SECURE UNIONS .COM
CYBERSECURITY

SECURE UNIONS RESEARCH | PRACTICE BRIEF

The ERISA Fiduciary Cybersecurity Brief

What Taft-Hartley Fund Counsel Need to Know in 2026

A COMPANY OF ONSITE LOGIC
CYBERSECURITY & STRATEGIC IT SERVICES

ORIGINALLY PUBLISHED MAY 2026 SU-BRF-2026-01 | V1.0

SECURE UNIONS .COM
CYBERSECURITY

SECURE UNIONS RESEARCH | PRACTICE BRIEF

ERISA Fiduciary Cybersecurity At A Glance

Cybersecurity is a fiduciary-process issue for ERISA-governed Taft-Hartley funds. This brief outlines how the 2021-2026 regulatory arc has made documented prudence, governance, and oversight central to fund counsel's role.

WHY THIS MATTERS NOW

The question isn't just whether an incident occurred, it's also whether the fund can document that a prudent process was followed before any inquiry arises.

2021

EBSA issued its first cybersecurity guidance in three parts: Best Practices, Tips for Hiring Service Providers, and Online Security Tips for Participants.

2024

EBSA clarified that the guidance applies to all ERISA-covered plans, including health and welfare plans.

2026

Cybersecurity was named a top national enforcement priority for FY 2026.

BEST PRACTICES

EBSA's 2021 guidance covers governance, risk assessment, access controls, encryption, service-provider oversight, incident response, and training.

-$68-$160 PER RECORD

Defensible direct response cost per compromised record in the Taft-Hartley context.

-$340K-$800K

Estimated direct response exposure for a 5,000-participant fund, before litigation, settlements, trustee exposure, or extended credit monitoring.

SHADOW AI BREACHES

IBM's 2025 research identified "shadow AI" — unsanctioned employee AI use — in 20% of analyzed breaches.

+$670K BREACH COST

Average added breach cost associated with shadow AI use.

ACTIONS FUND COUNSEL SHOULD TAKE

DOCUMENTED PRUDENCE

Reflect cybersecurity oversight in agendas, minutes, procedures, and governance records.

INSURANCE COVERAGE GAPS

Review potential gaps between fiduciary liability and cyber liability policies.

SERVICE-PROVIDER OVERSIGHT

Document how vendors are evaluated and monitored.

AI GOVERNANCE

Establish trustee-level rules for employee AI use and data handling.

SECURE UNIONS RESEARCH | PRACTICE BRIEF

The ERISA Fiduciary Cybersecurity Brief

What Taft-Hartley Fund Counsel Need to Know in 2026

Originally published May 2026 *For Fund Counsel and ERISA Practitioners*

> **ABOUT THIS BRIEF.** *This brief is published by Secure Unions Research, the analytical practice of Secure Unions — a managed cybersecurity firm serving ERISA-governed Taft-Hartley benefit funds. It is written for Taft-Hartley fund counsel and other ERISA practitioners and is intended as a practice reference, not as legal advice. Readers should consult their own counsel for advice on specific matters. The Brief reflects published practitioner commentary and regulatory guidance through the date noted above; the field is developing rapidly, and readers should consult current sources as the analysis evolves.*

The 2021–2026 Regulatory Arc

The Department of Labor's treatment of ERISA fiduciary cybersecurity has moved along a deliberate three-step arc since 2021. In April 2021, EBSA issued its first cybersecurity guidance in three parts: *Cybersecurity Program Best Practices* for plan sponsors and service providers, *Tips for Hiring a Service Provider*, and *Online Security Tips* for participants.[1] In September 2024, EBSA issued Compliance Assistance Release No. 2024-01, clarifying that the 2021 guidance applies to all ERISA-covered plans, including health and welfare plans. On the same date, then-Assistant Secretary Lisa M. Gomez stated that EBSA "continue[s] to investigate potential ERISA violations related to" cybersecurity.

