ASSESSING THE RISK OF DATA LOSS OR BREACH

Whether you're evaluating a proposed vendor relationship or your entire organization, the key is understanding your data.

BY MATT BARR

When sensitive data is to be transmitted to a vendor, regulations, regulatory guidance, and best practices dictate that you should have a written contract in place. That contract is an opportunity to fairly assign

the risk of data loss or breach between you and the vendor. As such, these contracts represent opportunities—and potential pitfalls.

You're not going to negotiate a one-sided risk allocation into every vendor agreement. You're not going to *negotiate* every vendor agreement. Some vendor arrangements don't present enough risk to justify redlining the vendor's boilerplate contract. So how do you prioritize? And for priority vendors, how do you determine the right contract language to allocate the risk of data loss or breach?

First, you have to evaluate the potential consequences of a failure under an agreement. To do that, you have to understand what data you'll be sending to the vendor. One tool that can be useful for these purposes is a Privacy Impact Assessment (PIA).

You're not going to negotiate a **one-sided risk allocation into every** vendor agreement. You're not going to **negotiate every vendor agreement.**

Consider performing a Privacy Impact Assessment

A PIA is a concept introduced in the federal E-Government Act of 2002. It requires that agencies of the federal government conduct an analysis of how personally identifiable information is collected, stored, protected, shared and managed, in new and existing systems. The assessment must be "commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information." An agreement with a vendor processing Social Security numbers would require a much more thorough assessment than the end user license agreement for Microsoft Word.

The Department of Homeland Security's guidance on PIA prep says that "the purpose of a PIA is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire life cycle of a system. This involves making certain that privacy protections are built into the system from the start, not after the fact when they can be far more costly or could affect the viability of the project." Closer to "home" for mortgage lenders and vendors, the Department of Housing and Urban Development says that a PIA

>> Identifies the type of personally identifiable information in the system (including any ability to combine multiple identifying elements on an individual);

>> Identifies who has access to that information (whether full access or limited access rights); and

>> Describes the administrative controls that ensure that only information that is necessary and relevant … is included.

HUD's PIA guide and form is available at http://www.hud.gov/offices/cio/privacy/pia/piaquestionnaire.doc.

The first step is to identify the type of information vendors will have access to. What is the nature and sensitivity of the data? What is its source? Is the data or the sharing of the data subject to a law or regulation, or contractual provisions with another vendor, or an internal policy?

Next, determine how the data will travel to the vendor. Does the system require authentication? Is the vendor accessing and pulling the information from a server of yours? Who will be able to access it?

Why is the data being transferred? To what use will the vendor put the data? Is the vendor's performance critical to your business?

What controls do you already have in place to help safeguard the data? What controls do the vendors have? Are they adequate?

Cataloguing data flows and vendor relationships in this way will help you gauge the level of risk of data loss or breach. What level of risk are you willing to assume? Can the risk be mitigated with additional administrative or technical controls, or by appropriate contract language?

In addition to the HUD guide, there are many other guides and examples of federal government privacy audits. DHS's guide is here: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_march_v5.pdf. The Department of the Interior has a guide here, https://www.doi.gov/sites/doi.gov/files/migrated/ocio/information_assurance/privacy/upload/DOI-PIA-Guide-09-30-2014.pdf, and the State Department has dozens of examples of PIAs from 2000-09 here: http://2001-2009.state.gov/m/a/ips/c24223.htm.

Some contract terms to include

The contract is one step in the vendor engagement process, after diligence and selection. The same regulations that require written contracts require thorough diligence, so you should know enough about your vendor and its systems to perform a PIA. But there shouldn't be any hesitation to ask for information you may be missing from

a potential vendor. You should know whether they wipe computers clean when an employee leaves. You should know if their facilities are access controlled.

In the contracting phase, anticipate the next step in the process, management. For higher-risk exchanges, insist on the right to audit your vendor during the term of the contract if it should become necessary. If you've collected documentation from the vendor respecting its security measures, require notice of any change, or an annual or other regular provision of updated documents.

Some other terms to be included in a good contract with a vendor include: the vendor's obligations upon data loss or breach, especially including immediate notice to you; a promise not to introduce any viruses or malware, if the vendor has access to your systems; and an agreement that the vendor will dispose of sensitive data as soon as practical after the exchange.

Legacy contracts

The costs associated with data breach are closer to the front of your mind now than they were three years ago. What do you do about contracts you entered into three years ago? Five years ago?

It's crucial to perform some level of diligence on existing vendor relationships. Vendors who do business in mortgage or settlement services fields are likely to be ready with any documentation you might have requested if you were contracting with them now. Regardless of what the contract says, simply asking for documentation is likely to yield positive results.

If you encounter delay or resistance, you might find a hook in the legacy contract that provides for audits of financials: you might be able to obtain security and other information under that clause as well. There may be a general promise that the vendor will "cooperate," and that might give you a leg to stand on. When all else fails, know the contract's term and termination rights. Often a contract term will automatically renew unless one party notifies the other of its intent not to renew. There may be a separate right of termination for convenience. These give you leverage to obtain any diligence documentation you need, and they also represent opportunities to amend the contract to better protect you and your data.

Some organizations find that an enterprise-wide privacy assessment would be beneficial. There are several existing **frameworks you** can draw from.

Enterprise-wide data security assessments

Some organizations find that an enterprise-wide privacy assessment would be beneficial. There are several existing frameworks you can draw from to plan such an endeavor.

The National Institute of Standards and Technology (NIST) is a federal government agency which has implemented the president's executive order requiring the development of a voluntary framework for "reducing cyber risks to critical infrastructure." Background, information and an Excel spreadsheet of the framework are available at http://www.nist.gov/cyberframework/.

The International Organization for Standardization (confusingly acronymed ISO) has developed ISO/IEC 27018:2014 which establishes objectives, controls, and guidelines for implementing measures to protect sensitive information in a cloud computing environment. Details can be found at http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498. ISO is a worldwide organization that promotes proprietary, industrial, and commercial standards.

And the Cloud Security Alliance, a non-profit organization that promotes security best practices, has available Security Guidance for Critical Areas of Focus in Cloud Computing at https://cloudsecurityalliance.org/group/security-guidance/.

Whether you're evaluating a proposed vendor relationship or your entire organization, the key is understanding your data. You can't effectively mitigate risk without knowing what you've got to lose. ❖

About The Author

Matt Barr is General Counsel and Compliance for Mercury Network, LLC. He is a former Communications Director and Associate General Counsel for a real estate technology company and Managing Editor for a publisher of settlement services market intelligence. A graduate of Chicago-Kent College of Law/Illinois Institute of Technology, he is admitted to practice in Illinois. He is local to the Atlanta area, where he lives with his wife and daughters.