PLAN SPONSOR
Digest

Issue 3, 2021 Your Challenge, Our Solutions™

Cybersecurity program best practices

Employee benefit plans can hold millions of dollars in assets as well as personal data on participants, which can make them targets for cybercriminals. Responsible plan fiduciaries are obligated to help prepare for these types of cybersecurity risks.

According to the Department of Labor, the Employee Benefits Security Administration has prepared the following best practices for use by providers responsible for plan-related IT systems and data, and for plan fiduciaries making decisions on hiring service providers.

Plan service providers should include these 12 components

1. A formal, well-documented cybersecurity program

To identify and assess internal and external cybersecurity risks that may threaten the confidentiality, integrity or availability of stored information, a sound cybersecurity program is recommended. Through the program, the organization implements information security policies, procedures, guidelines and standards to protect the security of the IT infrastructure and stored data.

2. Annual risk assessments

IT threats are constantly changing, so it is important to design a manageable, effective risk assessment schedule. Organizations should assess the risk assessment's scope, methodology and frequency.

3. A reliable annual third party audit of security controls

Having an independent auditor assess an organization's security controls provides a clear, unbiased report of existing risks, vulnerabilities and weaknesses.

4. Clearly defined and assigned information security roles and responsibilities

For a cybersecurity program to be effective, it must be managed at the senior executive level and executed by qualified personnel. The Chief Information Security Officer (CISO) generally establishes and maintains the vision, strategy and operation of the program.

5. Strong access control procedures

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to IT systems and data. It mainly consists of two components: authentication and authorization.

6. Assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and assessments

In the cloud, data is stored with a third-party provider and accessed over the internet. Organizations must understand the security posture of the cloud service provider in order to make sound decisions on using the service.

Continued on page 2

Continued from page 1

7. Cybersecurity awareness training conducted and updated annually

A comprehensive cybersecurity security awareness program sets clear expectations for all employees and educates everyone to recognize attack vectors, help prevent cyber-related incidents, and respond to a potential threat. Since identity theft is a leading cause of fraudulent distributions, it should be considered a key topic of training.

8. Secure System Development Life Cycle Program (SDLC)

A secure SDLC process ensures that security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the system development effort.

9. A business resiliency program

Business resilience is the ability of an organization to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and data. The core components of a program include the business continuity plan, disaster recovery plan and incident response plan.

10. Encryption of sensitive data stored and in transit

Data encryption can protect nonpublic information. A system should implement current, prudent standards for encryption keys, message authentication and hashing to protect the confidentiality and integrity of the data.

11. Strong technical controls implementing best security practices

Technical security solutions are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.

12. Responsiveness to cybersecurity incidents or breaches

When a cybersecurity breach or incident occurs, appropriate action should be taken to protect the plan and its participants.

Hiring a service provider with strong cybersecurity practices

As sponsors of 401(k) and other types of pension plans, business owners may rely on other service providers to maintain plan records and keep participant data confidential and plan accounts secure. Plan sponsors should use service providers that follow strong cybersecurity practices.

To help business owners and fiduciaries meet their responsibilities under ERISA to select and monitor such service providers, the Employee Benefits Security Administration (under the United States Department of Labor) has prepared the following tips for plan sponsors of all sizes:

1. Ask about the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other financial institutions.

2. Look for service providers that follow a recognized standard for information security and use a third-party auditor to review and validate cybersecurity, including the use of annual audit reports that verify information security, system/data availability, processing integrity and data confidentiality.

3. Ask the service provider how it validates its practices and what levels of security standards it has met and implemented. Look for contract provisions that give you the right to review audit results demonstrating compliance with the standard.

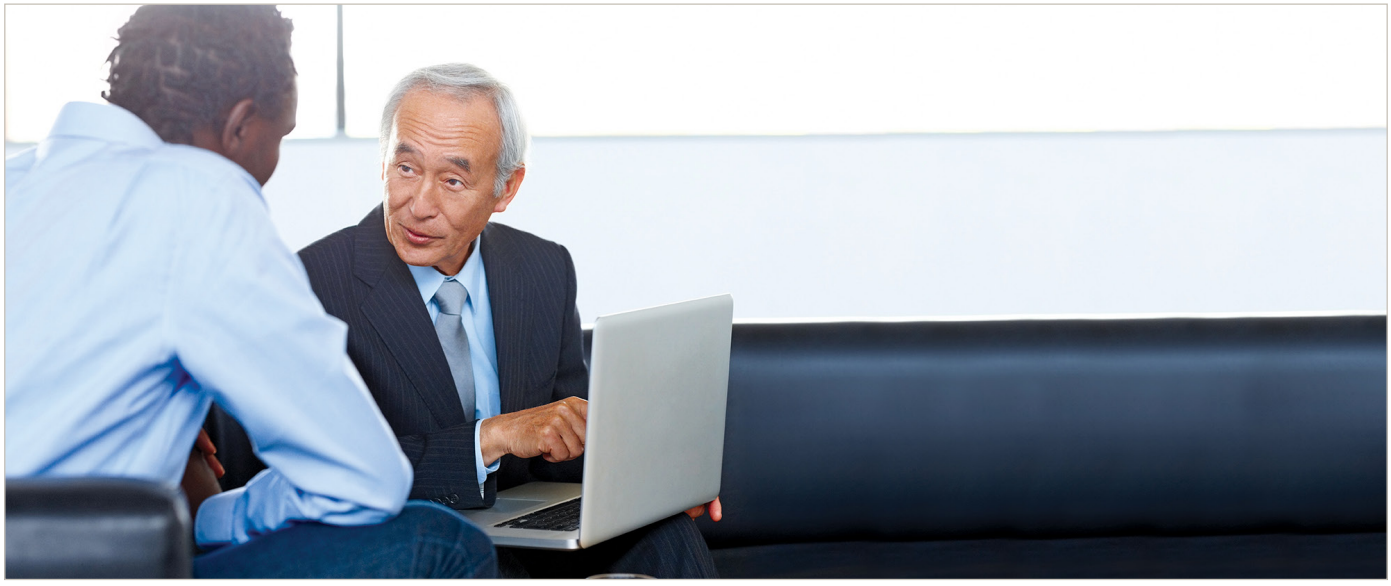
4. Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to vendor's services.

5. Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.

6. Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches, including breaches caused by internal threats and breaches caused by external threats.

7. Confirm the contract requires ongoing compliance with cybersecurity and information security standards—and beware contract provisions that limit the service provider's responsibility for IT security breaches. Also, try to include terms that enhance cybersecurity protection for the plan and its participants, such as:

- Information security reporting
- Clear provisions on the use and sharing of information and confidentiality
- Notification of cybersecurity breaches
- Compliance with records retention and destruction, privacy and information security laws
- Insurance



60 South Sixth Street | Minneapolis, MN 55402

21-20-01653_20181-CC (07/21)