Proskauer

Protecting the Security of Employer Data

In this video, Proskauer partners Paul Hamburger, co-chair, and Robert Projansky of the Employee Benefits & Executive Compensation Group, discuss how cybersecurity issues are affecting employee benefit plans, and how plan sponsors may proactively protect and prepare their companies from data breaches.

> **Paul Hamburger:** Employee benefit plan sponsors are talking more and more about cybersecurity for a lot of different reasons. First of all, cybersecurity is in the news with more and more hacks and more and more security breaches. Employee benefit plan sponsors are wondering how is this going to impact me.

What kind of sensitive data do employee benefit plans hold?

> **Robert Projansky:** Plans have social security numbers, dates of birth, financial and medical information, information about family members, information about people's bank accounts. In addition, a lot of information is housed at third-party vendors. You have less control over those vendors, creating whole new risk of breach.

How can plan sponsors proactively protect companies?

> **Robert Projansky:** There are a number of steps that we suggest that plan sponsors take proactively. The first is to devise a strategy as to how you're going to handle data. You have to look at your data with an eye toward how is it stored, how is it accessed, and how is it transmitted, then come up with a strategy for dealing with that.

> **Paul Hamburger:** You need to look at your vendors. Your vendors for your 401K plan, whether that is the record keeper or a trustee, will house a great deal of personally identifiable and sensitive information.

Robert Projansky: In the diligence process and the ongoing monitoring process you want to make sure that you're assessing the maturity of your vendors' procedures for dealing with cybersecurity. When you're contracting with a vendor you want to make sure that that contract has very specific terms that deal with cybersecurity: What kind of administrative and technical safeguards is the vendor going to impose? Where is the data going to be housed? What's going to happen if there is a breach? How is notice going to be provided? Who has liability? Will there be subcontracting and how will data be protected when there is? Finally, how will data be destroyed once it's no longer being used?

What are the lessons learned from other data breaches?

Paul Hamburger: The fundamental point to recognize is when it comes to data security the question isn't whether data will be breached, it's when the data will be breached, and what are you going to do? How are you going to stand poised and ready to address protecting that information before a data breach actually happens?

Related Professionals

- **Robert M. Projansky**
  Partner