SEPTEMBER 2025

CyberSecure
FOR LOCAL UNIONS

12

Six Questions to Help You Establish and Maintain Cybersecurity Compliance with Service Providers

Marsha R. Woodward
Director, Haynes Benefits PC

Cybersecurity breaches make headlines regularly, and the field is becoming increasingly complex as new threats emerge.

04

Third-Party Cybersecurity Oversight is Your Responsibility — Legally

Rebecca Rakoski
Co-Founder and Managing Partner, XPAN Law Partners

ERISA fiduciary cybersecurity responsibilities don't end at your office doors

14

Cybersecurity Guide for JATC Training Directors

Jason Kotlyarov
Attorney, Kutak Rock LLP

JATCs must comply with DOL cybersecurity best practices despite operating with limited budgets.

SECURE UNIONS .COM
CYBERSECURITY

LETTER FROM THE EDITOR

Cybersecurity Corner

Strong Unions Deserve Strong Security

In this issue of CyberSecure, we're leaning into a hard truth: Cybersecurity isn't just an IT task anymore, it's a leadership responsibility.

The threats are growing, the regulations are tightening, and the Department of Labor has made one thing clear: **if you're involved in managing benefit plans, you're also on the hook for protecting the data behind them**.

You probably didn't sign up for that. But if you're reading this, you've already shouldered it.

When Change Healthcare went dark, you kept the wheels turning (full story on page 8). You answered the phones. You worked through the mess. You did what union professionals always do: you showed up. Even though no one handed you a medal when it was over.

That story isn't the focus of this issue, but it's the backdrop. Because the real heart of this edition comes from the legal experts who lay out what's required now: how fiduciary responsibility extends to cybersecurity, how to evaluate your vendors, and how to document the work you're already doing so it holds up if you're ever asked to prove it.

This isn't about fear. It's about clarity. It's about knowing where you stand, what the law expects, and how to protect the people who count on you — your members.

So, we've included a new Cybersecurity Applicability Questionnaire to help you see exactly where your office stands and where it needs to go next. If you've been meaning to get started, now's the time. This tool, along with the insights in this issue, can help you move from thinking about compliance to actually building it, one practical step at a time.

Because at the end of the day, this isn't just about rules, it's about responsibility. And no one is better suited to carry that than the people who already protect workers' futures for a living. So, let's keep going. Let's keep getting stronger. And let's do it together.

Tim New
Secure Unions Founder/CEO

TimNew@SecureUnions.com
913-851-7483
SecureUnions.com

IN THIS ISSUE | **SEPTEMBER 2025**

Data Map

02
Cybersecurity Corner
Tim New
Secure Unions Founder/CEO

Tim New fills you in on the latest in cybersecurity.

04
Third-Party Cybersecurity Oversight is Your Responsibility — Legally
Rebecca Rakoski
Co-Founder and Managing Partner, XPAN Law Partners

ERISA fiduciary cybersecurity responsibilities don't end at your office doors

08
Inside the Breach That Crippled a Healthcare Giant and Left Union Funds Holding the Bag
Tim New
Secure Unions Founder/CEO

A breakdown on the 2024 ransomware attack on Change Healthcare, a processor handling 15 billion annual healthcare transactions.

12
Six Questions to Help You Establish and Maintain Cybersecurity Compliance with Service Providers
Marsha R. Woodward
Director, Haynes Benefits PC

Cybersecurity breaches make headlines regularly, and the field is becoming increasingly complex as new threats emerge.

14
Cybersecurity Guide for JATC Training Directors
Jason Kotlyarov
Attorney, Kutak Rock LLP

JATCs must comply with DOL cybersecurity best practices despite operating with limited budgets.

17
Save These Dates
A list of beneficial upcoming labor, benefit, and cybersecurity-related events and conferences around the nation.

18
ERISA Cybersecurity Applicability Questionnaire
This questionnaire will help you determine if your union or fund office is subject to the ERISA cybersecurity requirements laid out in the Department of Labor's (DOL) Employee Benefits Security Administration (EBSA) Cybersecurity Best Practices.

COMPLIANCE

Third-Party Cybersecurity Oversight is Your Responsibility — Legally

ERISA Fiduciary Cybersecurity Responsibilities Don't End at Your Office Doors

Rebecca Rakoski
Co-Founder and Managing Partner, XPAN Law Partners

SECURITY SNAPSHOT

Under ERISA, plan fiduciaries face increasing legal liability for cybersecurity breaches involving participant data. DOL guidelines require fiduciaries to evaluate vendor cybersecurity practices, conduct ongoing monitoring, and maintain documentation of oversight efforts. Trustees can be held personally liable for breaches resulting from inadequate vendor selection or monitoring, violating trustee duties of prudence and loyalty. Third-party vendors pose significant risks as potential entry points for cyberattacks. Key protections include thorough vendor due diligence, robust contract provisions, comprehensive documentation, ongoing audits, and retaining specialized cybersecurity legal counsel. Proactive cybersecurity oversight is now a legal imperative, not just best practice.

