

► **Managing Third Party Risk**

Executive Insight Series
by Richard E. Mackey, Jr.

© Copyright 2009 SystemExperts Corporation. All rights reserved.

► Managing Third Party Risk

Outsourcing services is a fact of life in today's business environment. However, while it may allow you to focus on what you do well and be more efficient, it can also bring both operational and compliance risk. In this article, Richard Mackey discusses the importance of understanding the risk associated with third parties and how to manage this risk. The article provides guidance on how to recognize third party operational and compliance risk, structure a provider management program to ensure that risk is assessed, understood, monitored, and managed appropriately.

Operational and Compliance Risk

When an organization shares information with another organization, the risk of that information being compromised is increased. In other words, the organization has increased its operational risk. In addition, if the organization sharing the data has not taken the necessary steps to ensure that the information is protected appropriately according to the requirements of applicable regulations and contracts, the organization has increased its compliance risk.

Many regulations including HIPAA, GLB, and the Massachusetts Identity Theft law require organizations to review their service providers' security practices and ensure that the information will be protected adequately. PCI, a contract rather than a regulation or statute, also requires merchants and service providers to ensure that service providers are compliant with the PCI Data Security Standard in the functions they provide. Given these regulatory requirements, it is imperative that organizations have an organized approach to evaluating the type of risk a particular service represents, the level of risk of both the service and the provider, and the adequacy of the security practices of provider in mitigating the risk of compromise and meeting compliance requirements.

What Is at Risk?

The first step in understanding risk is understanding exactly what information you are sharing. This may seem like a non-issue, but in many cases, organizations share information in bulk without considering the individual data elements. Lack of data analysis can lead to unnecessary risk of exposure, increasing both the risk of compromise and the risk of being found non-compliant with contracts and regulations. Assuming you have analyzed the information to be shared, you can ask the following questions:

- Does the information include personal identifying information, health care data, or credit card data?
- Is the information competitively sensitive for you or a business associate?
- What aspects of the information are sensitive? Is the confidentiality, integrity, and/or availability of the information critical in the context of the service that you or your business associate provides?
- Does the data fall under requirements and restrictions specified by an existing contract?
- Is the data regulated by an agency or government statute?

If we look at a hypothetical example, we can see how understanding the information can help you to measure the risks and understand requirements.

EXAMPLE:

St. Fictitious Hospital shares patient records including name, social security number, address, and treatment data with a service provider HealthService, Inc. that allows doctors to view and approve treatment records for submission of claims to insurance companies. The hospital recognizes that as a covered entity under HIPAA it is required to protect the confidentiality, integrity, and availability of Electronic Protected Health Information (EPHI). In the case of insurance claim

► Managing Third Party Risk

submission, the confidentiality and integrity of the records are more important than the immediate availability. Consequently, the hospital needs to ensure that HealthService's controls that affect those aspects of the information are effective.

The hospital also recognizes that there is a chance that some patient is a resident of Massachusetts, therefore the hospital will assume that its controls and the controls of the service provider must meet the requirements of the Massachusetts Identity Theft Law. Both laws require the hospital to assess the adequacy of security practices of business associates to which they entrust this protected information. In HIPAA parlance, the "covered entity" (the hospital) must ensure that all the administrative and technical controls are implemented by the business associate (HealthService), including appropriate encryption on transmission on unprotected networks, strict access controls on the data, and disciplined vulnerability management.

The hospital will then need to go through an organized process of evaluating the business associate's practices and requiring improvements wherever they fall short. If possible, the hospital should also look to anonymize or eliminate any data that is not necessary to be shared. This practice can mitigate risk substantially.

Assessing Partners

As we have said above, all relationships bring some degree of operational and compliance risk. However, not all relationships are created equal. Two of the most critical elements in managing partner risk are consistently assessing the inherent risk associated with the shared information or relationship and assessing the residual risk of dealing with a particular partner in the context of its implemented controls.

The first element, assessing inherent risk, requires you to look at the data shared and the effect a compromise would have on your business and state of compliance. You assess the relationship assuming no controls. This is a worst case analysis of the damage you would suffer in the event of a breach.

This analysis allows you to rank, by risk, the service providers you deal with based on the criticality of the information you share and the service they provide. Based on this analysis, you can then determine the depth of assessment you need to conduct to assure that your risk is mitigated appropriately.

The inherent risk analysis allows you to establish tiers of service providers, high risk, medium risk, and low risk providers. This ranking will allow you to devise appropriate assessment methods that are commensurate with the risk. Low risk partners may not require an assessment at all or may be required to only sign agreements accepting responsibility for whatever risk exists.

Medium risk providers may be required to answer a security practices questionnaire and only be investigated in more detail if their answers raised concerns. High risk providers might be required to submit a third party audit report or undergo a detailed assessment by your internal security group.

This tiered system not only allows you to closely inspect your highest risk partners, it helps you to mitigate both operational and compliance risk. The initial assessment in a relationship lays the groundwork for future periodic reviews that are required by many contracts and regulations (and simply make sense).

The Ongoing Partner Management Program

When you have established a relationship with a partner, your risk management responsibility has only begun. As time goes by, the risk associated with a given service change substantially as a result of changes to your business, your partner's business, your technology, the threat environment, or new regulatory or contractual requirements. Consequently, the risk associated with every service relationship needs to be re-evaluated periodically to both recognize and adapt to these changes.

The risk-based tier system can help maintain your partner risk management program by helping to set

▶ Managing Third Party Risk

the frequency of your periodic risk assessments and partner practice evaluations. The higher the risk associated with a given partner the more frequent your risk and practice assessments should be.

When planning your risk assessments, keep in mind that you need to understand whether changes in your partner's environment have an impact on your risk. For example, has your partner gone through a merger or acquisition? Has your partner's technical environment changed in important ways? Is your partner aware of regulatory requirements and changes that have occurred in the time since the previous review?

These questions can only be answered by communicating with your partners. This is a critical component of any partner management program.

Conclusion

Virtually all companies engage third party service providers. We know that these relationships bring with them certain types of risk. It is critical that we understand these risks and manage them, not only at the initiation of the relationship, but throughout its existence. A well-run, consistent, and methodical risk-based partner management program should be part of all organizations' security and compliance programs.