

An Ounce of Prevention: Business Continuity and Incident Response in Technology Service Provider Contracts

Bryan Handlos, Kutak Rock LLP



"Being old and lame of my Hands, and thereby uncapable of assisting my Fellow Citizens, when their Houses are on Fire; I must beg them to take in good Part the following Hints on the Subject of Fires. In the first Place, as an Ounce of Prevention is worth a Pound of Cure . . . The author goes on to talk of "Prevention" including regulating hearth sizes, licensing chimney sweeps, and organizing a] Club or Society of active Men belonging to each Fire Engine; whose Business is to attend all Fires with it whenever they happen; and to work it once a Quarter, and see it kept in order: Some of these are to handle the Firehooks, and others the Axes, which are always kept with the Engine; and for this Service they are considered in an Abatement or Exemption in the Taxes . . . These Officers, with the Men belonging to the Engine, at their Quarterly Meetings, discourse of Fires, of the Faults committed at some, the good Management in some Cases at others, and thus communicating their Thoughts and Experience they grow wise in the ehing, and know how to command and to execute in the best manner upon every emergency."

"On Protection of Towns from Fire, 4 February 1735," Founders Online, National Archives.¹

Introduction

In the steady stream of regulatory guidance that flows through banks today, the FDIC's recently issued Financial Institution Letter 19-2019 creates few ripples. The letter focuses on only a couple of vendor management tasks — business continuity and incident response preparedness.² The underlying risks are, for many banks, considered somewhat remote. Perhaps it is that remoteness which explains why bank examiners are observing gaps in bank vendor contracts with regard to vendors' business continuity and incident response obligations. Remote or not, the occurrence of a vendor business continuity event (e.g., a localized disaster) or a vendor information security breach has the capacity, like a building fire, to cause significant harm.

A bank should be able to determine with relative ease whether business continuity or incident response gaps exist in its vendor contracts. Preventing gaps in most new contracts should be relatively straightforward. Addressing gaps in existing contracts may require more effort. Unsurprisingly, FIL-19-2019 itself provides little specific guidance on the exact terms and steps a bank should use to avoid examiner criticism in this area. This article proposes some practical action steps to avoid or minimize the examiner criticisms called out in FIL-19-2019.

Regulatory Requirements and Observed Gaps

Managing third party risk should be nothing new to a bank. Vendor management and vendor management contracting considerations have been topics of regulatory attention for several years. As evidenced by FIL-19-2019, however, the FDIC believes banks still have room for improvement. The two primary areas called out for specific attention are vendor business continuity and incident response obligations.

Business Continuity: The FDIC baseline guidance for business resumption and contingency plans in vendor contracts states:

The contract should address the third party's responsibility for continuation of services provided for in the contractual arrangement in the event of an operational failure, including both man-made and natural disasters. The third party should have appropriate protections for backing up information and also maintain disaster recovery and contingency plans with sufficiently detailed operating procedures. Results of testing of these plans should be provided to the financial institution.

FIL-44-2008. The FFIEC's Business Continuity IT Examination Booklet has a considerably more extensive discussion on business continuity, and Appendix J in particular contains detail on outsourcing and contract issues. Despite this existing guidance, FIL-19-2019 recites that some banks' "contracts do not require the service provider to maintain a business continuity plan, establish recovery standards, or define contractual remedies if the technology service provider misses a recovery standard."

Incident Response: The FDIC baseline guidance for confidentiality and information security in vendor contracts states:

The contract should prohibit the third party and its agents from using or disclosing the institution's information, except as necessary to perform the functions designated by the contract. Any nonpublic personal information on the institution's customers must be handled in a manner consistent with the institution's own privacy policy and in accordance with applicable privacy laws and regulations. Any breaches in the security and confidentiality of information, including a potential breach resulting from an unauthorized intrusion, should be required to be fully and promptly disclosed to the financial institution.

FIL-44-2008. The FFIEC's Information Security IT Examination Booklet has a more extensive discussion of incident response generally. Despite this existing guidance, FIL 19-2019 observes that some bank "contracts did not sufficiently detail the technology service provider's security incident responsibilities such as notifying the financial institution, regulators, or law enforcement."

