CAPTRUST

Cyber Risk and Cybersecurity for Retirement Plan Sponsors

Two significant challenges of managing cybersecurity for retirement plans are their size and human impact. Those factors are also what make retirement plan cybersecurity so important. As CAPTRUST Chief Technology Officer Jon Meyer points out, “What’s at stake is participants’ largest nest eggs—their life savings—being put at risk due to insufficient management of cybersecurity.”

Also at stake: The plan sponsor’s reputation and financial health. Cybercriminals today are targeting large and small businesses almost indiscriminately, and to great effect. Research by the National Cyber Security Alliance found that more than 70 percent of cyberattacks target small or medium-sized businesses, and 60 percent of those attacked went out of business within six months. For larger businesses, the average cost of a data breach is now $4.88 million dollars, according to IBM’s 2024 “Cost of a Data Breach Report.” Publicly traded companies can also expect significant hits to stock values, waves of impact throughout their supply chains, and long-term damage to their brand reputation.

“It’s not just about securing the plan itself,” says Nick Brezinski, CAPTRUST director of information security and network. “It’s about securing the entire ecosystem, including recordkeepers, third-party administrators, participants, and anyone else with access to plan data.” That can seem daunting for plan sponsors that don’t know how to get started. But there are key practices that can help to light the way.

Fiduciary Cyber-Responsibility

The Department of Labor’s (DOL) “Cybersecurity Program Best Practices” provides a framework to help plan sponsors to act as prudent fiduciaries when it comes to cyber risk management. “These are guidelines and best practices, not specific technology recommendations,” says Meyer. “They emphasize the need for a full and effective information security program, rather than focusing on individual technological solutions.”

Under these guidelines, a plan sponsor's fiduciary duty is to safeguard participant assets, in a similar way to how they guard their own organization.

Typically, this means building up internal expertise or hiring external experts in cybersecurity, in the same way that they might hire an ERISA lawyer or an investment manager.

However, Brezinski warns, "Hiring external experts or service providers does not transfer the risk to that third party. The sponsor still owns the responsibility for securing their data and running the plan's broader cybersecurity program. External experts can supplement where internal resources are lacking, but accountability remains with the plan sponsor." Fiduciary responsibility itself cannot be outsourced, which means that sponsors have a duty to monitor their vendors.

Vendor Management and Accountability

Since many plan sponsors rely on third-party service providers, it's crucial to vet vendors rigorously, and confirm that they are complying with stringent security standards. This includes regular reviews and contractual obligations regarding data protection.

"When vetting technology partners, it's essential to have conversations about what you're looking for, considering the size of your organization and where you are in your cybersecurity journey," says Brezinski. Cost is often a significant factor, and it's important to balance capability with affordability.

Once the vetting process is complete, consider legal contracts to enforce cybersecurity standards. "It's not enough to have a handshake agreement," says Jon Atchison, CAPTRUST senior team lead for governance, risk, and compliance. "Where possible, make an effort to lock down your vendors with data privacy and security agreements." These agreements legally bind vendors to maintain certain standards, which are essential for ensuring that vendor security practices align with the plan sponsor's risk management strategies.

Vendor management also includes proactive engagement throughout the length of the partnership. "You don't need to be an expert on cybersecurity, but you do want to have a modicum of understanding of the threats and protective measures," says Atchison. "That way, you can ask good questions and understand where your partners are doing well, and where they might not be."

Fraud Awareness and Participant Education

Another critical aspect of cybersecurity is educating participants. Although fraud is a distinct threat from cybersecurity risks, it often gets lumped in. Plan sponsors have a responsibility to help employees understand how they can help protect their accounts from fraud and scams.

For example, participants could have their retirement funds stolen due to social engineering attacks, such as phishing or romance scams, which may not involve cybersecurity breaches. "In these cases, it's important for sponsors to understand their recordkeepers' guarantees, and how they plan to

handle cases of fraud," says Meyer.

Phishing is when scammers impersonate trustworthy sources and persuade people to reveal sensitive data like personal information or passwords. Through romance scams, malicious actors build trust over time, then ask for money. *Pig-butchering* is another type of scam to be aware of. According to the Financial Industry Regulatory Authority (FINRA), "These scams often involve fraudsters contacting targets seemingly at random, then gaining trust before ultimately manipulating their targets into phony investments, and ultimately disappearing with the funds." On its website, FINRA offers tips for identifying and avoiding specific scams like these.

"You can't rely on technical security alone," says Atchison. "Participants need to be taught how to recognize scams so that they don't become unwitting participants in their own attacks." The stakes are high because participants who fall for scams may not be reimbursed for the legitimate transactions they initiated. Recordkeeper guarantees only go so far to protect participants against cyber fraud.

Sponsors should also encourage participants to register for online services, regularly review their retirement accounts, and report suspicious activity to the plan sponsor and recordkeeper immediately, and sometimes to the FBI. "It's about building a culture of cybersecurity awareness at every level," says Brezinski.

The Limitations of Cyber Liability Insurance

While cyber liability insurance can provide a financial cushion in the event of a breach, it's important for plan sponsors to understand what this insurance covers, and, perhaps more importantly, what it doesn't. As Meyer says, "Cyber liability insurance may cover breaches caused by the plan sponsor, but it won't necessarily cover breaches by a third-party service provider, like a recordkeeper, and a huge number of breaches are third-party breaches."

Brezinski and Atchison recommend that sponsors carefully review their cyber insurance policies to verify that they provide adequate protection for plan-related data. Relying solely on insurance without a comprehensive cybersecurity program in place could leave sponsors and participants exposed to significant risks.

Brezinski reiterates the need for contractual coverage with vendors. "This will help ensure that, if a breach happens at the vendor level, the vendor will take responsibility," he says. "Cyber liability insurance alone might not offer full protection in such cases."

"At the end of the day, it's about safeguarding participants' retirement security," says Atchison. "The risks are real, but, with the right strategies, they can be minimized."

Undoubtedly, the cybersecurity landscape for retirement plans is complex, and rapidly evolving. To face today's and tomorrow's threats, plan sponsors should take a proactive approach, implementing a comprehensive cybersecurity program that includes proactive vendor management and participant

education. By staying attuned to emerging threats, and committed to robust cybersecurity as part of their fiduciary responsibilities, sponsors can better protect their participants' information and retirement savings.

"Plan sponsors would do well to look at cybersecurity as a continuum of shared responsibility—a continuum between themselves, their vendors, and their participants," says Meyer. An effective information security program, well-written vendor contracts, participant education, and a comprehensive understanding of fraud risks are essential components of an effective cybersecurity strategy for retirement plans.