Heartland Institute of FINANCIAL EDUCATION

Instructor's Tutelage

May 2017

Having financial knowledge for the future is essential, especially in today's ever changing financial market and economy. Now, more than ever, it is important to be thoroughly educated and balanced in your financial life. One of the best methods to reach this balance is through a comprehensive course that not only educates the participants but also encourages them to take action. These classes should cover everything from goal-setting and budgeting to risk management, college planning, tax and estate planning, and understanding all kinds of investments. This needs to include checklists on setting up files at home with information about what to keep, where to keep it, and how long to keep it. Everyone who attends should receive a workbook, and yes, homework, which will assist in helping them personally with a financial plan for the future.

How cybersecurity threats are affecting retirement plans

By Eugene S. Griggs 13 2017

The loss of employee personal information due to a cyber breach is an ever-increasing concern to all employers. After years of work to put into place protocols to comply with HIPAA's requirements on protected health information, the focus of plan sponsors and service providers now is broadening to include protection of employee information maintained in connection with other types of benefit plans, including retirement plans.

Retirement plan data — name, date of birth, address, Social Security number, compensation and other financial information — typically is maintained by the plan sponsor and provided to a plan record keeper and other plan service providers, And this information usually is sufficient to steal an employee's identity.

The cost of a cybersecurity breach, including detecting the extent of the break-in, recovering data and restoring systems integrity, can be substantial. In addition, an infiltration may trigger enforcement actions by governmental agencies, resulting in penalties arising under state or federal law, and potentially exposing the employer or plan service provider to civil claims under common law or various state statutes.

Regulatory structure

While there is no comprehensive federal regulatory scheme governing cybersecurity for retirement plans and their service providers, many state laws include breach notification and private rights of action for the unauthorized disclosure of protected personal information. Further, state attorney generals have been active in enforcing these laws in cyber breach cases.

In addition, existing guidance under ERISA already recognizes the risks associated with the electronic communication of plan

ISSUE GUIDE

How cybersecurity threats are affecting retirement plans (cont.)

information. Under DOL Regulation Section 2520.104b-1(c) (addressing the electronic distribution of plan information to participants) and DOL Technical Release No. 2011-03 (dealing with a secure continuously available website used to communicate information about participant-directed investment alternatives under a retirement plan), a plan sponsor has an obligation to ensure the electronic system used protects the confidentiality of personal information relating to the individual's accounts and benefits.

Whether cybersecurity is an ERISA fiduciary responsibility and whether ERISA preempts state cybersecurity laws, there remain important unanswered questions. A report on cybersecurity recently released by the DOL's ERISA Advisory Council provides extensive information to plan sponsors, fiduciaries and plan service providers on approaches for managing cybersecurity risks. It also highlights the need for additional clarification on the extent of plan sponsor and vendor responsibilities to protect participant information.

The report, however, includes the recommendation that plan sponsors and fiduciaries consider cybersecurity in safeguarding benefit plan data and assets and when making decisions to select or retain a plan service provider.

The Council, an influential body that advises DOL on issues under ERISA, has been studying benefit plan cybersecurity issues since 2011. While the report's recommendations do not have the force of law or regulation, in light of the broad scope of an ERISA fiduciary's obligation to act with prudence and the resources the Council has directed at this issue, this report may represent the foundation for future regulatory or statutory efforts addressing plan sponsor and vendor fiduciary responsibility for cybersecurity matters.

In addition, it could serve as a baseline standard-of-care in future tort actions by private plaintiffs.

Plan sponsor and fiduciary action steps

What should retirement plan sponsors and fiduciaries be doing now to address cybersecurity risks? They must develop, implement and maintain a retirement plan cybersecurity risk management strategy. The critical components of such a strategy may be divided into three broad categories: (1) development and maintenance of the strategy, (2) management of third-party risks, and (3) evaluation of enterprise and plan-specific insurance coverages and consideration of whether specialized cybersecurity insurance should play a role in the strategy.

1. Development and maintenance of a cybersecurity risk management strategy

- Consider a framework on which to base the strategy. Possibilities include the NIST framework, SAFETY Act, and industry-based initiatives, including SPARK Institute and the AICPA. In most cases, retirement plan cybersecurity risk management ideally is integrated with the cybersecurity strategy of the entity's core business.
- Own the strategy. Identify and document who has what responsibilities for strategy implementation and updating within the organization.
- Understand the data. What is it, what is it used for, where is it stored? How is data accessed? Is access properly controlled and limited to those

personnel who need access? When and how is data encrypted? Is the data collected limited to only what is minimally required? What data needs to be retained and when should it be destroyed?

- Consider whether an external certification, such as an AICPA Service Organization Control 2 (SOC2) report, is an appropriate measure to enhance security compliance and streamline testing procedures. Determine the frequency and type of systems testing, which might include threat detection, penetration testing, testing of backup and recovery plans, and systems resiliency testing. Establish how often and to whom the testing results should be provided, and how reports will be memorialized in the plan's official records.
- Require screening and background checks of new personnel with direct or indirect access to benefit plan data, and provide ongoing cybersecurity training.

