SCHNEIDER DOWNS

Big Thinking. Personal Focus.

OUR THOUGHTS ON

Third Party Risk Management Insights

How Third Party Risk Management Caters to Your Organization

Imagine you are hosting a dinner party.

You hired the caterer, queued up the Spotify playlist, and you uncorked the responsibly priced chilled champagne. You are ready to go. The guests arrive and start socializing as they dig into the hors d'oeuvres tastefully scattered on reclaimed wood platters... and then they start to feel sick. The caterer's food prep was not exactly vigilant. You think back to that single one-star online review.

Will the guests blame you or the caterer? Truth is, it doesn't matter. The damage is done and you have lost their trust. Expect your next event invitation to go right to the spam folder since you are now known as the host who gave everybody food poisoning.

Now, imagine hosting hundreds of dinner parties every day with caterers that you have to evaluate carefully, to ensure they do a great job and maintain your esteemed reputation.

That is not too far from what your organization's third-party risk management (TPRM) team must do every day, monitoring how the firm engages with each of your 100 to 1000+ third parties, and ensuring that those third parties represent your organization appropriately if engaging directly with clients. It is no small task, especially given that third parties are often the weakest link in a company's security, opening up back doors to proprietary systems and sensitive data and, possibly giving malicious actors an entry point.

Did you know the massive 60 million customer data hack of Target was caused by someone stealing the computer credentials of one of Target's many air conditioning contractors? It was literally the cyber equivalent to crawling through the air ducts to commit a robbery.

Third parties can include everyone that your organization works with, from the massive banks to the smallest technology third parties. TPRM teams must determine that anyone you do business with has the resiliency to respond to an adverse event, their information systems are adequately protected, and their reputations reflect well upon your organization, among many other things. And even though a breach may target a vendor's systems, your organization owns all these risks, making adequate risk-monitoring not just business imperative, but a regulatory requirement.

In order to properly monitor your third party relationships, your TPRM team works with the business to conduct due diligence and examine risk, ranks third parties by their potential impact on your organization. Those engagements deemed critical or high risk should be monitored regularly and reviewed annually. A recruiting agency, for example might be deemed lower risk because not much sensitive financial information would need to be shared and the agency wouldn't need access to your systems. On the other hand, a law firm could be deemed a higher risk, given the large amount of restricted information that may need to be exchanged in order to receive effective counsel. Other examples of higher risk engagements include payment and messaging systems used to transact with customers or human resources related systems which hold sensitive information about your employees.

Your TPRM team, along with the business lines, need to collaborate and stay vigilant together to ensure that your organization has safeguarded itself against malicious actors, knowing that they will go to extreme lengths to obtain information and that breaches can originate in the most unlikely of places. As they say, the supply chain is only as strong as its weakest link.

So when you hire a third party to cater your party, be like TPRM and do your due diligence. Chances are the next plate you serve guests won't send them home indisposed.

How Can Schneider Downs Help?

Schneider Downs is a registered assessment firm with the Shared Assessments Group, the clear leader in third-party risk management guidance. Our personnel are experienced in all facets of vendor risk management, and have the credentials necessary (CTPRP, CISA, CISSP, etc.) to achieve meaningful results to help your organization effectively achieve new vendor risk management heights.

For more information, please visit www.schneiderdowns.com/tprm or contact us at contactsd@schneiderdowns.com

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com

Pittsburgh
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

Columbus
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

Washington, D.C.
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003