In January 2026, EBSA issued Field Assistance Bulletin 2026-01, naming cybersecurity as a top national enforcement priority for FY 2026 — the first such elevation in the agency's regulatory history. The trajectory reflects a sustained and accelerating EBSA focus on cybersecurity as a fiduciary-duty matter. Notably, FAB 2026-01 also reinforces that ERISA is, in EBSA's own characterization, "a law of process, not results" — the agency stating it will generally avoid second-guessing fiduciary decisions where a prudent process is followed.[2] The implication for fund counsel is direct: documented procedural prudence is the defense, and the operative phrase, as Groom Law Group observed in February 2026 commentary on the enforcement priorities change, is to ensure "plan governance, procedures, and documentation are in order before any inquiry arises" — before any inquiry arises, not before any incident occurs.[3]

[1] U.S. Dep't of Labor, Emp. Benefits Sec. Admin., Cybersecurity Program Best Practices (April 2021); Tips for Hiring a Service Provider with Strong Cybersecurity Practices (April 2021); Online Security Tips (April 2021). The September 2024 update is issued as Compliance Assistance Release No. 2024-01.

[2] EBSA Field Assistance Bulletin 2026-01, as analyzed in Snell & Wilmer, "U.S. Department of Labor Signals Shift in ERISA Enforcement Priorities in FAB 2026-01" (April 2026). The bulletin characterizes ERISA as "a law of process, not results" and indicates EBSA will generally avoid second-guessing fiduciary decisions where a prudent process is followed.

[3] Groom Law Group, "DOL Enforcement Priorities Change in 2026" (Feb. 2026), commenting on EBSA's January 2026 National Enforcement Priorities announcement.

From "No Harm, No Foul" to "Documentation Is the Duty"

A common operational premise among fund fiduciaries has been that cybersecurity practices become material only when a cybersecurity incident occurs. Under that premise, the absence of a documented cybersecurity program is a gap that matters retrospectively — relevant if something goes wrong, inconsequential otherwise. The 2026 enforcement posture does not support this premise.

ERISA prudence under § 404(a)(1)(B) has always been a process-based standard. What has shifted is the evidentiary posture in examination. Document request letters issued in EBSA cybersecurity-focused matters now routinely demand "documents mentioning or discussing cybersecurity, including emails and minutes of plan committee or board of trustees/directors meetings where the plan's cybersecurity readiness was discussed."[4] That category of documentation is requested regardless of whether a cybersecurity event has occurred at the plan. The process, not the incident, is what EBSA examines.

The Retirement Learning Center, writing on the 2024 guidance update, drew the right analogy: "Prudent plan committees may also want to consider adding cybersecurity matters as a regular item to their meeting agendas moving forward, analogous to processes in place with respect to adopting, following, and monitoring the terms of investment policy statements and the like."[5] No fund counsel would advise waiting for a catastrophic investment loss before reviewing the IPS. The IPS review is the fiduciary duty. Cybersecurity program oversight is now being treated on the same terms.

The Insurance Coverage Gap

The fiduciary exposure created by this shift sits in a gap between two insurance coverages that most Taft-Hartley funds already carry. The ERISA bond required under Section 412 covers theft of plan assets but does not cover fiduciary-breach claims, cybersecurity incidents, or defense costs. Fiduciary liability insurance, typically carried above the bond, covers ERISA fiduciary-breach claims but has important limits.

Published practice analysis has identified the structural gap. Existing fiduciary liability coverage "will not cover risks relating to state law causes of action (that are not preempted) for data breaches as opposed to ERISA fiduciary liability resulting from a privacy or security breach."[6] Cyber liability insurance covers the state-law causes of action but "may exclude coverage for ERISA violations."[7] The result is a fund carrying both policies that, in a cybersecurity incident generating both ERISA fiduciary claims and state-law privacy claims — the dominant pattern in post-2024 plan-participant litigation — may find that neither policy covers the overlap.

