Cybersecurity Threats: What Retirement Plan Sponsors and Fiduciaries Need to Know—and Do

By Gene Griggs and Saad Gul

This article analyzes cybersecurity issues for retirement plans.

Introduction—What Is the Risk?

The loss of employee personal information due to a cyber breach is an ever-increasing concern to all employers. No organization or industry is immune from cyber threats, including benefit plan sponsors and plan service providers. In the world of employee benefits, employers historically were concerned only with protecting health plan information as required under HIPAA. Now there is increasing focus on protecting employee information maintained in connection with other types of benefit plans, including retirement plans. Retirement plan data and other information maintained and provided to a plan record-keeper typically includes name, date of birth, address, Social Security number, compensation, and other financial information. This personal information is often sufficient for someone to steal an employee's identity.

So what does a cyber breach of retirement plan data look like? It can be pretty much like any other cyber breach, or it can focus on the unique nature of retirement plan design, as illustrated by two widely reported breaches in 2016. In the first, a union's pension plan data was taken hostage by a hacker's "ransomware"—software that encrypts or locks data on a device or network—with a demand for three bitcoins (worth about $2,000) to unlock the data. In this case the data was retrieved from a backup server and the ransom was not paid. In the second widely reported breach, a governmental defined contribution plan with over $3.5 billion in assets lost $2.6 million, taken from the plan in the form of fraudulent loans from 58 participant accounts. Participants' personal information was used to set up Web profiles that were then used to take out the fraudulent participant loans. Reports indicate that in that case, the funds were restored to the plan by the company that administered the plan.

The cost of a breach, including detecting the extent of the breach, recovering data and restoring systems integrity, can be substantial. In addition, a breach may trigger enforcement actions by governmental agencies, resulting in penalties arising under state or federal law, and potentially expose the employer or plan service provider to civil claims under common law or various state statutes. Other costs frequently include restoring lost plan assets, making breach notifications, and providing post-breach identity-theft protection. Finally, the adverse impact on an organization's employee relations and public image may be substantial, even if difficult to measure.

Regulatory Structure

Many state laws, including North Carolina law, provide breach notification and private rights of action for disclosure of personal or private information, and states' attorney generals have been active in enforcing these laws in cyber breach cases.

Gene Griggs is a partner in Poyner Spruill LLP's employee benefit and executive compensation practice. **Saad Gul** is a partner in Poyner Spruill LLP's privacy and information security practice.
The authors acknowledge the contributions of Mike Slipsky, a partner of the firm practicing in the business organization group, in the preparation of this article. Mr. Slipsky regularly works with Mr. Gul in counseling clients on privacy and information security matters, including data breach prevention and responses.

California's data breach notification law was amended in 2014 to require the breached organization to provide affected individuals with at least one year of credit monitoring and identity-theft protection services.

There is no comprehensive federal regulatory scheme governing cybersecurity for retirement plans and their service providers. While there are laws that govern the financial industry's use and security of financial information, such as the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and the Fair and Accurate Credit Transactions Act, these laws do not apply directly to benefit plans or the sensitive individual data held in conjunction with those plans. However, that does not mean there is no obligation to keep employee personal plan-related information secure.

Under ERISA, a plan sponsor that chooses to distribute plan information electronically has an obligation under Department of Labor (DOL) Regulation Section 2520.104b-1(c) to ensure the electronic system used for furnishing the information results in (1) actual receipt of the transmitted information, and (2) it protects the confidentiality of personal information relating to the individual's accounts and benefits. A failure to comply with this security requirement could be the basis of a claim for failure to provide the required disclosure, which could subject the plan fiduciary to civil penalties. Similarly, 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) explicitly included as one of the conditions for utilizing the electronic media disclosure that the plan administrator take "appropriate and necessary measures reasonably calculated to ensure that the electronic delivery system protects the confidentiality of personal information."

A 2016 ERISA Advisory Council report on cybersecurity issued by the DOL in January 2017 fell short of directly addressing the questions of whether cybersecurity is a fiduciary responsibility and whether ERISA preempts state cybersecurity laws, but the report highlighted the need for additional clarification on the extent of plan sponsor and vendor responsibilities to protect participant information. However, the report provides extensive and useful information to plan sponsors, fiduciaries, and plan service providers on approaches for managing cybersecurity risks. The report recommends that plan sponsors and fiduciaries consider cybersecurity in safeguarding benefit plan data and assets and when making decisions to select or retain a service provider.

The Council is an appointed body created under ERISA and charged with advising the Secretary of Labor on the Secretary's role under ERISA. The Council has been studying benefit plan cybersecurity issues since 2011, and the report reflects the significant time and effort involved in investigating the issues and formulating an appropriate response. While the report does 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 this influential group have directed at this issue, this report may represent the establishment of a foundation for future regulatory or statutory efforts addressing plan sponsor and vendor fiduciary responsibility for cybersecurity matters. In addition, the report could be cited as a baseline standard of care in common law negligence claims by private plaintiffs.

