The EXCELLENT FIDUCIARY

Cybersecurity in the Committee Room

*Ronald E. Hagan**

It is essential to understand that cybersecurity includes protecting digital forms of personally identifiable information, personal health information, and employee benefit plan assets from exposure and protecting electronic systems from exploitation by hackers. Fiduciary committees are accountable for the results.

INTRODUCTION

Cybersecurity is a tech-centric term that often makes business unit leadership's eyes roll. That response is loaded with risk because cybersecurity ranks among the most vital issues facing human resources, finance, and administration executives. The truth is that cybersecurity, while highly technical in its domain, uses the same principles and concepts as many other business-related legal risks. Employee benefit plan (EBP) leaders should be asking the right questions and taking steps to protect their plans—and themselves—from cyberattacks.

This article discusses 10 questions that can equip leaders with insights that fuel a comprehensive response to regulatory pressure and threats in the cyber landscape. We also provide eight steps for upgrading a committee's management framework.

SPOTLIGHT ON EBP COMMITTEES

Anyone who serves on a committee formed by an enterprise to oversee any EBP governed by the Employee Retirement Income Security Act of 1974 (ERISA) should know their legal duty is highest in civil law. Fiduciary standards of care under ERISA bind executives and their employers to a rigid expectation of loyalty, independence, and prudence when the assets and data belonging to others fall under their care. Fiduciary committees tend to focus significant attention on retirement and pension plans while relegating health plan oversight to a lesser priority, even ignoring that category altogether. Recent developments dictate a change in that approach is essential.

WHY IS CYBERSECURITY AN HR CONCERN?

Human resources depart-

**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.

ments face the daunting task of complying with stringent federal laws enforced by various agencies. In addition, payroll operations and talent management responsibilities command leadership's uninterrupted attention. Notwithstanding the enormous effort required to execute those duties, HR executives must grasp their emerging responsibility to protect digital forms of personally identifiable information (PII) and personal health information (PHI), and EBP assets from exposure to hackers.

Cases such as the digital attack in 2021 on Kaseya, an information technology solutions developer whose clients are recordkeepers and other managed service providers, illustrate how a strategic attack can involve hundreds of employer organizations. Present estimates suggest that 800 to 1,500 small to medium-sized companies may have experienced a security compromise through their plans' vendors that use Kaseya's systems. The Kaseya case and other data security breaches involving retirement plan service providers illustrate the grave risks that fiduciary committees now face. HR executives often ask if they can be held personally liable for cybersecurity breaches. The answer is a resounding "yes." An EBP's designated plan administrator, typically an HR professional, is usually a named defendant in fiduciary breach lawsuits.

HEALTH PLANS IN THE CROSSHAIRS

In addition to the concerted efforts of bad actors to penetrate retirement and pension plans, the increasingly malicious cyberattacks experienced by healthcare organizations have led to data breaches that have increased healthcare delivery costs and, in some instances, affected patient health outcomes. According to the proposed Healthcare Cybersecurity Act of 2022, data reported to the Department of Health and Human Services (HHS) shows that in "almost every month in 2020, more than 1,000,000 people were affected by data breaches at healthcare organizations." The bill also states that cyberattacks on healthcare facilities affect over 33,000,000 people!

In addition to being exploited by cybercriminals, there are commonly legal repercussions with even minor cyberattacks. The most typical are investigations by regulatory agencies, breach notifications, and claims for damages for breach of contract.

REGULATORS AND NEW LEGISLATION SPARK RISK MANAGEMENT UPGRADES

In addition to class action cases, regulators are ramping up their response to cybersecurity breaches and increasing cybersecurity requirements for ERISA plans and the enterprises that sponsor them. Numerous agencies have levied fines and brought suits for cybersecurity-related issues, including the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), the Securities and Exchange Commission (SEC), and the Employee Benefits Security Administration (EBSA), the enforcement arm of the U.S. Department of Labor (DOL). Regulatory investigations can even trigger private lawsuits. For example, after discovering that Alight, a retirement plan recordkeeper, had processed unauthorized distributions due to cybersecurity breaches relating to its ERISA plan clients' accounts, the EBSA filed a lawsuit, which triggered private class actions against the fiduciaries of specific plans serviced by Alight.

In 2021, at least 45 states introduced or considered bills or resolutions concerning cybersecurity, more than 250 in total, and at least 35 states enacted cybersecurity-related laws. At the federal level, lawmakers have introduced at least 18 new bills concerning cybersecurity.

