Vendor Selection: Best Practices for Risk Management

By Robert H. Rosenzweig, RPLU, National Cyber Risk Practice Leader

Apr 20, 2021

When we talk about third-party vendors, we’re talking about the companies you employ to provide services to you or your customers. They can be incredibly useful and cost-effective resources, but they also present a big risk to those who contract with them. If third-party vendors experience a data breach, it potentially exposes you and your clients, and it will be your responsibility to investigate, respond, and cover the costs of the damage.

Vendors can range from custodial companies, to IT services, to professional service firms. Whatever their contracted function, they have access to your physical premises and/or your network data. So how can you make sure that when you’re signing a contract with an outside vendor, you’re not exposing yourself and your clients to excessive risk? We’ve outlined four best practices you should follow before signing the dotted line.

1. **Do your research.** Are you partnering with and hiring vendors that are thoughtful about their risk management and cybersecurity? Will they indemnify your business if they’re negligent and cause an issue? Your insurance policy may respond independently, but you want to make sure that your vendor has their own policy in place as well.

2. **Ask for proof.** When contracting certain professional service firms, you can ask the vendor to fill out a risk assessment before you sign with them. Have them show evidence that they’ve achieved certain certifications, have done an audit, adhered to certain accepted cybersecurity frameworks. A robust cybersecurity questionnaire and analysis will confirm that both you and your vendors have as many protections in place as possible to protect your customers.

3. **Vet your vendor with another vendor.** Depending on the nature and size of your vendor’s operations, executing some of these due diligence measures can become challenging. The biggest industry players may have the information you want but choose not to share it. Smaller vendors may be more willing to meet your requests for transparency, but less able to give the depth of answers you’re seeking. One way to work around this is to engage a company to give you a purely...
external look to quickly identify if there are any vulnerabilities at the surface level.

1. **Develop strong internal cybersecurity and risk management policies.** Even after being as thorough as possible, there is still the possibility for human error or malicious actors. Make sure that you are never relying too heavily on vendors to cover their bases. Assume that something could go wrong in the supply chain and make sure your cybersecurity protocols are up to date; have backups; have protections for physical assets as well as network data; and have a plan in place to mitigate any damage.

The biggest issue most people face in this process is a basic lack of awareness about what the potential issues may be if something does go wrong with a vendor. When you’re outsourcing a service, you’re also outsourcing potential liabilities and losing some control in the process. They are still a great potential asset for your company, but you should go into this process with your eyes wide open. Leave as little as possible up to chance.

*Want to learn more?*

*Find me on LinkedIn, [here](#).*

*Connect with the Risk Strategies Cyber Risk team at [cyber@risk-strategies.com](mailto:cyber@risk-strategies.com).*

*Email me directly at [rrosenzweig@risk-strategies.com](mailto:rrosenzweig@risk-strategies.com).*

---

**TAGS:**

Cyber