WHO’S YOUR DATA?
Getting to Know Your Vendors and Protecting Your Data
WHO’S YOUR DATA?

Getting to Know Your Vendors and Protecting Your Data

BY MARCIA GEIKE, CRCM AND DAVID McCREA, CRCM
Who Are Your Vendors?

Let’s first go for the low-hanging fruit. If you haven’t already done so, go to your accounts payable department and request a listing of the vendors that are paid on a monthly, annual, or other periodic basis. (You may also need to review one-time payments.) A quick review of this list will identify vendors that you don’t need to worry about. For example, you’ll immediately identify and assume you can ignore vendors such as gardeners, plumbers, pest control, subscriptions/periodicals, and utilities. Or can you? Accounts payable may be able to provide you a list quickly, but you need to take time and review your vendors carefully. If the vendors don’t have access to your facilities or customer data, you may be able to give them a very low risk rating—for example, vendors that provide subscriptions/periodicals that are received via mail or delivered to the exterior of the building (like a magazine or newspaper). Utilities, such as electricity, water, and natural gas could also be low risk, but that is assuming that you have a practice of accompanying all utility vendors while they are onsite. And when you are risk-rating your vendors, you should consider the importance of these vendors to your operations. You can keep an office open without water—even without heat—but keeping your operations going without electricity is more difficult. Your terminals won’t work, most phones won’t work, your security system could be compromised, and the office is dark and hot/cold—depending on the time of year and where you are in the country.

Communications utility providers tend to be higher risk, because they often do more than handle voice communications. They often handle data, too. And this is another area where your security systems could be compromised. How can your security system alert the police or your security company of an emergency if the technology used to reach them isn’t available? And to add to the complexity, there may be multiple communications vendors for each of your office locations (i.e., voice, data, cellular, etc.). Encryption of your data communications can reduce the risk associated with the loss or misuse of data, but encryption only prevents the wrong folks from using the data. It doesn’t address what happens when data cannot be reliably transmitted from one point to the other. So you need to consider the reliability of the vendor, its back-up facilities/plans, how
In all seriousness, you probably do trust your external auditors and your consultants, but since you likely share data with them, they might fit on the high risk list. And never underestimate the value of asking everyone what systems and vendors they use. In a community bank, you may actually be able to ask literally everyone. At a larger bank, you may have to limit your inquiries to key individuals and departments. Of course, not all vendors identified from asking will be “high risk” vendors, so you’ll need to identify the risk level as you evaluate each vendor relationship. And you can’t take “we don’t use any vendors” for an answer. Often, the individuals and departments you are working with aren’t aware that the services they use are vendors, or they don’t really want to take the time to document who their vendors are and share them with you. Just like you, they are busy. And they probably don’t enjoy vendor management as much as we do. Remember, it takes a village (lots of vendors) to operate and manage a bank, so don’t hesitate to keep asking and including examples of the types of vendors you’re looking for.

Other “obvious” vendors that carry a “high” risk might include those vendors you have partnered with to provide services directly to your customers. These vendors can include sales/marketing partners, investment services, insurance companies, service partners, debt collection firms, law firms (yes, even attorneys are vendors), loan and deposit account servicers, and check printing companies.

High Risk Vendors with Less Obvious Risks

Which are some of the less obvious vendors with a high risk level you should consider? These include your external auditors, consultants, temporary employees, and contract employees. But you say, wait, I trust my external auditors—and everyone trusts consultants, right? In all seriousness, you probably do trust your external auditors and your consultants, but since you likely share data with them, they might fit on the high risk list. Of course you’ll need to determine how secure your data is with these vendors, too. What sort of data center does your auditor or consultant have? And what data do they have and where is it stored? Is it stored on their servers, or is it stored on individual PCs? Do you know? Does your vendor know? And not only do you need to consider where it is stored, you need to consider whether it is backed up, and who has the back-up data.

