Cybersecurity Concerns for Employee Benefit Plans

In recent months, the Department of Labor (DOL) has raised concerns about cybersecurity and employee benefit plans. Employee benefit plans may be vulnerable to cyber-attacks and thus exposed to risks relating to privacy, security, and fraud. Plan administrators, or those charged with governance, have an ERISA fiduciary duty with respect to the management of the plan, which encompasses the duty to care for personally identifiable information (PII) and protected health information (PHI).

Most plan sponsors and service organizations now use electronic means to conduct financial transactions for the plan (such as the remittance of participant and/or sponsor contributions) and to interface with participants (for instance, permitting participants to electronically initiate a new loan or request a plan distribution). It is these electronic records, and the related investment transactions, that may be at risk to a cyber-attack. Potential at-risk PII data includes information such as social security number, date of birth, email address, etc. While PII might seem to be an unlikely target, it has significant value to cybercriminals since it is permanently associated with an individual (unlike a credit card account number, PII cannot be easily "cancelled") and therefore can be exploited over a longer period of time.

For plans that utilize service organizations for most (or all) of their electronic records and investment transactions, a common misconception may be that those plans have relatively little risk if the service organization's SOC 1 report on controls has no issues. It is important to note that a SOC 1 report addresses a plan's internal control over financial reporting, but does not address the broader entity (or plan)-related cybersecurity controls and risk.

Where to Start?

Plan management and those charged with governance of a plan should evaluate their plan's cybersecurity governance as part of the overall risk assessment and start the discussion in the Audit, Administrative or Benefit Committee meetings. Some initial questions to help start the conversation include the following:

- Who is in charge of cyber security for the plan sponsor?
- Has this individual or department considered the potential cyber risks for the employee benefit plan?
- What would be plan management's response if notified of a data breach by one of their service providers or an employee? In such a situation, what would be the sponsor's obligation to the plan and to the participants?
- Has plan management identified the key individuals/providers involved in processes for the plan (e.g., who does what, when, and how)?
- Does the sponsor require mandatory training on cybersecurity for all employees?
- What are the current legal and regulatory concerns?
- What are the applicable state laws should there be a data breach?

A potential next step would be to then start cybersecurity discussions with the plan's third-party service providers and to review current policies or procedures relating to data security, including passwords, social media, document retention, internet privacy, etc. Even seemingly mundane employee-related policies may need to be considered since, according to a 2016 Association of Corporate Counsel Foundation report, employee error is the number one reason cited for cause of breach.

What about Cybersecurity Insurance?

Cybersecurity insurance is a growing market. Most organizations are familiar with their commercial insurance policies, which provide general liability coverage to protect the business from injury or property damage. **However, standard commercial insurance policies may not cover cyber risks.** Since the specific cyber risks vary based on industry, policies for cyber risk are more customized than other types of insurance policies and can be based on a variety of factors. Such factors include the type of data collected and stored by the entity, the entity's presence on the internet, and how employees and others are able to access data systems, along with any IT updates and disaster response plans. Coverage may also include liability for security or privacy breaches, costs associated with a privacy breach, or business interruption.

In summary, cybersecurity is a growing concern for all entities, including employee benefit plans. This issue is expected to become more pressing with each new announcement of a system failure or data breach. Plan management and those charged with governance need to assess their plan's risks and develop a specific strategy to address those risks as, unfortunately, there is no "one-size-fits-all" approach related to cybersecurity.