



Cybersecurity Best Practices for 401(k) Plan Sponsors



Neil Plein, CPFA, AIF®
Lead Retirement Plan Consultant
Aldrich Wealth



Peggy Kitzmiller
Managing Director
Aldrich Technology



Randall W. Cook
Employee Benefits Attorney
Saalfeld Griggs, PC



Peter Adams
Vice President – Business Strategy
Aldrich Technology



AGENDA

- Introduction
- Quick overview of new guidance
- Expert panel discusses current FAQs



- **The setting:**
 - 106 million 401(k) plans
 - 34 million defined benefit plans
 - \$11 trillion in collective assets
- **The problem:**
 - Cyber crime costs \$10.5 trillion a year
 - **U.S. retirement plans quickly becoming #1 target**
- **The response:**
 - Highlights of new guidance
 - Significant change in fiduciary responsibility
- **The bottom line.**

Focuses on 6 key areas:

- Information security standards
- Practice validation
- Track record
- Past breaches
- Applicable insurance policies
- Contract provisions

Peggy / Peter

Randy

Most impactful:

- Framework for prudent process
- Existing or future contracts, RFI/RFP
- Roadmap for ongoing monitoring



EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR

TIPS FOR HIRING A SERVICE PROVIDER WITH STRONG CYBERSECURITY PRACTICES

As sponsors of 401(k) and other types of pension plans, business owners often 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 prudently select and monitor such service providers, we 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.
 - Look for service providers that follow a recognized standard for information security and use an outside (third-party) auditor to review and validate cybersecurity. You can have much more confidence in the service provider if the security of its systems and practices are backed by annual audit reports that verify information security, system/data availability, processing integrity, and data confidentiality.
2. 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.
3. 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.
4. Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.
5. 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, such as misconduct by the service provider's own employees or contractors, and breaches caused by external threats, such as a third party hijacking a plan participants' account).
6. When you contract with a service provider, make sure that 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 in the contract that would enhance cybersecurity protection for the Plan and its participants, such as:
 - **Information Security Reporting.** The contract should require the service provider to annually obtain a third-party audit to determine compliance with information security policies and procedures.

closure
ong
zed

y
ch. In
on to

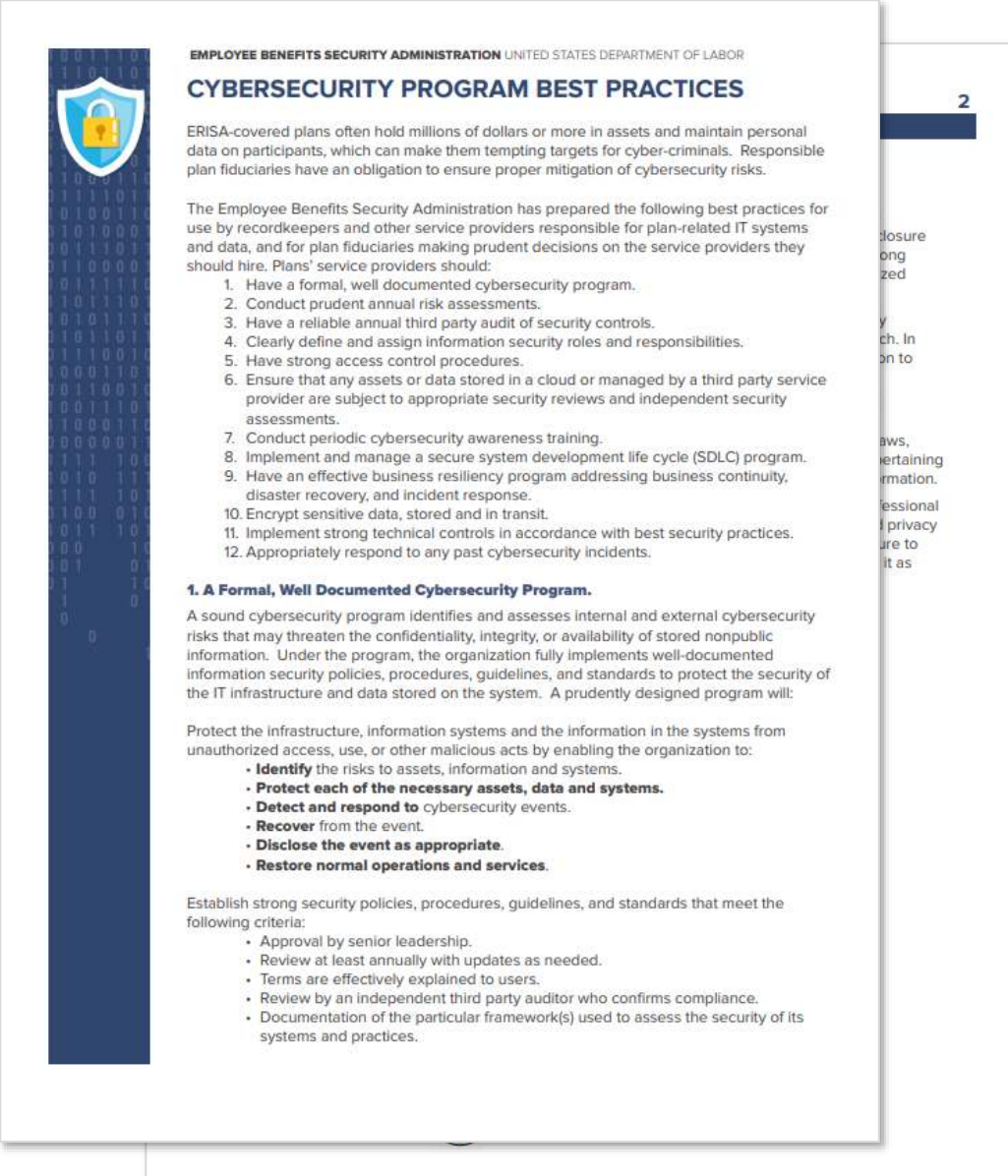
aws,
ertaining
rmation.

