Managing data security and privacy risk of third-party vendors

Submitted by: Norm Parkerson, Executive Director
Grant Thornton, LLP
Norm.Parkerson@us.gt.com
Tel. 404.475.0065

The use of third-party vendors for key business functions is here to stay. Routine sharing of critical information assets with cloud providers, consultants, business process outsourcers, third-party transaction processors, and others has become standard business practice. Yet inevitably, as data moves out of the organization's protected infrastructure into that of a third-party vendor, a certain degree of control is relinquished. Organizations must remain vigilant and engaged in assessing risks to their data, even though it resides at a vendor location.

How can organizations protect their information assets while entrusting them to third parties? Moreover, how can they ensure compliance with a changing landscape of security and privacy regulations, many of which differ by industry, state and country?

At issue is the fact that many third-party vendors, which store, process or transmit personally identifiable information/electronic protected health information (PII/ePHI) and intellectual property (IP) on behalf of users, may not have appropriate controls in place to secure the data, manage risk, or enable users to meet their privacy and security obligations. Even when an organization outsources data management and processing activities, regulations require that it retain responsibility for ensuring that its data is protected.

The onus is on user organizations to select vendors with an appropriate approach to risk management. In order to do so, user organizations need to carefully vet vendors prior to selection, and then actively monitor their security and privacy control environments throughout the life of the contract. Monitoring third-party data security and privacy risk requires a strong and effective process for ongoing vendor management that starts long before the contract is even signed.

What is at risk?
Data breaches resulting from the use of third-party vendors are growing and have become exceedingly expensive to manage. In fact, according to a recent study by the Ponemon Institute, 39 percent of data breaches in 2010 involved third-party organizations such as outsourcers, contractors, consultants and business partners.[1]

These breaches tend to be very expensive to resolve. For instance, the cost of such third-party breaches rose by $85 from 2009 to 2010, reaching $302 per data record — an increase of 39

[1] Ponemon Institute, LLC. 2010 Annual Study: U.S. Cost of a Data Breach, March 2011.

percent. Breach costs overall are still rising: In 2010, they reached $214 per compromised record and averaged $7.2 million per data breach event, up from $6.75 million in 2009.[2] In the event of a breach, companies may also face fines, civil penalties and legal repercussions.

Theft of IP is another growing threat, with yearly losses estimated to be in the billions of dollars. According to the FBI, the rise of digital technologies and Internet file-sharing networks provide the means by which trade secrets, proprietary products, plans and schematics may be stolen. Much of the theft takes place outside of the United States, where laws can be lax and more difficult to enforce.

Security and compliance

Most organizations must comply with rules and regulations that address the handling of information assets, such as the Payment Card Industry Data Security Standard, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act, and others. Many of these rules and regulations apply not only to user organizations that collect the information, but increasingly to third-party vendors that provide outsourced services.

There may be other rules and regulations to consider, depending on where your organization does business. For example, a growing number of states (e.g., Massachusetts, California, Texas, Michigan) now have their own privacy and security laws, and many other states are considering them. European Union countries, along with other international governments, also have specific data privacy and security laws.

Interestingly, a Ponemon Institute study published in April 2011 reveals a difference of opinion between cloud providers and users about who is primarily responsible for security in the cloud.[3] Nearly seven in 10 (69%) third-party vendors see users of their cloud service as being primarily responsible for their own data security, while only 35 percent of users perceive themselves to be mostly responsible.

This apparent confusion about who is responsible for data security may lead users to become complacent about securing their data, since they may assume that their third-party vendor has strong security and privacy controls in place when, in fact, that vendor may not. Simply put, users need to take a more proactive approach toward ensuring that their data is adequately protected.

What can you do to protect yourself?

Organizations that are considering the use of third-party services need to perform appropriate due diligence when selecting a vendor, and data security, privacy and compliance considerations should be top of mind.

During the due diligence process, organizations should ask a number of key questions about data security and privacy considerations:

---

[2] Ibid.

[3] Ponemon Institute, LLC. Security of Cloud Computing Providers Study, April 2011.

- Data protection—How will data be protected? What controls does the vendor have in place for intrusion detection, perimeter security, physical security, timely application of security patches, and data leak prevention, among other safety measures?
- Data access—Who will have access to our data, and how can we confirm this? Does the vendor have the right security controls to protect our data? How will the provider ensure that others (e.g., those whose data resides on the same server as ours) are not able to view our data?
- Data security—Does the vendor have policies and procedures in place to adequately detect, prevent and mitigate incidences of identity theft that may occur? Have there been any incidences of identity theft experienced by the third-party vendor within the last two years? Does the vendor scan employee email and company social media platforms for potential breaches of customer data? How are incidents and breaches reported? Will we receive notification if a breach to our data occurs?
- Disaster recovery and business continuity planning—Does the third party have a disaster recovery plan? In the event of a disaster, how will the vendor protect our information assets? Can we get our data back if the vendor goes out of business?

