plans

Issue Chair: Glenn Butash
Issue Vice-Chair: Alice Palmer
Drafting Team: Beth Halberstadt, John Harney, Ed Schwartz, Holly Verdeyen

Concerns regarding cyber-attacks, cyber theft and the need for strong cybersecurity measures continue to grow in prominence. The 2022 Advisory Council intends to examine the role that cybersecurity insurance plays in addressing cybersecurity risks for employee benefit plans.

The Council intends to build on prior Council reports focused on privacy and security issues (2011) and cybersecurity for retirement plans (2016). In 2011, the Council addressed whether it is a fiduciary's duty to reduce the risk of personal employee information being disclosed to unauthorized persons. In 2016, the Council expanded on its 2011 work and focused on cybersecurity issues and employee benefit plans. The 2016 Council produced suggested materials for plan sponsors, fiduciaries and service providers to utilize when developing a cybersecurity strategy and program. The Council also recommended to the Secretary of Labor that the Department of Labor raise awareness about cybersecurity risks and the key elements for developing a cybersecurity strategy specifically focused on employee benefit plans.

In 2021, the Employee Benefits Security Administration published sub-regulatory guidance for plan sponsors, plan fiduciaries, recordkeepers and plan participants regarding cybersecurity.[*] The guidance included tips for plan sponsors/fiduciaries for hiring service providers that have strong cybersecurity practices, a list of "best practices" for use by recordkeepers and other service providers, and a description of online security practices for use by plan participants.

The 2022 Advisory Council hopes first to gain an understanding of cybersecurity insurers and the current market for cybersecurity insurance. This will include learning about insurers that are writing cybersecurity insurance coverage, the underwriting standards that insurers use for such insurance, and controls that insurers require or recommend that insureds have in place as a condition to underwriting coverage for cybersecurity risk.

The Council also intends to investigate the terms of typical cybersecurity insurance policies, including who are the "named insureds," what risks (and losses) are

[*] https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity (accessed June 23, 2022).

covered, exclusions from coverage, the cost of such insurance, limits of liability and deductibles, and the circumstances that could result in a loss of coverage.

The Council also hopes to gain an understanding of the views of plan administrators (including the trustees of multiemployer plans) with regard to cybersecurity insurance. This is expected to include exploring the prevalence of benefit-plan coverage, whether (for single-employer plans) coverage is part of corporate insurance policies or whether it is specific to the benefit plan(s), whether coverage is part of the administrators' or trustees' fiduciary liability insurance coverage, the extent to which plan assets are or could be used to pay for cybersecurity insurance coverage, due diligence activities that responsible plan fiduciaries undertake when selecting insurers (including the role of insurance company ratings and the implications of state guarantee association protections), activities undertaken to compare policies and coverage, and issues surrounding the renewal of insurance.

Finally, the Council intends to explore the interplay between a plan's existing "cyber-hygiene" practices and the availability (and cost) of cybersecurity insurance coverage.

The Council does not intend, at least at the outset of its work, to limit its focus to insurance as it relates to individual account/defined contribution plans. Rather, the Council intends to look at the insurance topic as it relates to all types of benefit plans--not only defined contribution and defined benefit pension plans but also group health and other welfare benefit plans. Additionally, the Council does not intend to focus on insurance coverage that service providers (e.g., recordkeepers, asset custodians) might have as part of their business with respect to employee benefit plans. Rather, the focus will be on coverage for the plan itself. Finally, the Council does not intend to explore various "reimbursement" policies that plans (or plan service providers) might have or offer to participants to compensate for losses due to cyber-incidents/cyber-theft.

The ultimate goal of the 2022 Council is share what we learn with the public and the Department, to call out any "best practices" identified, and make recommendations to the Secretary.