

## Third-Party Risks: How You Can Protect Your Business

Most businesses today depend on third-party partners. These partners could provide products, services or even expertise that help keep your business running and reach your goals. But sometimes, these relationships get tested when a data mishap or a cybersecurity incident at the vendor end snowballs into a major issue for you.

That's why it's important to understand how third-party risks can impact not just your business operations, finances or brand but also your business's future. In this blog, we'll discuss the key third-party risks that can make you vulnerable and share best practices for building a resilient third-party risk management strategy.

### How third parties compromise your security?

Your partners can sometimes expose you to unexpected risks. So, knowing where these vulnerabilities stem from makes it easier to protect your business.

Here are some of the most common third-party risks that can compromise your business:

**Third-party access:** At times, you'll have to give your third-party partner access to your sensitive data or systems. If the partner experiences a data breach, your data could be exposed, turning your business into a victim.

**Weak vendor security:** When you partner with a third party, they, by default, become part of your supply chain. If they don't have adequate security measures, your risk increases, especially if they have indirect access to your critical information.

**Hidden technology risks:** A security flaw in third-party software or pre-installed malware in hardware can leave your business vulnerable to external threats. Attackers can exploit the compromised software or hardware to launch an attack on your systems.

**Data in external hands:** Many businesses today entrust their data to third-party storage providers. Even though this makes for a good business decision, don't overlook the fact that this decision also comes with its share of risks, as a breach at the provider end can compromise your data as well.

### Best practices for managing third-party risks

Here are some best practices to help you mitigate third-party risks:

**Vet your vendor:** Before signing a contract, thoroughly vet your vendor. Don't commit to them without conducting background checks, security assessments, reviews of track records and evaluation of security policies. Also, ask for certifications and evidence of compliance with industry norms.

**Define expectations:** You can't take a chance on your business. Draw up a contract that clearly outlines your expectations on security, responsibilities and liabilities. Ensure you have a clause that makes it mandatory for the vendor to maintain certain security standards at all times and makes them obligated to report any or all security incidents.

**Be transparent:** Your vendor plays a key role in the success of your business. So, it's in your interest to establish open lines of communication with your vendors about security. Make it a standard practice to share updates on evolving threats and vulnerabilities. Also, encourage your partner to be transparent and report any security concerns promptly.

**Stay vigilant:** You can't just assess your third-party vendor once and assume they will always stay secure. The threat landscape is constantly evolving—what if your vendor isn't? Continuously track their security posture by conducting periodic security assessments, vulnerability scans and pen testing.

**Brace for the worst:** Things can go wrong, and sometimes they do without warning. Have a detailed incident response plan that lays out procedures for dealing with security breaches involving third-party vendors. In your comprehensive plan, clearly define roles, responsibilities and communication protocols. Also, conduct regular mock drills to improve your preparedness.

## Build a resilient business

The future of your business relies on how your customers perceive you. Customer trust is hard to win and easy to lose. Even if you have done everything to protect your customers, one mistake by a third-party vendor can destroy your reputation and your customers will hold you responsible.

Don't let a third-party breach damage your reputation. Take control of your security posture.

Contact us today for a comprehensive assessment of your third-party risk management strategy. We can help you build a robust defense to protect your business, your data and your reputation.

Schedule your free consultation now at <https://calendly.com/tritter-kdatechsolutions>