Vendors

Insurance companies, including healthcare payers, appear much more likely to make de-risking moves, with cost concerns and a lack of internal expertise to evaluate vendor controls cited as other primary reasons. The study, now in its fourth year ...

Dec. 03, 2017

53 percent of organizations surveyed are likely to exit or change (de-risk) relationships with some vendors due to heightened risk levels. The reason cited most often was fourth-party risk issues and an inability to resolve them. That's according to the annual *Vendor Risk Management Benchmark Study* by global consulting firm Protiviti and the Shared Assessments Program's.

Insurance companies, including healthcare payers, appear much more likely to make de-risking moves, with cost concerns and a lack of internal expertise to evaluate vendor controls cited as other primary reasons. The study, now in its fourth year, finds that 71 percent of these organizations will likely change their high-risk relationships over the next 12 months. Nearly half of all respondents (48 percent)

said it has become imperative from a risk and regulatory standpoint to assess

key components of their vendor risk management approaches.

"While our study revealed increased board engagement in cybersecurity, there is an 'engagement gap' in that boards remain more engaged in their own companies' internal cybersecurity risks than the cybersecurity risks of the organizations' vendors, which can have negative repercussions if even one of those vendors has a severe data breach," said Cal Slemp, managing director, security program and strategy services, Protiviti. New cybersecurity-related regulations, such as the EU's General Data Protection Regulation (GDPR), China's complex Cyber Security Law (CSL) and the stringent New York Department of Financial Services (NYDFS) Cybersecurity Requirements, have taken effect in the past year or are set to go into effect in the near future. "Even though companies have made strides in their vendor risk management practices as evident in this year's survey results, many organizations may not have access to enough vendor risk management expertise to mitigate their risks," added Slemp.

"Despite some improvement in vendor risk management overall, our study has found that – with some notable exceptions – progress has been incremental since the study's first iteration in 2014. The single most important step an organization can take to improve its third-party risk management performance is to undertake periodic, arm's length evaluations of its program's effectiveness. Regular benchmarking is extremely important given the challenges associated with a rapidly evolving, volatile external risk and regulatory environment," said Gary Roboff, senior advisor, The Santa Fe Group, Shared Assessments Program.

The research, which looks at organizations' maturity of vendor risk management, is based on the comprehensive Vendor Risk Management Maturity Model (VRMMM) developed by the Shared Assessments Program.