Managing Vendor Risk: Misunderstanding the Vendor-Cyber Connection

By Michael Berman

Firewalls and penetration testing are top of mind when it comes to cybersecurity, but a bank's greatest vulnerability may be its vendors[1].

Target's well-publicized data breach was caused by an HVAC vendor that had access to its system. Hackers exploited the connection to steal 40 million credit and debit card numbers and the personal information of 70 million customers. Similarly, a community bank found itself reimbursing customers for fraudulent debit card transactions after a security breach at its third-party core processor.

Regulators have taken notice, increasing regulatory expectations for both cybersecurity and vendor management. Many financial institutions fall short of understanding just how much these expectations overlap.

It happens at banks across the country. The IT department handles cybersecurity while the compliance department tackles vendor management. The result is a silo. The people focused on cybersecurity know to look at vendor management, but they do not realize there is a whole set of other guidance on the topic. The vendor management team does not think to share its work with IT, which is a big mistake.

With the release of the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool last June, the regulatory expectations for cybersecurity and vendor management overlap more than ever before. Of the 441 questions designed to help financial institutions evaluate their cybersecurity risk, 10 percent are dedicated to what regulators call "external dependencies"—also known as third-party vendors.

This presents a huge challenge for banks that don't have a holistic approach to compliance and operational risk management. They often struggle with three key problems:

1. Redundancies. The regulatory agencies, including the Federal Reserve, the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC) and the FFIEC, all address regulatory expectations for third-party vendor management. The FFIEC's tool draws on many of the same best practices, including due diligence, inherent risk assessments, ongoing monitoring and contract issues. Most of its assessments are nothing new—inquiring about policies and procedures for managing third-party relationships, including cybersecurity controls that banks should already have.

---

[1] FEI. (2012, November). Retrieved February 25, 2016, from http://www.financialexecutives.org/KenticoCMS/Financial-Executive-Magazine/2012_11/Is-Vendor-Screening-Really-Necessary-.aspx#axzz41By2xPKs

IT should be building on and leveraging this work, yet in many cases, the IT department does not have this information—and doesn't even know it exists. This is especially true at institutions where compliance is managed manually.

For example, vendor management expectations require banks to assess and identify high-risk vendors, implement controls and develop policies and procedures to regularly update assessments. That includes assessments of credit risk, reputation risk, operational risk, strategic risk, transaction risk and cyber risk.

When IT is told to review the FFIEC's assessment tool and doesn't have access to these materials, it may unknowingly duplicate those efforts. Time is wasted compiling lists of third-party vendors, assessing individual vendors and developing processes for conducting due diligence and ongoing monitoring when the vendor management team has already done it.

2. Inefficiencies. Duplicating efforts obviously wastes time and resources. However, silos create other layers of inefficiencies as well—especially when it comes to policies and procedures.

When compliance assesses a third-party vendor's cyber risk, some person or team must study what cyber risk is, determine appropriate levels of risk and make plans to monitor and mitigate them. Policies and procedures are then drafted.

There is a good chance that cyber risk knowledge already exists in the IT department. Leveraging that expertise saves time and can result in better oversight. Not only that but input from the IT team can help draft policies and procedures that are more practical for the bank to implement. Working together can create stronger, more efficient policies that reduce risk and minimize resource use. Banks need to ask if existing vendor management policies and procedures help or hinder cybersecurity efforts.

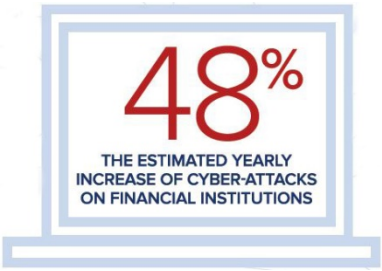
3. Discrepancies. Regulators have already begun integrating the FFIEC Assessment Tool into their exams. The FDIC has said examiners will discuss it with banks "to ensure awareness and assist with answers to any questions." The Fed plans to include it when "evaluating financial institutions' cybersecurity preparedness in information technology and safety and soundness examinations and inspections."

That means your staff needs to be prepared to confidently answer questions raised by the assessment tool. Many institutions have unknowingly put themselves in an uncomfortable position—one where different staff members have different answers.

For instance, the assessment tool addresses whether third-party vendor contracts have adequate notification of breach provisions. If the IT and compliance teams have not collaborated, their separate policies and procedures may not agree. The IT team may require notification within one hour while compliance may say 24 hours. Alternatively, the IT department might tell an examiner that there are no issues while someone in compliance might say there are issues the bank is working on remediating. These kinds of discrepancies are red flags for regulators—and easily avoidable by eliminating silos.

When regulators raise issues about a compliance program, there's often the temptation to hire more staff to deal with the problem. However, in a silo situation, adding staff can actually increase duplication and discrepancies. If a single control is being tested five times by five different people, adding another

person into the mix just means that control will be tested a sixth time. But when you address the core problem—taking a broader view of compliance management and increasing communication—employees become more productive with one person testing a control that appears in five different reports.



The disconnect between vendor management and cybersecurity is just one example of the kinds of problems banks experience when they do not have a comprehensive and bank-wide approach to vendor management and compliance. Such systems not only help banks integrate cybersecurity and vendor management compliance functions but reduce compliance and risk issues throughout the bank.

At a time when low-efficiency ratios are critical to success, and the cybersecurity[2] stakes are high, it is a connection no bank should miss.

Michael Berman is founder and CEO of Ncontracts, a leading provider of risk management software and services to financial institutions. To learn more about how your bank can streamline vendor risk management and compliance, call us at 888-370-5552, email us at info@ncontracts.com, or visit us on the web www.ncontracts.com.

[2] Ginovsky, J. (2014, October 16). Security breach incidents up 48% this year-and counting - Banking Exchange. Retrieved February 25, 2016, from http://www.bankingexchange.com/news-feed/item/4993-security-breach-incidents-up-48-this-year-and-counting