benefits
MAGAZINE

A properly conducted cybersecurity compliance review will help retirement plan sponsors mitigate risks while also demonstrating compliance with recent guidance from the Department of Labor.

Conducting a Cybersecurity Compliance Review: A HOW-TO GUIDE

by | **Justin P. Musil**

The Department of Labor (DOL) cybersecurity guidance issued in April 2021 signaled that benefit plan fiduciaries could no longer ignore cybersecurity risks that their plans face and must take appropriate steps to mitigate these risks.[1]

Cybersecurity compliance and regulatory compliance are nothing new for health plan covered entities and their business associates governed by the Health Insurance Portability and Accountability Act (HIPAA). However, for retirement plan fiduciaries and many of their service providers, the DOL guidance should serve as a call to action to start addressing cybersecurity at the plan and participant level by conducting a cybersecurity compliance review.

Such a review has become increasingly important for at least two reasons. First, plans covered by the Employee Retirement Income Security Act (ERISA), collectively, hold trillions of dollars in assets and maintain volumes of personal and other sensitive information in electronic form. As a result, plans and participant retirement accounts are increasingly targeted by cyberattacks and cyberfraud. Second, following publication of its guidance, the DOL quickly pivoted to begin auditing retirement plans with a focus on cybersecurity programs.

Fortunately, a properly conducted cybersecurity compliance review will help plans mitigate risks while also demonstrating the procedural prudence required under ERISA. This article will highlight several best practices that have emerged that should form the basis of a cybersecurity compliance review, particularly if a plan has never conducted one or is just beginning the process.

Components of a Cybersecurity Compliance Review

The scope of a cybersecurity compliance review—one that accounts for the DOL guidance—can vary among plans due to a variety of factors. These factors include regulation of the plan sponsor's industry, past experiences with breaches and cyberattacks, and remediation measures undertaken following an enforcement action or litigation. Even for plans (or service providers) with robust cybersecurity programs, it is prudent to ensure that the program accounts for the DOL guidance. Similarly, for employer plan sponsors, any businesswide cybersecurity program should factor in plan data and processes because of the unique threats and regulatory scrutiny faced by plans.

A cybersecurity compliance review should include at least the following components.

- Development of a vendor questionnaire and evaluation
- Service contract review
- Examination of cybersecurity policies and procedures
- Evaluation of participant communication
- Security risk assessment

Following is a detailed discussion of each of these components, along with recommendations for how to implement them.

1. Vendor Questionnaire and Evaluation

Many benefit plans outsource various plan functions to third-party service providers (vendors). Unsurprisingly, most breaches and security incidents affecting plans and their participants occur with these vendors. Thus, one of the most crucial components of the cybersecurity compliance review is vendor due diligence. Sending cybersecurity questionnaires (or surveys) is among the simplest ways to conduct due diligence and has been successfully employed in other industries. The cybersecurity questionnaire is similar in scope and format to other periodic requests for proposals or information (RFPs or RFIs) that plans issue to vendors. In fact, in addition to sending the questionnaire to current vendors, plans could send it to prospective vendors during the RFP stage.

The questionnaire helps the plan fiduciary document and, thereafter, evaluate vendor measures to secure plan data, information systems and assets. At the same time, no questionnaire will be perfectly suited to every vendor. Various business, operational, regulatory, environmental and economic factors will dictate the scope and content of the program. To account for this variability, vendors should be given latitude to respond. In the wake of the DOL guidance, many vendors are also reviewing their cybersecurity programs. For this reason, if a vendor is working on a compliance area or planning to address it in the future, the vendor should be permitted to note this in the response and be marked for subsequent follow-up.

Depending on the vendor's IT resources, industry and cybersecurity sophistication, some vendors may have questions or concerns on how to respond. However, even small vendors with limited resources may have policies and procedures in place that address privacy and security (even if not labeled as such), and these can be enough to help the plan conduct a meaningful compliance review. Examples of such policies and procedures include the following.

- Remote work/employee travel/telework policy
- Employee training modules addressing privacy and security
- Employee handbook sections addressing privacy and security
- Employee confidentiality agreements
- Employee technology/bring your own device (BYOD) policy
- Plan office visitor access policy
- Vendor management policy
- Record/data retention and destruction policy

If the policies or practices are not formally documented in writing, the vendor can describe them in its response and submit a formal policy if one is prepared in the future.

In terms of content and format, the questionnaire should inquire about the vendor's cybersecurity program and practices, with a focus on the compliance items raised by the DOL in its guidance and during audits. The sidebar on page 23 lists the areas that are generally included.