Under the Employee Retirement Income Security Act (ERISA), plan fiduciaries and sponsors are subject to duties of prudence and loyalty — which courts and regulators increasingly interpret to require careful vendor selection and robust ongoing cybersecurity oversight, especially for vendors with access to protected health information (PHI) and personally identifiable information (PII).

The Department of Labor's (DOL) Cybersecurity Guidelines emphasize fiduciaries must evaluate vendor cybersecurity practices, require breach notifications, conduct risk assessments, require vendor audits, and maintain documentation of oversight efforts. DOL guidelines also clarify that fiduciaries are responsible for cybersecurity oversight of vendors. A fiduciary duty includes protection of plan assets, which may include PII/PHI and certainly extends to the financial aspects of the plan. Furthermore, there's some discussion that data itself could be considered a plan asset subject to fiduciary protection, regardless of whether financial loss occurs.

Given the amount of financial transactions funds deploy, and the large amount of plan assets being distributed, it's no wonder the DOL issued cybersecurity guidance in an effort to protect the benefits of America's workers. In addition to the direct threat to plan assets that threat actors/hackers pose, there's a growing wave of litigation concerns involving cybertheft-related fraud, and an argument that plan sponsors could face liability for insufficient vendor cybersecurity practices even for subcontractor breaches.

> **The concept of liability for fiduciaries is not new**, and certainly has not developed simply in response to DOL guidelines, but those guidelines do provide a roadmap for any plaintiff's attorney to demonstrate a breach of a fiduciary duty.

Trustees can be sued for a data breach resulting from failure to uphold their fiduciary duties. Trustees are responsible for managing plan assets and participant information with a high level of diligence, including ensuring that appropriate cybersecurity measures are in place to protect sensitive data. If the trustees neglect to adopt reasonable data protection policies, fail to monitor third-party service providers, or ignore industry standards for cybersecurity, they may be deemed to have breached their fiduciary duty of care. Such negligence could expose them to significant legal liability if participants suffer harm from a breach.

Fiduciary duty also requires trustees to act solely in the interest of plan participants and beneficiaries. If a data breach leads to identity theft, financial loss, or medical fraud, and it can be shown that the trustees knew of certain and/or specified vulnerabilities but failed to act, plaintiffs could argue that the trustees prioritized convenience or cost savings over participant protections. By law, this would violate the duty of loyalty. Courts could find that trustees breached their obligations by failing to act prudently in the selection and oversight of service providers that handle participant data, especially if those providers lacked proper cybersecurity safeguards

CONTINUED *on page 6 ...*

CONTINUED *from page 5 ...*

Lawsuits against trustees in such cases may be brought under federal statutes like ERISA, which imposes fiduciary duties on those managing employee benefit plans. Additionally, plaintiffs could raise state law claims such as negligence or breach of confidence, depending on the circumstances. **More significantly, and arguably triggering further-**

> In sum, **proactive vendor risk management is not just a best practice** but a legal imperative for fiduciaries managing modern benefit plans.

reaching consequences, if the trustees failed to maintain confidentiality of personal health or financial information, and this resulted in harm to plan members, it has been suggested courts may hold these trustees personally liable. In order to mitigate this risk, trustees must implement robust cybersecurity protocols, routinely assess their effectiveness, and document all actions taken to protect participant data.

Therefore, third-party vendors — like recordkeepers, claims administrators, and IT providers — pose a significant cybersecurity risk to benefit plans. These vendors often have access to sensitive participant data, making them potential entry points for cyberattacks. As established above, trustees have a fiduciary responsibility to ensure vendors safeguard member data by following the same strict guidelines they have to themselves. Courts and regulatory agencies, including the Department of Labor, have emphasized that fiduciaries cannot outsource their obligations. Failing to properly vet and monitor vendors is a breach of the trustees' duty of prudence. This includes assessing vendors' cybersecurity policies, incident response plans, encryption standards, and past breach history, for example.

If a data breach occurs from a vendor's failure to protect participant information, trustees will be scrutinized to verify they exercised due diligence in selecting and overseeing that vendor. If they didn't, those trustees will be held liable.

Fiduciaries are expected to conduct thorough initial evaluations and ongoing audits to ensure vendors meet industry security standards. This includes executing robust service agreements that clearly define security expectations, breach notification protocols, and liability provisions. Accordingly, if trustees fail to take these precautions and a breach results in participant harm, like identity theft or financial fraud, trustees could face lawsuits for breach of fiduciary duty under ERISA and related state claims.

