Assess Your Third Parties' Cybersecurity & Quantify Their Breach Vulnerability

The more sensitive information your third-party vendors have access to, interact with, manage or administer, the greater your risk of a data breach.

Review your organization's vulnerability to a third-party data breach of your confidential, sensitive and non-public data and learn about taking concrete steps for risk mitigation.

You should:

- Determine you're working with service providers that have strong cybersecurity practices.
- Quantify the likelihood that you'll experience a data breach via one of those same service providers.

Survey your service providers about their cybersecurity practices

Hiring service providers that have strong cybersecurity protocols and defenses is one of the key components of the cybersecurity program best practices identified by the DOL's Employee Benefits Security Administration. That guidance, which was created for plan sponsors and fiduciaries of plans that are subject to ERISA, is a helpful resource for all plan sponsors and fiduciaries.

To ensure that your third-party vendors, trading partners and other service providers have strong cybersecurity practices, you should ask precise and pertinent questions; review and evaluate the responses; and follow up to perform due diligence as needed on a regular basis.

Quantify the risk of a breach

Additionally, to quantify the risk of a data breach of your organization's sensitive information, perform a probability analysis to determine the individual and population likelihood of a data breach from any one of your third-party service providers as well as your entire vendor population. This probability estimate is a statistically valid assessment of the likelihood of a reportable data breach.

Data breach probability estimates for each of your third-party service providers (and thus the overall cumulative probability of your vendor population) support and enhance a questionnaire or other risk management process by providing additional information that third parties cannot answer through other methods.

Seek the right expertise

Segal's Administrative and Technology Consulting (ATC) Practice can help you perform these informative assessments. In fact, these assessments are two pillars of our vendor-risk-management services.

Segal

Detailed service provider surveys

Ask us to conduct the surveys. We're experienced in fielding detailed questionnaires. You decide what questions to ask, choosing from our library of questions. We take it from there! We send the questionnaire; review the responses to make sure the vendor answered all key questions; and analyze and score the responses based on how thoroughly a vendor has implemented certain standard, widely recognized cybersecurity controls to aid in the protection of your data.

You'll receive a report that outlines the overall risk profile of each vendor and your vendor population overall. We'll present what we learned and will explain how we developed the risk profile.

Our approach to analyzing data breach probability

We partner with Vivo Security, our expert modeling partner, which is focused on quantifying cybersecurity risk. We anonymize key data elements from your vendor population and their associated questionnaires, feeding that information, among other variables, into Vivo's models. (None of your data is ever shared with Vivo.)

The first probability estimate is of an individual vendor's risk of a data breach. Next, all your vendors' risks are considered, to calculate an overall cumulative risk and probability of a breach to your organization.

You receive a thorough assessment of potential data breaches that identifies the vendor or vendors that most contribute to the likelihood of a breach affecting your organization.

Get risk-reduction recommendations

To reduce your risk, we provide recommendations for actions a particular vendor can take to improve its cybersecurity defenses. If you're interested, we provide vendor follow-up services. We also suggest steps you can consider taking to reduce the cumulative risk of your overall vendor population.

Additionally, when necessary or appropriate, we work with you to select new vendors that will help keep your information secure.

The Questionnaires

You have options. Choose from our proprietary database of 180 questions that includes our 89 recommended core questions.

We also have the flexibility to create custom questions tailored to your specific requirements.

The Probability Analysis

The analysis is based on widely used and accepted statistical modeling known as regression modeling.

For the analysis, we define a "data breach" as any security-related incident that results in the confirmed disclosure — not just potential exposure — of personal information to an unauthorized party that requires reporting by law (e.g., PII and ePHI). The modeling doesn't predict other negative events. such as the likelihood of ransomware attacks, breach of intellectual property, data corruption, loss of service or financial failure among your third parties.

Contact

Michael Venezia
VP, ATC
Corporate Practice Leader
mvenezia@segalco.com
484.705.8038

Michael Stoyanovich
VP, Senior Consultant, ATC
mstoyanovich@segalco.com
248.910.2637

Segal is a leading global employee benefit and HR consulting firm delivering trusted advice that improves lives. Visit segalco.com.

Segal