Published on *The National Law Review* https://natlawreview.com

Cybersecurity Risks to Employee Benefit Plans - Are You Prepared?

Article By:

Belinda S. Morgan

Unless you've been living on a remote mountaintop or inside a cave for the past 10 years, chances are good you've either been affected by a cybersecurity breach or know someone who has. Among many other businesses, recent cybersecurity breaches have affected large retailers and bankers, internet providers, and even the U.S. government. The 2017 breach of Equifax (one of the largest credit bureaus in the U.S.) left the names, Social Security Numbers, birthdates and addresses of more than 140 million Americans exposed to hackers.

Cybersecurity Threats to Employee Benefit Plans and Service Providers. In light of the high cost of a cybersecurity breach – including not only financial costs, but also potential damage to a business' reputation – most companies have strengthened their overall cybersecurity protocols. They may not, however, have fully considered the threat hackers pose to participant data collected for their employee benefit plans.

Hackers have recently targeted benefit plans and plan service providers (such as third-party administrators, record keepers, trustees, etc.), viewing them as valuable targets due to the participant data they must maintain. Plans and service providers have fallen victim to schemes to steal participant data, fraudulent transfers of participant assets (through direct transfers and fraudulent plan loans), and ransomware attacks. Even though only a relatively small number of such attacks have occurred (so far), they have resulted in millions of dollars in losses.

Duty to Protect Participant Data. The Employee Retirement Income Security Act of 1974, as amended (ERISA), doesn't currently require plan sponsors to safeguard participants' personally identifiable information (though that may one day change). Even without a specific statutory or regulatory requirement to protect such data, however, ERISA Section 404 still requires benefit plan sponsors and other fiduciaries to administer their plans for the exclusive benefit of plan participants and beneficiaries, and with the "care, skill, prudence, and diligence under the circumstances that a prudent man acting in a like capacity and familiar with such matters would use." That likely includes protecting participants' personal information.

ERISA Advisory Council Recommendations. The ERISA Advisory Council (the Advisory Council), a committee that advises the Department of Labor on ERISA matters, has been concerned about

cybersecurity risks to employee benefit plans for several years. In its 2016 report discussing those risks, the Advisory Council advised plan sponsors to adopt procedures for: (i) understanding what data might be subject to cyberattacks; (ii) responding to cyberattacks; and (iii) recovering from cyberattacks. The Advisory Council stressed the need for plan sponsors to thoroughly vet their service providers and to negotiate contract provisions to lower or mitigate the costs of correcting a possible cyberattack on a plan. Finally, the Advisory Council encouraged plan sponsors to review and understand the limitations of their business insurance coverage, and consider cyber insurance to address possible coverage gaps.

As part of their ERISA duty to monitor plan service providers, plan sponsors must understand how their service providers store and protect the participant data they handle. Plan sponsors should also understand the providers' procedures for breach notification, including any obligations they may have to notify participants or governmental authorities. Plan sponsors can glean this information from reviewing the agreements with their benefit plan providers and from discussions with those providers.

If (or more likely, when) a cybersecurity breach occurs, plan sponsors should have a plan in place for addressing the breach. It should include procedures for how the sponsor, likely working with its service providers, will communicate with plan participants who may be anxious about the breach and protecting their data. Sponsors should also have a process for determining how a breach will be corrected and what remedies will be used. Sponsors should document both their overall process for responding to cybersecurity breaches and any steps they take in correcting an actual breach. This will help show that they acted prudently in the face of the breach.

When implementing a cybersecurity risk management strategy, plan sponsors should remember that one size does not fit all. The sponsor's approach will depend on its own circumstances, balancing the need to protect plan participant data and the sponsor's own business needs. For instance, rather than adopting a completely new cybersecurity policy for its benefit plans, a sponsor might "piggyback" that policy onto the sponsor's general cybersecurity policies.

Given the growing cybersecurity risks to employee benefit plan participant data, plan sponsors should have procedures and policies in place to protect that data, and should be prepared to quickly respond to and resolve any breaches that may occur.

© 2025 Foley & Lardner LLP

National Law Review, Volume VII, Number 352

Source URL:https://natlawreview.com/article/cybersecurity-risks-to-employee-benefit-plans-are-you-prepared