7 Layers of Protection Against Third-Party Cybersecurity Risk

Cybercriminals are using increasingly sophisticated methods to steal or compromise valuable data. Protecting your organizational and customers' data is more important than ever, as data breaches can harm your reputation and put you at risk for regulatory fines and legal fees.

But how do you keep the data safe when it's processed, stored, or transmitted by a third-party vendor?

Cybersecurity protection requires a multi-layered approach that evaluates different elements both internally and externally with your vendor.

7 Layers of Cybersecurity Protection

The following 7 layers are designed to help protect your organization from third-party cybersecurity risk.

1 Vendor Identification

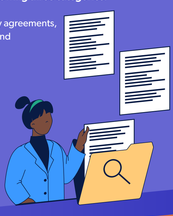
This may seem like an obvious statement, but it's important to identify the vendors, including fourth-party vendors, that have access to your data or systems. Every vendor in your inventory will have different levels of cybersecurity risk, some high and some very little risk at all. This layer of vendor identification will ensure that you're not spending excess time and resources on vendors with very little or no cybersecurity risk.

2 Due Diligence

One of the most effective ways to assess a vendor's cybersecurity posture is to collect and review due diligence documents. These reviews should always be performed by qualified subject matter experts (SMEs).

Cybersecurity documents will generally fall under the following three categories:

- **Legal and procedure** documents such as confidentiality agreements, mutual non-disclosure agreements, employee background checks, and security awareness training
- **Policy** documents that cover topics like information security, privacy, encryption, data retention and destruction, data classification, and mobile devices
- **Planning** documents that provide details on areas such as incident management and response, third-party vendor management, and business continuity and disaster recovery



3 Cybersecurity Awareness

Human error plays a large part in cybersecurity risk, meaning that your vendor's employees will potentially be the source of a data breach that can impact your organization. Although vendor data breaches aren't 100% avoidable, your vendor can reduce the likelihood of an incident through consistently educating and training employees on cybersecurity best practices.

4 Contract Provisions

Your vendor contract is one of the best ways to set expectations about appropriate cybersecurity practices and protect your organization from unmitigated risk. It's important to include details such as breach notification requirements and the disposal or return of any data after the contract ends. A right to audit clause will also ensure that you can review the vendor's cybersecurity documents as needed.

5 Ongoing Testing

Your vendor should be performing regular testing, including vulnerability and social engineering, as well as annual penetration tests. Frequent and consistent testing helps proactively identify and address any weaknesses found in their systems that could expose your data to attacks.

6 Regulatory Compliance

Protecting your organization from third-party cybersecurity risk is more than a best practice, it's a regulatory expectation. Data breach notification requirements have been issued from regulators, like the National Credit Union Administration (NCUA) and Securities and Exchange Commission (SEC) and are a focal point in regulations like the Health Insurance Portability and Accountability Act (HIPAA). These notification requirements, along with various state privacy laws, have proven that regulators are seeing the importance of protecting data and lessening the likelihood of an incident. Adding a layer of regulatory compliance requirements will ensure that your vendor's processes are meeting the expectations of regulators in your industry.

7 Cyber Insurance

Your vendor's cybersecurity insurance coverage will generally be the final layer of protection. It's important to verify that the vendor's policy is current and covers applicable details such as errors and omissions.

Third-party cybersecurity risk is critical to manage because of its evolving nature and impact on other risk types. Data breaches and other cyber incidents will always be a possibility, but these layers of protection will give you a strong foundation to manage cyber risk and help prevent incidents that can significantly harm your organization and its customers.