Conclusion

ERISA fiduciary duty litigation tied to data privacy and cybersecurity is evolving rapidly. Combined with escalating DOL guidance and commentary treating PII/PHI as plan assets, fiduciaries must proactively integrate robust cybersecurity oversight into their ERISA compliance frameworks to mitigate litigation and regulatory risk. Trustees have a critical fiduciary obligation to protect the sensitive personal and health information of plan participants, which includes proper oversight of data security practices. A failure to implement and maintain reasonable cybersecurity measures, or to conduct due diligence when selecting and managing third-party vendors, can expose trustees to significant legal liability. As data breaches become increasingly common and costly, courts and regulators are holding fiduciaries to higher standards of care and vigilance. Therefore, in order to fulfill their legal and ethical responsibilities, trustees must deliberately prioritize cybersecurity as an essential element of plan administration, regularly reviewing internal practices and ensuring that all service providers meet strict data protection requirements. Taking these steps is not only necessary to protect participants but also to shield trustees from potential lawsuits and reputational harm, not only in a business capacity but possibly a personal one as well.

WHAT TO DO:

1. Cybersecurity due diligence must be specific, including vendor and subcontractor technology reviews, incident history, and breach response protocols.
2. Ongoing monitoring expectations should be part of fiduciary governance: Audits, annual reviews, red flag tracking, two-factor security measures, and documented oversight actions are essential.
3. Contract provisions must comprehensively cover cybersecurity, breach-notification obligations, indemnity, and audit rights that includes the vendor chain. A contract should provide vendors with the fund's expectations and provide a roadmap for liability and responsibility in the event of a data breach.
4. Documentation matters: meeting minutes, vendor questionnaires, incident reports, and risk assessments help demonstrate fiduciary prudence. Also, funds should have a documented cybersecurity and data privacy program with supporting evidence to demonstrate compliance. Rote policies drafted by IT are not sufficient. These are the legal documents that show how the fund complies with its legal obligations.
5. Documented, consistent remediation of vendor incidents, even if not related to your plan, can support a defense against monitoring claims.
6. Retain qualified cybersecurity and data privacy legal counsel to guide the fund through to its legal obligations. Always utilize an attorney with deep insight and experience in cybersecurity and data privacy. This is not an area for fund counsel to "assess on the fly" due to the nuances and interconnection between state and federal laws, as well as sudden complexities that can arise especially after a cyber event or responding to regulatory enforcement actions.

Rebecca L. Rakoski *is a co-founder and managing partner at XPAN Law Partners LLC, a boutique cybersecurity and data privacy law firm. She analyzes client legal obligations and creates tailored cybersecurity and data privacy programs. She also advises clients on proactive, multi-jurisdictional approaches to data privacy and security legal issues, helping them identify and address compliance gaps and corresponding legal liabilities. Rebecca currently serves on the Board of Governors for Temple University Health Systems and is the Acting Dean of Online Learning at Drexel University's Thomas R. Kline School of Law, where she teaches cyber law, international data privacy, and enterprise risk management as an adjunct professor.*

SECURITY SNAPSHOT

In February 2024, ransomware group ALPHV/BlackCat attacked Change Healthcare, a processor handling 15 billion annual healthcare transactions. The breach was caused by a lack of multifactor authentication (MFA) on a Citrix portal, which attackers exploited using stolen credentials. They accessed systems for nine days before deploying ransomware and stealing six terabytes of data including PHI and PII. The MFA vulnerability existed because Change Healthcare, acquired by UnitedHealth Group in 2022, hadn't been integrated under UHG's security standards. UnitedHealth reportedly paid a $22 million Bitcoin ransom. Union funds faced halted claims, frozen payments, and communication blackouts, exposing third-party risk management gaps.

CRITICAL UPDATE

Inside the Breach That Crippled a Healthcare Giant and Left Union Funds Holding the Bag

Tim New
Founder/CEO, Secure Unions

When Change Healthcare, a back-end processor responsible for more than 15 billion healthcare transactions annually, went offline in February 2024, the disruption was immediate and widespread. Pharmacies couldn't confirm eligibility. Claims stopped mid-stream. Payments were suspended indefinitely. But this wasn't a technical glitch, or a system upgrade gone wrong. It was a deliberate ransomware attack.

The threat actors behind the attack, organized cybercriminal syndicate ALPHV/BlackCat, used stolen credentials to access a Citrix remote access portal that lacked even the most basic cybersecurity control: multifactor authentication (MFA). That single vulnerability was the digital equivalent of leaving a back door propped open with a brick. Once inside, the attackers quietly navigated Change Healthcare's internal systems for nine full days, harvesting data and laying the groundwork to paralyze operations.

When the ransomware payload detonated on February 21, more than six terabytes of data — including protected health information (PHI) and personally identifiable information (PII) — had already been nabbed.