For fund counsel, the practical implication is that a conversation about cybersecurity program implementation is also a conversation about insurance coverage adequacy, and neither can be resolved

[4] Morgan Lewis ML BeneBits, "DOL Continues Active ERISA Enforcement and Focus on Cybersecurity, Including Health and Welfare Plans" (Feb. 2023), summarizing the categories of documentation requested in EBSA cybersecurity-focused audit document request letters.

[5] Retirement Learning Center, "Case of the Week: The DOL's Recent Cybersecurity Guidance Update" (Oct. 2024), published by the National Association of Plan Advisors.

[6] José M. Jara, ERISA Fiduciary Insurance, practice note republished via BenefitsLink, discussing the scope and exclusions of fiduciary liability insurance in the cybersecurity context.

[7] ERISA Advisory Council, Cybersecurity Insurance and Employee Benefit Plans (2022), as summarized by Mercer, noting that cybersecurity insurance policies may exclude coverage for ERISA violations.

without the other. A fund that has implemented the 2021 framework has both the regulatory defense (documented prudence) and the insurance defense (demonstrable reasonable care). A fund that has not is exposed on both axes simultaneously.

ON SCALE

Per-record breach-cost data from IBM's 2025 *Cost of a Data Breach Report* requires careful adaptation to the Taft-Hartley context. The general commercial per-compromised-record figure of approximately $160 includes "lost business" as its largest cost component — customer churn, reputation-driven revenue loss, and replacement-customer acquisition — dynamics that do not apply to multiemployer funds, where participation is governed by collective bargaining and participants cannot freely exit.

The same methodology reports a public-sector per-record figure of approximately $68, drawn from organizations that similarly lack customer-churn dynamics and whose cost profiles are concentrated in detection, notification, and post-breach response.

A defensible range for fund-specific direct organizational response cost therefore falls between $68 and $160 per compromised record. For a 5,000-participant fund, this implies direct exposure of roughly $340,000 to $800,000 — before any civil litigation defense or settlements under ERISA § 502 or state privacy laws, trustee personal-liability exposure under § 409(a), or extended participant credit-monitoring.

Per-record cost modeling is directional rather than precise; independent researchers at the Cyentia Institute have noted methodological limitations in per-record approaches generally. The figures are offered here as scale context, not as definitive exposure estimates.

The Documented-Prudence Framework

The 2021 EBSA guidance comprises twelve best practices covering cybersecurity program governance, risk assessment, access controls, encryption, service-provider oversight, incident response, and training. Individually, none is technically novel. Collectively, they constitute the operational specification of "reasonable care" for ERISA cybersecurity purposes in the current enforcement environment.

A fund that can document adherence to the twelve practices is defensible on three distinct axes: EBSA examination (documented prudence under § 404(a)(1)(B)), plan-participant litigation (demonstrable reasonable care as an affirmative defense), and insurance coverage (the cooperation and reasonable-care conditions in fiduciary liability policies). A fund that cannot document adherence is exposed on all three. The framework is not cybersecurity best practice as a technical matter — it is the documentary and operational foundation on which every defensive position depends.

AI Governance: The Newest Layer

A distinct development requires separate attention. Over the past eighteen months, staff at fund offices have increasingly adopted consumer-grade generative AI tools — ChatGPT, Claude, Gemini, Copilot — in day-to-day work, frequently without formal approval or a governance framework. The parallel to the legal profession's own AI adoption curve is instructive. Law firms have converged on closed-system, domain-specific deployments — Harvey, Thomson Reuters' CoCounsel, LexisNexis Protégé, and firm-hosted

enterprise models — because consumer-grade open-system tools are incompatible with attorney-client privilege and client confidentiality obligations. Firmwide enterprise deployments of these platforms by major law firms accelerated through 2025.

