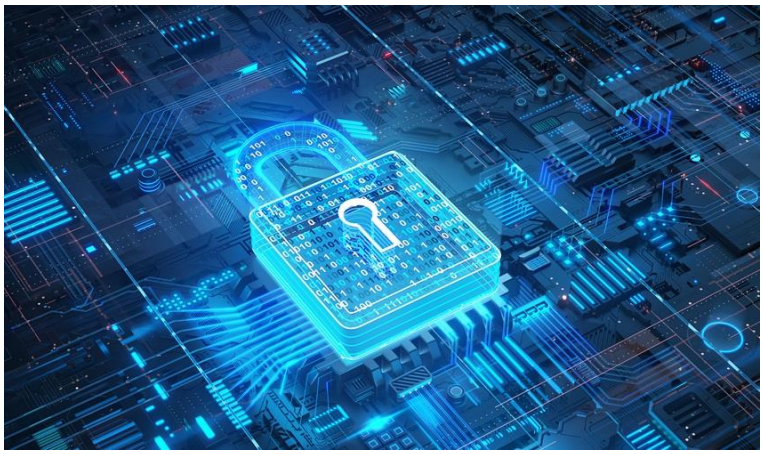
Fiduciary Pension Partners

Cybersecurity and How to Deal with Data Breaches as a Plan Sponsor



Retirement funds are a target for cybersecurity attacks and identity fraud more than ever before. For most people, a retirement account is one of their biggest assets, yet they rarely check it, making these accounts a prime target for cybercriminals. Data breaches with recordkeepers are common. Last month, a data breach at a large financial institution leaked the information of over 1,800 participants in the Walmart 401(k) plan due to an employee's email error. Proper precautions can reduce the risk of similar incidents. Even with the best precautions in place, a data breach can still occur, and having an established response plan with your recordkeeper is key to minimizing the damages.

Participant education is a meaningful precaution sponsors can take to prevent security breaches. Cybersecurity defense relies on everyone, and educating plan participants about common scams and digital attacks helps prevent data leaks. Including updates on the latest cybercriminal attack methods in ongoing participant education can enhance digital safety moving forward. Plan sponsors should also ensure their recordkeepers use technologies like two-factor authentication apps that require photo ID verification at login or employ advanced facial recognition software to detect suspicious login attempts.

Plan sponsors should consider purchasing cybersecurity insurance as an additional precaution. For more information regarding cybersecurity insurance, please reach out to Fiduciary Pension Partners at info@fiduciarypp.com or (833)-FPP-401K. When evaluating this type of insurance, they need to determine liability in case of a breach, insured parties, the method of purchase, and the scope of coverage.

Despite these precautions, data breaches can still occur, so plan sponsors must establish a cybersecurity attack plan with their recordkeeper. When breaches do occur, sponsors should first collaborate with their IT department to isolate compromised systems and prevent further leaks. It’s crucial to identify the type of compromised data. If private

.

participant information leaks, prioritizing the safety of their accounts is essential. Increased surveillance of distributions in such situations is important to preventing theft. Finally, sponsors should craft a communication plan for affected customers in the event of a compromise.

By continuously updating security procedures and fostering a proactive approach to cybersecurity, plan sponsors can provide a strong defense against evolving threats. These efforts not only help prevent attacks but also establish confidence in plan participants regarding the protection of their digital assets. By staying prepared, the security of retirement funds can be effectively safeguarded, ensuring peace of mind for everyone involved.

Sources :

https://www.plansponsor.com/how-should-a-plan-sponsor-respond-to-a-data-breach/

https://www.bdo.com/insights/assurance/retirement-plans-cybersecurity-insights-for-plan-sponsors