A 2013 presidential executive order, "Improving Critical Infrastructure Cybersecurity," resulted in the federal government leading a collaboration via the National Institute of Standards and Technology (NIST) with private-sector industry stakeholders to set voluntary standards and best practices for managing cybersecurity risks to critical infrastructure services. One year later, NIST published the "Cybersecurity Framework" to provide a set of industry standards and best practices to help organizations manage cybersecurity risks. The NIST framework is a voluntary guideline, targeting organizations that own or operate critical infrastructure. However, the framework's principles and best practices for assessing, planning, and improving cybersecurity capacity and programs are not industry-specific. Therefore, they can be used as a reference to establish a cybersecurity program or complement an organization's existing risk management processes. Focused on using business drivers to guide cybersecurity activities, and recognizing there is not a one-size-fits-all approach to managing cybersecurity risk, the framework will evolve and be updated as the retirement industry provides feedback on implementation. Notably, the ERISA Advisory Council report encourages plan sponsors, fiduciaries, and service providers to use the NIST framework.

The Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 (SAFETY Act) encourages the use of anti-terrorism products, services, and technologies in civilian settings, and includes liability limitations for claims arising out of an act of terrorism where designated or certified technologies have been

employed. The ERISA Advisory Council report notes that while the financial harm arising from a cybersecurity attack against a benefit plan may not have been contemplated when the SAFETY Act was adopted, the Department of Homeland Security has increasingly been vetting processes and procedures in the cybersecurity arena. As a result, plan sponsors and fiduciaries may want to consider whether SAFETY Act certifications have a place in their cybersecurity risk management strategy. For most organizations, the best way to take advantage of the SAFETY Act's liability limitations may be by hiring vendors that have or use technologies approved by the SAFETY Act.

New York State enacted a cybersecurity regulation designed to protect the state's financial services industry and consumers from the threat of cyberattacks. These regulations, which took effect on March 1, 2017, are risk-based and set certain minimum standards while encouraging financial services firms to keep pace with evolving technologies. The regulations include the following requirements:

- Governance framework controls, including requirements for an adequately funded and staffed cybersecurity program that is overseen by qualified management, with periodic reporting to the organization's highest governing body;
- Risk-based minimum standards for technology systems including access controls, data protection including encryption, and penetration testing;
- Required minimum standards addressing cyber breaches including an incident response plan, preservation of data to respond to such breaches, and notice to regulators of material events; and
- Accountability by requiring identification and documentation of material deficiencies, remediation plans, and annual certifications of regulatory compliance to regulators.

These regulations likely will become a national benchmark for managing cybersecurity risks relating to financial information, and plan sponsors and fiduciaries should carefully consider the requirements of these regulations when designing and implementing their response to cybersecurity risks.

Industry Resources

Industry organizations are working to help plan sponsors and service providers understand and respond to the evolving cybersecurity landscape. The SPARK Institute is developing uniform data management standards for the defined contribution plan market. The goal is to facilitate transparency to outside parties and provide the necessary elements for a cybersecurity certification program. SPARK's Data Security Oversight Board is leading the effort, which includes representatives from plan administrators, consultants, SPARK staff, and the Department of Homeland Security. Their work is in its early stages but has the potential to be useful for retirement plan sponsors, fiduciaries, and plan service providers.

The April 2016 Employee Benefit Plan Audit Quality Alert #365 published by the American Institute of Certified Public Accountants (AICPA) relates the concerns expressed by the DOL's chief accountant regarding plan cybersecurity threats. Because most plan sponsors and service providers use electronic means to exchange plan data, conduct financial transactions, and interface with participants, plan and participant records are at risk of cyberattack. Suggesting the responsibility to implement processes and controls to restrict access to a plan's systems, applications, and data resides with those charged with plan governance, DOL's chief accountant encouraged plan sponsors and fiduciaries to evaluate plan cybersecurity governance protocols, including those of plan service providers and their vendors, to determine that appropriate processes and controls are in place to secure and to restrict access to the plan's data.

The AICPA also is working on tools and resources to assist plan sponsors in developing and implementing a cybersecurity risk management strategy. For example, AICPA Service Organization Control (SOC) reports may be particularly helpful to plan sponsors when outsourcing plan administration and other functions to service providers. AICPA's SOC1 report addresses controls relevant to a service provider's internal controls over financial reporting, while an SOC2 report addresses risk of IT-enabled systems and privacy programs beyond those necessary for financial reporting controls. An SOC2 report focuses on the security, availability, processing integrity, confidentiality, or privacy of a service provider's IT-enabled systems and the ability of those systems to protect the data and confidentiality of the parties who utilize the service provider, such as a plan utilizing a record-keeper. The AICPA also has formed a Cybersecurity Working Group to work in conjunction with the Auditing Standards Board to develop a profession-wide approach to performing and reporting on attestation engagements related to cybersecurity.

