Cybersecurity

RETIREMENT MANAGEMENT SERVICES, LLC
Plan Consulting • Administration • Design

RETIREMENT MANAGEMENT SERVICES, LLC
905 Lily Creek Road Louisville, KY 40243

4/29/2025

The importance of cybersecurity for plan sponsors of retirement plans cannot be overstated. As stewards of sensitive financial and personal data, plan sponsors have a fiduciary and legal obligation to protect that information. Retirement plans handle sensitive data like social security numbers, dates of birth, addresses and contact information, employment and income history and account balances and investment choices. A breach could lead to identity theft, fraud, and financial losses for participants.

Under ERISA (Employee Retirement Income Security Act), plan sponsors have a fiduciary duty to act in the best interests of plan participants. Plan Sponsors are now expected to formally incorporate cybersecurity into their fiduciary process. Cybersecurity is no longer "optional" it's part of the core duty of prudence and loyalty to plan participants. Ignoring cybersecurity risks could be viewed as a breach of fiduciary duty, opening the plan sponsor to liability. If the breach results in a direct financial loss to the participant (theft from accounts) it can lead to regulatory fines and legal action from affected participants and costs of breach mitigation (forensics, notifications, legal fees).

The Department of Labor (DOL) has updated guidance underscoring the critical importance of cybersecurity for all ERISA-covered retirement plans, including 401(k)s, 403(b)s, and pension plans. It emphasizes that plan sponsors, fiduciaries, recordkeepers, and service providers must implement robust cybersecurity practices to protect plan participants' sensitive information and assets. This guidance aligns with the DOL's ongoing efforts to enhance cybersecurity measures within the retirement plan industry, aiming to safeguard the retirement savings of American workers. The guidance included tips for hiring service providers with strong cybersecurity practices, best practices for maintaining cybersecurity programs and online security tips for participants.

Most retirement plans involve third-party administrators, recordkeepers, custodians, and service providers. Plan sponsors must evaluate and monitor third-party vendors not just on performance and cost, but also on their cybersecurity controls. Plan sponsors must ensure prudent selection and monitoring of service providers as well as take reasonable steps to safeguard plan data.

Periodically asking vendors about their cybersecurity certifications, policies, breach history, and insurance should be standard practice. By vetting the cybersecurity practices of vendors annually may aid to identify, evaluate, and remediate cybersecurity risks. Requiring contractual language that document all assessments and remediation efforts to address data security, breach notification, and responsibility with each provider should be readily available to assist in keeping plan information safe.

Another way to ensure data is only accessed by authorized users it is important to use multi-factor authentication (MFA) for all systems, limit access to data based on job responsibilities and require regular password updates and adopt a strong password policy.

All plan data must be encrypted in transit and systems must be updated regularly with security patches, use firewall, antivirus, and anti-malware software and most importantly maintain audit logs for access and activity. Maintain documentation of all cybersecurity policies and procedures. Keep records of vendor assessments and internal training and have documentation of security audits, testing, and results.

Participants must be informed how to protect themselves. Using strong passwords, monitoring their account activity and properly recognizing phishing attempts. Plan sponsors should provide educational materials or partner with vendors who offer these services to educate their participants periodically.

Participants trust sponsors with their financial future. A breach could severely damage that trust and a company's reputation—both internally and publicly. So what if a breach happens? Plan administrators must activate the Incident Response Plan that is in place, notify affected parties and regulatory agencies (if applicable), document the breach, investigation, and remediation actions taken and review and update security protocols post-incident.

The DOL's guidance should be uses as a benchmark. Plan sponsors should adopt a formal cybersecurity program, conduct annual risk assessments, ensure strong access controls and encryption, have an incident response plan and provide cybersecurity awareness training to their staff/participants. Plan sponsors are expected to follow these guidelines as part of prudent plan management. If you need assistance in understanding how these requirements impact your responsibilities as a plan sponsor or fiduciary, or if you require support in implementing these cybersecurity measures, please feel free to ask.