Your external auditors and consultants often assist you with financial, operational, and compliance matters. As a result, you probably have contracts that outline data security and privacy obligations. But do the contracts address...
the security of your data on individual PCs or the security of your data when it is stored in the servers of your vendors? And if the contract does address these issues, what due diligence have you done? You should obtain copies of any third-party audits that have been performed, such as Service Organization Controls (SOC) reports, Payment Card Industry (PCI) compliance reports, etc. (NOTE: If you haven’t already done this, you will want to identify the different steps you’ll take with each vendor relationship commensurate with the level of risk they pose.)

What if you are a smaller financial institution, and your ability to negotiate contracts with your vendors is limited? In other words, what do you do if your vendor declines to amend the contract to include the provisions you believe should be in the contract? Let’s face it. Vendors need to evaluate the risks in the relationship from their side and they are likely to be different than the risks we have in the relationship, but what do we do when these challenges happen? First, you should consider using another vendor. If the vendor won’t include the contract provisions you require, find one that will. But what if another vendor is not an option? Then you will need to work hard to negotiate the provisions that you can, and you may be forced to accept the risk that some of the provisions are not in the contract.

And for all of the vendors that we have mentioned, do you have a certificate of insurance? Have you reviewed their disaster recovery plan? Have you reviewed their financials? Because if something happens to your vendor, what happens to your data? What happens to your operation? There have been several cases of industry vendors that were unable to stay in business and simply stopped operating. What will you do if that happens to you? And to complicate matters, you now may need to consider your vendors’ vendors as your own vendors.

Let’s Not Forget—Cybersecurity Risks

Cyber threats have increased year to year and require a strong cybersecurity program to identify, prevent, detect, and recover from attacks. Vendors are a key source of the risk as well as a link in managing cybersecurity risk. It’s said that cybersecurity is only as good as your weakest link, and you don’t want vendors to be that link! Think about the number of vendors that might have access to your systems, or the vendors whose systems contain your data and might be vulnerable to intrusion, including:

- Managed IT services—outsourcing vendors for network and intrusion detection
- IT support—managing routers and servers
- Cloud services—Software as a Service (SaaS)
- Non-IT providers—high-tech heating and air conditioning, security companies

You might recall a major US retailer’s breach in 2013 where the security, or lack thereof, with an HVAC provider opened the door to what was a breach for over 100 million people. It is estimated that the cost to manage the breach was $248 million before receiving $90 million in insurance receivables. So a robust vendor program can also save you money!
Once you've identified the risks your vendors present, you have to start thinking about your vendors’ vendors.

Monitoring Your Vendors’ Vendors

Once you've identified the risks your vendors present, you have to start thinking about your vendors’ vendors. Companies wishing to be your long-term partner may portray themselves as a “one-stop shop” while outsourcing some of the services to another vendor or sub-contractor. Who are these additional companies? What data do they access and how secure is their system? How strong are your vendors’ controls in their vendor relationships? There could be another layer in identifying your weakest link.

Your vendors’ vendors, also referred to as sub-servicers or sub-contractors, might be the least obvious of your vendors. When you identify them, you will need to ensure that proper due diligence on them occurs. First, you will need to identify who they are, what service(s) they provide to you or your vendor, what data they may have access to, and when they may have access to the data. Also, you need to complete the same level of due diligence and vendor risk rating on them, too. And the chain can keep going. You may need to identify your vendors’ vendors’ vendors. (This can keep going, but you get the idea.) And this is where a well-designed contract helps mitigate the risks. You will need to review the contract to determine who the vendors are, or whether the contract grants you the authority to question your vendors as to who their vendors are and what services are performed by them. This level of review may bring to light the fact that you need to update or re-write your vendor contracts to have the authority to perform this level of due diligence. But this can also bring you back to having to choose between accepting the fact that you are unable to make changes to the contract or switching vendors.

When technology is a major component of the vendor relationship a review of the internal controls should be conducted prior to entering the relationship and periodically, depending upon the risk level of the service. This usually involves a report from a trusted third party, like an accounting firm.

