IS YOUR BUSINESS THOROUGHLY EVALUATING AND MONITORING ITS VENDORS AND SUBSERVICE ORGANIZATIONS?

Your Guide to Securing Outsourced Services as a Third-Party Service Provider

DiSanto Priest & Co.
Certified Public Accountants

It seems like hardly a day goes by where we don't hear about organizations large and small experiencing a data security breach. As a result, more and more businesses who have outsourced some portion of their operations to third-party service providers are requesting that these third-party service organizations provide a System and Organization Controls (SOC) report on their system.

A SOC report, specifically a type 2 report, is an internal report that describes the controls in place at a company to safeguard customer data and it speaks to how effectively those controls are operating. A SOC 2 report can cover one or more of the following trust services categories: Security, Confidentiality, Availability, Processing Integrity or Privacy. In fact, more and more businesses are willing to terminate a relationship with a third-party service provider in favor of a competitor who has a SOC report available. If a business is thinking about obtaining a SOC report in order to stay competitive and meet your customer needs, there is one area, in particular, that has become a major focus of SOC 2 examination engagements - the monitoring of vendors and subservice organizations.

So many services can be outsourced today to help businesses save time, as well as money, and focus company resources on what they do best. However, a company can't simply hire a vendor or subservice organization and focus solely on operations handled internally. Businesses are responsible for ensuring that sensitive information shared with vendors and subservice organizations is properly handled at all times. Since sensitive data is outside of a company's direct control when it is in the hands of these third-parties, there is always a risk that sensitive data will be mishandled. This risk needs to be actively managed and monitored.

Prior to hiring a vendor or subservice organization, companies must perform their due diligence to ensure that sensitive data will be handled in a manner that lines up with the security and confidentiality policies of their business. This can be accomplished in a variety of ways including:

- Doing research to find out as much as possible about the vendor or subservice organization, such as what their reputation is like, how long they have been in business, recent security breaches that have been experienced, the cause of any breaches and how they have been handled.
- Have information technology staff and those in charge of security perform an on-site visit of the prospective vendor's facilities to better understand its operations and walk through security-related controls. This is also a good time to assess the reputation of senior management and how serious they are about security and confidentiality. If the tone at the top is good, the chances are very good that others within the organization also take security and confidentiality seriously.
- Make detailed inquiries of personnel at the vendor or subservice organization who are responsible for physical and logical data security as well as confidentiality. Making unplanned inquiries of employees who are not in leadership positions can also help in determining understanding of security and confidentiality matters within the service organization in relation to discussing policies and procedures in practice every day to keep sensitive data secure and confidential.
- Make inquiries about the staffing procedures utilized at the vendor or subservice organization for all types of personnel (including temporary and seasonal help): whether background and credit checks are performed, whether confidentiality and non-disclosure agreements are required and the types and frequency of staff training provided. Companies should also ask about the vendor's use of third-party contractors and controls in place to ensure that any third-party contractors also adhere to security and confidentiality policies and procedures.

- Make inquiries of current customers who utilize the services provided by the vendor or subservice organization and ask about what their experience has been with respect to the security and confidentiality of sensitive information handled at the third-party service organization.
- Obtain copies of policies and procedures surrounding data security and confidentiality and read through the provided documentation. Make inquiries as needed based on what is documented.
- Obtain a copy of the draft service level agreement and review it in detail to understand the roles and responsibilities of all parties to the contract, particularly as it relates to security and confidentiality. Have an attorney review the agreement to ensure that nothing important is left out and make changes to the agreement as deemed necessary before it is finalized and signed by all parties.
- Obtain a copy of the vendor or subservice organization's most recent System and Organization Controls (SOC) reports, if available. These reports are detailed, very informative, and should be read in detail. SOC 2 reports will typically include a user entity control considerations section which includes a list of controls that are expected to be in place at the company using the services provided by the vendor or subservice organization. This is a company's way of letting the vendor or subservice organization know that it can't simply rely on them and that the responsibility for keeping sensitive data secure and confidential is shared. These controls should be reviewed and implemented at both companies if a decision is made to utilize the vendor or subservice organization.

Many times, businesses will perform their due diligence when they are considering utilizing a vendor or subservice organization for the first time and then once they start working with the provider, no ongoing evaluation and monitoring occurs. This is a very serious mistake. Providers who handle a company's sensitive data must be evaluated and monitored throughout the business relationship since things change constantly. With controls, technology, procedures and personnel changing constantly, many factors can put sensitive data at risk, which is why monitoring is so critical. Procedures, including the ones discussed above, should be done on a routine basis by designated qualified individuals who are charged with the responsibility of evaluating and monitoring vendors and subservice organizations. The actual frequency of the monitoring will depend on a company's assessment of risk. The vendors and subservice organizations that a company deems higher risk should be evaluated and monitored more frequently than lower risk ones. The point is, due diligence can't just be performed at the beginning of the business relationship.

It is also important to document the due diligence that is performed for each vendor or subservice organization both at the beginning of the business relationship as well as throughout the relationship. If it's not documented, it's as though it never happened. A company should take credit for what is done and document that work, including what it saw, what it read and who it spoke with, so that the business can demonstrate that due diligence was performed and the evaluation and monitoring of these providers is taken seriously.

There needs to be an understanding that there is a shared responsibility when it comes to keeping sensitive data secure and confidential. A business cannot rely completely on the vendors and subservice organizations and have a hands-off approach to the monitoring of the provider.

Many data breaches have been caused due to vulnerabilities that existed at these types of providers. Hackers are always looking for vulnerabilities. A business could have the best security and confidentiality policies and procedures in place but if its vendors and subservice organizations do not, that could be just the vulnerability hackers will find and use to access the company's valuable sensitive data.

So, one simply can't ignore how sensitive data is handled by these providers. While a company can outsource the service itself, it can't outsource the responsibility for safeguarding sensitive data. The stakes are high and data security breaches can be costly in so many ways. A company could be subject to penalties and its reputation could be negatively impacted, resulting in lost business. Business interruption and legal costs could also be incurred. Insurance premiums would also likely increase. Money may also be spent on damage control such as enrolling people in credit monitoring services. The list goes on, so the prevention of a data security breach is key and the proper evaluation and monitoring of vendors and subservice organizations is an important piece that can't be overlooked. So, be sure that policies and procedures are in place at your company to evaluate and monitor the vendors and subservice organizations that you work with.

If your customers haven't asked your service organization about a SOC report yet, the chances are quite good that they will be very soon, given that cybersecurity threats are on the rise. As you begin to prepare for either your first or next SOC report examination engagement, it is important to keep the above hot topic in mind. DiSanto, Priest & Co. performs many SOC examination engagements and would be happy to discuss this topic as well as other SOC related topics with you.

About Disanto, Priest & Co.
Disanto, Priest & Co. is a full service public accounting firm headquartered in Warwick, Rhode Island with expertise in assisting companies in evaluating their current and planned third party assurance needs, like those described above. Give us a call if you need assistance as we would be glad to talk with you about your needs.

Headquarters
117 Metro Center Boulevard
Suite 3000
Warwick, Rhode Island 02886
Telephone 401.921.2000
Facsimile 401.921.2010
www.disantopriest.com