CAPTRUST

Cybersecurity and Retirement Plans: What Plan Sponsors Need to Know (Webinar Recording)

With participant assets and retirement security on the line, cybersecurity weighs heavily on many retirement plan sponsors' minds. While the recently issued cybersecurity guidance from the DOL provides a roadmap to help prevent against cyber threats, the heightened emphasis indicates that cybersecurity will likely remain a DOL focus for years to come.

In this webinar recording, CAPTRUST Chief Technology Officer Jon Meyer and Financial Advisors Devyn Duex and Mike Webb are joined by Jennifer Doss, CAPTRUST's senior director and defined contribution practice leader, to discuss:

- DOL cybersecurity guidance and its impact on plan sponsors
- Effective approaches to evaluate and monitor plan providers
- The future of information security in the retirement plan space

Webinar Recap — Practical Cybersecurity Playbook for Plan Sponsors

CAPTRUST's Jennifer Doss moderates a hands-on discussion with Chief Technology Officer Jon Meyer and advisers Devyn Duex and Mike Webb that breaks down the Department of Labor's first-ever guidance on retirement-plan cybersecurity and what it means for fiduciaries.

Why the DOL Weighed In

The agency released three companion pieces in April 2024—one for plan sponsors (vendor selection and monitoring), one for service providers (cyber “best practices”), and a participant-level checklist.

Webb reminds committees the guidance does not create new fiduciary duties; it simply clarifies how the long-standing prudence standard applies to data protection and fraud prevention.

Cybersecurity vs. Cyber-Fraud Prevention

Cybersecurity is the realm of information-security teams: protecting confidentiality, integrity, and availability of systems.

Fraud prevention addresses transactional theft—often human-engineering attacks that occur outside pure IT controls.

Meyer notes that sponsors must assess both arenas; some recordkeepers excel at firewalls but have fuzzy participant-loss indemnification.

What Sponsors Are Asking—and How to Respond

“Do we have to rewrite our IPS?” No, but minutes should show the committee has mapped DOL guidance to current vendor contracts and internal procedures.

“Which questions matter most?” Focus on SOC 1 / SOC 2 results, multi-factor authentication coverage, incident-response testing, and participant-fraud reimbursement terms.

“How often should we review?” At least annually—more frequently after a platform upgrade, M&A event, or breach elsewhere in the industry.

Building a Vendor-Oversight Framework

Pre-hire: Issue a cyber due-diligence questionnaire drawing directly from the DOL’s 12 best-practice bullets; require proof of independent audit and cyber-insurance limits.

Contracting: Embed right-to-audit language, breach-notification timelines, and clear indemnification for both cyber intrusion and participant-level fraud.

Ongoing monitoring: Maintain a standing agenda item for cyber updates, request SOC reports each year, and invite the recordkeeper’s security lead to present findings to the committee.

Action Items You Can Execute This Quarter

Inventory your data flows—which vendors, payroll feeds, and internal systems touch PII or plan assets?

Compare current contracts to the DOL checklist; flag gaps in encryption standards, penetration testing, or participant-loss reimbursement.

Educate participants with the DOL's consumer-facing tip sheet; emphasize registering online access and enabling MFA.

Run a tabletop exercise simulating a fraudulent distribution request to test HR, payroll, and recordkeeper response times.

Document every step—if it isn't in the minutes, regulators will assume it never happened.

Key takeaway: the new DOL guidance doesn't change fiduciary duties, but it does spell out how regulators will judge "prudence" in the digital age. Committees that embed these controls—and record them—can protect participants, satisfy auditors, and sleep better at night.