You may recall that in 2010, the American Institute of Certified Public Accountants (AICPA) retired the old SAS70 report, used to review controls on financial statement reliability, for the Statement of Standards for Attestation Engagements #16 (SSAE16) using the SOC-1 report. Over the years the industry has come to utilize these reports and vendors have expanded their independent reviews beyond the SOC-1 to include other types like the SOC-2 which focuses on the principles of security, system availability, processing integrity, confidentiality and privacy. In May 2017, the AICPA released an enhanced tool that can help you evaluate the protection of your vendors’ systems—a new SOC-1 report The AICPA has updated the standards as part of the SSAE18 rules and added several sections to the SOC-1 so you can evaluate the data risk not only for your vendors but also your vendors’ vendors. It could include data centers, cloud infrastructure, and other outsourced services that have access to your data and could increase the risk of breaches.

Accounting firms performing the SOC-1 testing should inquire about your vendors’ oversight of their outsourced services. Examples of this type of activity could include:

▪ Reviewing and reconciling output reports;
▪ Holding periodic discussions with the subservicer;
▪ Making site visits or performing audits at the subservicer location;
▪ Testing controls at the subservicer;
▪ Reviewing the subservicer’s SOC-1 reports (on financial reporting controls) and SOC-2 reports (on non-financial reporting controls); and
▪ Monitoring external communications, such as customer complaints.

These controls may have been conducted all along but now their process will be formalized and documented.

This should sound familiar because it is similar to the controls that the regulators are expecting of your own vendors. The consistency should provide institutions with a better understanding of who has access to your information and the established controls and risks. These new SOC-1 standards should start to be seen in reports being issued in late summer and do not impact SOC-2 or SOC-3 non-financial reporting.
REGULATORY AGENCIES hold institutions responsible for the activity of their vendors. As regulators have stated for many years, banks can outsource a task or function but cannot outsource the responsibility. Much like a function performed in-house, you need to ask the detailed questions about how tasks are completed, take the time to review marketing materials designed by the vendor for your clients, and ensure that consumers receive clear information timely when required. It’s a good bet that the corrective action from an enforcement action will at least roughly translate to “best practice” in examinations.

Let’s look at a few enforcement actions to see what third-party relationship weaknesses have been identified to ensure that your program can withstand scrutiny in this area. There have been several actions in recent years and let’s look at one from August 2016, when the Office of the Comptroller of the Currency (OCC) penalized a Midwest bank after reviewing its process for offering identity theft products to its clients. According to the enforcement action, from 1997 to 2013, clients were assessed a monthly service fee even though they had not completed the registration process for the service and, therefore, were not receiving the full benefits of the identity theft service. This program had not been identified by the bank as being deceptive. Besides the penalties and reimbursement requirements, the bank had to build a vendor management program that includes an analysis of any new servicer performing the marketing, sales, delivery, servicing, and fulfillment of services. New and renewed contracts had to include third-party responsibilities to maintain adequate internal controls, appropriate training of third-party employees, the ability of the bank to perform onsite reviews, and the right to terminate the contract if any terms were not met. Since its controls were insufficient to identify this issue timely, the bank also had to develop a written enterprise-wide risk management program monitoring consumer products for unfair, deceptive, or abusive acts or practices (UDAAP).

In July 2016, a bank entered into a consent order with the Bureau for not obtaining affirmative Reg. E opt-ins before charging overdraft fees with ATM and one-time debit card transactions. This order entered the vendor management realm because it was a vendor’s employees who sold the product to the bank’s customers through “vigorous” telemarketing campaigns. The vendor was incentivized to enroll as many customers as possible with a premium if it hit sales goals. The vendor’s employees had hourly sales goals and if they were not meeting the goals in the morning they were sent home and unpaid for the rest of the day. If goals continued to be unmet, employment was terminated. The bank received complaints and conducted research that alerted them to the aggressive process by the vendor. This resulted in a temporary halt to the campaign and training for the employees. However, the bank continued the incentive program and allegedly conducted insufficient vendor oversight resulting in its failure to detect that the inappropriate activity was continuing. As well as building a better vendor management program, the bank was told to fire the vendor and discontinue all business with it—an unusual step in consent orders. The bank paid a civil money penalty of $10 million and had to re-verify all consumers who opted into the Reg. E program.

