Risky Business

Choosing Information Service Providers

Robert Johnson

Organizations seeking service providers that will handle their corporate information must ensure the providers' ability to comply with a variety of regulatory requirements and industry standards for protecting it – or leave themselves open to legal liability, public embarrassment, or financial ruin if that information is compromised.

There is liability inherent in selecting any service provider, whether for landscaping the campus or cleaning the office. Mitigating such liabilities usually falls to the purchasing or contracting department or to a firm hired to handle procurement and contracting.

But, there is one type of service provider that every organization must scrutinize more closely: information-related vendors, such as records storage firms, billing services, imaging services, IT asset management firms, and data disposal contractors. Following are important criteria to evaluate when selecting a service provider in this category.

Regulatory Requirements

Data protection laws around the globe apply to selecting data-related vendors, including these U.S., Canadian, and EU regulations.

HIPAA, GLB

The grandfathers of these U.S. laws are the Health Insurance Portability and Accountability Act (HIPAA) and the Financial Services Modernization Act, which is more commonly referred to as Gramm-Leach-Bliley (GLB). The former law applies to medical information and the latter to personal financial data.

Ironically, neither is a data protection law at heart; they both deal with a wide range of issues surrounding the explosion of electronic data, and GLB concerns issues as eclectic as interstate banking and co-mingling of banking, equities, and insurance by financial institutions. Still, they both include meaningful and specific provisions on data protection.

A quote on the U.S. Department of Health and Human Services' (HHS) website speaks to an organization's due diligence burden:

> The [HIPAA] Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity.

In this context, the "covered entity" is the information owner, or the organization for whom the information is being handled. The "business associate" is the service provider.

A defense for this provision can be found in *Proposed Modifications to HIPAA under HITECH*, a 2010 HHS publication that provides early implementation advice.

> …The covered entity remains liable for the acts of its business associate agents, regardless of whether the covered entity has a compliant business associate agreement in place. This change is necessary to ensure, where the covered entity has contracted out a particular obligation under the HIPAA rules, that the covered entity remains liable for the failure of its business associate to perform that obligation on the covered entity's behalf.

Further evidence is less direct but also telling. Under the new breach notification requirements, the service provider must notify only the information owner that a breach has occurred.

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

While the service provider *could* be held responsible for the HIPAA violation that caused a breach, it is apparent the information owner would bear the liability and cost to perform the actual notification of individuals, media, and regulators, as well as bear the public embarrassment.

In the financial sector, there are a number of similar examples indicating the information owner's responsibility for validating the data-related service provider's qualifications. Within GLB, data security regulations are contained in the Safeguards Rule.

As quoted specifically from the *Federal Register* (Vol. 67, No. 100), "[T]he Safeguards Rule covers any financial institution that is handling "customer information" – i.e.,

Selection Criteria for Information Service Providers

Protect your organization by choosing information service providers that:

- Demonstrate compliance with regulatory requirements (e.g., U.S. HIPAA, Gramm-Leach-Bliley, FACTA; Canada's PIPEDA; other countries' privacy acts and directives)
- Screen potential employees for criminal backgrounds and substance abuse, and to verify previous employment and experience
- Train and verify employee training on information-handling policies and procedures
- Disclose subcontractors
- Agree to return or destroy informations at the end of the engagement

not only financial institutions that collect nonpublic personal information from their own customers."

It further explains the financial institution's responsibility for service provider selection:

> (d) Oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring your service providers by contract to implement and maintain such safeguards.

FACTA, IRS Pub 1075, PCIDSS

If HIPAA and GLB represent the first generation of meaningful data protection regulations in the United States, the Fair and Accurate Credit Transaction Act (FACTA) Final Disposal Rule represents the second generation. The FACTA Final Disposal Rule, one of 19 FACTA provisions, was enacted on June 1, 2005. It and the Red Flags Rule – which requires many organizations to implement a program that identifies the warning signs, or "red flags," that indicate possible identity theft in their daily operations – are the only two provisions dealing with data protection.

The Final Disposal Rule requires the destruction of all discarded "consumer information," as defined by the law. During the rulemaking, the U.S. Federal Trade Commission (FTC) was concerned that the new law – the first national law specifically requiring the destruction of discarded data – would lead to a proliferation of unqualified vendors attracted to a new demand for destruction services.

From the *Federal Register* (Vol. 69, No. 235), here is how the FTC addressed the specifics of performing due diligence when selecting such providers:

> After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule. In this context, due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.

So, while references to service provider selection due diligence in HIPAA and GLB apply to all data-related service providers and the FACTA Final Disposal Rule refers specifically to data destruction firms, each clearly indicates the expectation of the information owner for demonstrating care in its selection of vendors.

And it doesn't stop there. Other standards, such as Internal Revenue Service *Publication 1075* and the Payment Card Industry Data Security Standards, clearly define a similar responsibility.

Global Requirements

The responsibility is not confined to the United States. The European Data Protection Directive, Canada's Personal Information Protection and Electronic Document Act (PIPEDA), Australia's Privacy Act, and other data protection laws and guidelines either specify or refer to the same requirements.