At the heart of the breach was a breakdown in change management. Change Healthcare was acquired by UnitedHealth Group (UHG) in 2022 and was still undergoing integration into UHG's infrastructure at the time of the attack. According to sworn congressional testimony by UHG CEO Andrew Witty, the Citrix system exploited in the attack had not yet been updated to UHG's security standards, including MFA requirements. That delay proved catastrophic.

In the days following the breach, it became clear the attack was a calculated act of cyber extortion. UHG reportedly paid a $22 million ransom in Bitcoin to the attackers in an attempt to restore operations and limit further exposure of stolen data. That wasn't the end of the story.

In April 2024, a second criminal group, possibly linked to ALPHV or one of its affiliates, claimed to have retained additional stolen data and issued a fresh extortion demand. While UnitedHealth has not confirmed a second payment, the mere existence of another threat underlines how difficult it is to regain control once a breach has occurred, and how easily threat actors can replicate, share, or resell compromised data.

The Fallout for Union Funds

Union offices that relied directly on Change Healthcare systems, or used third-party administrators and processors that did, found themselves in the dark. Claims submissions halted. Reimbursement checks didn't go out. Pharmacy benefit systems froze. Fund liquidity was impacted as cash-flow planning collapsed.

Perhaps more troubling than the disruption itself was the communication vacuum that followed. Many fund administrators said they were never contacted by Change Healthcare or UnitedHealth directly. Instead, they discovered the outage the same way participants did, when systems failed. For some, the only "official" word came days later, filtered through downstream vendors.

The timing couldn't have been worse. In recent years, fund administrators have faced increasing pressure to comply with Department of Labor (DOL) cybersecurity best practices, particularly around third-party risk management and data protection. This breach exposed not just a vendor's failure, but a governance blind spot that now sits squarely in the crosshairs of fiduciary responsibility.

UnitedHealth Was a Victim, Too

To be clear: UnitedHealth Group was a victim of a highly coordinated criminal attack. After discovering the intrusion, UHG immediately retained multiple industry-leading cybersecurity and incident response firms, initiated a full-scale system rebuild, and worked with regulators, law enforcement, and government agencies. MFA was promptly enforced across remaining unsecured systems, and containment efforts prevented the breach from spreading beyond Change Healthcare's network segment.

But good intentions don't erase consequences. The integration delay that left Citrix without MFA was known. The gap between acquisition and full security alignment proved longer and more dangerous than anticipated. And while UHG's internal response was swift, external communication lagged, leaving thousands of affected organizations struggling to understand what had happened and how to respond.

In the end, UnitedHealth may have paid the ransom. But union funds paid the price — in time, in trust, and in exposure they never agreed to.

Takeaways for Fund Fiduciaries

This was a governance failure as much as a cybersecurity lapse. Citrix without MFA, lack of DLP, zero detection for data exfiltration — all rooted in change management failure during an acquisition. But the responsibility doesn't stop at the vendor's doorway; once a vendor is compromised, you answer the phones.

Union funds must transform from passive service consumers into empowered guardians:

- Don't just rely on vendor claims, ask for audits of their controls.
- Embed MFA, DLP, EDR requirements into every agreement.
- Run tabletop exercises that include vendor downtime scenarios.
- Don't wait when disruption lands. Track your losses, document your exposure, and engage legal counsel promptly.

WHAT | HOW | WHEN

Entry Point: Citrix

Citrix is a remote access platform that allows offsite users to access internal systems like they're onsite. It's widely used in healthcare and finance for system centralization. In this case, the Citrix portal didn't require multifactor authentication (MFA). Once cybercriminals acquired valid credentials — likely through phishing or credential stuffing — they logged in undetected. Without MFA, there was nothing to stop them.

Multifactor Authentication (MFA) Explained

MFA adds a second verification step beyond a username and password, like a code sent to your phone or a biometric check. Even if credentials are stolen, MFA blocks unauthorized access. It's an extremely simple and extremely effective cybersecurity control. In this case, Change Healthcare hadn't yet enabled MFA on its Citrix systems.

DLP: The Missing Layer That Let 6 TB of Data Walk Out the Door

Data Loss Prevention (DLP) tools monitor for suspicious data movements, like someone copying huge amounts of sensitive records to an external server. Had DLP been properly configured, the exfiltration of nearly six terabytes of PHI and PII over nine days could have triggered alerts, or the transfers could've been blocked entirely.

CONTINUED *on page 10* ...

... CONTINUED *from page 9*

Timeline of the Attack

FEBRUARY 12, 2024
Attackers access Change's Citrix portal using stolen credentials (no MFA enabled on Citrix).

FEBRUARY 12–20, 2024
Intruders download approximately six terabytes of sensitive health and identity data.

FEBRUARY 21, 2024
Ransomware is deployed across Change systems, disrupting claims, pharmacy transactions, and payments nationwide.