The questionnaire should be sent to any vendor that creates or maintains confidential information for the plan, handles or transfers plan assets, or hosts or maintains critical information systems. The DOL has also informally stated that its compliance efforts are particularly focused on those key vendors "running the systems," such as recordkeepers and third-party administrators (TPAs).[2] Therefore, the following retirement plan vendors are usually among those that should receive the questionnaire.

- Recordkeepers
- Custodian banks

- System/software vendors
- Third-party storage providers
- Consultants and actuaries
- Audit firms
- Law firms
- Payroll vendors
- Search and death audit vendors
- Mailing/copying vendors
- Medical reviewers

A vendor may consider some of its reports, such as penetration test results, to be confidential and may ask the plan to execute a nondisclosure agreement or seek to limit the scope. In these cases, after conferring with legal counsel, IT consultants or other advisors, plan fiduciaries will need to determine whether pursuing such additional information from the vendor is necessary to conduct a meaningful evaluation.

Following receipt of the completed questionnaire, the next step is to evaluate the vendor's responses and any accompanying documentation. Due to the technical nature of some of the documents and subject matter, it may be prudent to obtain assistance from

Sample Cybersecurity Questionnaire

1. **Policies and procedures.** Does your organization have written information security standards, practices and policies? If so, please provide. Such policies and procedures may include (as applicable to your business operations and information systems):
   - Organization chart showing the structure of the information security team, along with names and contact information
   - Data governance, collection, classification, sharing, anonymizing, storage and deletion/disposal
   - Access controls and identity management, including use of multifactor authentication (MFA)
   - Technical safeguards, including encryption to protect sensitive information, whether stored or in transit; firewalls; anti-malware software; patch management; and data backup and recovery
   - Business continuity, disaster recovery and incident response
   - Configuration management
   - Asset management
   - Risk assessment
   - Risk management
   - Data privacy
   - System, application, and network security and monitoring
   - Systems and application development and performance
   - Physical security and environment controls
   - Vendor and third-party service provider management
   - Cybersecurity awareness training.
2. **Audits.** Does your organization undergo internal/external audits addressing cybersecurity? If so, please provide your most recent internal/external audit reports and results, including penetration test reports and supporting documents. If your organization follows a recognized cybersecurity standard or framework, please describe.
3. **Validation.** How are your security practices validated? What levels of security standards have been met and implemented?
4. **Prior incidents.** Please provide a description of any past privacy and security incidents, including what happened, what was reported to regulators and how those incidents were resolved or litigated.
5. **Asset and data storage.** Please provide any documents describing security reviews and independent security assessments of the assets or data of the plan stored in a cloud or managed by you or your contractors or subcontractors.
6. **Risk assessments.** Does your organization undergo periodic risk assessments? If so, how often? Please provide your most recent security risk assessment report(s).
7. **Secure system development life cycle (SDLC).** Please provide all documents or policies describing any SDLC program, including penetration testing, code review and architecture analysis.
8. **Cross-marketing.** If applicable, please describe all uses or disclosures of plan data for the direct or indirect purpose of cross-selling or marketing products and services.
9. **Insurance.** Does your organization carry insurance that would cover losses or liabilities caused by security or privacy incidents, fraud, cyberattacks and identify theft (including breaches caused by internal threats, such as misconduct by your employees, agents or contractors and breaches caused by external threats, such as a third party hijacking a participant's account)? If so, please provide evidence of such coverage.

personnel with cybersecurity audit experience. This could mean requesting help from in-house IT experts or retaining an outside security audit firm.

The IT expert would help perform the following functions.

- Identify any deficiencies in the vendor's cybersecurity program
- Assign a corresponding level of risk and priority status
- Provide recommendations for follow-up or remediation

Ideally, the IT expert would summarize these findings in an easily understandable, written report. Plan fiduciaries would then consult this report to help determine whether further actions must be taken. Every service provider relationship is unique, and there is no one-size-fits-all approach to conducting an evaluation. Unfortunately, neither ERISA nor the DOL has explicitly defined what constitutes a compliant cybersecurity program. Still, the DOL seems to offer some suggestions.