Attestation reports—if vendors have them—can offer a useful look at a vendor's security and privacy control environment. The AICPA's Service Organization Control(SM) (SOC) reports — specifically its SOC 2(SM) and SOC 3(SM) reports — provide service auditors and service organizations with reporting options that address controls related to security, availability, processing integrity, confidentiality and privacy. These reports help vendors demonstrate the strength of their controls to current and would-be customers; however, it is up to prospective users to evaluate these reports with care. Users must carefully read and thoroughly understand their content, evaluate any findings in the context of the outsourcer's services that they are considering, and determine how weaknesses in their own user control environment may affect the overall control environment.

Develop ongoing processes for evaluation and monitoring

Ultimately, organizations should put in place a consistent process to assess, monitor and manage risks related to vendor operations. (See "Establishing an effective vendor management program" below.)

Even though many organizations execute vendor agreements with service providers, too few of them build protections into the contract to support an ongoing program to monitor and assess vendor control risks. For example, organizations may insist on a right-to-audit provision that gives them the authority to periodically audit and monitor controls on-site, whether or not a SOC 2 or SOC 3 reporting process is in place. If the vendor is not willing to allow the provision — particularly if a SOC report or similar attestation report is not available — the user organization should consider its options.

Conclusion

The use of third-party vendors for key business functions has become standard business practice, but the security control environments of vendors vary greatly. It is essential for organizations to be vigilant in assessing risks to their data, even when it resides at a vendor location.

Records show that vendor data breaches can result in fines, civil penalties and brand erosion for users. In the event of a data breach, anticipated cost efficiencies and other benefits can evaporate as a result of costly breaches and enforcement actions. Intellectual property may be similarly at risk, which can cost the organization dearly in terms of lost investment.

Organizations considering the use of third-party vendors need to ask themselves, "Once we share our information assets with third-party vendors, will we still be in compliance?" Those that answer affirmatively must be prepared to spend time vetting their vendors and carefully monitoring their security and privacy control environments over time.

Establishing an effective vendor management program

If your organization does not currently have a vendor management process, putting one in place can feel like going from zero to 60 miles per hour in an instant. We generally recommend that our clients approach vendor management as a three-stage process: first, implement a "quick-wins" stage; second, establish a standardized, streamlined vendor management process; and third, enhance the vendor management process with an ongoing program of vendor risk management.

1. Initiate a quick-wins process.
   For many companies, a vendor inventory either does not exist or is out of date. Service level agreements, likewise, may not be kept up to date. As a result, the first step is to identify the vendor population by determining which vendors have access to confidential or sensitive data and how much PII/ePHI is collected, used or disclosed by those vendors.

   If a SOC 2 or SOC 3 report is not available, conduct a quick privacy and security risk assessment against the inventoried vendors by using surveys, questionnaires or on-site visits. Questionnaires should inquire about a range of controls related to financial stability, adoption and enforcement of robust security and privacy controls, performance, and other crucial topics. Identify the control gaps and risk-rank gaps for each vendor. Based on these risk assessment results, flag high-risk vendors.

   Once high-risk vendors have been identified, focus on getting them to mitigate the most immediate risks. There are a number of ways to do so, such as reducing the sharing of PII/ePHI and IP, implementing data protection solutions, digital rights management, or other actions to minimize data security and compliance risks.

2. Develop a streamlined vendor management process.
   Going forward, it is a good idea to develop and implement a standard process for assessing and monitoring changes to vendors' data security and privacy risk environments, in addition to looking at the traditional set of vendor management criteria such as financial stability, ethics, manufacturing/service quality, order fulfillment and invoice accuracy. The results of vendor questionnaires, on-site inspections and attestations may be compared from year to year in order to identify potential degradation in the security control environment.

3. Establish an ongoing vendor risk management approach.
   When outsourcing or co-sourcing high-risk business functions such as processing of

health claims or tracking account holder transactions, consider establishing strategic vendor relationships, as well as adopting a centralized approach to managing the vendor population and associated risks. Often internal audit takes the responsibility for managing and assessing vendor risks. Through this process, many organizations can pare down the number of vendors with which they conduct business. In so doing, organizations may be able to reduce the amount of vendor risk and at the same time, negotiate special discounts to decrease vendor costs.