LATE FEBRUARY – EARLY MARCH 2024
Change Healthcare allegedly pays the cyberattackers a $22 million ransom in Bitcoin.

APRIL 2024
A second extortion attempt emerges from a group claiming to hold additional stolen data.

JULY 2024 *AND BEYOND*
United Health Group begins breach notifications; class action lawsuits are consolidated; federal investigations continue.

Should Your Fund Be Going After Money?

If your fund experienced tangible harm — delayed claims, financial strain, member service issues — you should considering joining the multi-district litigation (MDL) class action lawsuit against Change Healthcare. Document your fund's losses and additional expenses, and talk with your legal counsel to join in the Provider Track.

TAKE ACTION NOW! 3 Steps for Fund Offices

1	**Join the MDL** *(class action suit)*	If your fund had delayed reimbursements or claims processing, consult legal counsel about provider class inclusion.
2	**Track restitution**	For your team: monitor settlement updates — especially class certification and notice dates, as they can affect eligibility.
3	**Pressure for funds**	Advocate for fund-specific compensation for administrative costs, participant complaints, and fiduciary risks, not just provider losses.

ALPHV / BlackCat The Ransomware Kingpin

Who they were, how they operated, and how the threat endures today.

Born from the ashes of infamous cybercrime syndicates

First observed in **November 2021**, ALPHV—also known as **BlackCat** or **Noberus**—emerged as a sophisticated **ransomware as a service (RaaS)** platform written in Rust. Its operators allegedly include former members of DarkSide and REvil, and **they offer affiliates up to 90% of the ransom payment, making it one of the most lucrative RaaS operations around**.

A public extortion billboard

Where others hid in darknet forums, ALPHV went public. Affiliates would post **victim data samples** on an open web portal — or even mimic victim websites — to pressure targets into paying. This "double" or even "triple extortion" tactic (encrypt, expose data, threaten service disruption) typifies BlackCat's aggression.

High-value targets

ALPHV has targeted hundreds of organizations globally, including MGM Resorts, Caesars, Reddit, and numerous healthcare institutions. In **February 2024**, it launched the devastating Change Healthcare attack, one of the largest U.S. healthcare breaches.

What Is RaaS?

And who exactly are these "affiliates"?

Ransomware-as-a-Service (RaaS) is the **cybercrime version of Third Party Administration**. Instead of a single hacker doing everything — from writing the malware to negotiating the ransom — RaaS splits the process between different players, each with a specialty. It's a business model that has **industrialized extortion** on a global scale.

Here's how it works:

The RaaS Platform Operators

These are the core developers. They write the ransomware code, maintain the infrastructure, and manage the encryption/decryption keys. Groups like **ALPHV/ BlackCat** run these platforms. They don't always carry out attacks themselves—they license their software to others.

The Affiliates

Affiliates are the "boots on the ground." **They gain access to victims — often through phishing, stolen credentials, or exploiting vulnerabilities** — and then deploy the ransomware payload. In return, they **split the ransom with the platform operator, usually keeping 60% to 90% of the payment**.

Affiliates come from all over the world. Many are part of independent hacking crews or are ex-members of defunct groups like REvil or Conti. They don't have to write code, just know how to break in and upload the payload.

What the RaaS Platform Provides

- The ransomware software
- A control panel to track infections
- Encryption/decryption key management
- Payment portals on the dark web
- Leak sites for public extortion pressure
- Customer support for ransom victims

ALPHV even developed a searchable public leak site indexed on Google and offered an API to let affiliates automate pressure tactics, such as timed data leaks if payment deadlines weren't met.

SECURE UNIONS.COM
CYBERSECURITY

ILA must express our sincere gratitude for Secure Union's exceptional security, cybersecurity services and the profound impact they've had on our organization.

Secure Union's security team has **fundamentally transformed our approach to security**. We particularly appreciate how they've made cybersecurity accessible and relevant to our entire team. **What truly sets their team apart is their commitment to education**. Rather than simply implementing security measures behind the scenes, they've taken the time to help us understand the importance of cybersecurity and empowered us with knowledge to make smarter decisions in our daily digital interactions. This has also allowed us to become active participants in our own security posture.

Secure Union's security team **ROCKS!**

ELISE DIXON
Fund Manager

INTERNATIONAL LONGSHOREMEN'S ASSOCIATION

SECURITY SNAPSHOT

Your ERISA plan fiduciary cybersecurity compliance responsibilities don't end with your office, they also include your service providers! It is your ongoing duty to prudently select, monitor, and hold providers accountable for cybersecurity standards. Fiduciaries must ensure all providers and their subcontractors meet the same compliance requirements, maintain regular communication about emerging threats, and provide documented evidence of security measures. Red flags include vague responses, unfair liability terms, and inadequate insurance coverage. The article emphasizes proactive measures like encryption, staying informed about industry breaches, documenting decision-making processes, and continuously evolving cybersecurity practices alongside advancing technology.