In another example, a bank partnered with a vendor to provide student checking accounts. College students frequently fund their education with student loans. In this case, students had the ability to hold excess funds above their tuition in a checking account established at a specific bank, receive a paper check to deposit or an ACH transfer to an account at their own bank. However, the vendor was not clear in explaining these options to students and primarily shepherded them into opening a new bank account. It did not explain its fees until after the account was opened so students found themselves paying fees they didn’t expect such as a $0.50 for each debit card transaction used with a PIN and 3.5% for withdrawing funds using a bank teller. The website and material set up by the vendor for the students had “material omissions” about the fees and features of the account. It was not until the final page of the online registration, after they had entered all of their personal information and selected the checking account feature, that the student was shown any of the fees. The website featured the college logo, which was deemed to have led students to believe that the checking account at this bank was a “preferred” method. Shortly after the agreement between the bank and the vendor was signed, and after 220,000 new checking accounts had been opened, the bank recognized that the vendor website could be misleading and began requiring all impacted students. The bank had self-identified the UDAAP issues and demanded that the vendor remediate. It is possible that since the bank made timely appropriate changes, the Federal Reserve assessed a civil money penalty of only $960 thousand.
GETTING TO KNOW YOUR VENDORS AND PROTECTING YOUR DATA

Keeping up with Changes
It seems that as soon as we think we’ve finished building a strong vendor management program we learn about new rules and interpretations that require amendments to our program. Vendor management should be a dynamic program and, as always, we need to keep the program current! To illustrate, let’s look at a few recent publications that might have missed our radar.

In July 2016, the Federal Deposit Insurance Corporation (FDIC) proposed third-party lending guidance covering safety, soundness, and compliance in business relationships with third parties. This could cover loan participations, indirect lending, mortgage brokers, and correspondent lending. The proposal details what would be expected in policies, procedures, and oversight of vendors, if the proposal is made final. The comment period ended this past October, but the guidance has not yet been finalized.3

When it comes to your vendor management program, one size does not fit all.

In November 2016, the Federal Financial Institutions Examination Council (FFIEC) rolled out the updated Uniform Interagency Consumer Compliance Rating System, which took effect March 31, 2017. While the third party section represents no additional expectations, leaving the details to the individual agency pronouncements, the system clarified that the topic would be covered as part of the overall consumer compliance program while historically it’s been part of the IT examination. This reinforces the regulatory concern that while vendors are utilized to offer products and create efficiencies that it may open the institution to compliance risk, whether the credit union or the bank.

So your vendors will vary from the “low hanging fruit,” to the less obvious vendors, to the “high hanging fruit” which is your vendors’ vendors. And to complicate matters, vendors often change (sometimes you deal with the same people who are now working under a different company name), so you will need a dynamic program that can respond to changes to ensure that your vendor management program is current.

Your responsibility does not end when you sign the dotted line on an agreement. Depending upon the risk level of the service provided by the vendor, ongoing oversight of the relationship, even if it’s just to collect the latest insurance coverage declaration periodically, is the basis upon which your program will be measured. One size does not fit all when it comes to your vendor management program or to managing each vendor. Banks need to be flexible and make changes when necessary, which could include saying goodbye to a vendor. ■

Endnotes
1. The AICPA website has all of the changes on its website, but the section referred to in the article is AT-C Section 320, http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-C-00320.pdf

ABOUT THE AUTHORS:
MARCIA GEIKE, CRCM, is Vice President and Senior Compliance Officer at Home State Bank, a community bank in northern Illinois. Along with managing the compliance program at her bank she has responsibilities for the Community Reinvestment Act, privacy, record management, and third-party risk management. She currently serves on the ABA’s Bank Compliance magazine Editorial Advisory Board, has served on several ABA committees, and taught at the ABA Graduate School of Compliance Risk Management. She can be reached at mgeike@HomeStateOnline.com.

DAVID MCCREA, CRCM, is a Director with Treliant Risk Advisors and is an experienced executive with a background in compliance, Bank Secrecy Act/Anti-Money Laundering (BSA/AML), operations, vendor management, security, and fraud/loss control at banks, thrifts, and a core banking software company. He currently serves as a Faculty Member of the American Bankers Association’s (ABA) Compliance School, is an instructor for an Executive Development Program provided to several state banking associations, and is a frequent speaker for state banking associations. He can be reached at dmmcra@treliant.com.