A **Cybersecurity** Checklist for Employers

Safeguarding Your Company's 401(k)

In today's digital age, safeguarding your company's 401(k) plan against cyber threats is crucial.

The Department of Labor (DOL) has issued recommendations to aid employers in securing their plans. By adopting these guidelines and integrating cybersecurity best practices, you can significantly reduce the risk of data breaches, cyber fraud, and theft.

The Employee Benefits Security Administration (EBSA), a division of the DOL, has provided a list of best practices that can serve as a cybersecurity checklist for employers seeking to protect their company's 401(k) plan. For more detailed information, refer to the full "Cybersecurity Program Best Practices – EBSA" document here.

For plan fiduciaries, here are some ways you could apply these **best practices to manage your company's retirement plan**:

1

Have a formal, well documented cybersecurity program

Establish a written policy outlining the procedures for safeguarding 401(k) plan data, including participant information and investment details.

2

Conduct prudent annual risk assessments

Annually review your 401(k) plan provider's security measures or hire a cybersecurity firm to test for vulnerabilities that might expose participant data.

3

Have a reliable annual third-party audit of security controls

Contract with an independent auditor to evaluate the effectiveness of the security controls in place for your 401(k) plan data.

4

Clearly define and assign information security roles and responsibilities

Designate a specific team or individual within the HR or IT departments to manage and monitor the cybersecurity practices related to the 401(k) plan.

5

Have strong access control procedures

Implement procedures like two-factor authentication for accessing 401(k) plan data and limit access to only those employees who need it for their job functions.

6

Ensure that any assets or data stored in a cloud or managed by a third party are subject to appropriate security reviews and independent security assessments

Request and review the cybersecurity policies of any third-party service providers involved in the administration or management of your 401(k) plan.

7

Conduct periodic cybersecurity awareness training

Provide training to all employees on how to identify phishing attempts and other cyber threats that could compromise their 401(k) accounts.

8

Implement and manage a secure system development life cycle (SDLC) program

If you have a custom-built platform for managing your 401(k) plan, ensure that secure coding practices are followed, and security is considered at each stage of the software development process.

9

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

Develop a plan for how you will continue to manage and secure 401(k) data in the event of a business disruption or cyber attack.

10

Encrypt sensitive data, stored and in transit

Ensure that all 401(k) data is encrypted when stored and transmitted. This includes participant names, Social Security numbers, and account balances.

11

Implement strong technical controls in accordance with best security practices

Regularly update and patch your systems, use firewalls, and continuously monitor your networks for any suspicious activity related to your 401(k) plan data.

12

Respond to incidents and breaches in a timely manner

Have a response plan in place to quickly address any potential breaches involving 401(k) data. This includes notifying affected participants, informing law enforcement, and taking steps to remediate the issue.

13

Clearly communicate to participants and beneficiaries about the plan's cybersecurity policies and procedures, and how they can report suspected incidents or vulnerabilities

Send regular communications to employees about the measures you're taking to protect their 401(k) data and how they can report any suspected cybersecurity incidents.

These examples are general in nature and should not be considered as legal advice or recommendations. However, they provide a framework for how an employer could seek to comply with the EBSA's recommendations in the context of managing a 401(k) plan.

Cybersecurity Best Practices

Protecting your company's 401(k) plan from cyber threats can be complex, but you don't have to navigate this landscape alone. Partner with an experienced 401(k) advisor who can help guide you through the intricacies of securing your plan.

Don't leave your 401(k) plan vulnerable

– instead, reach out to our team for assistance with interpreting Department of Labor (DOL) recommendations for safeguarding your plan.