ABA Insurance Services | MEMBER OF GREAT AMERICAN INSURANCE GROUP

SafeTalk®

Carefully review your third-party service provider contracts. Don't just accept, negotiate!

Cybercriminal gangs continue to use new technologies to find new and innovative ways to access prized data to turn a profit. They may target you directly or target your service providers. Dozens of insureds have been implicated in the recent MoveIt vulnerability through third-party providers who were holding the financial institution's customer data. Even when a contracted or partner company is attacked, financial institutions still bear responsibility in protecting the bank's data and customer account information. Do your vendor due diligence before a breach happens.

Using third-party service providers may increase confidence and capacity for financial institutions, but a systems breach occurring at a third-party vendor, (i.e. the MoveIt data breach and zero-day vulnerability attacks) can also create havoc for any bank that hasn't considered the risks in advance.

Regulators have stressed the importance of applying a comprehensive risk management process throughout the life cycle of the vendor relationship—from vendor selection and performance monitoring through to relationship termination.

One vendor risk management area receiving more attention lately is contract negotiations, and for good reason: Third-party providers have long shifted the bulk of liability and responsibility for their system breaches to the bank; however, banks should recognize that they have a voice in contract negotiations and should look for their own contractual protections. Such protections should address:

- Banking and customer information protection
- Shifting liability and expense risk of a vendor breach back to the vendor
- Compliance with federal and state laws, such as the Gramm-Leach-Bliley Act (GLBA) and the Massachusetts Data Security Regulation
- Compliance with regulatory guidance, such as **OCC Bulletin 2023-17, "Third-Party Relationships: Interagency Guidance on Risk Management"**

Key Contractual Provisions to Consider

While there is no one-size-fits-all approach in crafting third-party contracts, here are some key contractual provisions to consider as requirements in all provider agreements:

Legal Compliance. If the third-party provider will have access to personal identifiable information, some security procedures are required by law. For example, the Gramm-Leach-Bliley Act requires service providers to adhere to the Safeguards Rule requiring organizations to have a security program in place that ensures the security and confidentiality of customer records.

Security Standards. Providers should commit to adhering to an up-to-date security program that addresses physical safeguards, data and system safeguards, employee training, risk assessments and data destruction policies.

Personnel Policies. Providers should perform background checks on all employees who will have access to the bank's data. Further, any personnel access to the bank's data should be on a "need-to-know" basis.

Data Encryption. Encryption is a safe legal harbor in nearly all data breach notification laws; therefore, it is critical for vendors (and banks) to always transmit or store sensitive data in an encrypted format.

Response in the Event of a System Breach. A provider should be required to investigate and remediate the cause of the breach, and the bank should expect full cooperation and notification of all breach investigatory findings. The bank will want the right to control all customer-facing aspects of the breach response, including breach notifications.

Continued ⇨

Audit Access. Contracts should allow the financial institution and its regulators the right to audit the vendor's security practices. Additionally, consider requiring third-party audits with reports copied to the bank.

Termination Rights. Maintain or obtain the right to terminate the contract if the supplier fails to comply with its security obligations. Do not tie the right to termination to an actual security breach.

Expense Reimbursement. Providers should be required to reimburse the bank for expenses incurred by the bank while responding to a breach event, such as credit monitoring services, notification expenses, and professional service fees. Vendors may push back on this and request an expense cap or require a negligence standard of liability.

Require Contractual Liability. Most vendors include contractual disclaimers of consequential damages and a general liability cap (which is surprisingly small), but banks should insist on certain exceptions to the cap, including any indemnification obligations pertaining to provider breaches of confidentiality or security procedures.

Source: David J. Ackley, Jr., Senior Vice President, Senior Information and Corporate Security Officer, Camden National Bank, and Joshua T. Silver, esq., Shareholder, Bernstein Shur Sawyer & Nelson; Speakers at the ABA Risk Management Forum 2015 Session, "Cyber Governance: Managing the New Risks."