More to Vendor Due Diligence: The Information Security Side

By John Cuneo, senior consultant, information security services, Sollievo

Vendor due diligence (VDD) is a program that evaluates service providers to ensure that they meet your organization's needs and to assess the risk of working with them. Most VDD programs ask these questions: Who is the vendor? Where is the vendor located? What products and services does the vendor offer?

In addition, you'll generally perform a deep-dive analysis of the vendor's financials to understand the sustainability of the partnership and to collect SSAE 16 reports to satisfy information security requirements.

But, should we also question how the vendor is protecting sensitive data?

When dealing with a vendor that is performing IT services or is handling sensitive information for your organization, VDD should include information security due diligence, as well additional terms within your contract to provide extra protection. What should these terms include?

They should clearly define data security metrics, data ownership, data security standards and the right to audit. Your contract should also have specific service level agreements (SLAs) and results defined should those SLAs fall outside the metrics.

SSAE 16s is a good starting point when delving into information security controls, but weight should be given to the fact that the scope of the audits are at the discretion of the vendor. An SSAE 16 SOC 2 Type 2 is preferred for looking at information security measures, but the SSAE 16 SOC 1 Type 2 is the more common audit available.

In addition, security questionnaires, reviewing product documentation and requesting references are other ways to gain information on the security controls for a particular vendor. Ask questions similar to the following:

1) Does the vendor provide encryption in transit and at rest?
2) Will third party vendors have access to our sensitive data?
3) What level of privileges are required to run the application/system?
4) Does the application/system require additional software?
5) Can I receive a periodic user access report?
6) Does the vendor have patching/security testing processes?

Many more questions can be asked of the vendor to provide a clearer picture of the information security controls they have in place. Make sure to do this before any decisions are made so you can be sure you've found a vendor you are comfortable working with.

For more information on vendor due diligence, information security or any of Sollievo's services, please contact a senior consultant at (855) 605-5664 or seniorconsultant@sollievo.com.

About John Cuneo

John Cuneo is senior consultant, information security risk management services for Sollievo. With over 10 years of information technology experience, Mr. Cuneo is well versed in conducting information system risk assessments, security awareness training, and analyzing security controls and reports.