UPDATE

Six Questions to Help You Establish and Maintain Cybersecurity Compliance with Service Providers

Marsha R. Woodward
Director, Haynes Benefits PC

Cybersecurity breaches make headlines regularly, and the field is becoming increasingly complex as new threats emerge. This Q&A-style article is part two of a series highlighting key concepts and legal considerations for creating and maintaining a cybersecurity compliance action plan. This particular article focuses on finding responsible service providers, ensuring their compliance aligns with your plans and offices, and maintaining a relationship of compliance with these providers over time.

1 Why do I need to address cybersecurity with service providers?

The cybersecurity compliance process does not end with hiring an IT professional or third-party administrator. Though delegation of responsibility is an important part of your action plan, it is only a first step in an ongoing, dynamic process. Both ERISA rules and federal regulations require all ERISA plan fiduciaries to use reason and prudence in selecting service providers, to require those providers to follow the rules that apply to your plan, to monitor the providers you select, and to take swift and appropriate action when concerns arise. This process extends from initial interviews with providers until the last bit of protected information is either destroyed or returned to you. These duties apply even after your contractual relationship has ended. As with any fiduciary duty, personal liability could result if appropriate action is not taken and a breach occurs.

2 Where are your service providers in the compliance process?

Service providers should be fully compliant with all requirements of the laws and regulations that apply to your plans and offices. Providers should furnish information about their compliance with the same best practices you have learned and used to evaluate your own in-house cybersecurity. If subcontractors are used, they must be held to the same standards and answer the same compliance questions as your offices and plans. Regular communication and evidence of a dynamic process with consistent evolution to ward off emerging threats is essential. The more documentation you have illustrating compliance with best practices, the better.

3 Who do your providers use to help them achieve compliance?

Any cybersecurity compliance program is only as strong as the weakest point of contact with protected information. Service providers must identify any entity associated with or providing services to them. All questions about security, the use of protected information, or contractual and insurance protections should be seriously addressed in sufficient detail, with documentation to back it up. Any business conflicts or incentives should be identified and addressed early in the process. Promises or guarantees must be in writing. Any question you ask your own plans or offices and service providers must be asked of any and all related entities. You should have access to documentation confirming compliance at all times.

4 How often do I need to check in with my service providers?

Regular monitoring is the legal standard. At minimum, annual reviews are recommended. Additionally, address cyber protection and insurance coverage at every contract change or renewal, whenever policies and procedures change, and whenever an incident — not just a breach — occurs. A business merger or acquisition should prompt inquiries as if you are beginning a relationship with a new company. You should be told when any service provider or third party has a cybersecurity incident — not just a breach — or is in the news or social media as impacted by an incident, with regular updates until the matter is fully resolved.

5 What are "red flag" responses from my service providers?

Challenge providers who deliver a different product or response than was promised in initial presentations and marketing communications. If a statement is unclear or vague, it should be immediately clarified upon inquiry. Contract terms that unfairly place liability on you or the plan, or aggressively limit the liability of the service provider, are not acceptable. Each party should bear responsibility for regulatory penalties or fines for their breach, which can be the most expensive part of an incident. Inconsistent communications should be rectified quickly, along with an explanation of how and why they occurred. Insurance coverage should be sufficient to cover costs of litigation, audit defense, and notifications to participants, along with the cost of correcting the breach and any fines or penalties.

6 How else can I protect my union and fund office?

Be proactive. Encrypt everything, in movement and at rest. Pay attention to news and social media breach notices and find out whether the entities named have ever had access to information from your offices or plans. Document everything that shows your effort and decision making prudence. Be curious about new technology, how it is used, and how it can be misused. Talk with others in your industry about what they are doing proactively to protect their offices and plans. Talk with professionals at conferences and training events and take any new or unusual ideas back to your professionals for evaluation. Pay attention to the process and evolve with technology.

Marsha Woodward *is a director at Haynes Benefits PC, a Kansas City, Missouri firm whose sole focus involves advising clients on the laws affecting the entire landscape of employee benefit plans. The nationally recognized attorneys of Haynes Benefits PC are experienced and focused, providing practical legal counsel and education-helping to prepare their clients for whatever comes next. Learn more about the services and attorneys by visiting haynesbenefits.com.*

GUIDE

Cybersecurity Guide for JATC Training Directors

Jason Kotlyarov
Attorney, Kutak Rock LLP

SECURITY SNAPSHOT

JATCs must comply with DOL cybersecurity best practices despite operating with limited budgets. In 2024, the DOL clarified that JATCs face the same cybersecurity requirements as retirement and health plans. Training directors should review DOL guidance, conduct comprehensive cybersecurity inventories covering data storage, access controls, policies, and insurance, then communicate findings to their Board of Trustees. Failure to report issues could result in personal liability. Given budget constraints, JATCs should implement feasible measures while working with attorneys and cybersecurity professionals to prioritize improvements and develop creative solutions for protecting apprentice and staff data.