Of course, it would be difficult to justify any other approach to selecting such service providers. Individuals are entrusting their information based on assurances given by the information owner and the regulations. It would be completely antithetical to the intent of those regulations – and illogical – not to hold those information owners responsible for demonstrating care in selecting downstream service providers who will touch the same information.

If those service providers are found obviously inadequate, no one would accept the information owner saying, "Oh well, they offered the lowest price" or "We liked their logo." Organizations finding themselves in such a position must be able to defend their decisions with documented vendor qualifications and selection criteria.

Due Diligence Requirements

The good news is the elements of information-related vendor qualifications and the selection process do not differ much across the spectrum of services that fit in that category. The major categories to be evaluated are:

- Employee screening and training
- Written policies and procedures
- Contracts/fiduciary warranties
- Certifications/third-party monitoring

Employee Screening, Training

With employee screening, two types of problems often arise: false claims and inadequate screening. Any service provider can claim it conducts employee screening, but it is critical to require proof. Periodic inspection of invoices from screening companies is a good way to get that proof without looking at each file.

Consider these additional screening-related questions for your service provider:

- Are criminal and substance abuse screening done only pre-employment or periodically?
- Are criminal background screens limited to a local police report, or are they also done at the county, state, and federal levels? (The latter is far more preferable.)
- Is past employment verified?
- Is a Social Security header check used to validate, as best as possible, past employment and residence? (This check helps identify applicants who are trying to hide something in their past.)

Employee training is also important to validate. This requires evaluating the policies and procedures that show training is required, identifying what the employee is trained to do, addressing how subcontractors are vetted, and verifying that regulatory issues, such as security breach notification and whistleblower assurances, are included.

Policies and Procedures

It is unlikely an information owner would be found non-compliant for failing to intensely evaluate a service provider's policies and procedures, and it remains to be seen how deeply the new, random HIPAA audits will probe. Regardless of the risk of non-compliance resulting from an outside audit, the absence of such policy scrutiny would certainly reflect poorly on any organization should it come to the attention of regulators – or plaintiffs' attorneys – after a data security breach involving a service provider.

The information owner must document the use of such subcontractors and its expectations for how they are vetted and contractually bound by its information-related service providers.

Contracts/Fiduciary Warranties

Vetting service provider contracts and fiduciary warranties is another important component of due diligence. While a full discussion of this issue is worthy of its own lengthy article, these are areas that are often overlooked or misunderstood:

- Disclosure on the use of subcontractors
- The destruction or return of sensitive information
- Employee awareness and acceptance of fiduciary responsibilities
- Indemnification expectations and limitations

Third-Party Involvement

Data-related vendors sometimes use subcontractors to fulfill their contractual obligations. At face value there is nothing wrong with this. A subcontractor could be used to transport materials or provide an intermediate or isolated service beyond the main operations of the primary contractor. Policymakers acknowledge this fact within the regulations.

The information owner must document the use of such subcontractors and its expectations for how they are vetted and contractually bound by its information-related service providers. It may not be reasonable to expect every subcontractor be named, depending on the scope of service and the information owner's comfort level. It is, however, only prudent to acknowledge contractually that they might be used and their expectations of these engagements.

Depending on the type of service it is providing, the subcontractor may end up in possession of the information owner's sensitive information. While this would not be an issue for a data destruction firm that is hired to make the information unrecoverable or unreadable, it would be for

A BETTER WAY

The document conversion market is growing as more companies are deciding to convert their paper to digital. More organizations are getting into the business of scanning archived records – often a natural extension of their offerings to clients.

This increased competition demands more aggressive bids that often result in tighter margins. As a result, every business is looking for ways to squeeze more waste out of the document conversion process and hopefully turn a profit. In addition, the best companies are constantly vying for fresh streams of income and new ways to add to their customer base. In order to be successful in this market, companies need to be resourceful and manage their costs more effectively than their competitors.

Service bureaus are always looking for new scanning projects across a wide range of industries. Therefore, the type of work processed constantly changes. Operations managers design jobs by calculating the most efficient way to prep documents, extract data, and determine document breaks on items that are usually difficult for the software to identify automatically.

There is a lot to consider when bidding for this work: The client's demand for superior image quality, numerous image settings, a multitude of index fields or document separator sheets, and tight service level agreements (SLAs) across a broad array of clients. Looming over all of these considerations is the question, "How much labor needs to be applied to this bid to meet those requirements and still turn a profit?"

Here's the harsh reality: Document prep labor is the most time-consuming, tedious, and often most expensive component of any scanning job.

Most service bureaus perform document prep as a separate step before scanning. Operators touch almost every page because they have to check for staples, paper clips, folded items, and post-it notes. Their goal is to create piles of paper that are clean enough to be auto-fed on their scanners. As needed, pieces are unfolded, flattened, repaired, taped onto larger sheets, and placed into auto-feed ready stacks.

Documents with meaningful color require special handling. Other pieces require photocopying, such as the front of every folder that contains a label with vital information, or that piece that just will not scan without tearing. Some sections demand heavy prep such as taping credit card receipts to full sheets of paper and center-aligning class registration cards on the pile so that they can be auto-fed. Moreover, document separator / index sheets need to be added, tracked, and then manually outsorted for re-use.

