Broadridge®

THE BROADRIDGE WEBINAR PROGRAM

Ready for Next

Cybersecurity and Retirement Plans:

Thwarting the Modern-Day Willie Sutton

Learning Objectives

- Understand the latest guidance on cybersecurity for qualified retirement plans
- Adapt the tips for hiring a plan service provider
- Know cybersecurity program best practices for qualified retirement plans
- Recognize the role of the financial advisor in cybersecurity

Agenda

The latest guidance on cybersecurity for qualified retirement plans

Tips for hiring a plan service provider

Cybersecurity program best practices for qualified retirement plans

The role of the financial advisor in cybersecurity

Cybersecurity and Retirement Plans

Why did Willie Sutton rob banks?

Because that's where the money is.

Cybersecurity and Retirement Plans

Why are retirement plans a target?

Because that's where the money is...and it's pretty easy

An Easy Target?

- The retirement plan industry, for better or worse, is a disparate industry of large and small providers
- Different degrees of capabilities and wherewithal among plan providers to invest in the necessary technological and system advances to help safeguard these all-precious retirement assets

The Latest Guidance on Cybersecurity

Not Much Historical Guidance

- DOL Reg. Sec. 2520.104b-1(c)(i)(B): Electronic delivery regulations
  - Plan sponsor must ensure the electronic system it uses keeps participants' personal information relating to their accounts and benefits confidential
- No comprehensive cybersecurity protocol for retirement plan administration exists at the federal level
- Many states have cybersecurity laws in place for business owners

However, Plan Cybersecurity is a Growing Concern

- *Bartnett v Abbott Labs et al* (2020)
  - $245,000 stolen from former employee account
  - Alleged that the defendants failed to enforce a security question and instead provided the one-time code over the phone, among other issues
  - Court found the plan sponsor not liable, but the recordkeeper, "…failed to protect Bartnett's personal information and properly notify her of important changes to her account."

Government Accountability Office (GAO) Report

GAO recommends that the DOL

- Formally state whether it is a fiduciary's responsibility to mitigate cybersecurity risks in defined contribution plans and
- Establish minimum expectations for addressing cybersecurity risks in defined contribution plans

Trifecta of DOL Guidance: "Three points of light"

- On April 14, 2021, DOL issued three cybersecurity directives
  - Tips for Hiring a Service Provider
  - Cybersecurity Program Best Practices
  - Online Security Tips

Test your knowledge

Q: As it relates to cybersecurity, the DOL's current policy:

A. Has specific rules and regulations for plan sponsors to follow.

B. Does not require plan sponsors to have formal policies and procedures.

C. Has guidelines for plan sponsors to follow its best practices.

D. Both B and C

Test your knowledge

Q: As it relates to cybersecurity, the DOL's current policy …

A. Has specific rules and regulations for plan sponsors to follow.

B. Does not require plan sponsors to have formal policies and procedures.

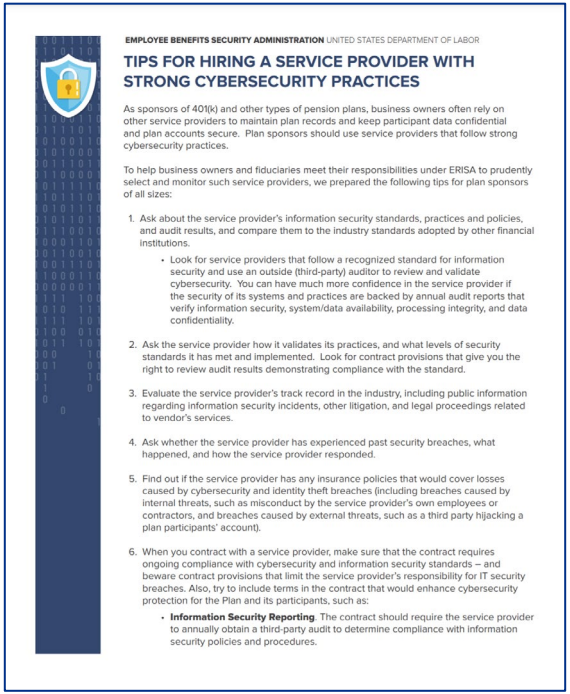
C. Has guidelines for plan sponsors to follow its best practices.

