INSIGHTS

Cyber made simple.

one brightly cyber

THIRD-PARTY RISKS MULTIPLY

BY JAY BORDEN

Third-parties are your business partners that either have access to your systems or you have access to theirs, or both. It can also refer to software or cloud providers or other suppliers that are essential to your business. In this context, third-parties are also referred to as part of your supply chain.

Connections with third-parties are typically by API, application programming interface, meaning that the systems connect directly to each other without need for a person. This makes it very simple to exchange or access needed information. The API connections add convenience and dependence but also add to risk.

Third-party risk has been a topic of interest for a while. A recent study by a security firm found that 98% of firms world-wide have a relationship with a company that has been breached within the last 24 months. The study went on to find that 50% of firms globally have 4th party relationships, that is third-parties of your third-parties, with firms that have been breached within the last 2 years.

Another study found that 82% of companies give their partners access to all of their cloud data. One more study found that over 40% of companies have insufficient visibility into their supply chains.

Remember SolarWinds? They provide software to manage the infrastructure, systems, and networks of company's IT environments. SolarWinds was hacked and their next software update gave hackers access to the systems of their customers.

More examples – two payment processors for health insurance companies in France were breached revealing the information on about 50% of the population of the country. One more study found that over 40% of companies have insufficient visibility into their supply chains.

onebrightlycyber.com
(888) 773-1920

INSIGHTS

Cyber made simple.

Third-Party Risks Multiply

Continued

A breach of a technology partner of Bank of America exposed private information including Social Security numbers for about 57,000 of the bank's customers.

What about your third-parties? Do you know how they are protecting their information and their systems?

Doing an assessment of the security posture of a partner takes time and effort. It also requires the partner to provide significant detail about their security, which they may be hesitant to do as it can expose them to risks.

Having partners fill out a form and a standard assessment may be a good place to start but you need to do more. Site visits may not be possible for more than the biggest partners, if at all. Remember any partner, no matter how minor the service they provide, has access to your systems and data making them a potential risk.

Speak with them, understand how they protect their own data and systems. Do those third-party APIs have access to more of your data and systems than necessary? Do you have access to more of their data and systems than necessary?

We have written before about role-based access and zero-trust. Follow the least access approach meaning only provide access to systems and data that is essential to their role. We understand it is easy to provide access to everything to all partners, but that significantly increases your risks.

Remember to find out who their partners are and what protections they employ. Just because a firm is not your partner doesn't mean they aren't a risk to you. If they have access to your partner's systems, and your partner has access to your systems and data, then if they are breached a cybercriminal can access your systems and data.

Third-party and fourth-party risk is not to be discounted. As the examples above illustrate, it is very real and very serious.

Take it seriously. Regulators and cyber insurers surely will.

To learn all the ways we can help make your company safer, visit onebrightlycyber.com and contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920