First, as previously noted, the DOL may expect a higher level of scrutiny of key vendors compared with others whose services require minimal interaction with plan data or assets and, therefore, pose less risk. In this respect, a TPA or recordkeeper should be expected to have a more comprehensive and sophisticated cybersecurity program compared with a vendor with minimal or no access to plan data or assets. Second, the DOL seems to favorably view vendors that follow a recognized industry framework such as the NIST Cybersecurity Framework, ISO/IEC 27001, HITRUST and PCI DSS. Third, the DOL guidance states that plan fiduciaries can have much more confidence in vendors whose cybersecurity practices are periodically audited or validated by an independent third party to ensure the vendor is meeting its standards. One example of such an audit is a System and Organization Controls (SOC) 2 audit conducted by an independent certified public accountant. Some of the preceding cybersecurity frameworks permit or require an organization to undergo independent validation to certify compliance. Finally, while not a substitute for a strong cybersecurity program, the DOL mentions a vendor's cyberliability insurance and crime coverage as a way to help protect the plan and participants against losses and liability arising from cybersecurity incidents and fraud. The DOL warns, however, that plan fiduciaries must be sure to understand the policy's terms and limits before relying on it as a protection from loss.

If a vendor's program is deemed satisfactory, a fiduciary might determine that no further action is necessary. If a vendor is found to have deficiencies, such as a history of security incidents, a fiduciary may flag that vendor for follow-up and request evidence to confirm that remedial measures were implemented. Extreme cases might require terminating the vendor or seeking services from a new one.

Because the DOL expects cybersecurity compliance to be ongoing, plan fiduciaries may wish to request updates periodically, such as annually, to determine whether a reassessment is required. Reassessment may also be appropriate, for example, if a vendor experiences a privacy breach or cyberattack. ERISA imposes a duty on plan fiduciaries to monitor their service providers, and the DOL has made clear that cybersecurity compliance is now part of this obligation.

takeaways

- The Department of Labor (DOL) released three publications addressing cybersecurity for retirement plan fiduciaries, vendors, participants and service providers in April 2021. Following publication of this guidance, the DOL began auditing retirement plans with a focus on cybersecurity programs.
- Retirement plan fiduciaries should conduct a cybersecurity compliance review to help reduce risks and demonstrate procedural prudence required under the Employee Retirement Income Security Act (ERISA).
- A plan vendor questionnaire and evaluation is a crucial component of a cybersecurity compliance review. Most breaches and security incidents affecting plans and their participants occur with these vendors.
- Plans should have formal, well-documented cybersecurity policies and procedures. Examples of necessary policies include data governance, classification and disposal, data privacy and security risk assessments.
- A security risk assessment is a great starting point for plans conducting their own cybersecurity due diligence process and is foundational to most other compliance steps.

2. Service Contract Review

The DOL guidance lists contractual terms and protections that plan fiduciaries should seek from vendors regarding cybersecurity. As the initial step, plan fiduciaries should coordinate with legal counsel to review existing service agreements to determine whether

they sufficiently address data privacy and cybersecurity. This contract review is particularly important with respect to key vendors that have been identified to receive the cybersecurity questionnaire.

Next, plan fiduciaries should consider whether to request revisions to the service agreement, either as an amendment or as part of an upcoming contract renewal. A streamlined approach is to ask all vendors to execute a standalone, model addendum to be incorporated into the service agreement. One of the benefits of this approach is that fiduciaries can be confident that the plan will have standard contract language with all vendors. Similar in concept to a HIPAA business associate agreement, the addendum should require vendors to agree to comply with all DOL requirements, applicable data privacy and security laws, and other industry best practices.

3. Cybersecurity Policies and Procedures

As noted, the DOL has commenced auditing retirement plans for cybersecurity compliance. In these audits, the DOL is asking plans specific questions and requesting detailed documentation, much of which corresponds to the information requested from vendors in the questionnaire. The DOL is imposing strict response deadlines on these requests, often as short as two weeks. Accordingly, a self-administered plan office, TPA or employer plan sponsor should have on hand formal, well-documented cybersecurity policies and procedures relating to the plan.

As a starting point, many plans, TPAs and employers already have in place various policies, procedures and practices that overlap with and can be used for a cybersecurity compliance review and potential DOL audit. For example, technical safeguards an employer has implemented to protect against malware may be "enterprise-wide" and apply to systems holding both company data and retirement plan data. In addition, HR personnel, who also help administer the retirement plan, may receive initial and ongoing cybersecurity awareness training as part of their regular employment duties.

Following are some of the policies and documents the DOL has requested in recent audits. Benefit plan personnel should coordinate with IT personnel as needed to compile the following documents and have them on hand in case of an audit.

- **Policies and procedures.** All policies, procedures or guidelines for:
  - –Data governance, classification and disposal
  - –Implementation of access controls and identity management, including any use of multifactor authentication (MFA)
  - –Processes for business continuity, disaster recovery and incident response
  - –The assessment of security risks
  - –Data privacy
  - –Vendor management, including notification protocols for cybersecurity events and the use of data for any purpose other than the direct performance of their duties
  - –Cybersecurity awareness training
  - –Encryption to protect all sensitive information, stored or in transit.
- **Documentation.** All documents, reports and communications relating to:
  - –Any past cybersecurity incidents
  - –Security risk assessments
  - –Security control audits, audit files, penetration testing and any other third-party cybersecurity analyses
  - –Security reviews and independent security assessments of the assets or data of the plan stored in a cloud or managed by service providers
  - –Any secure system development life cycle (SDLC) program, including penetration testing, code review and architecture analysis
  - –Security technical controls, including firewalls, antivirus software and data backup.

