

Fi360

A Broadridge Company

Cybersecurity Risk on the Rise: Is your Firm's Framework in Place

Bonnie Treichel, Chief Solutions Officer at Endeavor Retirement

Sarah Chase-McRorie, Senior Legal Counsel at Matrix Financial Solutions



Breaches in Action

They may be right in front of you



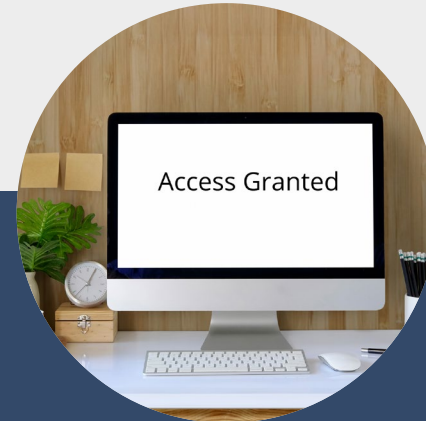
Phishing Emails

Bad actor sends email intended to trick someone into divulging PII, such as passwords, plan asset data or bank account info etc.



Ransomware

Malicious software used to deny access to information technology systems or data; bad actor holds systems or data hostage until a ransom is paid



Privilege Abuse

An insider uses legitimate access to systems and data to perform malicious activities



Third Parties

Reliance on third-party vendors presents risks to a company when it relies on them to support its business operations, such as payroll and recordkeeping



23 days

Average days of downtime for a company from a ransomware attack (according to Coveware)

Understand the risks to you + your clients

- Reputational harm
- Operational disruption
- Significant financial impact + cost
- Regulatory risks
- Exposure to lawsuits



Know the Guidance what applies to your firm?

SEC Guidance

- ✓ Policies + Procedures
- ✓ Risk Assessment
- ✓ Training
- ✓ Access/Controls

DOL Guidance


- ✓ Policies + Procedures
- ✓ Risk Assessment
- ✓ Training
- ✓ Access/Controls

- SEC issued Cybersecurity and Resiliency Observations in 2020
- DOL issued sub-regulatory guidance in April 2021
- Overlap between the guidance
 - Identify what is already implemented
 - Determine where additional protocols are required

Regulatory Risk


Example of DOL Inquiries to Plan Sponsors

All policies, procedures, or guidelines relating to such things as:

- The implementation of access controls and identity management, including any use of multi-factor authentication.
 - The processes for business continuity, disaster recovery, and incident response.
 - Management of vendors and third party service providers, including notification protocols for cybersecurity events and the use of data for any purpose other than the direct performance of their duties.
 - Cybersecurity awareness training.
 - Encryption to protect all sensitive information transmitted, stored, or in transit.
- 

Regulatory Risk

Example of DOL Inquiries to Plan Sponsors

- All documents and communications relating to any past cybersecurity incidents
 - All documents and communications from service providers relating to their cybersecurity capabilities and procedures.
 - All documents and communications from service providers regarding policies and procedures for collecting, storing, archiving, deleting, anonymizing, warehousing, and sharing data.
 - All documents and communications describing the permitted uses of data by the sponsor of the Plan or by any service providers of the Plan, including, but not limited to, all uses of data for the direct or indirect purpose of cross-selling or marketing products and services.
- 

Cybersecurity Requires Teamwork



1. Service Providers

Implement strong cybersecurity programs + educate clients re: the program in place



2. Plan Sponsor

Identify plan data, evaluate service providers, monitor service providers + hire experts, when necessary



3. Participants

Protection of accounts + prompt notification upon breach



Assembling your Cybersecurity Program


- **Build a program:** cybersecurity is not a one-time project or review
- **Buy-in matters:** having the buy-in of senior leadership is critical to the process
- **Assemble a team:** cybersecurity is not a one man or woman job, but requires a team for which outside experts may be required
- **Ongoing training is essential:** training for staff, partners, and clients on an ongoing basis will ensure better outcomes for the program



Framework for Service Providers

with access to PII + plan data (that might be you)


In general, service providers with access to plan data should have a program that allows the service provider 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.
- 

