Lessons from COVID: Vendor Management

Selecting the right vendors to work with isn't an easy task for any company. Rapid changes in technology, coupled with the need to work remotely due to the Covid-19 pandemic, have changed the of how companies do business. In this article our Covid-19 Solutions Group information security advisors discuss areas of concern that businesses should consider addressing as they move forward in their vendor selection and annual review processes.

Consideration	Action Item
Critical / High Risk Vendors High risk vendors are those that have access or potential access to private client data and or corporate proprietary information. Critical vendors are those who are most important based on function, infrastructure and process.	☐ Determine your critical and high-risk vendors. ☐ Additional criteria should be applied to these vendors as they require additional oversight and scrutiny.
Financial Stability It is important to determine if the vendor is financially sound enough to navigate a disaster or pandemic without any service disruptions.	☐ Review SOC-1, SSAE 18, financial statements, insurance policies, coverage, etc. ☐ Determine areas of strengths and weaknesses. ☐ Major changes such as fluctuations in stock prices, pending law suits, etc. should be cause for concern and possibly investigated.
Business Continuity Preparedness and Resiliency It's important to make sure your vendor is as prepared as you are. Some of the action items they should have taken are: • Documenting a business continuity plan (BCP) and test it frequently. • Documenting a pandemic plan that is tested frequently. • List any fourth party vendors that would be relied on in the event of a possible service disruption. • Identifying their critical/high risk fourth party vendors.	☐ Review the vendors and its fourth party BCP plans, service restoration ability, testing and ongoing monitoring, and cyber resiliency. ☐ Review the vendors and its fourth party pandemic plan, compare with CDC expectations. ☐ Review vendors pandemic plan testing results. ☐ Review the vendors BCP testing results. ☐ Determine areas of strengths and weaknesses.

Consideration	Action Item
Personnel When it comes to personnel, vendors should be prepared and consider: • How to maintain operations in the event of widespread absenteeism. • Ensure cross training and / or succession planning in place. • Having a documented work from home (WFH) strategy in place that ensures both security and functionality.	☐ Review the vendors WFH strategies as well as related polices and controls. ☐ Review the vendors BCP testing results. ☐ Review the vendors pandemic plan testing results. ☐ Determine areas of strengths and weaknesses.
Communication Make sure the vendor has a documented communications strategy in the event of a data breach, disaster, pandemic, etc.	☐ Review the vendors incident response plan and testing results. ☐ Determine areas of strengths and weaknesses.
Service Level Agreements Find out what the current service level agreements (SLAs) are offered by the vendor. Make sure that they can sustain them in the event of a pandemic or disaster.	☐ Review all vendor contracts for current SLAs. ☐ Review the vendors BCP testing results. ☐ Review the vendors pandemic plan testing results. ☐ Determine areas of strengths and weaknesses.
Geographic / Supply Chains It's important to find out more information about your vendor's plan to handle service disruptions, including if they have established alternate supply chains, if there are alternate sites, backups, data centers and processes for moving to an alternate facility should it be necessary.	☐ Review the vendors BCP plan to determine what if any alternate sites, backups, data centers and processes the vendor has in place. ☐ Review the vendors BCP testing results in relation to its alternate sites, backups, data centers and processes. ☐ Determine areas of strengths and weaknesses.

Consideration	Action Item
Physical Access Vendors should be aware of: • Who has access to the vendors' facility outside of its employees. • If access will change in the event of a pandemic or disaster and how. • If physical access controls been established and documented for work from home events.	☐ Review the vendors physical security policy. ☐ Determine areas of strengths and weaknesses.
Supporting Change The vendor needs to be able to adapt to changes quickly when provided with new guidance or direction. They should have a documented process for capturing emergency change and they should be documenting these events for a postmortem review.	☐ Review the vendors BCP and incident response plans. ☐ Review the vendors Change Management policy and procedures. ☐ Determine areas of strengths and weaknesses.

We're Here to Help!

Have more questions about vendor considerations? Contact us at COVIDTECH@mcmcpa.com for more information. A member of our team will be in touch.