ROBERT H. CARPENTER, JR.
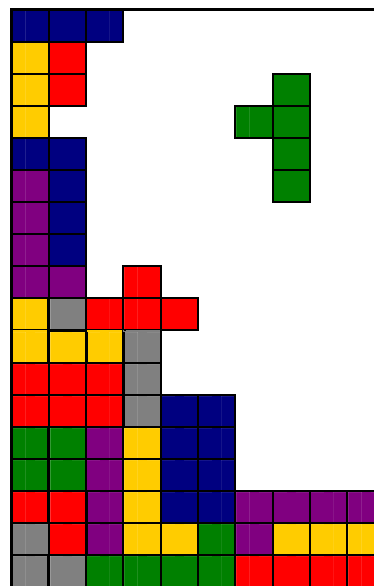
ATTORNEY AT LAW

5912 CASTLEBAR LANE

PLANO, TEXAS 75093

—

TELEPHONE 972.473.4834

—

email: Bob.Carpenter@CarpenterLaw.net

—

www.CarpenterLaw.net

July – August 2009

"The Perfect Fit for
Your Business"™

Data Loss Prevention
Can Business Failure Affect You?

Fannie Mae, Freddie Mac, Bear Stearns, Lehman Brothers, Merrill Lynch, AIG, Wachovia, GM, Chrysler – will the threat of business interruption or discontinuance end? With these recent examples of business failure, one can no longer rely upon the size or institutional reputation of any U.S. business. Bankruptcy, or at least severe government intervention, is now a real possibility for almost any company.

> *"What's good for General Motors is good for the country."*

The "cloud computing" model that is electrifying the marketplace presents significant business continuity risk, particularly for those third-party serviced businesses involved in industries that support the economic structure and contribute directly to individual financial security, like financial services. Can a vendor management program effectively eliminate or even significantly mitigate this risk? Probably not.

Cloud Computing

Today information technology (IT) is exploring the new "cloud" frontier. Cloud computing is the enticing alternative to do-it-yourself, in-house information technology solutions.[1] Simply put, "plugging into the IT cloud . . . [is] browser access to an application hosted on the Web."[2] The U.S. Government has its own working definition of "cloud computing" that is a bit more complicated:

> Cloud computing is a model for enabling convenient, on-demand network access to a shared pool
> of configurable computing resources (e.g., networks, servers, storage, applications, and services)
> that can be rapidly provisioned and released with minimal management effort or service provider

---

[1] *See* Scott Morrison, *'Cloud Computing' Makes Gains*, Wall St. J., Aug. 20, 2008, at B3B.

[2] J. Nicholas Hoover & Richard Martin, *Demystifying the Cloud*, INFORMATION WEEK, Jun. 23, 2008, at 30, *available at* http://i.cmpnet.com/informationweekreports/doc/2008/208700713.pdf [hereinafter *Demystifying the Cloud*].

interaction. This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**.[3]

Financial institutions – particularly banks, thrifts and credit unions – have been for many years familiar with this kind of outsourcing model, which they call the service bureau. Data ownership, security and portability remain at the top of the list of concerns for them and, indeed, for all who aspire to cloud computing services.

"Possession is 9/10[ths] of the Law"

Each of the service models for cloud computing contemplates that not only are software applications deployed on a vendor's infrastructure, but also that the serviced business's data is stored there.[4] Thus, while ownership of the data may be confirmed by the contractual IT services arrangement, the serviced business has no practical means to seize that data without its service provider's cooperation. And, what happens when there is a business collapse, like bankruptcy?

As businesses begin to better realize in the context of the current economic crisis the operational risk that outsourcing presents, they are struggling for an answer to how to reestablish their outsourced data processing environment when a third-party service provider fails or halts production beyond an acceptable time limit.

Vendor Management

For many years Federal banking regulators have been urging their regulated entities to establish and practice rigorous vendor management programs (VMP).[5] They have urged such VMPs because of a marketplace reality: "The ability to contract for technology services typically enables an institution to offer its customers enhanced services without the various expenses involved in owning the required technology or maintaining the human capital required to deploy and operate it."[6] This is true for any business, and the vendor management practices that banking regulators have recommended can apply to any business that outsources IT services.

