Advisory

pillsbury

Finance | Global Sourcing

Privacy, Data Security & Information Use | Executive Compensation & Benefits

February 23, 2016

An Overview of Cybersecurity Issues Affecting Retirement Plans

By Brian E. Finch, Jeffrey D. Hutchings, Christine L. Richardson, Susan P. Serota and Jessica Lutrin

Retirement plan sponsors face ever-evolving cyber-related threats to plan assets and participant personal information. To combat such threats, plan sponsors should proactively assess the third-party service providers' ability to detect, prevent and respond to cyberattacks against the retirement plan. In order to minimize a retirement plan's overall cyber risk profile, its sponsor(s) must implement a cyber risk management strategy, including focusing on evaluating its third-party service providers' cybersecurity programs, performing periodic assessments of such programs, and ensuring that the retirement plan has mitigated risks from losses in the event of a cyberattack.

This advisory is the first in a series of advisories dedicated to understanding cybersecurity issues affecting retirement plans.

Cyber Risk Management Strategy

Due to the increasing sophistication and often opaque nature of cyber threats and attacks, it is virtually impossible to develop and implement a cyber risk *elimination* strategy. Instead, retirement plan sponsors should focus on developing and implementing a comprehensive cyber risk *management* strategy.

An effective cyber risk management strategy requires a retirement plan sponsor to:

- thoroughly diligence its third-party administrators and vendors (TPAs);
- implement and periodically review contractual protections and insurance requirements in arrangements with its TPAs;

- periodically monitor the TPAs' cybersecurity compliance and related risks, and
- consider and, if appropriate, utilize the SAFETY Act and purchase cyber and privacy insurance.

Due Diligence of TPAs

Many TPAs are affiliated with mutual funds, banks or insurance companies that are required to comply with extensive regulations regarding privacy and security of data in the ordinary course of their business, and at least some of these financial institutions have required that their affiliated TPAs comply with these regulations, even though the regulations may not require such compliance. However, there are a number of other TPAs who are not affiliated with financial institutions, e.g., consulting and actuarial companies. In the absence of a TPA's affiliation with a financial institution, no comprehensive regulatory framework exists that governs the cybersecurity protocols that TPAs of retirement plans must follow. As a first step, it is useful to know what regulatory landscape the TPA is subject to and, accordingly, the extent to which the TPA is already complying with a host of privacy and security laws. In addition, it is important to identify what operations impacting the retirement plan are handled offshore and may be subject to a lesser or more stringent level of scrutiny.

It is critical that a retirement plan sponsor take affirmative measures to vet its TPA's cybersecurity program. As part of this exercise, consider the following:

- **Cybersecurity Assessment Tool.** The U.S. Federal Financial Institutions Examination Council issued the Cybersecurity Assessment Tool to provide financial institutions with five criteria to evaluate their cybersecurity profile and determine their level of cybersecurity preparedness. While the assessment is voluntary, asking TPAs who are affiliated with a financial institution for the results of their assessment (if any) may provide a measurable means of assessment.
- **Formal Requests.** It is recommended that a plan sponsor make a formal request of its TPAs for information regarding their security systems and risks. Examples of questions that should be specifically directed at TPAs include:
  - Does the TPA have a cybersecurity program in place and, if so, does it have an officer who is responsible for overseeing, implementing and enforcing the program?
  - How does the TPA share cybersecurity threat information with its customers?
  - Does the TPA regularly review and rate its risk level for potential or actual cyberattacks?
  - What controls does the TPA have over sensitive data, and what is its ability to respond to potential threats to this data?

Contractual Protections

A plan sponsor or plan administrator should review and, as necessary, amend its agreements with TPAs to ensure that there are appropriate contractual commitments for the protection of data and a fair allocation of liability risk. Among other things, agreements should address:

- The TPA's commitment to maintain a comprehensive data security program (as evidenced by the responses to the above-mentioned examples of inquiries made of the TPAs) that is in compliance with

applicable data privacy laws and the IT security standards and practices of relevant industry standards organizations.

- Appropriate restrictions on the location and use of plan and participant data by the TPA, and access to, and utilization of, such data by the TPAs' affiliates, subcontractors and other third-parties.
- Requirements regarding the encryption of data, as well as the secure erasure or destruction of data when removed from storage media.
- Responsibility for the security of PINs assigned to both participants to access their accounts and retirement plan sponsors to access employer and plan data.
- The TPA's obligations in the event of a cybersecurity incident, including notification of the plan sponsor and/or administrator, and affected participants; investigation, control and remediation of the incident; preservation of evidence; and provision of information and assistance to the plan sponsor and/or administrator in addressing legal compliance and other issues.
- The TPA's liability for security breaches, including reimbursable costs (e.g., notices to affected individuals, credit monitoring, call center support, forensics and legal costs, and fines and penalties), indemnification obligations and any limitations on liability.
- Ability of the plan sponsor or plan administrator to terminate the contractual agreement within a reasonable period as required under the Employee Retirement Income Security Act (ERISA) and/or impose damages on the TPA in such circumstances as a breach of security provisions in the agreement or a data breach.

