The Excellent Fiduciary: Bridging the Gap Between Fiduciary Committees and IT

*Ronald E. Hagan**

Technology-empowered threats to the security and confidentiality of retirement plan assets and data are exploding. Current fiduciary management methods largely lack a formal interface with the information technology function and its storehouse of expertise. These two realities demand that fiduciary committees embrace their enterprises' information technology departments in a new era of collaboration.

INTRODUCTION

The Employee Benefits Security Administration (EBSA), which enforces the Employee Retirement Income Security Act of 1974 (ERISA), has issued cybersecurity guidance to enterprises that sponsor ERISA-qualified retirement plans. That guidance is forcing the need for a change in the attitude of retirement plan committees toward their enterprises' information technology (IT) departments. Generally, regular interaction between fiduciary committees and their IT departments related to plan data security is sporadic at best, and nonexistent at worst. Pervasive threats of cybersecurity attacks and conformance to the EBSA's cybersecurity guidance require an overhaul of the fiduciary-to-IT relationship. We will examine how the lack of collaboration between fiduciary committees and IT departments is an existing obstacle to protecting ERISA-qualified retirement plans' assets and data. We will also discuss an action plan for improvement.

A NEW PARDIGM FOR FIDUCIARY COMMITTEES

For the first time, the EBSA released cybersecurity advice to retirement plan fiduciaries in 2021. The recommendations contained in three publications that comprise the EBSA's guidance do not rise to the level of regulation. Instead, they are an outline of best practices for maintaining cybersecurity. It is up to plan fiduciaries to interpret those practices' intent and transpose them into actionable procedures. That is a job that will challenge many chief financial officers (CFOs) and human resources leaders.

The purpose of the guidance is uncomplicated and principled. Its implementation makes the point that not all guidance or advice from the EBSA is equal—some carry greater impact with more significant potential penalties. The EBSA has clarified the intensity of its commitment to driving change in asset and data security fiduciary behavior by fashioning a new cybersecurity audit initiative around the precepts defined in the rollout of its guidance. Random investigations of ERISA plan sponsors began shortly thereafter. Considering the investigations' immediacy and the makeup of the document requests accom-

**RONALD E. HAGAN* is Chairman of Roland|Criss' Risk Standards Committee. Roland|Criss is the premier risk manager for employee benefit plan sponsors, foundations, and endowments. Mr. Hagan has a lengthy career in enterprise risk management. He has pioneered many certification programs, standards practices, and fiduciary risk management strategies preferred by boards of directors and C-level executives. Reach him by e-mail at ronhagan@rolandcriss.com.

panying the investigations, it is wise to view the EBSA's "advice" as imminent de facto regulation.

It would be easy to conclude that conforming to the government's guidance rests primarily in the domain of information technology. But Bryan Smith, the Section Chief for the FBI's Cyber Division, warns that cybersecurity is more a business challenge than an IT issue. Recently he stated, "*The value of information is dependent on the degree to which it affects the viability of an enterprise. The more critical the data, the more emphasis is needed on securing it. An IT department is not the best-equipped office to prioritize the value of all corporate information.*" As if to make Bryan's point, a CFO who serves on the Employee Benefit Plan Cybersecurity Working Group commented, "*I've always thought IT was taking care of our 401(k) plan's data security needs. I've been surprised to learn that it's not all that high on their priority scale.*"

Against this backdrop, investment and retirement plan committees face a significant challenge in defining the boundary between benefit plan management and their enterprise's IT infrastructure. The lack of provisions addressing data security in the hundreds of fiduciary committee charters we have seen likely means that the retirement plan community needs new protocols for how committees interact with their organizations' IT departments.

THE DOMAIN OF IT IN CYBERSECURITY

For a proper connection between a retirement plan committee and the related employer's computer department, fiduciaries need to understand that cybersecurity and information technology are not the same things. Information technology embraces the installation of new computing systems to support an enterprise's growth. Examples include maintaining existing applications, developing new computer-based solutions, maximizing digital network performance, improving communications, and facilitating information sharing. In addition, information technology ensures the security of an organization's data in any form, physical or electronic, from internal threats.

On the other hand, cybersecurity addresses the protection of data from threats introduced by electronic means. It involves safeguards against attackers gaining access to networks, computers, programs, and data. Both disciplines, information technology and cybersecurity are concerned with the protection of data. It is typical for enterprises to consolidate these two disciplines under the purview of the IT or computer systems business unit.

However, IT is not primarily responsible for compliance with the fiduciary principles defined in ERISA. Decisions in recent lawsuits brought against employers for breach of their fiduciary duty in cases involving theft of retirement plan assets and accounts by electronic means make it clear who is legally responsible. For example, in *Leventhal v. Mand-Marblestone Group,*[1] the court ruled that the third-party administrator, who was sued initially by a participant in Leventhal's 401(k) plan for a cyber breach, may bring counterclaims against the employer and its plan fiduciaries because of the plan sponsor's alleged "carelessness" in its "computer/IT systems" and "employment policies." The *Leventhal* case illustrates the expanding liability for boards of directors, CFOs, and HR leaders in retaining and managing retirement assets and the personally identifiable information of plan participants. It is essential to grasp the reality that such liability is not born directly by information technology managers, who usually do not fall under the umbrella of an ERISA fiduciary.

