Are DOL Cybersecurity Guidelines Mandatory?

JULY 2021

QUESTION:

The Department of Labor released cybersecurity guidelines for plan sponsors, fiduciaries, brokers and other participants in retirement plans. Are these mandatory and how do we comply with these guidelines if we're holding retirement plan participant records?

ANSWER:

The guidelines you refer to are part of an ambitious new government effort to get companies to take cybersecurity seriously, that were released at the end of April. Unlike past efforts, these guidelines are targeted not just at service providers, but at customers, employees and everyone else involved in the entire supply chain for retirement programs. They contain some strong language directed towards Plan Sponsors, informing them of how to conduct due diligence on their service providers, and ensure that employee and financial data will be well protected before they commit to working with a provider. This places service providers squarely in the crosshairs, to make sure they have strong and effective cybersecurity practices in place, because there could now be an existential threat to the business and selling operations of providers who cannot prove compliance with best practices.

To answer your question specifically, no, these guidelines are not "mandatory", from a legal or regulatory standpoint. But they are absolutely mandatory from a best practices standpoint, and providers will ignore them at their peril. The DOL has very clearly thrown down the gauntlet here regarding the standards they expect from recordkeepers, fiduciaries, and other parties entrusted with handling sensitive data. While noncompliance does not automatically expose you to legal consequences, failure to enhance your cybersecurity programs will certainly not be viewed sympathetically by the relevant parties (including your insurance carrier) should you ever experience a breach.

Before this turns into a doom-and-gloom response, however, be aware that the DOL's recommendations are not onerous new requirements. The 12-step best practices plan consists of nothing more than common practices that IT and Cybersecurity providers have been recommending for years. Specifically, those 12 best practices are:

1. Have a formal, well documented cybersecurity program. General advice — basically having a written plan for performing the below.

2. Conduct prudent annual risk assessments.

3. Have a reliable annual third party audit of security controls.
   These involve engaging an external provider to verify that your practices are effective and working. This will be an expense for most companies, but is one that is well worth it. Far better to have the "good guys" test your practices, before the "bad guys" do! Also, having a qualified third party already involved in your operations will help minimize problems should a cybersecurity incident ever occur.

4. Clearly define and assign information security roles and responsibilities.

5. Have strong access control procedures.
Both of these are critical to ensuring cybersecurity. The "old way" of doing things presumed that every employee in your company could have access to all of your company data. This is no longer a wise idea. Employees should have access to data on a need-to-know basis, and that access should be strongly enforced. Most modern servers and systems provide the means to control this access already. It's mostly an exercise in taking a clear and critical look at who needs access to what in your organization, and then acting accordingly to ensure that is enforced.

6. Ensure that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments. Hold your vendors and other third parties to the same standards you are holding yourself.

7. Conduct periodic cybersecurity awareness training.
Once again, having the "good guys" test your staff before the "bad guys" do, is a wise practice. Anti-phishing training & testing, and other cybersecurity training resources are readily available, at low-cost, from several online providers.

8. Implement and manage a secure system development life cycle (SDLC) program.
Only applicable if your company creates and manages its own software. However, in-house (or contracted) software development creates many other cybersecurity considerations that companies without custom software do not need to address. While these guidelines recommend documenting a SDLC, that is one of a much larger number of precautions, testing, audits and response plans that your company will need to put in place.

9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.

10. Encrypt sensitive data, stored and in transit.

11. Implement strong technical controls in accordance with best security practices.
These three are all part of a robust data management plan, outlining how you protect and handle data from the moment you receive it, until the day it is eventually destroyed and disposed of. This is arguably the most difficult part of complying with these guidelines, and the answers are not "off the shelf". They will need to be customized specifically to your business and will require engaging a qualified third party — possibly the same party as in #2 & #3 — to help you inventory, classify, and protect all of the data your company handles.

12. Appropriately respond to cybersecurity incidents. If all has gone well, this simply means: Follow the plans you've put in place for the above. Make sure your staff are well-trained and know what to do at the first report of trouble.

You may note that none of these items contain the words "fiduciary", "participants", "beneficiaries" or anything else specific to retirement plans! That's because they're not. These are really the same best practices that apply to any industry who handles sensitive financial or personal data. The DOL is simply focusing these recommendations on retirement plans because of the stakes involved, and the recent increase in cybersecurity incidents targeting retirement plan providers. So the retirement industry is an area of concern as a potential high-value target for criminals, NOT a special field that requires special precautions. Therefore any qualified cyber consultant or provider should be able to address the needs of this industry, because they are common with most other industries.

As a business owner, you may not fully understand what is involved in implementing the above, and that's okay! These are complex issues, and so it's critical that you identify and engage a qualified service partner to help you through them. Everyone involved realizes (or is rapidly coming to realize) that cybersecurity is both essential and not something that happens for free. Costs may go up. New restrictions on what data you will accept and how you will accept it will need to be imposed. (ie: No more sending sensitive social security numbers and bank account information by email!!) But the investment in cybersecurity now, is one that will pay dividends for years to come in the claims and losses you don't incur. Providers are already in the crosshairs of the bad guys... the DOL is trying to help build a shield to protect you, your partners, your customers, and your industry. It's rare that the government takes such a clear and consistent stance with an entire industry, so wise firms will take advantage of this opportunity to strengthen their protections.