JATCs are some of the most complicated ERISA funds to administer because they operate simultaneously as an ERISA plan, a business/employer, and a registered apprenticeship program. This means they must follow relevant rules and regulations for all the above.

In 2024, the Department of Labor (DOL) issued "DOL Compliance Assistance Release No. 2024-01," clarifying that JATCs should do their best to follow the DOL's cybersecurity best practices. Unfortunately, the release made it clear the DOL intends to hold JATCs responsible for cybersecurity measures currently imposed on retirement and health/welfare plans, which isn't necessarily practical or realistic. This article is a starting point to help JATC training directors and coordinators find their footing and take control of their JATC's cybersecurity.

DOL's Cybersecurity Guidance

The first thing a training director should do is familiarize themselves with existing DOL cybersecurity guidance. They are: "Cybersecurity Program Best Practices," "Tips for Hiring a Service Provider", and "Online Security Tips." All three documents are on the DOL's website — scan the QR code next to this paragraph to access them. We won't address the guidance in these documents in detail here. If you have specific questions on this guidance, contact Secure Unions and/or an experienced JATC-focused attorney.

Visit **DOL** online for their cybersecurity guidance.

Take Inventory

We're talking about more than taking physical inventory, here. The training director should familiarize themselves with the following:

- [ ] **What data does the JATC collect for both students and staff and how is it stored?**
  Data includes everything from personnel files to disciplinary records and applications.
- [ ] **Who has access to that data? Has access been appropriately restricted?**
- [ ] **Does the JATC have a formal, well-documented cybersecurity program?**
  If so, is it actually being followed? Does the program include a breach response plan?
- [ ] **Does the JATC have a data and document retention policy?**
  If so, is that policy actually being followed? Not following an existing policy is a negative in the event of a DOL audit.
- [ ] **Does the JATC conduct cybersecurity training for its staff?**
  If so, how often is that training conducted? What cybersecurity training is done when onboarding new hires and is it good enough?
- [ ] **Does the JATC have an annual third-party audit of its security controls?**
- [ ] **Where are passwords kept and who has access to them?**
  Keeping passwords on piece of notebook paper in the training director's drawer is not sufficient protection for the DOL.
- [ ] **What cyber liability or other insurance policies exist to cover a cybersecurity incident loss?**
  If there is an insurance policy, what does the policy cover and when does the carrier need to be notified of an incident to avoid a lapse in coverage?

CONTINUED *on page 16 ...*

... **CONTINUED** *from page 15*

Communicate Inventory Results with Board of Trustees and Cybersecurity Professionals

Once inventory is taken, the training director should present their findings regarding any concerning issues to the Board of Trustees. The Board of Trustees is the ultimate decision maker for the JATC, but the Board cannot decide to remedy an issue it's not aware of. If the training director discovers an issue regarding cybersecurity protocol failures or policies not being followed, the JATC's attorney and the Board of Trustees should be notified as quickly as possible. If the training director fails to notify the Board of such an issue in a timely fashion, the training director could be held personally liable for the consequences of their failure to address such issues, depending on the facts and circumstances. The training director should also work with the JATC's attorney and a cybersecurity services provider (if one is retained by the JATC) to ensure the program is running in a manner that adheres to guidelines as best as possible.

Budgetary Issues

The cybersecurity solutions recommended in the DOL's Cybersecurity Program Best Practices can be very costly because the document was initially written specifically for retirement plans. Unfortunately, many JATCs are often the least funded compared to companion benefit plans of their unions and may not have the resources to implement all best practices listed by the DOL. The DOL has not addressed how a JATC, or other employee benefit fund with limited means should prioritize which practices to implement if the budget is simply not there to meet all the best practices.

A JATC's "best practice" (for lack of a better term) for compliance with the DOL's cybersecurity guidance is for training directors to implement what they can, and work with the JATC's attorney, Board of Trustees, and cybersecurity service provider to:

> **Take Inventory:** Learn what cybersecurity measures and practices the JATC has and where such practices are deficient, then shore up those deficiencies as best as possible.
>
> **Communicate with Trustees:** Do your best to work with your Board of Trustees to ensure that data related to the JATC, staff, and apprentices remains safe, while being mindful of any budgetary concerns.
>
> **Work with Professionals:** Use the team of professionals assembled by the JATC, including the attorney and the cybersecurity services vendor to understand and implement existing practices and come up with creative solutions to keep JATC data safe.