D. Both B and C

Tips For Hiring a Service Provider

Tips for Hiring a Service Provider

- For plan sponsors
- This piece helps **plan sponsors and fiduciaries** prudently select a service provider with strong cybersecurity practices and monitor their activities as ERISA requires.



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.

Tips For Hiring A Service Provider With Strong Cybersecurity Practices

Document:

- **Information security standards**
- Practices, policies and procedures
- Audit results
- Benchmark them to some reasonableness standard

Document:

- Security provider validation practices
- Security levels and standards
- Implementation processes and procedures

Document:

- Service provider's track record
- Any security incidents, litigation, and legal proceedings
- Remedies service provider has been involved in

Tips For Hiring A Service Provider With Strong Cybersecurity Practices

- Document past security breaches and remedies (i.e, ABB v Tussey)
- Review insurance contract

- Document service provider insurance policies that would cover losses caused by cybersecurity and identity theft breaches

Document

- Specific contractual language, note any cybersecurity red flags
- Information security standards
- Limitations on provider's liability

Get it all in writing!

Get it all in writing!

If it's not documented … it didn't happen.

Get it all in writing!

Get it reviewed … and translated.

Test your knowledge

Q: Plan sponsors should request documentation from the following service providers regarding their policies, procedures, and remediation for cybersecurity breaches:

A. The payroll provider

B. The recordkeeper

C. Their plan advisor

D. All the above

Test your knowledge

Q: Plan sponsors should request documentation from the following service providers regarding their policies, procedures, and remediation for cybersecurity breaches:

A. The payroll provider

B. The recordkeeper

C. Their plan advisor

D. All the above

Cybersecurity Program Best Practices

Cybersecurity Best Practices

- For plan recordkeepers and other service providers
- This piece assists plan fiduciaries and record-keepers in their responsibilities to manage cybersecurity risks by following 12 steps

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.

Plan Fiduciary and Recordkeeping Guidance

Plan Fiduciary and Recordkeeping Guidance

Plan Fiduciary and Recordkeeping Guidance

Plan Fiduciary and Recordkeeping Guidance

Get it all in writing!

Test your knowledge

Q: True or False, plan sponsors should require written policies and all insurance contracts from their service providers regarding cybersecurity?

A. True

B. False

Test your knowledge

Q: True or False, plan sponsors should require written policies and all insurance contracts from their service providers regarding cybersecurity?

A. True

B. False

Online Security Tips

Online Security Tips

- For plan participants
- This piece offers plan participants and beneficiaries who check their accounts online basic rules to reduce the risk of fraud or loss

EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR

ONLINE SECURITY TIPS

You can reduce the risk of fraud and loss to your retirement account by following these basic rules:

• REGISTER, SET UP AND ROUTINELY MONITOR YOUR ONLINE ACCOUNT

- Maintaining online access to your retirement account allows you to protect and manage your investment.
- Regularly checking your retirement account reduces the risk of fraudulent account access.
- Failing to register for an online account may enable cybercriminals to assume your online identify.

• USE STRONG AND UNIQUE PASSWORDS

- Don't use dictionary words.
- Use letters (both upper and lower case), numbers, and special characters.
- Don't use letters and numbers in sequence (no "abc", "567", etc.).
- Use 14 or more characters.
- Don't write passwords down.
- Consider using a secure password manager to help create and track passwords.
- Change passwords every 120 days, or if there's a security breach.
- Don't share, reuse, or repeat passwords.

• USE MULTI-FACTOR AUTHENTICATION

- Multi-Factor Authentication (also called two-factor authentication) requires a second credential to verify your identity (for example, entering a code sent in real-time by text message or email).

• KEEP PERSONAL CONTACT INFORMATION CURRENT

- Update your contact information when it changes, so you can be reached if there's a problem.
- Select multiple communication options.