2. Third-party risk management

- Identify all service providers and their vendors with access to plan data, and request and evaluate their cybersecurity programs and controls, including encryption and

How cybersecurity threats are affecting retirement plans (cont.)

transmission protocols. Determine whether the service provider uses any external review of controls, such as SOC2 reports or industry certifications. Consider the frequency and manner for monitoring service providers' cybersecurity systems, and whether testing is appropriate to assess service provider risk and compliance.

- Review, and amend as necessary, service provider agreements to ensure there are appropriate contractual obligations for data protection and a fair allocation of liability risk. Consider the extent to which the agreement should address compliance with applicable data privacy laws, relevant industry standards or certifications, requirements regarding data encryption and destruction of data, obligations of the parties in the event of a cybersecurity breach, and the extent of service provider's liability for cybersecurity breaches.
- Determine the level and type of insurance coverage the service provider maintains, including the extent of coverage provided for cyber-security breaches, and whether and to what extent third-party loses are covered.
- **3. The role of insurance** Traditional liability, errors and omissions, directors and officers, ERISA bonds and fiduciary coverages may not cover, or provide only limited coverage, for a cybersecurity breach. Evaluate existing coverage in light of a plan for cybersecurity risk assess-ment and determine whether cybersecurity insurance will operate efficiently to address gaps in other coverages.
- Cybersecurity insurance is still an evolving segment of the insurance industry, and policies should be carefully reviewed to determine the type and scope of coverage, policy and individual incident limits, and other important terms and limitations of the coverage.
- **Final considerations** Eliminating all risk of cyber-attacks is not a realistic goal, so plan sponsors and fiduciaries instead should focus on developing a reasonable and proportionate response to the risk of a cybersecurity breach of plan data.
- While the question remains whether the responsibility to address cybersecurity risks is a fiduciary duty under ERISA, the loss of employee personal information due to a breach nevertheless could result in serious costs and other consequences, including possible third-party liability, fines, notifications and required remediation under state and other federal laws. Additionally, a breach of employee data is almost certain to leave losses of productivity and lowered workplace morale in its wake.
- Therefore, prudent plan sponsors and fiduciaries should develop a cybersecurity risk management strategy specific to and appropriate for their benefit plans, leveraging where possible existing cybersecurity efforts in the sponsor's core business.

5 simple steps employers can take to boost workers' financial wellness

By Joe DeSilva March 15, 2017

Now more than ever, employers offer a wide array of benefits to build engagement and culture within their walls. Healthy snack options adorning the kitchen? Check. Fitness stipends? Check. Competitive work-from-home policies? Check. These are all nice -to-have extras, but employees are increasingly concerned about a more fundamental concern: retirement planning. And it's here where employers are not providing enough enticing options as they are with the other, flashier perks.

One of the biggest issues employees face as they plan for retirement is economic uncertainty.

Boosting financial wellness programs not only can help employees' finances in the long term, it can possibly help employees manage stress and increase productivity in the short term. Employers seem to understand this.

Yet, even though many employers appreciate the value of these programs, 32% are not considering implementation.

THE HEARTLAND INSTITUTE
OF FINANCIAL EDUCATION

8301 E Prentice Ave.
Ste. 312
Greenwood Village, CO 80111

Phone: (303) 597-0197
Fax: (303) 369-3900
Email: info@hife-usa.org
www.hife-usa.org

5 simple steps employers can take to boost workers' financial wellness (cont.)

Here are five simple steps an employer can take to start helping employees find tools and information to help them better manage their finances and grow more confident in their financial futures.

1. Teach employees critical planning skills. Experts suggest retirees will need 75%-90% of their working income to live comfortably in retirement. To help employees determine the optimal amount to meet their needs, consider providing them with tools that look at factors such as current annual pre-tax income, estimated Social Security benefit amount, current age and the age they would like to retire, and any retirement savings and project possible retirement savings outcomes. Helping them estimate savings needs and retirement investing now can pay off in the future.

2. Offer access to automatic enrollment and auto-escalation features. No matter how well employees do with other investments, the 401(k)'s advantages of tax-deferred growth and a company match is likely unbeatable. By automatically enrolling employees in retirement plans with savings increases, you may be able to position your employees for a more confident financial future.

3. Provide resources so employees can seek investment advice from a professional. Employees may want to seek advice on their investments so they will not bear the stress of retirement on their own. There are a lot of options available to employees, but they may not be familiar enough with those options to determine whether or not they'd benefit. Providing access to professional investment advice with respect to retirement accounts may help employees feel confident in their retirement decisions.

4. Deliver tools and personalized materials that integrate with real data. Working with a service provider that integrates payroll and recordkeeping data can give a retirement plan the ability to deliver targeted personalized information that employees can use for planning purposes. By delivering relevant information, employees can get engaged and have a better sense of the progress of their retirement planning.

5. Make self-learning tools available for honing financial skills anytime, anywhere. A financial wellness program can help employees face their financial decisions with confidence. Most programs offer a library of tools and resources that gives employees access to information about planning, saving, and providing for their home, family and retirement. With financial education, employees may make better financial choices and set realistic goals.

At a time when employee retention is crucial, it's important to create a support system for employees as they plan their financial futures.