5 STEPS TO THIRD-PARTY CYBER RISK MANAGEMENT

by Cyber GRX

1 IDENTIFY THIRD PARTIES

Build a list of all third-party vendors. Payment information can identify third-party relationships. Also, survey department and team leaders to identify shadow IT assets and services.

2 UNDERSTAND INHERENT RISK

Scope out the business use case with your vendors and use analytics and/or risk scoring capabilities to understand the risk exposure your third parties create. Spend does not equal risk. Focus on access to data, networks, applications, and devices.

3 PRIORITIZE & ASSESS

Using the information from your inherent risk review, identify critical, medium, and low priority third parties. Issue appropriate level of assessments on those vendors and validate the responses to identify critical controls. Remediate identified risks for the highest priority third parties. Set a schedule of regular assessments for others.

4 STREAMLINE & EXPAND

Leverage dynamic delivery models like third-party risk exchanges to both expand and streamline assessments of your third parties. Your third parties are someone else's third parties - delivery models like exchanges allow you to leverage each other's work and collaborate with vendors to validate and fix identified issues that introduce risk.

5 REVIEW & REPEAT

Use solutions and approaches that leverage analytics and enable informed decision making, so your efforts can be measured, reviewed, and optimized and your results can be reported to the C Suite and Board of Directors.

Learn more about Third-Party Cyber Risk Management and get a jumpstart on your TPCRM program by visiting our website at CyberGRX.com

Cyber GRX