MULTNOMAHGROUP

Top of Mind Considerations for Plan Sponsors on Cybersecurity

Cybersecurity is a multifaceted and ongoing conversation.
DOL released cybersecurity best practices in April 2021. Many organizations have since provided beneficial guidance; however, it is still ultimately the plan fiduciaries' obligation to ensure proper risk mitigation is in place.

Organizations need to establish and continue to maintain well-documented processes that encompass all aspects of their retirement program.

Make sure you are familiar with the following DOL guidelines and tips:

- Cybersecurity Program Best Practices
- Tips for Hiring a Service Provider with Strong Security Practices
- Online Security Tips for Participants

If an audit were to happen, the DOL's cybersecurity document requests can be extensive.

Part of a formal cybersecurity program includes education.
Employers need to be aware of the types of cybersecurity threats and ensure their employees receive ongoing education.

Everyone has the potential to fall victim to cybercrime.
No matter the fraud attempt, whether phishing, social engineering, or fake schemes, the threat is real.

Talk to your service providers.
Employers should work with their service providers to ensure communication is consistent across channels. Take the time to understand established safeguards already in place and where potential gaps may exist.

Communication, communication, communication!
Communicating ways your participants can be diligent is just as important as promoting participant engagement. Participants will likely have greater comfort in knowing their savings are protected.