Until recently, a lack of clar-

ity about what would qualify as an ERISA-compliant process for demonstrating prudent data security policies and procedures handcuffed fiduciary committees. That changed with the introduction of sub-regulatory guidance in 2021 from the EBSA.[1]

The EBSA's guidance is a long overdue outline of privacy and security protocols that elevate PII protection in retirement and pension plans to a level that rivals well-established PHI requirements.

In the face of an exploding number of cybersecurity breaches of employers' in-house IT systems, retirement plan recordkeepers, payroll services, and healthcare providers, the standard of care documented in the EBSA's guidance demand upgrades in two fundamental fiduciary disciplines; *governance* and *controls*. Now is the time for EBP committees to evaluate their readiness, and the following 10 questions will reveal where they stand:

1. What is our fiduciary committee's data security policy?
2. Who has access to PII, and what are our most significant data security risks?
3. What are the tools in use to protect PII?
4. How do we know if there has been a data breach?
5. In case of a breach, what is our response plan?
6. Are we sure our service providers and their subcontractors adhere to appropriate data security policies and practices?
7. Do our electronic systems use encryption technology?
8. Does our cybersecurity system work across all platforms, devices, tablets, phones, and laptops, including personal devices?
9. What is the committee's role in the event of a cybersecurity incident?
10. How often does our committee evaluate our approach against industry best practices?

EIGHT STEPS TO ASSURANCE

At a minimum, although not exhaustive, eight action steps divided between *governance* and *internal controls* should have a short timeframe for completion to quickly align a committee's oversight with the current regulatory environment.

I. Governance

Cybersecurity Policy

Regardless of an EBP'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 maintained by defined contribution and defined benefit plan fiduciaries. The IT departments of most organizations maintain a data security policy at the enterprise level, but rarely do such policies expand to include an ERISA plans' PII. If your fiduciary committee currently lacks a CPS, do not delay adding one to the other policies you would rely on to guide your committee's prudence. You may download a helpful policy checklist from Roland|Criss at rolandcriss.com/data-security-checklist.

Monitoring Agenda

The agendas of fiduciary committees should include a permanent entry for monitoring a *security management plan*. Best practices for ERISA governance, risk management, and compliance—or GRC systems—now require evidence of robust monitoring. Using a technology application tailored for that purpose is a must. Ask Roland|Criss about Fiduciary GRC(tm), a state-of-the-art ERISA 3(16) fiduciary solution

covering the entire risk spectrum; cyber assessment, standards, technology, and monitoring.

Service Provider Management Standards

The modern EBP committee should have written cybersecurity rules for hiring, monitoring, and re-engaging vendors as recordkeepers, investment firms, healthcare plans, payroll operations, and any other service provider possessing PII or PHI. It is also essential for committees to know if any of their EBPs' service providers utilize agents or subcontractors to perform the services, and to examine such providers' data security policies and procedures.

Make ERISA Cybersecurity Training a Committee Prerequisite

Managing conformance to the EBSA's guidance is not a technology-based discipline, and it is, for the most part, a process management undertaking. Understanding how the various cybersecurity standards bodies impact regulatory rule-making is essential. So, ask your information technology unit for awareness training in cybersecurity standards such as those promulgated by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO).

II. Internal Controls

Adopt a Control Framework

While the EBSA's guidance is an excellent place to start, a proper workflow for executing a committee's rules transcends the EBSA's guidelines. Consultation with an ERISA fiduciary risk management firm like RolandlCriss to build an appropriate fiduciary management framework would ensure a committee's ability to prove its prudence.

Commission an 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, and a review offers a way to ensure continued improvement. Ask RolandlCriss for a list of the requirements at rolandcriss.com/contact-us.

Establish Rules of Engagement with Information Technology Leaders

From the perspective of plan operations, technology IS the plan. Technology is the enabler from payroll to managing retirement accounts and health plans. 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.

Expand Insurance Coverage

Cybersecurity insurance covers risks that errors and omissions and fiduciary liability insurance policies do not. Typical coverages embrace disaster recovery and data breach response assistance when an EBP incurs a security breach.

CONCLUSION

The issues concerning EBP security grow continuously. The regulatory environment is undergoing dramatic change. For example, EBSA plan auditors expect to find employers fully aligned with its "guidance." (You may obtain a copy of the documents the EBSA has requested from employers in several of its plan audits at excellentfiduciary@rolandcriss.com.) Other laws are evolving. While lawmakers try to keep up, the risks are real and expanding. Fiduciary committees must not overlook the dangers those realities represent.

NOTES:

[1]April 14, 2021, EBSA News Re-

lease Number 21-358-NAT.