Framework for Service Providers

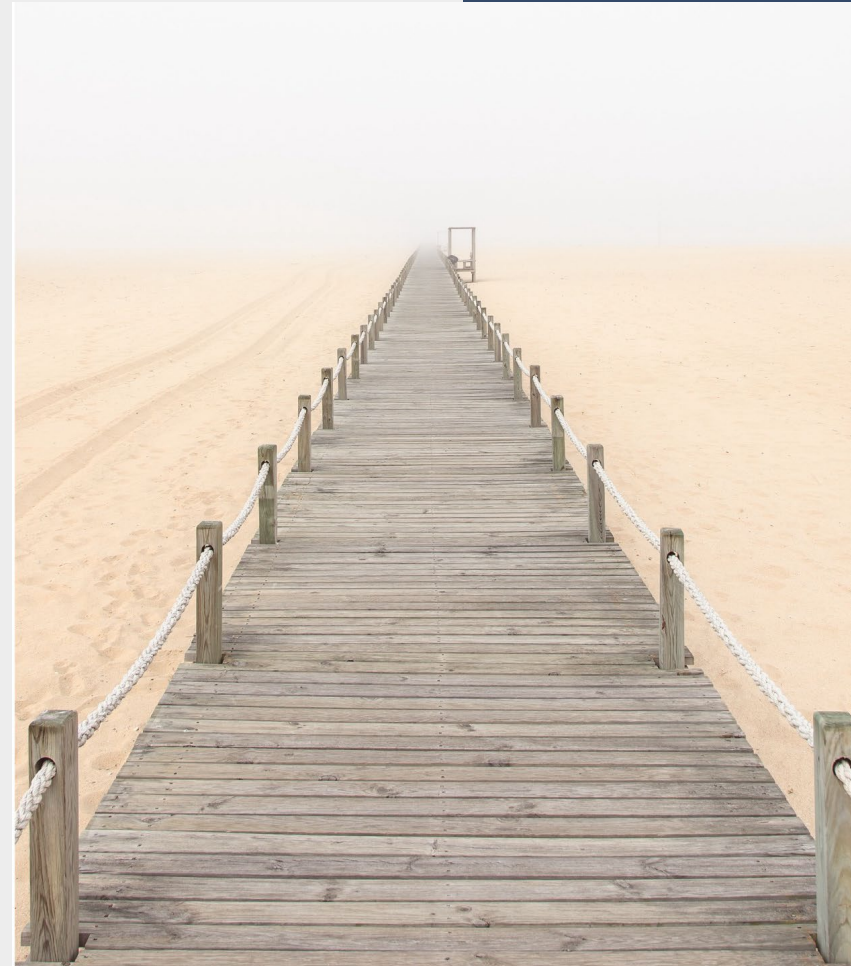
with access to PII + plan data (that might be you)

More specifically, the program should meet these [minimum] requirements:

- 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.
- 

Tips for Working with Plan Sponsors

- Educate plan sponsors
- Educate participants
- Convey how the firm complies with applicable guidance
 - Tip: Use caution when responding to inquiries from plan sponsors. Consider whether disclosure may create a cybersecurity risk for the firm.
- Proactively communicate to plan sponsors when there is an update to your program
- Proactively review agreements for new and existing clients related to cybersecurity, data and privacy provisions



Prudent Selection + Monitoring

Requires a prudent process and loyalty to participants and beneficiaries (ERISA Section 404)



Identify the plan data + personally identifiable information (PII)

Inventory the service providers with access to associated plan data + PII

Using the criteria from the regulatory guidance, evaluate whether service providers are reasonably handling plan data + PII

Make an objective decision for each service provider with plan data + PII and document

Revisit at appropriate intervals



Additional Considerations

- Review cybersecurity insurance + update if needed
- Update the participant mindset from “set it and forget it”
- Go beyond cybersecurity and consider the intersection of cybersecurity + privacy balanced with the benefits of sharing data for better participant outcomes

Review

recent guidance from DOL

Implement

cybersecurity program

Monitor

the program and continually improve

Contact Us

Bonnie Treichel, JD

Chief Solutions Officer

endeavor-retirement.com

503.683.2545

bonnie@endeavor-retirement.com

Sign up for our newsletter to get the latest updates on governance, including cybersecurity:

endeavor-retirement.com