Plan Sponsor and Fiduciary Action Steps

What should retirement plan sponsors and fiduciaries be doing now to address cybersecurity risks? First and foremost, develop and maintain a retirement plan cybersecurity risk management strategy. The critical components and action steps 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 (NIST; SAFETY Act; industry-based initiatives, including SPARK Institute, AICPA). Ideally, retirement plan cybersecurity risk management should be integrated with the strategy of the larger enterprise (for example, corporate entity, controlled group, or a multiemployer/union organization). When plans are part of a larger enterprise, plan fiduciaries should seek guidance on whether there are valid cost-sharing protocols if plan resources are sufficient and available.
   - Ownership of the Strategy. Identify and document who has what responsibilities for strategy implementation within the plan sponsor organization, the fiduciary body, and at third-party service providers. Include responsibility for updating the strategy as circumstances and resources evolve.
   - 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 personnel who have a need to access the data?
     – When and how is data encrypted? What are vendor policies on data encryption at rest and in transmission? Is encryption automated or manual?
     – What data needs to be retained and when should it be destroyed or permanently protected? Establish timeframes and protocols for getting rid of old or unnecessary data to reduce cyber risks.
     – Collect, maintain and share only the data and asset information that is necessary to meet the needs of the plan and no more.
   - Testing/Updating. Entities involved in benefit plan cybersecurity should agree to the frequency and type of testing procedures to be conducted and by whom. Testing might include threat detection, penetration testing, testing of backup and recovery plans, and systems resiliency testing. Determine how testing results will be used to update and enhance the strategy.
   - External Certifications. Consider whether an outside certification, such as an AICPA Service Organization Control 2 (SOC2) report, may enhance security compliance and help streamline testing procedures.
   - Reporting. Plan sponsors and fiduciaries should consider the level and frequency of reporting on plan cybersecurity issues, to whom reports should be provided, and how reports will be memorialized in the plan's official records.
   - Training. Include ongoing training of staff involved with benefit plans and with direct or indirect access to benefit plan data. This training should occur within the plan sponsor entity and across any service providers who collect, maintain, or transmit benefit plan data.
   - Hiring Practices. Require background checks and screening of new personnel with direct or indirect access to plan data.

2. Third-Party Risk Management.
   - Identify all service providers (and their vendors) who will have access to plan data.
   - Evaluate service provider controls and security programs, including review of written policies on data security, encryption, and transmission protocols (see 'Understand the Data' above); periodically monitor and test compliance and risks; determine appropriate periodicity of updating and reporting by the service provider; will the service provider agree to voluntary external review of controls, such as SOC2 reports or industry certifications?
   - Review, and amend as necessary, provider service 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 or relevant industry standards or certifications; requirements regarding data encryption and destruction of data; obligations of the parties

in the event of a cyber breach or other incident, including reporting to the plan sponsor or fiduciary and notification of affected participants; incident investigation and remediation, including assistance to the plan sponsor; extent of the services provider's liability for cyber breaches, including direct costs (notification, credit monitoring, legal fees, fines, and penalties), indemnification, and limitations of liability.

- Determine the level and type of insurance coverage the service provider maintains, including the extent of coverage provided for cybersecurity breaches and whether and to what extent third-party losses are covered.

3. The Role of Insurance.

Most retirement plan sponsors and service providers likely have a broad range of insurance coverage, including commercial liability, errors and omissions, directors and officers, fiduciary, and other coverage. However, traditionally these policies have not covered, or provided only very limited coverage for, cybersecurity risks. Cybersecurity insurance is a developing segment of the insurance industry and has evolved significantly over the past few decades. While prices have come down and coverages improved, policies should be carefully reviewed to determine the type and scope of coverage, and policy and individual incident limits.

Cybersecurity insurance policies typically provide third-party coverage, and some also include first-party coverage. Third-party coverage is triggered by a lawsuit, and covers third-party damages and defense costs, and may include coverage for forensic investigations, and the cost of credit monitoring and remediation. First-party coverage is contractual coverage triggered by a cybersecurity breach, so it does not require third-party damages or a third party to sue the insured over a cybersecurity incident. First-party coverage may include the costs associated with direct risk management, disaster response, and recovery assistance. Evaluate how the coverage compares to the cybersecurity risk assessment and whether cybersecurity insurance operates efficiently to address gaps in other coverages.

Final Considerations

Due to the increasing number and evolving nature of cyberattacks, preventing or eliminating all risk of an attack is not a reasonable goal. 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 at the time this article was written whether or not the responsibility to address cybersecurity risks is a fiduciary duty under ERISA, the loss of employee personal information due to a cyber breach could result in substantial adverse consequences, including liability, fines, and required remediation under other state and other federal laws, loss of productivity and lower employee morale. Therefore, prudent plan sponsors and fiduciaries should develop a cybersecurity risk management strategy appropriate for their benefit plans. Where possible, they should leverage existing cybersecurity efforts in the sponsor's core business. ■