WINSTON & STRAWN LLP

ARTICLE

Cybersecurity and Employee Benefit Plans: What Prudent Steps Should a Fiduciary Take?

SPRING 2018

Reprinted with permission from Benefits Law Journal. *Any opinions in this article are not those of Winston & Strawn or its clients. The opinions in this article are the authors' opinions only.*

Many issues keep fiduciaries of employee benefit plans awake at night, but cybersecurity is especially troubling for many reasons. Employee benefit plans face significant cybersecurity threats and, given the incredibly significant amount of assets involved, the consequences of even one single attack can be devastating. Further, a plan fiduciary can have the best cybersecurity procedures in place, and yet the plan or a plan participant can still experience a cyber breach because of the numerous interfaces. Specifically, retirement plans, 401(k) plans, and 403(b) plans are typically administered by numerous parties. In addition to the plan sponsor, there is typically a trustee and a plan administrator (recordkeeper). Health and welfare plans have insurers or third-party administrators, a custodian or trustee (sometimes), and the plan sponsor. Participants can log into benefit portals through their home, phone, and/or work computers.

These numerous interfaces each provide potential entryways for cybercriminals. A diligent plan fiduciary may wonder what it can do to prevent such a cyber breach. There are numerous nonprofit, industry sector, and government resources that can assist a fiduciary in understanding best practices in securing employee benefit plan data.

1 Min Read

Related Locations

Chicago | Houston

Related Topics

Cyber Security | Employee Benefits | Retirement | Retirement Plans | 401(k)

Related Capabilities

Privacy & Data Security | Employee Benefits & Executive Compensation

Related Regions

North America

Related Professionals

Amy Gordon

Joseph S. Adams