THE DOMAIN OF ERISA PLAN FIDUCIARIES IN CYBERSECURITY

Plan fiduciaries must take steps to protect participant information; the steps must be "appropriate and necessary," and the "system" used to communicate with the participants must have embedded protections.[2]

The systems on which fiduciaries rely are owned and operated by third parties—recordkeepers and third-party administrators (TPAs). The "buyer" of the services provided by such third parties is most often an enterprise's CFO or human resources executive acting at the behest of a fiduciary committee. Since evaluating service providers' technology capabilities is outside the professional skills of those constituents, that aspect of a provider's offering rarely gets examined. Consequently, the cybersecurity readiness of the recordkeepers and TPAs that serve most retirement and pension plans is unknown to their clients. In years preceding the mass digitization of plan data and the emergence of the cybercriminals that followed, IT was not a participant in the vendor selection process. That must change dramatically under the EBSA's cybersecurity guidance.

The careful selection and monitoring of an ERISA plan's service providers is a fundamental duty of plan fiduciaries. A formally stated process, and proof of adherence, is the evidence needed to prove the care demanded by ERISA. For those fiduciary committees that have not adopted a framework of internal control related to their vendor oversight methods, now is the time to obtain the help needed to ensure rapid implementation with proper cybersecurity provisions. Any existing internal control procedures need expanding to include cybersecurity considerations.

Boards and executives need to begin the hard work of governing cyber risks by following best practices and standards, allocating appropriate resources to cybersecurity, and developing risk transfer strategies.

CONNECTING THE DOMAINS

From the perspective of retirement plan operations, technology is the plan. From payroll to the management of participants' accounts, technology is the enabler. The lines between human resources functions and technology functions are blurring. Yet, the information technology groups of most employer organizations are in a silo far away from fiduciary committees. The modern fiduciary looks for ways to engage more deeply with technology. Especially in light of the EBSA's intense investigation program related to its cybersecurity guidance.

It is worth noting that a fiduciary committee's ideas on how to reimagine the role of IT can sometimes be at odds. For example, the chief information officer (CIO) of a business that sponsored an ERISA-qualified retirement plan was at loggerheads with the organization's CFO. The CFO's emphasis on costs was seemingly at odds with the CIO's focus on hiring a different recordkeeper with better security controls, even though its fees were higher than the CFO's favorite. Both leaders identified a viable vendor for the retirement plan, but they could not effectively prioritize because neither had considered the bigger strategic picture.

To help eliminate such stalemates, consider the following actions:

- Consider making your enterprise's CIO a regular non-member guest of the fiduciary committee's meetings.
- Involve a representative from IT periodically in meetings conducted between human resources

and the retirement plan's vendors.

- Include the CIO on the distribution list of the responses the plan's vendors give to human resources' inquiries of their cybersecurity practices and ask for IT's evaluation of those responses.
- Ask IT for awareness training in cybersecurity standards (for example, those promulgated by the National Institute of Standards and Technology and International Organization for Standardization (ISO)).

CONCLUSION

Benefit plans often maintain and share sensitive employee data and asset information across multiple unrelated entities as a part of the benefit plan administration process. Consider this data carefully when implementing cybersecurity risk management measures.

Because ERISA regulates benefit plans, anyone who interacts with the plan should be particularly aware of the impact that breaches have on participants and beneficiaries and the associated rights and duties of plan fiduciaries arising under ERISA.

Everyone who comes in contact with personally identifiable information (PII) has a role in protecting plan data. Here's where to start:

- **Adopt a Cybersecurity Policy.**

  Regardless of a retirement plan's size or complexity, the need for a fiduciary committee authored *cybersecurity policy statement* (CPS) has escalated to the same level of importance as an investment policy statement. The IT departments of most organizations maintain a data security policy at the enterprise level. Rarely do such policies expand to include an ERISA plan's PII. If your fiduciary committee currently lacks a CPS, do not delay adding one to the other policies you would rely on to prove your fiduciary committee's prudence.

- **Conduct a Cybersecurity Risk Assessment.**

  Initiate an examination of your plan's current cybersecurity sensitivities, resourced either internally or by a qualified third-party expert. A legally defensible risk assessment should adhere to 18 essential criteria. A review offers a way to ensure continued improvement. Ask RolandCriss for a list of the criteria at rolandcriss.com/contact-us.

- **Elevate Cybersecurity to a High Monitoring Priority.**

  The agendas of benefit plan-related committees should include a permanent entry for monitoring a *security management plan*. Best practices for ERISA governance, risk management, and compliance (GRC) systems now require evidence of robust monitoring. Using a technology application tailored for that purpose is a must. Ask RolandCriss about Fiduciary GRC™, a state-of-the-art ERISA § 3(16) fiduciary solution covering the entire risk spectrum: cyber assessment, standards, technology, and monitoring.

Fiduciary committees, CFOs, and human resources executives have hard work ahead to manage cybersecurity threats. The solution is found by adopting best practices and adhering to guidelines now in place by federal regulators. Collaboration with an enterprise's information technology group is essential; admittedly, it is a sea change for many fiduciary committees.

NOTES:

[1]Leventhal v. MandMarblestone Group LLC, 2020 Employee Benefits Cas. (BNA) 197040, 2020 WL 2745740 (E.D. Pa. 2020).

[2]29 C.F.R. § 2520.104b-1(c)(1)(i).