How to effectively manage Technology Service Providers (TSPs), reduce cyber risk, and ensure compliance

Data breaches continue to make headlines – it's important to make sure that third-party vendors are not putting your business at risk.

By Brian Smith

Vendor risk is real. Two out of three companies rely on third parties. The value that third-party technology service providers (TSPs) bring can quickly be eroded by the associated cyber risks. You need to know what's happening and what to do before the problem strikes. The Federal Financial Institutions Examination Council (FFIEC) expects financial institutions to be more diligent in managing their TSPs under the new guidance release in February 2015. So how can your financial institution effectively manage its third-party service providers, reduce cyber risk, and ensure compliance with a variety of regulations?

An effective vendor management program provides appropriate oversight and risk management of significant third-party relationships. The FFIEC defines third-party service providers broadly to include "all entities that have entered into a business relationship with the financial institution, whether or not they are a bank, regulated or nonregulated." All vendors that have access to customer information and vendors who are deemed to be mission critical should be thoroughly evaluated, typically on an annual basis.

An effective vendor management program includes a risk assessment, due diligence in selecting a third-party, contract provisions, and third-party reviews, oversight and ongoing monitoring.

Risk assessment

A solid vendor management program begins with a cyber risk assessment. The risk assessment will reveal how critical each vendor is to a financial institution's operations, which vendors have access to customer data, and whether or not the activities vendors perform present additional risk to the institution.

A cyber risk assessment should enable management to ensure that capital is sufficient to support the institution's underlying risk exposures and that the third party is operating in a manner consistent with federal and state laws, rules, and regulations, including those intended to protect consumers as well as the institution.

Due diligence in selecting a third party

When performing your community bank's risk assessment, take into account the due diligence performed before selecting a vendor. Make sure your bank understands what the relationship will accomplish for the institution, and why the use of a third party is in your best interest. Performing periodic due diligence throughout the vendor relationship may take into account the vendor's financial

condition, the scope of their internal controls, cyber security and privacy protections, their use of subcontractors, their SSAE16 or Service Organization Control (SOC) reports (if they store sensitive customer information); as well as their business continuity planning efforts.

Contract provisions

Once a third party is selected and prior to entering into an agreement, your community bank should ensure that the associated written contract outlines the specific expectations and obligations. Such expectations and obligations should include a requirement that the third party complies with all applicable laws and regulations; that authorization for access to records of the third party as are necessary or appropriate to evaluate compliance with laws and regulations; that insurance coverage to be maintained; and that authorization to monitor and periodically review the third party for compliance with the agreement.

Other considerations may include outlining the fees to be paid; clearly defining industry and performance standards; stating the reports to be received from the third party; delineating how nonpublic information is to be handled; and ensuring the third party's disaster recovery and contingency plans are adequate and complete.

Third-party reviews and oversight

An oversight program will generally include monitoring the third party's quality of service, cyber risk management practices, financial condition, and applicable controls and reports. Institutions should periodically review the third party's operations to verify that they are consistent with the terms of written agreements and that cyber risks are being controlled.

The review and oversight the institution puts in place should address all the requirements set forth by the FFIEC. As stated by the FFIEC, operational risk is the primary risk associated with technology service providers, because operational risk may arise due to inadequate or failed processes or people-related issues. Additionally, these operational risks may also affect other risks such as, credit, interest rate, liquidity, price, compliance, strategic or reputation.

Not only should the institution have a well-defined risk management approach, the institution should perform due diligence on the service providers' risk management approach to ensure they don't have inadequacies that require corrective action. Identified weaknesses should be documented and promptly addressed. The level of supervision required is, of course, dependent on your community bank's risk assessment for the service being provided.

Consequences of non-compliance

FDIC examiners review a financial institution's management of these relationships to ensure that its third parties comply with consumer protection laws and regulations. Examiners pay special attention to an institution's ability to assess, measure and control the risks associated with service providers.

It's worth emphasizing that an institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, as well as for identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution.

Examiners may pursue corrective actions for deficiencies found that pose a safety or compliance violation during the examination. Deficiencies can result in corrective actions or fines against the institution and potentially the directors.

Billions of dollars are spent on cybersecurity, yet breaches still happen. Simply increasing spend is not the always the best option – InfoSight is helping customers build programs that respond to their material business risks while balancing resource expenditures. We can help you understand your risk profile with an IT risk and vulnerability assessment, and then help you manage risks in line with the complexity and risk profile of your institution. This assessment is part of a full range of information security services we offer to help you develop and maintain a comprehensive cyber security program.

Contact us for free copy of our Vendor Management Toolkit, or visit our website to learn more about our solutions and service offerings.

Brian Smith (Brian.Smith@InfoSightInc.com) is Chief Information Security Officer at InfoSight Inc., a company in Miami, Fla., that provides managed security, IT compliance and vulnerability management services.