BDO UNITED STATES

RETIREMENT PLAN SPONSORS: IS CYBERSECURITY PART OF YOUR FIDUCIARY DUTY?

July 2018

We've all received suspicious-looking emails asking us to provide personal information to redeem a prize that we've won or alerting us that someone we know needs financial help. By now, most of us recognize these scams—and don't open the email.

But what if the message looked like it was coming from an official, known source? Would you open an email you thought was coming from your 401(k) service provider or the sponsor of your retirement plan?

It's vitally important for plan sponsors to consider questions like these because retirement plans and the $28 trillion that they currently hold in the United States are major targets for cyber hackers. Cyber criminals are becoming increasingly sophisticated in targeting entities that manage vast amounts of assets and personal data—two characteristics inherent in retirement plans and their service providers.

Today, protecting stakeholders' data is no longer just an issue that information technology departments need to worry about. By law, fiduciaries to 401(k) and other retirement plans have a duty to act in the best interests of the participant—and protecting sensitive online information is part of that job.

Understanding the Threat

Communications about plan benefits contain significant amounts of personal data including: Social Security number, birth dates, home address, salary, password and general payroll information. Service providers to retirement plans store much of that material as well. As a fiduciary to the plan, the plan sponsor has a responsibility to make sure all that information—whether it is stored directly or by a third-party service provider—is kept safe.

Just as stolen identities are often used to hack credit card accounts, they can be used by criminals to access 401(k) and other retirement accounts. If cyber criminals gain access to the proper information about a participant, they may be able to trick an ill-prepared call center employee into releasing additional account information or making an unauthorized distribution, loan or transfer.

In many cases, security breaches will trigger state and federal fines for plan sponsors, as well as expose them and their service providers to lawsuits by participants. In addition to these legal costs and potential damage to the company's reputation, data breaches are extremely disruptive and time-consuming to deal with for plan sponsors, service providers and participants alike.

Recommendations for Plan Sponsors

While it's impossible for any organization to be completely bullet proof when it comes to cybersecurity, there are basic steps that plan sponsors can take to improve data protection strategies and limit the threat of an attack. The Department of Labor's Advisory Council on Employee Welfare and Pension Plans describes many of these practices in its report, Cybersecurity Considerations for Benefit Plans.

The report outlines cybersecurity issues that are specific to retirement plans and suggests that plan sponsors create a cybersecurity strategy that addresses the specific Plan concerns that complement the company's overall cybersecurity plan. The DOL's Advisory Council stressed that because each plan is unique, its cybersecurity management should be more than a checklist that simply mirrors language used across the industry. Instead, the cybersecurity plan should be tailored to the distinct characteristics of the benefit plan, its systems and its participants.

Before a breach happens, plans should have a risk management strategy in place. The DOL report identifies several considerations for plan sponsors as they develop their strategies, including:

- Establishing who is responsible for designing, documenting, implementing and maintaining the strategy
- Creating a process for eliminating unnecessary data to reduce cyber risks
- Evaluating service provider security programs and documenting how they will gain access to sensitive data
- Understanding current insurance coverage arrangements to determine whether additional protection is needed to adequately safeguard the plan sponsor and participants

Other organizations have developed initiatives that can help plans sponsors deal with cyber threats. The American Institute of Certified Public Accountants (AICPA) developed a cybersecurity risk management framework, SOC for Cybersecurity, to assist organizations as they communicate relevant and useful information about the effectiveness of their cybersecurity risk management programs. The AICPA also has created a Cybersecurity Resource Center to help organizations learn how to best protect data.

In September 2017, the SPARK Institute, an organization focused on strengthening U.S. retirement policy, issued its Industry Best Practice Data Security Reporting to help plan sponsors understand how record keepers should communicate—to plan consultants, clients and prospects—the full capabilities of their cybersecurity systems. In 2014, the National Institute of Standards and Technology created its Framework for Improving Critical Infrastructure Cybersecurity, setting guidelines to manage cyber risks.

BDO Insight: Start With the Basics—and Keep Customizing

Given the complexity and rapidly evolving nature of cybersecurity threats, developing a plan to address and mitigate these risks can feel extremely daunting for plan sponsors. But as with any challenging endeavor, knowing where to start is essential. Building on the DOL's recommendations above, BDO recommends that the following actions be part of a plan sponsor's cybersecurity efforts:

- Identify what information you manage that could be at risk
- Monitor what service providers are doing to address risks at their organizations
- Review existing frameworks and current industry developments through resources provided by the AICPA, SPARK, DOL and others
- Review the AICPA's SOC for Cybersecurity and ask service providers if they have adopted those practices
- Understand your organization's broader cybersecurity plan and identify ways it should be tailored to address the unique risks that retirement plans and participants face

These basic steps are just a starting point. It's critical to remember that every plan and every organization is unique. No checklist or set

of industry best practices will be sufficient in protecting your plan and your participants from the growing threat of data breaches.

BDO provides a range of cybersecurity services and solutions to help plan sponsors fulfill their fiduciary obligations in these areas, including: cyber risk assessment and security testing; cybersecurity strategy, policy and program design; and incident response planning. BDO can help you assess your plan's current needs and assist in implementing an appropriate cybersecurity strategy today.

CONTACT:

Lara Stanton
Assurance Director

Beth Lee Garner
Assurance Partner
National Practice Leader

PRINT OR SHARE

Subscribe to receive the latest BDO News and Insights

First Name*

Last Name*

Company*

Email Address*

Topics Of Interest

- Corporate Governance
- Business Services & Outsourcing
- CPE Webinars

- [ ] Technology
- [ ] Federal Tax

View All Available Topics

- [ ] Create a BDO Account to manage your subscriptions

SUBSCRIBE

BDO LOCATIONS

Select an Office Location

View Global Locations

Country: United States Change

Sitemap