• CLOSE OR DELETE UNUSED ACCOUNTS

- The smaller your on-line presence, the more secure your information. Close unused accounts to minimize your vulnerability.
- Sign up for account activity notifications.

• BE WARY OF FREE WI-FI

- Free Wi-Fi networks, such as the public Wi-Fi available at airports, hotels, or coffee shops pose security risks that may give criminals access to your personal information.
- A better option is to use your cellphone or home network.

• BEWARE OF PHISHING ATTACKS

- Phishing attacks aim to trick you into sharing your passwords, account numbers, and sensitive information, and gain access to your accounts. A phishing message may look like it comes from a trusted organization, to lure you to click on a dangerous link or pass along confidential information.

Online Security Tips

- Register, set up and routinely monitor your online account
- Use strong and unique passwords
- Use multi-factor authentication
- Keep personal contact information current
- Close or delete unused accounts
- Be wary of free wi-fi
- Beware of phishing attacks
- Use antivirus software and keep apps and software current
- Know how to report identity theft and cybersecurity incidents

The Role of the Financial Advisor in Cybersecurity

Practical and Tactical Actions for Plan Sponsors

- Ensure the safe and secure transport of employee deferrals from payroll provider to the recordkeeper
  - Send a letter to the payroll provider requesting their processes, procedures and remediations
- Document the recordkeeper's processes, policies, procedures, and remediations request.
  - Request them in writing from the recordkeeper
- Ensure participants have “adequate information to mitigate potential breaches”
  - Incorporate general cybersecurity best practices into your financial wellness offering. Request that from your service providers.

How Advisors Can Support Plan Sponsors

- Embrace the Chief Governance Officer role

  "The person identified to coordinate and oversee the plan's governance process and service providers."

- Assist in gathering written documentation from payroll providers and retirement plan providers
  - What are their cybersecurity policies, procedures, best practices and safeguards, as well as their restitution processes in case of a breach?
  - Do they have dedicated cybersecurity resources?
  - How much have they invested in cybersecurity?

How Advisors Can Support Plan Sponsors

- Educate participants
  - Support Financial Wellness programs that incorporate cybersecurity best practices
  - Help participants understand how to protect themselves from cyber criminals, fraud and breaches
  - AND don't forget to document your educational efforts
- Customize a strategy taking into account resources, integration, cost, cyber insurance, etc.

How Advisors Can Support Plan Sponsors

- Demystify contracts with service providers
  - Define security obligations
  - Identify reporting and monitoring responsibilities
  - Conduct periodic risk assessments
  - Establish due diligence standards for vetting and tiering providers based on the sensitivity of data being shared

How Advisors Can Support Plan Sponsors

- Advise whether cybersecurity insurance is needed
  - Understand overall insurance programs covering plans and service providers
  - Evaluate whether cybersecurity insurance has a role in a cyber risk management strategy
  - Consider the need for first party coverage

Test your knowledge

Q: Which of the following is a cybersecurity best practice?

A. Have a formal, well-documented cybersecurity program
B. Conduct prudent annual risk assessments
C. Have a reliable, annual, third-party audit of security controls
D. All of the above

Test your knowledge

Q: Which of the following is a cybersecurity best practice?

A. Have a formal, well-documented cybersecurity program
B. Conduct prudent annual risk assessments
C. Have a reliable, annual, third-party audit of security controls
D. All of the above

Takeaways

- The DOL requires plan sponsors to ensure the electronic systems they use for plan administration in keep participants' personal information confidential.
- No comprehensive cybersecurity protocol for retirement plan administration exists at the federal level.
- We do have a series of guidelines, suggestions and best practices from the DOL and other sources.
- Financial advisors can play a critical role in supporting their plan sponsor clients in this new area of concern.
- Protect against the onslaught of the modern-day Willie Sutton

Q & A

THE BROADRIDGE WEBINAR PROGRAM

Thank you for joining

broadridge.com/webinar/webinar-program

Broadridge

Ready for Next