Cybersecurity & Employee Benefit Plans

The threat of a cyberattack is prevalent throughout the business world. Given the highly sensitive data held within employee benefit plans, it should come as no surprise that they have become a major target for hackers. Protecting participants' personally identifiable information is a responsibility no longer limited to IT departments. Plan sponsors, fiduciaries and service providers of all employee benefit plans have an obligation to establish strong information systems practices to help prevent these attacks.

In November 2016, the Department of Labor's Advisory Council on Employee Welfare and Pension Benefit Plans released a publication entitled, "Cybersecurity Considerations for Benefit Plans" to help plan sponsors protect their clients' data (*https://www.dol.gov/sites/default/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf*). Listed below are the three principal recommendations included in this publication for plan sponsors, fiduciaries and service providers managing benefit plan cybersecurity:

- **Establish a Strategy:** Plan sponsors should identify how data is accessed, controlled, transmitted and stored, and assess the risks associated with these processes. Management strategies must be customized and dynamic to provide the best fit for their individual plan.
- **Contract with Service Providers:** Plan sponsors should have frequent discussions with the plan's third-party service providers and review each provider's current policies and procedures relating to data security, including determining the best approach for evaluating the effectiveness of existing controls.
- **Understand Insurance:** Any individual dealing with employee benefit plan information should have a clear understanding as to whether or not the current insurance/bond policies protect against the consequences of a cyberattack. It is important to be educated on the appropriate cyber insurance policy needed to cover the plan.

Schneider Downs can help you assess your plan's current needs and assist in implementing an appropriate cybersecurity strategy today.