Addressing Contract Gaps on a Going Forward Basis

If a bank is currently entering into new vendor contracts that contain business continuity and incident response gaps, the bank should promptly correct its policies and procedures:

Counselor's Corner — continued on page 18



LIVE FEARLESS
BlueCross BlueShield Nebraska

Proudly offering group insurance to
NBA members for more than 30 years.

To learn about our plans, visit nebankers.org

An Independent Licensee of the Blue Cross and Blue Shield Association

- **Identify Gaps:** The bank should review existing policies, procedures, checklists and templates for new contracts to verify that appropriate business continuity and incident response provisions are included. The bank may also wish to consider whether the level of gaps uncovered in any review of existing contracts (see below) indicates the existence of deficiencies that should be addressed in its policies, procedures and templates on a going forward basis.
- **Start with Diligence:** As with most third party risk management issues, diligence is key to business continuity and information security/incident response issues. The bank should verify that its diligence process covers new vendors' policies, procedures and related controls with regard to business continuity and incident response. Specific concerns coming out of diligence should be shared with the bank's contracting team for special treatment in the contract if necessary. In some cases, diligence may indicate that business continuity and/or incident response issues do not pose significant risks.
- **Consider a Standard Template:** Consider preparing standard templates for basic business continuity and incident response provisions. Templates can of course be risky if they are used without contemplation of specific circumstances. On the other hand, templates can also provide a standard starting point and minimize the chance that a contract is entirely silent on an important topic. Some banks will build vendor business continuity and incident response obligations into standard templates that they use for privacy and information security generally.
- **Don't Forget Related Provisions:** Business continuity and incident response issues can implicate other vendor management contract topics. Depending on the circumstances, these may or may not need to be specifically addressed in other contract provisions. For example:
 - ▶ Audit Rights — audit rights can be an important tool to verify that relevant business continuity and incident response testing occurs and to verify that business continuity and incident response obligations are passed through to subcontractors;
 - ▶ specific performance Standards and SLAs — contracts should generally include specific recovery time and recovery point objectives for business continuity and should require prompt reporting of security breaches for incident response purposes;
 - ▶ events of default and termination — a bank ought to consider whether these provisions should specify whether

failure to meet business continuity and incident response obligations will trigger specific breach or termination rights and whether cure periods and remedies specifically appropriate to those types of defaults should exist;

- ▶ subcontracting — vendor contracts should address the permissibility of subcontracting and vendors should also be obligated to pass their business continuity and incident response obligations on to their subcontractors; and
 - ▶ foreign service provider issues — banks should evaluate the special impacts of offshore activities on business continuity and incident response obligations, including the potential impacts of other jurisdictions' laws and the need for the vendor, even though offshore, to comply with U.S. law.
- **Conduct Ongoing Monitoring:** Similar to diligence, ongoing monitoring is a key element of third party risk management. Contract provisions may be worth only the paper they are written on if the vendor does not live up to its commitments. Monitoring is critical to actually managing risks. Business continuity plans may evolve over time and require ongoing testing. Incident response programs are of course critically dependent on incident identification which will rely upon systems that are updated from time to time and subject to periodic testing. Without monitoring, a bank may be in for a nasty surprise about a vendor's actual preparedness despite having a tidy contract provision to point to.
 - **Consider Backstops:** Bankers should evaluate what contingency plans the bank can make and implement, if any, against the possibility that a vendor will fail to fulfill its business continuity and incident response obligations. If such plans require any resources or assistance from the vendor, include those requirements in the contract.

Addressing Contract Gaps on Existing (Deficient) Contracts

If deficiencies exist in the bank's existing contracts, the bank should take steps to remedy those deficiencies if possible:


- **Identify Gaps:** The bank should review its existing contracts (or at least some prioritized subset of them) and note the absence of appropriate business continuity and incident reporting provisions.
- **Consider Current Standards:** In reviewing existing contracts, evaluate how the contract would have been prepared according to current contracting policies, procedures, checklists and templates (assuming those current standards are adequate).
- **Prioritize What to Remediate:** If many potentially deficient contracts are identified, prioritize remediation based on criticality and length of the remaining contract terms (long term contracts may present higher risk; those coming up for renewal shortly may present

a fair opportunity for an amendment at that time to remediate the deficiency).