As part of this process, any applicable IT personnel, legal counsel and other advisors should also be consulted to help determine whether new policies are warranted or whether existing policies should be updated. While the DOL is reviewing all areas of cybersecurity compliance, some key areas of focus have been risk assessments, third-party audits and penetration testing, management of cloud service providers, cybersecurity awareness training, access controls and identity management (especially password management and multifactor authentication), encryption, incident response and business continuity.

4. Participant Communication

Plan participants should have a reasonable expectation that their personal information and retirement savings will be kept secure, while understanding that they also play a

critical role in the process. The DOL guidance includes security tips to be shared with participants who have online access to their retirement accounts. To ensure that participants have received such information, a plan fiduciary or sponsor should review what notices have already been sent to participants, inquiring with other service providers as needed. Following this review, it may be prudent to furnish a copy of the DOL's *Online Security Tips* to participants and beneficiaries.

The summary plan description (SPD) is another participant-facing document that informs participants and beneficiaries about their rights under the plan. Though not mentioned in the DOL guidance, the SPD is an appropriate vehicle to communicate a plan's cybersecurity procedures and participants' responsibilities within those procedures. There is case law supporting reduced liability for a plan if a participant failed to take reasonable security precautions set forth in the SPD.[3] Thus, a review of the SPD, possibly leading to issuance of a summary of material modifications or restatement language, may be prudent.

5. Security Risk Assessment

A security risk assessment helps identify and assess internal and external risks and threats to information systems and sensitive data. After conducting an assessment, an organization will be better informed on what measures it can take to eliminate, or at least reduce, those risks or threats. The risk assessment should result in a written report, which will help demonstrate procedural prudence while also providing a road map to help plan fiduciaries and sponsors address security threats to the plan and its participants.

An organization can perform a risk assessment internally, usually with assistance from IT personnel, or it can hire a third-party auditor. If a plan or organization has undergone a recent risk assessment, it may consider whether an updated risk assessment is appropriate to ensure that it incorporates the DOL guidelines. In any case, the DOL suggests that a risk assessment be performed periodically, such as annually, or as necessary to account for technological, environmental or operational changes.

Documentation

As with other matters of fiduciary due diligence, all cybersecurity decision-making and compliance measures should be documented in trustee and benefit committee meeting minutes to help demonstrate procedural prudence in this newer, yet increasingly important, area of compliance for plans.

Conclusion

The DOL issued its guidance in the form of best practices for maintaining cybersecurity. A cybersecurity compliance review is one viable strategy available to help plan fiduciaries act on this guidance.

bio

Justin P. Musil is a shareholder in the employee benefits practice at Reinhart Boerner Van Deuren s.c. in Milwaukee, Wisconsin. He advises multiemployer and corporate health and retirement plan clients on a variety of legal issues, including regulatory compliance matters and plan administration. Musil is also a member of Reinhart's data privacy and cybersecurity group. He holds the Certified Information Privacy Professional/United States (CIPP/US) credential from the International Association of Privacy Professionals. Prior to pursuing a law degree, Musil served for five years on active duty in the U.S. Army as a noncommissioned officer and communications specialist. He holds a J.D. degree from the University of Wisconsin Law School and a B.S. degree from the University of Wisconsin–Madison.

Endnotes

1. The guidance came in the form of three publications: *Cybersecurity Program Best Practices,* aimed at plan sponsors, recordkeepers and other service providers; *Tips for Hiring a Service Provider with Strong Cybersecurity Practices,* aimed at plan fiduciaries; and *Online Security Tips,* aimed at plan participants and beneficiaries. They can be accessed at www.dol.gov/newsroom/releases/ebsa/ebsa20210414.
2. See www.asppa.org/news/dol-cyber-scrutiny-higher-%E2%80%98those-running-systems%E2%80%99 (summarizing remarks from EBSA's Deputy Assistant Secretary, Timothy D. Hauser).
3. See, e.g., *Foster v. PPG Industries* (10th Cir. 2012) (plan sponsor not liable for fraudulent withdrawal by a participant's ex-spouse because the participant failed to adhere to SPD language addressing security of his account and the plan otherwise followed its established distribution procedures).