While the Federal banking agencies' vendor management program recommends many contract issues that should be addressed, there are two that focus on the viability of the third-party service provider: audit and reports. An IT services contract should provide for timely conduct and delivery of the third-party service provider's audits, both financial audits and Service Auditor Reports (SAS70).

---

[3] Peter Mell & Tim Grance, Nat'l Inst. of Standards and Tech., Info. Tech. Laboratory, Draft NIST Definition of Cloud Computing (Aug. 21, 2009) [hereinafter Draft NIST Definition], http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc (lasted visited Sep. 12, 2009).

[4] *Id.* ("cloud computing" includes three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)).

[5] *See generally* FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK, OUTSOURCING TECHNOLOGY SERVICES (2004), *available at* http://www.ffiec.gov/ffiecinfobase/booklets/outsourcing/Outsourcing_Booklet.pdf [hereinafter OUTSOURCING BOOKLET], *and* FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK, SUPERVISION OF TECHNOLOGY SERVICE PROVIDERS (2003), *available at* http://www.ffiec.gov/ffiecinfobase/booklets/tsp/tech_ser_provider.pdf.

[6] OUTSOURCING BOOKLET at 1.

A serviced business should require timely and frequent financial data. An annual audit may come too late to identify a problem with the third-party servicer's business viability. Quarterly certified, un-audited financial statements can serve to give a more prompt alert to viability issues. The business should maintain careful monitoring of the scope and frequency of SAS70 Reports. An enhanced VMP might include prior review of the SAS70 audit plan and input into scope and frequency decisions to ensure that the SAS70 is in fact useful in evaluating the viability of the third-party servicer.

There is another contract issue that VMP recommendations do not address at all – the identity of the contract counterparty. For many good reasons, publicly held companies contract through subsidiaries and affiliates, and so do some privately-held companies. The identity of the true counterparty can be critical to not only rights and remedies in the event of a breach of the contract, but also in determining whether in fact there is a breach.

In this season of enhanced concern for the viability of all kinds of businesses, large and small, it is critical that the VMP of a business that outsources critical IT functions be vigorously observed. Notwithstanding a robust and exercised VMP,

> [t]here may not be sufficient advance notice of termination [of an IT services outsourcing contract], an effective contingency plan, or adequate access to [third-party service] provider personnel. In such a situation, the serviced institution is put into the position of having to find an alternate processing site with little advance notice.
>
> At this point, a serviced institution has several alternatives including:
> - Paying off the servicer's creditor(s) and hiring outside specialists to operate the center;
> - Obtaining required equipment and software for in-house processing; and
> - Transferring data files to another provider.
>
> Most options are costly and may cause harmful operating delays.[7]

Software Escrow

For years businesses that rely, either in-house or on an outsourced basis, on the technology of a third-party have resorted to the escrow of source code for that third-party's software applications. Escrow is often claimed as a means to ensure business recovery if the vendor discontinues its business or at least its support for the applications.[8]

For those that compute "in the cloud," source code may only be a part of the picture. The serviced business's data, at least in its most readily useable format, is warehoused with the third-party service provider. Delivery of this data can, of course, get hung up not only in contract disputes,[9] but also in bankruptcy and other forms of business discontinuance.

---

[7] *Id.* at 21–22.

[8] See *Secrets of the Code*, CARPENTER LAW OFFICE CLIENT NEWSLETTER (Robert H. Carpenter, Jr., Plano, Tex.), Apr. 2005, http://www.carpenterlaw.net/images/Secrets_of_the_Code__Apr._2005__2007.pdf, for a discussion of the benefits of source code escrow.

[9] *See, e.g., The Handsome Ransom*, CARPENTER LAW OFFICE CLIENT NEWSLETTER (Robert H. Carpenter, Jr., Plano, Tex.), Nov. – Dec. 2008, http://wsm.ezsitedesigner.com/share/scrapbook/43/430741/The_Handsome_Ransom__Nov._-_Dec._2008__2009.pdf .