- **Evaluate Opportunities and Leverage for Remediation:** For contracts that need remediation, the bank should assess the circumstances of the bank's current relationship with the vendor and evaluate the prospects for voluntary vendor cooperation or the availability of leverage needed to remedy the deficiency.
- **Approach the Vendor:** Use existing contracts rights (if any) and/or a good working relationship with the vendor to seek relevant diligence information on the vendor's existing business continuity and incident response policies, procedures, plans and resources. A bank may wish to consider inviting the vendor to proactively assist in resolving any deficiency (e.g., does the vendor have a business continuity or incident response provision it finds acceptable and will offer to the bank?).
- **Seek an Amendment, If Appropriate:** Amending an existing agreement may be an appropriate request, even if the contract is in mid-term. Business continuity and incident response obligations do not necessarily need to add significant costs to the vendor's ongoing performance (and thus should not present an excuse to raise prices). Hopefully, an underlying business continuity planning process already exists at the vendor, as does an incident response program. If not, the vendor may be in the wrong business as a service provider to banks. In many cases, vendors may already be subject to state law incident reporting obligations.
- **Implement Alternative Remediation If Necessary:** If a gap in an existing contract cannot be filled with an appropriate contractual provision, the FDIC indicates that a bank should take alternative steps such as modifying its own business continuity plan to address contractual uncertainties. This may well be difficult or impractical, depending on the service. Unless the bank is in a long term relationship with exclusivity or minimums, an important vendor with such an unbridged business continuity or incident response gap may need to be replaced.

Conclusion

Vendors' business continuity and incident reporting obligations are central to a bank's preparedness when a disaster or information security breach strikes without warning. Such obligations, piled on with other modern vendor management obligations, often feel burdensome to the bankers and vendors who must bear them (and that burden usually feels heavier than an ounce). When a fire strikes though, whether in the form of a vendor business continuity event or a security breach, well-organized business continuity and incident response preparedness will be worth a pound of cure. We can also hope that bankers' internal vendor management, business continuity and incident response teams will "grow

wise in the thing, and know how to command and to execute in the best manner upon every emergency." 

¹ <https://founders.archives.gov/documents/Franklin/01-02-02-0002>. [Original source: *The Papers of Benjamin Franklin*, vol. 2, January 1, 1735, through December 31, 1744, ed. Leonard W. Labaree. New Haven: Yale University Press, 1961, pp. 12-15.]

² The letter also: (i) notes that "some contracts do not clearly define key terms used in contractual provisions relating to business continuity and incident response. Undefined and unclear key contract terms could contribute to ambiguity in financial institution rights and service provider responsibilities, and could increase the risk that technology service provider business disruptions or security incidents will impair financial institution operations or compromise customer information"; and (ii) reminds banks of their notification obligations under the Bank Service Company Act.



For more information, contact Bryan Handlos at Kutak Rock LLP: (402) 346 6000 or Bryan.Handlos@KutakRock.com. Bryan, a member of Kutak Rock LLP's banking practice group, concentrates on bank regulatory matters.

Together,
let's
make
it happen.

Lynn Paulson
Call me at 701.298.7138
Based in Fargo, N.D., and serving the region

Gene Uher
605.201.1864
Based in Sioux Falls,
S.D., serving South
Dakota, Nebraska,
Minnesota and Iowa

Ready to Talk Farming and Financing?

With over three decades of lending experience – and being directly involved in farming himself – Lynn understands the complex challenges, cycles and opportunities your farmers and agribusinesses face each season.

Bell is committed to ag lending – and that means a commitment to you and the farmers or agribusinesses you work with.

Ag participations with Bell help you give your ag customers greater stability from season to season or increase cash flow to their operations.

Bell Bank

bellbanks.com

Member FDIC
LENDER 20172