What is Third Party Risk and Why Does It Matter?

3 minutes

Written by Whistic

In the world of information security, third party risk is a topic that comes up often. As more and more organizations turn to SaaS-based vendors and move their operations to a cloud-driven environment, third party risk has become one of the most critical topics for an organization at any level, not just in the InfoSec world.

Here, we'll take a high-level look at what third party risk entails, why it matters so much to information security and data privacy teams, as well as go through a few tips and tricks teams can take to mitigate this risk.

What is Third Party Risk?

A third party vendor is defined as any entity that enters into a partnership or business relationship with an organization where the vendor may be accessing, sharing, or leveraging an organization’s protected data assets. Modern corporations have dozens, sometimes hundreds, of vendor partners across various departments within the business. Anything from your email service provider (like Microsoft or Google) to your CRM (Salesforce, etc.) to your internal communication tool (Slack or Zoom, for example) counts as a third-party vendor.

What Can InfoSec Teams Do to Mitigate This Risk?

As more companies take their businesses online and embrace the ‘open data’ economy, opening up internal and customer data to a seemingly unlimited number of vendors, third party risk is becoming a bigger issue – and a bigger opportunity for InfoSec teams. Putting a proactive vendor risk management strategy in place early, and scaling this process across all potential third-party access points, can ensure your organization’s customer and internal data is safe and secure from potential threats.

By implementing an on-demand, scalable vendor risk management process in place, InfoSec teams can effectively:

- Work with third-party vendors to close any potential gaps that could leave data vulnerable to malicious attacks.
- Control the entire vendor security process and ensure that third-party risk management is a key focus of the entire organization.
- Ensure your security protocols are always up-to-date and know for sure that your vendors have access to these updated workflows.
- Gather data and insights from across third-party vendor workflows and leverage this information to make better, more informed decisions for your security processes moving forward.
- Establish your organization as a security thought leader both with your vendors as well as potential customers and competitors in your market.

Reprinted from: https://cloudsecurityalliance.org/blog/2020/09/14/what-is-third-party-risk-and-why-does-it-matter/