essional
d privacy
ure to
it as

Focuses on 12 key areas:

- Have a formal cybersecurity program
- Conduct annual risk assessments
- Third party audit of controls
- Define security roles and responsibilities
- Strong access control procedures
- Security reviews for cloud storage
- Conduct cybersecurity training
- Secure system development life cycle
- Business resiliency program
- Data encryption
- Strong technical controls
- Appropriately respond to incidents

Checklist for service provider review



EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR

CYBERSECURITY PROGRAM BEST PRACTICES

ERISA-covered plans often hold millions of dollars or more in assets and maintain personal data on participants, which can make them tempting targets for cyber-criminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

The Employee Benefits Security Administration has prepared the following best practices for use by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire. Plans' service providers should:

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
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.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
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.
12. Appropriately respond to any past cybersecurity incidents.

1. A Formal, Well Documented Cybersecurity Program.

A sound cybersecurity program identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information. Under the program, the organization fully implements well-documented information security policies, procedures, guidelines, and standards to protect the security of the IT infrastructure and data stored on the system. A prudently designed program will:

Protect the infrastructure, information systems and the information in the systems from unauthorized access, use, or other malicious acts by enabling the organization to:

- **Identify** the risks to assets, information and systems.
- **Protect each of the necessary assets, data and systems.**
- **Detect and respond to** cybersecurity events.
- **Recover** from the event.
- **Disclose the event as appropriate.**
- **Restore normal operations and services.**

Establish strong security policies, procedures, guidelines, and standards that meet the following criteria:

- Approval by senior leadership.
- Review at least annually with updates as needed.
- Terms are effectively explained to users.
- Review by an independent third party auditor who confirms compliance.
- Documentation of the particular framework(s) used to assess the security of its systems and practices.

For Participants: Online Security Tips

Focuses on 9 key areas:

Routinely monitor your account

Use strong passwords

Use multi-factor authentication

Keep personal info current

Close or delete unused accounts

Be wary of Wi-Fi

Beware of phishing attacks

Use antivirus software

Know how to report identity theft

Comes short of requiring cybersecurity training for employees, but....

FAQs for our expert panel:

- What to do now?
- What to ask for?
- How to manage responses?
- Policy/contract changes?
- What do my employees need to do?
- Where do I start?

Please feel free to submit your questions!



We're here to help!

Neil Plein

Aldrich Wealth

nplein@wealthadvisors.com

503-620-5329

Peggy Kitzmiller

Aldrich Technology

pkitzmiller@aldrichadvisors.com

503-620-5329

Peter Adams

Aldrich Technology

padams@aldrichtechnadvisors.com

503-620-5329

Randy Cook

Saalfeld Griggs

RCook@SGLaw.com

503-399-1070



Disclosure

The information contained in this presentation is provided for informational purposes only, is not complete, and does not contain material information about making investments in securities including important disclosures and risk factors. Under no circumstances does the information in this document represent a recommendation to buy or sell stocks, bonds, mutual funds, exchange traded funds (ETF's), other securities or investment products.