EPIC Insurance Brokers & Consultants

CYBERSECURITY ALERT

Where to Start on Vendor Due Diligence?

Start With Three Easy Vendor Due Diligence Steps

Organizations of all sizes and industry verticals are increasingly turning to outsource business functions to capitalize on economies of scale. Although outsourcing can help organizations reduce costs and increase efficiencies, the greater the reliance on third-party vendors, the greater the network security and data privacy risk to the organization. According to the Verizon 2022 Data Breach Investigations Report, 62 percent of all data breaches happen via third-party vendors. Recognizing the problem – the significant increase in the cyber-related risk associated with outsourcing – is the first step to trying to solve the problem.

Conducting due diligence on third-party vendors you share data with and rely upon to conduct your business is essential. However, the more third-party vendors you have, the more difficult it is to keep up with due diligence questionnaires and assessments. There are, of course, third-party vendors you can outsource this due diligence function to. Unfortunately, this is not always a realistic or practical option for a variety of reasons. Several different resources can help you get started, but the amount of information can be overwhelming and confusing. The Cybersecurity and Infrastructure Security Agency (CISA), together with the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force has put together a **Vendor Risk Management Template** available for your use.

But, if you are looking for a valid starting point, below are three easy, practical steps any organization can take to get moving on the process of vendor due diligence:

- **Step 1 – Prioritize:** Start by **prioritizing** your vendors according to their importance to your business and access to critical data. Not all vendors will require the same level of due diligence. The idea is to approach your due diligence in such a way that it aligns with the level of risk the third-party vendor presents to the organization. One way to approach this prioritization is via Vendor Tiering. The number of tiering levels will depend on the organization. The most basic vendor tiering structure is typically comprised of three levels – Tier 1, Tier 2, and Tier 3 – with Tier 1 representing high-risk vendors. Remember, this will be different for every organization, so spend time customizing this to your organization.
- **Step 2 – Establish General Categories of Due Diligence:** Unfortunately, vendor due diligence is not one-size-fits-all. The approach must be tailored to fit each organization. Once you have prioritized or tiered your vendors, the next step is to establish general focus categories. The following are *sample* categories: **General Business Information, Financial Stability, Corporate Image/Reputation, Insurance, and Approach to Corporate Governance (focus on Network/Data Security).**
    - **General Information:** Collect general basic information from all your vendors, such as Name of Company/Key Contacts, Number of Employees, Number of Offices and Office Locations, Annual Revenue, Years of Experience Providing the Service/Product, etc.

- **Financial Stability**: Consider the financial health and viability of your vendors. Request basic information necessary for you to determine financial stability and strength.
- **Corporate Image/Reputation**: Conduct high-level internet research on your vendors regularly to help identify any red flags (controversial social media posts, public regulatory investigations or civil actions, mergers/acquisitions, etc.) and follow up with your contact if you find anything concerning.
- **Insurance**: Require your vendors to maintain comprehensive cyber insurance at a level commensurate with your reliance on that vendor, along with other relevant insurance protection and/or bonding. For example, if your vendor provides professional services, consider requiring Errors & Omissions/Professional Liability and cyber insurance.
- **Approach to Corporate Governance – Focus on Network and Data Security Practices**: Do they have a dedicated Risk Manager – if not, who in the organization is responsible for managing risk? How frequently do they conduct network security and data privacy awareness training? Do they have a Business Continuity/Disaster Recovery Plan that includes an Incident Response Plan – how frequently do they update and test that plan? Have they had any network security/data breach events in the last three years? What is their position on the use of Generative AI and other emerging technologies – how are they managing potential risk?

- **Step 3: Consider your organization's exposure to "Fourth-Party Risk:"** Fourth-Party Risk is the risk posed to your organization by your vendors' vendors. Consider asking questions and requiring some level of transparency from your third-party vendors about their supply chains and how they manage those risks. Find out if the vendor is conducting due diligence on subcontractors used to perform services.

Of course, the above is just scratching the surface and is not intended to provide a comprehensive approach to vendor due diligence. However, it is a step in the right direction and should provide organizations with a solid framework to build on and a better understanding of the risks they face from their vendors.

Let's Talk!

Find our how EPIC Insurance Brokers & Consultants can help your business