Bankruptcy

Once a bankruptcy filing is made, the filing business is subject to the jurisdiction and oversight of a Federal bankruptcy court. The primary duty thereafter is to provide means for "the equitable treatment of creditors and financial relief for over-burdened debtors."[10]

This duty focuses first on protecting the bankruptcy estate – that is, the assets of the filing party and the proper administration of them. Property, like a serviced business's data that is warehoused on a third-party service provider's infrastructure, is not property that belongs to the bankrupt's estate.[11] But, it may take time, even days or weeks, to sort out that matter and obtain return of the data to its rightful owner. State receivership and conservatorship statutes likely provide no less of a maze that will delay release of assets from the estate of a dissolving business.[12]

Data Escrow

One obvious solution to a serviced business's obtaining its data from a failed third-party service provider is to escrow the data (and other IT elements such as application object code and technical requirements documents), like escrow for a software application's source code. The object in such an escrow is to have the ready ability to transfer data processing as quickly as possible.

NEW PRACTICE

Iron Mountain Intellectual Property Management offers such data escrow services.[13] Other vendors like InnovaSafe, Inc., a smaller Southern California vendor, also offer data escrow solutions.[14] Dynamic data vaulting – that is, data backup that can occur via the Internet or a private network connection – makes such an escrow service practicable and reliable even for a serviced business that has a recent recovery point objective (RPO) and a recovery time objective (RTO) that may be as short as 24 to 48 hours.[15]

---

[10] *In re* Depew, 115 B.R. 965, 969 (Bankr. N.D. Ind. 1989).

[11] *See* 11 U.S.C. § 541(a), (b) (2006).

[12] One consultant who provides computer services to failed businesses observes, "Company servers, once I restore them to operation, are handed over to the bankruptcy trustee's representative. The data they contain is considered to be a corporate asset and it is conveyed to the new owners in every situation I've seen." Pam Baker, *When A Company Folds, Who Guards Your Data's Privacy?*, CIO (Feb. 24, 2009), http://www.cio.com/article/print/482187 (last visited Sep. 12, 2009).

[13] Iron Mountain's product is known as the SaaSProtect Escrow Service™ and promises to protect not only data, but also the SaaS application in its object code format. Both data and object code format application are available upon demand by the serviced business so that it can promptly re-establish data processing operations at a new site. Iron Mountain, SaaSProtect Escrow Service, http://ironmountain.com/ipm/escrow/saasprotect.asp (last visited Sep. 1, 2009).

[14] *See* John J. Stulman, InnovaSafe, Inc., *Technology Escrow Agreements and Software-as-a-Service*, http://www.innovasafe.com/pdf/Technology%20Escrow%20and%20SaaS.pdf (last visited Sep. 12, 2009).

[15] RPO "describes a point in time to which data must be restored in order to be acceptable to the owner(s) of the processes supported by that data." RTO is "the latest point in time at which the business operations must resume" after a failure in the third-party service provider's IT support. Iron Mountain Incorporated, *Protect your SaaS application, your data and your business against the unexpected*,

Some businesses collect data frequently but analyze and employ it in operations on a less frequent basis. For example, the owner of renewable energy generating capacity may collect generated electricity statistics on a continuous basis, but aggregate that data only quarterly in order to document the creation of renewable energy certificates. On the other hand, a bank collects data in real time and must process it daily so that on the following business day a customer's account will accurately reflect its condition. The bank's RTO may be as short as 24 hours, and the RPO must be as of the prior business day. Data escrow becomes more reliable and available as the RTO lengthens and the RPO becomes less frequent.

There are other factors that must also be considered in implementing the data escrow solution:

- Can the escrow agent's systems handle data file updating as often as is needed?
- Is the data file size that must be escrowed so large that Internet or private network updates are problematic?
- Where will the serviced business find IT support, including the hardware and operating system platform and software installation?

These questions pointedly reflect the reality that data escrow is a "new practice" that must become a time-tested one before many are comfortable.

Data escrow also raises some of the same issues that banking regulators have raised with respect to VMPs. Data escrow, however, presents an intriguing option that businesses whose IT services are provided by third parties must explore. Conversely, third-party servicer providers must consider data escrow as a value-added service that can enhance their product offerings and instill customer confidence.[16]

---

http://www.ironmountain.com/resources/services/doc/DatasheetSaasProtectEscrowService.pdf (last visited Sep. 12, 2009).

[16] See Frank Bruno, Iron Mountain Incorporated, *How Software as a Service (SaaS) Providers Can Instill Customer Confidence,* http://www.ironmountain.com/resources/services/doc/217-com-saas-providers-can-instill-confidence.pdf (last visited Sep. 12, 2009), for a general discussion of the competitive advantage that data escrow can give a third-party service provider.