COVID-19 IMPLICATIONS FOR RISK MANAGEMENT

Risk management and especially third-party risk management have played a significant role in protecting company assets and client/patient information and achieving regulatory compliance. But Covid-19 has had a deleterious effect on risk and risk management.

IT risk management focuses on weaknesses related to the technology itself, how people use the technology, the processes governing it's use, and regulatory compliance.

Before the Covid-19 pandemic assessing risk was relatively straight forward. Typically, you selected a well-accepted methodology and followed the templates and processes.

Then came Covid-19. Workers moved from the office to their homes overnight. Remote servers and networks had to handle far more than their anticipated number of remote workers. Home workers were outside the company network protections and firewalls. Home computers were often shared, sometimes by family members also working at home, and sometimes by children doing remote schooling. Either way, they didn't have the protections of the office computers. IT teams worked hard to bring protections to the new home workers.

But the harder risks to address concern the third parties used by most firms for payroll, billing, credit card processing, cloud storage, or many other functions.

Visibility into their security and risk was always a challenge. Before Covid-19 companies would review the third party's security procedures and then make visits to the third party's location to see how information was protected in daily work.

With Covid-19, the third-party home workers presented more risk and the visits to their locations could no longer be made safely. And even if visits were made, with many of the workers at home, the purpose of the visit was not met.

This significantly impacted security and the ability of companies to confirm that third parties were properly protecting their information. With the pandemic, it became almost impossible to ensure personal information was being protected. This is especially of concern in regulated industries where protection of information is mandated.

Companies have been adapting the internal measures to protect remote workers and providing computers to use at home or insisting on the installation of the same types of protective software as on office computers. And these measures worked. But the inability to inspect third parties remains a significant risk for many companies. Some companies are turning to objective security scores from outside firms to determine risk and identify what is needed for compliance.

Whichever method you use, be aware of the additional complexity added by Covid-19 and adjust your evaluations accordingly. Remember, the pandemic is not a valid excuse for security breaches or compromise of information entrusted to your firm and won't be accepted by regulators, cyber insurance carriers, or your clients/patients.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.