Periodic Risk and Threat Assessments

Throughout the relationship with the TPA, it is essential that the retirement plan sponsor or plan administrator be able to, and do, conduct periodic risk assessments of the TPA's programs and systems. The reason for this is two-fold: (1) ongoing assessment ensures that the initial legwork does not go to waste; and (2) legacy cybersecurity programs are often the most vulnerable to attacks. In addition, the plan sponsor or administrator should endeavor to stay abreast of new tactics and techniques so that it can evaluate whether the TPA's cybersecurity program is at risk of being compromised.

Cyber and Privacy Insurance

Because traditional commercial general liability and property insurance policies (in addition to ERISA fiduciary riders to such policies) may not provide full coverage for cyber-related risks, cyber and privacy insurance should be obtained to cover any potential gaps. This insurance can be obtained to cover both first-party damages and liability to third-parties, including crisis management event expenses; security breach remediation and notification expenses; business interruption and similar expenses; network and information security liability; communications and media liability; and regulatory defense expenses, including fines and penalties coverage.

Use of the SAFETY Act[1]

Retirement plan sponsors and plan administrators should examine whether they can benefit from utilizing the SAFETY Act, a liability management statute managed by the Department of Homeland Security. Briefly, the SAFETY Act is a federal law that limits or eliminates third-party liability tort claims following a terrorist or cyberattack. Retirement plan sponsors and administrators could utilize the SAFETY Act in one of two ways: (1) by having their internal cybersecurity plans and policies SAFETY Act approved, thereby significantly limiting the possible scope of litigation claims they would face after a cyberattack; or (2) by requiring TPAs to hold SAFETY Act protections, as that would allow retirement plan sponsors and administrators to be dismissed from a broad array of claims alleging negligence or poor performance attributed to the third-party security products and services. Obtaining SAFETY Act protections may serve as evidence that the retirement plan's cybersecurity programs were reasonable and that the plan's sponsors or administrators exercised their fiduciary obligations with respect to cybersecurity.

ERISA Fiduciary Considerations

ERISA does not directly address cybersecurity as it relates to retirement plans, and the Department of Labor is yet to issue formal guidance on the topic. As such, much consideration is now being given by practitioners as to whether or not the responsibility to address cybersecurity is a fiduciary function. Assuming it is a fiduciary function, while the occurrence of a cybersecurity breach does not necessarily give rise to a fiduciary breach under ERISA, the failure to avoid, mitigate or respond to such a breach may create such exposure. This is because the rules of ERISA fiduciary liability are rooted in a duty to act with prudence.

Due to the prolific nature of cyberattacks, it may be difficult to argue that a prudent man would not consider and react to cyber risks. For this reason, retirement plan administrators and other fiduciaries should be cautioned against viewing protection of plan assets and participant information as part of the responsibility of external plan trustees and TPAs and, accordingly, such fiduciaries would be well-served to demonstrate and document the development and implementation of their cyber risk management strategies. In addition, although ERISA's preemption of state laws is well-established, the extent to which ERISA preempts state privacy and data laws is currently being actively litigated. As such, retirement plan sponsors and administrators should not disregard state laws in developing and implementing their cyber risk management strategies.

Finally, administrators and other fiduciaries would be well-advised, as noted above, to consider all aspects of their insurance coverage, including their level of coverage under their fiduciary liability insurance to ensure that they are adequately protected.

Practical Considerations

Due to the dynamic nature of cyber threats, a retirement plan sponsor and plan administrator should focus on risk management, and not risk elimination, that can be achieved by the sponsor's and plan administrator's vigilance in establishing cybersecurity procedures and protocols with respect to its TPAs. Failing to do so may result in irreparable consequences for the plan sponsor, the plan administrator, the retirement plan and the participants.

[1] See here for a more general discussion of the SAFETY Act.

If you have any questions about the content of this advisory please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Brian E. Finch (bio)
Washington, DC
+1.202.663.8062
brian.finch@pillsburylaw.com

Jeffrey D. Hutchings (bio)
Washington, DC
+1.202.663.8163
jeffrey.hutchings@pillsburylaw.com

Christine L. Richardson (bio)
San Francisco
+1.415.983.1826
crichardson@pillsburylaw.com

Susan P. Serota (bio)
New York
+1.212.858.1125
susan.serota@pillsburylaw.com

Jessica Lutrin (bio)
New York
+1.212.858.1090
jessica.lutrin@pillsburylaw.com

Pillsbury Winthrop Shaw Pittman LLP is a leading international law firm with 18 offices around the world and a particular focus on the energy & natural resources, financial services, real estate & construction, and technology sectors. Recognized by *Financial Times* as one of the most innovative law firms, Pillsbury and its lawyers are highly regarded for their forward-thinking approach, their enthusiasm for collaborating across disciplines and their unsurpassed commercial awareness.