

Sharing Sensitive Data with Vendors? Three Critical Steps to Reducing Risk

Most companies—large and small—have embraced outsourcing services as a cost-saving strategy. Outsourcing not only reduces overhead, it can provide competitive advantages by improving quality or time to market. Financial institutions often depend on key service providers to operate more effectively and better serve customers. Key functions that service providers commonly deliver include credit scoring, check printing, credit card issuance, home banking, statement processing and financial auditing.

However, because of this growing trend, an unprecedented amount of sensitive data, including personal customer and employee information, is being shared with outside vendors. And there lies the rub.

Companies that outsource and share personal data assume that their vendors will protect the privacy of that information. But with more stringent regulations governing the privacy and security of personal data and harsher penalties for those who don't, that leap of faith could result in an irreparable reputation and financial loss.

It is imperative that organizations have an effective program in place to select and manage its key vendors. Here are some practical vendor management suggestions that will keep you from operating on blind faith and will help you protect your company's sensitive data and reputation:

Step 1 - Categorize vendors based on their role and the type of information they have

Start by dividing your list of vendors into three distinct groups:

- Low: These vendors have minimal impact on your operations and it would be easy to replace them.
- Moderate: It would be inconvenient to find an alternate source for the service(s) that these vendors provide. Without them, you may incur mild disruption, e.g., marketing and public relations firms.
- High: These vendors either have access to sensitive information (e.g., personal employee or client information, intellectual property) or provide services that are critical to operations. Examples in this category include payroll and statement processors, credit bureaus, legal and accounting firms, and outsourced IT service providers.

Step 2 - Document vendor controls appropriate for each category

Since each type of vendor plays a different role—and has access to a different level of information—your vendor controls should vary by category. The higher the category, the more information you should request and the more stringent the controls.

- Low: Since these vendors have little impact on daily operations, simply identify alternate sources for the services these vendors provide.
- Moderate: In addition to identifying alternate vendors, you should include a confidentiality and privacy clause regarding safeguarding company information in these vendors' contracts.

- High: For vendors that you rank in the “high” category, be sure they have sufficient physical, technical and administrative controls in place to ensure the security, confidentiality, integrity and proper disposal of information.

One way to do this is to use a checklist to assess each vendor before hiring them and then conduct an annual review. Below are recommendations to include in your checklist for critical vendors.

General Information

- Company background and history
- Qualifications: Include information that makes your vendor the ideal choice for the service they provide, i.e., size, experience, certifications, number of other customers similar to your company.
- References: Contact references and inquire about the length and scope of their relationship as well as the quality of service.
- Financial condition: Include audited information about the current and past two years. Privately held vendors may be reticent to share this information, but most will cooperate by providing a current balance sheet and income statement under non-disclosure.

Administrative Controls

- Hiring and employment practices: Have your vendors describe screening and monitoring controls for current and prospective employees. Internal security breaches are the most common and destructive to an organization, so you should verify that your critical vendors conduct criminal background and drug testing on all employees.
- Insurance: Beyond general liability and workman’s compensation, be sure that your vendor has adequate professional liability insurance (errors and omissions). This provides you a safeguard that if a material breach requires litigation, the vendor can offer restitution.
- Dual control procedures and segregation of duties for vendor employees who have access to confidential information.
- Employees and subcontractors: Find out if the work will be performed by employees or subcontractors. If work is completed by subcontractors, understand how the vendor controls are enforced with the subcontractors and whether or not insurance covers subcontracted work.

Physical Controls

Where practical, schedule an on-site visit to understand where your data resides at the vendor and review the facility and access safeguards, including:

- Physical access controls (e.g., card access, biometrics)
- Surveillance and monitoring systems
- Policy and restrictions at vendor location to allow only authorized personnel in areas that contain sensitive information.



Technical Controls

- Perimeter security: Determine if the service provider has sufficient prevention and monitoring safeguards against an external data breach, including remote access controls, identify authentication and intrusion prevention and detection.
- Electronic data handling: Encryption of sensitive data should occur at all times, whether it is stored on laptops and USB devices, in transit via email or stored on networks or systems to which unauthorized individuals may have access.
- Data backup, retention, off-site storage and destruction policies.
- Business continuity and disaster recovery: If a vendor is critical to the uptime of your business operation, conduct a detailed review of its disaster recovery/business continuity plan. Review its DR testing results and offer to participate in DR test exercises to validate service continuity.
- Security risk assessment/audit findings and response to them as well as the auditor's qualifications.

Step 3 – Manage the program

Ensure that the appropriate vendor controls are evaluated and documented for all new business relationships that your organization is considering and annually review the controls for existing vendors.

As uncomfortable as it may seem to ask this information from your vendors, those that serve financial institutions should have responses already prepared. If they do not, it may be red flag.

Remember that you can delegate authority, but not ultimate responsibility for the security and protection of sensitive information. Organizations that outsource must come to grips with how to effectively deal with this issue.

By: Jeff Olejnik, President
Assurity River Group, Inc.
4500 Park Glen Road, Ste. 120
Minneapolis, MN 55416
952-230-6488
jolejnik@assurityriver.com
www.assurityriver.com