Fiduciary Pension Partners

Protecting Benefit Plans from Cybersecurity Threats

Many plan sponsors focus on external cybersecurity threats, such as hackers attempting to breach their systems, but disgruntled employees can also pose a risk.

Recently, the Department of Labor (DOL) extended the scope of its cybersecurity guidelines to include all Employee Retirement Income Security Act (ERISA) plans, which include retirement, health, and welfare programs. This means that plan sponsors now have considerably more private information to safeguard.

Sean Fullerton, senior investment strategist at Allspring Global Investments, says that fortunately, most workers do not have direct access to sensitive data like participant account passwords or retirement funds, which are handled by recordkeepers and custodial banks. According to the Verizon 2022 Data Breach Investigations Report, internal threats make up about 20% of security breaches, making them less common than external cyberattacks. Jenny Eller, principal in Groom Law's retirement services practice, notes that in her 25 years of practice, she’s only encountered one case where an employee attempted to commit fraud by creating a fake account.

Nevertheless, certain employees, such as those in HR, IT, or treasury, may have access to sensitive plan information or personal data. However, there are ways to mitigate the risks posed by disgruntled employees.

Limiting Access. The Department of Labor advises plan sponsors to follow several best practices, one of which is restricting access to the plan administration. Sentinel Group's Julie Doran Stewart, head of fiduciary advice services, emphasizes the value of having written internal control procedures. These policies outline how HR or IT teams should deactivate employee access and how soon they should notify vendors of these changes. “If we have a client that doesn’t tell us that this happens, then we’re only as good as the information we have,” she says.

Sentinel ensures access points are routinely verified by conducting routine audits of who has access to the plans they manage. Fullerton also advises plan sponsors to review their service providers' information security standards to ensure comfort with how these organizations handle cybersecurity.

.

Fiduciary Pension Partners

To verify their cybersecurity practices, Doran Stewart advises submitting an annual due diligence questionnaire to advisors, recordkeepers, and third-party administrators, the questionnaire should specifically ask about access limits. “The Department of Labor obviously has made this a priority from a fiduciary governance perspective, so they are going to be looking for procedures and records related to that due diligence being done,” she says.

The threat of fraud increases with the number of people who have access to plan data, according to Tim Rouse, executive director of the SPARK Institute, which contributed to the development of several of the DOL's suggested cybersecurity procedures. At the advisor level, SPARK is cautious about allowing advisors too much access to participant accounts, including using tools like screen-scraping, which have the potential to be misused.

Leveraging Technology. Plan sponsors should encourage employees to log into their accounts regularly and use security features such as multi-factor authentication. This is particularly important following a change of recordkeepers because inactive accounts expose themselves to hackers. Stewart notes that while some participants might think that keeping their accounts unlogged keeps them secure, doing so actually makes it easier for malicious actors to access them.

There is also the potential for disgruntled employees at the sponsor level to embezzle funds before they reach participant accounts and internal controls, such as audits, can help prevent this, Rouse adds.

As an alternative to emailing spreadsheets for data transmission, SPARK is collaborating with a committee of third-party administrators to standardize file formats for Application Programming Interface (API) connectivity. Additionally, APIs are less susceptible to attackers.

Using detective controls to monitor data usage can help IT departments identify suspicious activity, such as logging in at odd hours or large data downloads, according to Lou Steinberg, founder and managing partner of CTM Insights LLC, a cybersecurity research firm.

Given that employee benefit plans can be accessed via phone, computer, or mobile apps, plan sponsors should ensure both their benefits and IT teams collaborate during vendor due diligence. “Those are two different skill sets … so keeping an open line of communication [about] how they can mutually assist each other … is important,” Doran Stewart concludes.

Sources:
https://www.plansponsor.com/insider-threats-are-disgruntled-employees-a-cybersecurity-risk/