The fiduciary analysis for Taft-Hartley funds is structurally analogous. Participant data entered into an open-system AI tool has been disclosed to a third party without a service agreement, without security review, and without the trustee-level oversight the 2021 framework requires. IBM's 2025 research identified "shadow AI" — unsanctioned employee AI use — in 20% of breaches, adding an average of $670,000 to breach costs.[8] Funds that have not established an AI-use policy at the trustee level are, as a practical matter, permitting a form of third-party data disclosure that would not be permitted through any other channel.

Practice analysis published through 2025 and 2026 has identified AI-related risks as squarely within ERISA fiduciary obligation. Jackson Lewis attorneys writing in Benefits Law Advisor have observed that "[r]eliance on 'black box' AI systems — where the internal logic is opaque — could run afoul of ERISA's prudence standards."[9] Practitioner commentary in March 2026 confirms that EBSA has incorporated cybersecurity questions into standard plan audit protocols, with investigators now requesting documentation regarding cybersecurity policies, service provider agreements, and incident response procedures.[10] Counsel should anticipate that AI governance documentation will be examined within the same framework, and that the absence of a documented policy will receive scrutiny on terms similar to any other gap in the documented cybersecurity program.

Practical Considerations for Fund Counsel

Three considerations follow from the foregoing for counsel preparing to advise trustees under the post-2026 enforcement posture:

First, cybersecurity program oversight belongs on the standing trustee agenda, not in the service-provider-oversight file. A fund whose trustee minutes reflect no cybersecurity discussion in the calendar year is in a documentation gap that is difficult to cure retrospectively.

Second, the fund's insurance portfolio should be reviewed against the specific coverage gap between fiduciary liability and cyber liability policies. Questions to carriers about ERISA exclusions in cyber policies, and state-law privacy exclusions in fiduciary policies, frame the relevant analysis.

Third, AI governance is developing faster than formal guidance. Counsel who raise it now are likely to be seen by trustees as anticipating a foreseeable exposure rather than reacting to an examination finding.

[8] IBM Security / Ponemon Institute, Cost of a Data Breach Report 2025, identifying "shadow AI" as a factor in approximately 20% of analyzed breaches, adding an average of $670,000 to total breach costs.

[9] Melissa Ostrower & Joseph J. Lazzarotti, "Harnessing AI Under ERISA: A Compliance and Oversight Guide for Retirement and Health Plan Fiduciaries," Benefits Law Advisor (July 2025) (Jackson Lewis P.C.).

[10] "Cybersecurity in the Age of AI: Best Practices for Employee Benefits Administration," National Law Review (March 2026).

Coming Next in the Series

The next Brief in this Series — *The AI Governance Brief*, planned for June 2026 — addresses the AI corollary of the documentation-of-prudence framework. AI is already in fund operations, primarily through service providers acting on the fund's behalf. The next Brief examines what the prudent process looks like at the layer where the technology has been moving most quickly and most quietly.

About Secure Unions

Secure Unions is a managed cybersecurity firm serving ERISA-governed Taft-Hartley benefit funds. Our work is structured around the 2021 DOL cybersecurity best-practices framework and the trustee-level governance documentation the post-2026 enforcement environment now expects. We publish this brief to support the fund counsel community and do not solicit engagement through this publication. Counsel with questions about a particular fund's posture are welcome to contact us directly for a confidential peer conversation — no engagement required, no follow-up sales process.

Disclosure. Secure Unions develops and operates Guardbox AI, an on-premises closed AI appliance designed for labor union benefit fund offices, leased to fund offices on a fixed monthly basis. The brief is published as analytical commentary, and subscribers do not receive product outreach through this publication. Counsel evaluating any specific cybersecurity, AI, or service-provider deployment should conduct independent diligence appropriate to the fund.

SUBSCRIBING TO THE SERIES

Counsel may request notification of future installments in the Secure Unions Research Practice Brief Series at **SecureUnions.com/counsel**. Subscribers receive each installment upon publication and are not placed on sales-outreach lists. If you received this Brief from a colleague, the same channel is open to you.

Secure Unions Research | SecureUnions.com | 913-851-7483