Jason Kotlyarov *focuses his practice on providing full-service representation to employee benefit plans, plan sponsors and fiduciaries, which includes issues pertaining to governance, compliance, amendment/policy review and drafting, contract negotiation and litigation. Jason primarily represents multi-employer plans, including defined benefit plans, defined contribution plans, welfare plans and apprenticeship plans. He is regularly invited to speak on and train fiduciaries on ERISA-related topics with recent speaking engagements at the International Foundation of Employee Benefit Plans Institute for Apprenticeship Training and Education Programs, Midwest Apprenticeship Coordinators Conference, the National Business Institute, the Kansas City Metropolitan Bar Association, the Earl O'Connor Inn of Court and the Made in America Conference.*

UPCOMING EVENTS

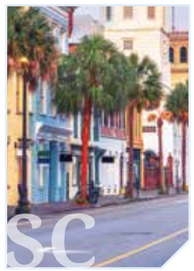
Save These Dates

September 25
Health & Benefits Expo
New York, New York

This expo offers trustees and administrators of benefit plans up-to-date information on critical issues affecting their organizations.

October 1-3
Midwest Apprenticeship Coordinators Conference
Lake of the Ozarks, Missouri

Midwest building trade union training directors, coordinators, and instructors gather with Department of Labor reps to discuss training, recruitment and retention, fiduciary liabilities, emerging technologies, mental health, veteran transitions, and topics to improve apprenticeship programs.



October 14-16
EBAA Conference
Charleston, South Carolina
*Secure Unions is a proud event sponsor

The EBAA Conference offers information and assistance on employer-sponsored retirement benefit and health benefit plans. A Secure Unions rep will present on Cybersecurity Best Practices during the conference.

November 9-12
IFEBP 2025 Annual Employee Benefits Conference
Honolulu, Hawaii
*Secure Unions is a featured speaker

This event brings together nearly 5,000 employee benefits peers! With 120-plus sessions presented by industry experts, attendees will gain insights on pressing topics, along with best practices.

ERISA Cybersecurity Applicability Questionnaire

Is Your Union/Fund Office Subject to the DOL's Cybersecurity Requirements?

This questionnaire will help you determine if your union or fund office is subject to the ERISA cybersecurity requirements laid out in the Department of Labor's (DOL) Employee Benefits Security Administration (EBSA) Cybersecurity Best Practices. If your union or fund office is subject to these requirements you must work to establish compliance with DOL EBSA Cybersecurity Best Practices ASAP to avoid potential legal ramifications in the event of a cybersecurity breach.

Section 1: Plan Data Access

1 Do any union or fund office staff members access participant or plan data (e.g., names, SSNs, DOBs, contribution info, EINs, Member IDs, addresses)?

- ☐ Yes
- ☐ No

2 Do any of your office computers, mobile devices, or email accounts receive reports, spreadsheets, or communications from a TPA, consultant, insurance carrier, accountant, attorney, or other plan service provider?

- ☐ Yes
- ☐ No

3 Do any staff or trustees log into a TPA portal or other online system related to eligibility, claims, or plan administration?

- ☐ Yes
- ☐ No

4 Does your office send, receive, or store plan contribution reports or remittance data from employers, or on behalf of the plan, in an electronic format? Are faxes received electronically? Are records scanned and/or saved in email or on computer drives?

- ☐ Yes
- ☐ No

Section 2: Fiduciary Role

5 Do any of your board members or staff serve as trustees or fiduciaries on a Taft-Hartley trust or benefit plan?

- ☐ Yes
- ☐ No

6 Are you responsible for selecting, monitoring, or reviewing office employees or third-party vendors, like TPAs or IT firms, for your plan?

- ☐ Yes
- ☐ No

Section 3: Systems in Use

7 Do any of your computers or cloud services (e.g., Microsoft 365, Dropbox, Google Drive) store benefit-related data?

- ☐ Yes
- ☐ No

8 Are benefit-related documents printed or filed physically in your office?

- ☐ Yes
- ☐ No

9 Do trustees or staff access plan information from personal devices (phones, tablets, laptops, home PCs, etc.)?

- ☐ Yes
- ☐ No

Scoring & Guidance:

If you answered YES to any of questions 1-6:
You are subject to ERISA cybersecurity requirements as a fiduciary handling plan data.

If you answered NO to all of questions 1-6, but YES to any of questions 7-9 :
You may not be technically under ERISA for cybersecurity, but you still have exposure that may require protections like training, device security, or written policies.

Visit **SecureUnions.com** to schedule a free cybersecurity review.

This content is for informational purposes only and is not intended as legal advice. For legal questions, contact your ERISA attorney.

SECURE UNIONS .COM
CYBERSECURITY

STRONG UNIONS DESERVE STRONG SECURITY.

Secure *your* union.

We're your digital PPE with union-focused cybersecurity solutions to help keep your information safe and secure.

SecureUnions.com

A COMPANY OF
ONSITE LOGIC
CYBERSECURITY & STRATEGIC IT SERVICES