But what if there was a better way?

What if you could prep and scan as fast as or faster than your current prep-only rate?

There is a better way to handle the wide range of media described above and reduce or eliminate much of the document prep. It is simply not necessary to constantly tape small or odd-shaped items to full sheets, photocopy folders and fragile pieces, or manually flatten sheets before scanning.

What if you could eliminate most separator sheets, or your need to re-use them? There is a better way to handle document separation. Most separator sheets can be eliminated by using the physical characteristics of a piece or by deploying electronic intervention, based on the requirements of each project, in line with the scanning process. Generic separator sheets are easily re-used by automatically outsorting them.

What if you could improve image quality, adjust image capture settings, and decrease re-scans by optimizing exception items during scanning? There is a better way. By defining page types via software, operators can apply different settings on each image (i.e."snippets"), and capture them quickly and easily.

There is a better way, and we'll always help you find it.

OPEX Corporation knows efficiency. Over the years, we have developed innovative products that address the root causes of the workflow issues our customers face. We strive to understand and solve those issues by designing the best products to meet those challenges rather than simply addressing the symptoms.

This market-driven approach, coupled with unparalleled service and excellent ROI, form the backbone of our long-term customer relationships. We continuously look for ways we can team with third-party integrators and software vendors to provide our clients with complete solutions.

As a result of these efforts, OPEX offers various prep-reducing scanners, including the DS2200 and AS7200 models, that provide you with attractive business opportunities and the flexibility to:

- Identify and aggressively bid projects with more challenging paper, or more recurring-revenue transactional work (we have thousands of scanners in the field capturing transactional documents);
- Decrease prep headcount, or increase output using the same number of people; and
- Increase your profit margin.

OPEX CORPORATION

Learn more at www.opex.com/harshreality

a scanning firm, a records storage firm, and a host of other service providers.

While no current data protection regulation requires the service provider to indemnify the information owner for loss of any type, the information owner has every right to ask for it.

Contract Requirements

Contracts with information service providers should address several issues, as follows.

Disposition of Information

Contracts should specifically detail the fate of the information that resides with the subcontractor when it is no longer needed. In fact, this provision could easily be justified when dealing with any vendor that will possess the organization's client, employee, or competitive data.

The options are to have the information destroyed, which brings up the issue of subcontractor requirements, or to be returned. Either way, expectations and agreements on its fate must be detailed. Typically, if they are mentioned, the requirements are so loosely worded as to be of little value should the information owner need to hold the vendor accountable in the future.

Employee Training

According to the eighth annual *Ponemon Global Cost of a Data Breach* study, employee error was the leading cause of data breaches in 2012. This finding applies to service providers to the same extent as the information owners. While policies and training are critical in mitigating such risks, it is also important that employees accept that they are exposed to sensitive data. They must acknowledge their responsibility to protect it at all times and make management aware of potential security breaches.

Recent amendments to HIPAA set a precedent for holding individual employees legally responsible for breaches they knowingly cause. No employee of a service provider should ever be able to seek refuge in the fact that he was unaware of his responsibilities or the nature of the information he was entrusted with. Contractually, service providers should be required to obtain such fiduciary employee acknowledgements.

Liability, Indemnification

The final service provider contract issue to discuss is fraught with misconceptions: vendor liability and indemnification. While no current data protection regulation requires the service provider to indemnify the information owner for loss of any type, the information owner has every right to ask for it.

A common professional indemnification mistake made by information owners is to require their vendors to accept such liability but then fail to confirm if they have enough coverage. A second common mistake is requiring unreasonable or unrecoverable indemnification limits.

It will surprise no one that professional liability is becoming a staple of data-related vendor contracts, but what is surprising is there's often no requirement to *confirm* the service provider has coverage. Sometimes general liability coverage is mistakenly accepted, and other times the professional liability policy supporting vendors is an off-the-shelf policy so riddled with exclusions that it would be useless in protecting the vendor or the information owner.

These mistakes are often exacerbated by service contracts that require the vendor to accept unlimited liability. There is no such thing as professional liability coverage with unspecified limits. Essentially, the information owner is asking the service provider to put its entire enterprise on the line.

Because aggressive restrictions and irrational fiscal requirements are typically tossed out by the courts, it's best to agree on a reasonable indemnification limit that's based on the mutual risks and the amount of business transacted. No information owner is likely to collect on a professional liability claim beyond what the vendor is covered for, and even then only if the policy is appropriately vetted.

Trust, but Verify

Most of us are trustworthy and are eager to be trusting as well. Unfortunately, when it comes to service providers' claims and promises, we can be too eager to trust. There will always be some vendors who have credible-looking websites, who know the jargon and the hot buttons, and who offer temptingly low prices. That's why regulatory compliance requires, and common sense dictates, that information owners make reasonable attempts to look deeper and to test the service providers' assertions. **END**

Robert (Bob) Johnson is the chief executive officer for the National Association for Information Destruction. He can be reached at rjohnson@naidonline.org. *See his bio on page 47.*