EMPOWER RETIREMENT®

INSTANT **INSIGHTS**

Cybersecurity guidance

The topic of cybersecurity as it relates to retirement savings has garnered increased interest from Congress as well as from regulatory agencies. Recently, we've received guidance and recommendations on this issue.

In mid-March, the Government Accountability Office (GAO) released a report entitled "Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans." The report was released at the request of Senator Patty Murray (D-WA), the Chair of the Senate Health, Education, Labor and Pension Committee, and Representative Bobby Scott (D-VA), Chair of the House Education and Labor Committee. While the report did not recommend any legislative initiatives, it did recommend that the Department of Labor (DOL) formerly state whether it is a fiduciary's responsibility to mitigate cybersecurity risks in defined contribution plans and to establish minimum expectations for addressing cybersecurity risks.

In its comments in response to GAO, DOL noted that with respect to the first recommendation on fiduciary responsibility, ERISA requires plan fiduciaries to act prudently and solely in the interests of participants and beneficiaries and does not draw a distinction between cybersecurity risk and other types of risks. DOL agreed with the second recommendation and referenced its efforts in drafting compliance assistance materials to help plan sponsors with the selection and monitoring of service providers.

On April 14, 2021, DOL published the guidance mentioned above. The guidance is sub-regulatory and does not constitute a final regulation from DOL. Three documents were published: "**Cybersecurity Program Best Practices**," "**Tips for Hiring a Service Provider With Strong Cybersecurity Practices**" and "**Online Security Tips**."

The document on "Cybersecurity Program Best Practices" included 12 specific recommendations to service providers regarding cybersecurity efforts:

1. Have a formal well-documented cybersecurity program.
This policy would cover identifying risks, protecting data, the detection and response to cybersecurity events, appropriate disclosure and recovery from any event.

2. Conduct prudent annual risk assessments.
This assessment should recognize the changing risk environment and identify, estimate and prioritize information systems risks.

3. Have an annual third-party audit of security controls.
An independent audit would be focused on providing an unbiased assessment of any existing risk, vulnerabilities or weaknesses.

4. Clearly define and assign information security roles and responsibilities.
This reflects the belief that cybersecurity should be managed at a senior executive level.

5. Maintain strong access control procedures.
This control should ensure that only the authorized users have access to IT systems and data.

6. Ensure that data stored in the cloud or managed by a third-party provider have appropriate security reviews and assessments.

7. Conducting periodic cybersecurity awareness training.
Training should be conducted at least annually and updated to reflect current risks.

8. Implement and manage a secure system development life cycle (SDLC) program.
A SDLC process would ensure that security assurance activities such as penetration testing, code review and architecture analysis are considered in system development.

9. Have an effective business resiliency program.
This would focus on the ability of an organization to quickly adapt to any business disruptions and maintain continuous business operations.

10. Encrypt sensitive data in storage and in transit.

11. Implement strong technical controls in accordance with best security practices.
Best practices would include ensuring that systems are kept up to date and appropriate firewall and intrusion detection tools are in place.

12. Appropriately respond to cybersecurity incidents.
In the event of a breach, actions should be taken to protect the plan and participants, including (where appropriate) reporting the breach to law enforcement, investigating the incident and giving the plan and participations the information necessary to reduce or prevent any injury.

The second document, "Tips for Hiring a Service Provider With Strong Cybersecurity Practices," contains recommendations that plan sponsors and fiduciaries should consider when selecting and monitoring service providers. The recommendation primarily focuses on what questions

should be asked of service providers and reflects the best practices referenced above. The tips include suggestions as to what might be part of the service contract, such as:

- Annual third-party audits.
- Guidelines on the use and sharing of potentially private or confidential information.
- Notification of breaches.
- Compliance with federal, state and local laws.
- Consideration of insurance coverage by the service provider.

The third document, "Online Security Tips," contains a number of common-sense recommendations for individuals regarding how to protect their online presence, including monitoring account activity, using strong passwords and being aware of phishing attacks.

In its report, GAO noted industry efforts to establish best practices in cybersecurity, and the DOL guidance reflects those efforts. At Empower Retirement we have always taken our cybersecurity responsibilities seriously, and we are proud to have taken a leadership role within the industry in developing the best policy and procedures. We are committed to protecting our plan sponsors and their participants and will continue to keep you apprised of new developments.