Managing Your Risk: Assessing Service Providers' Cybersecurity Practices

Developing a risk management program for service providers

By Steve Weil

The Challenge: How secure is your third-party service provider?

No organization wants to be the victim of a cyber-attack. In late 2015, an attacker gained unauthorized access to two cloud service providers used by Gyft, an online gift card retailer. The attacker was able to download personal information about at least 83,000 Gyft users that was stored with the cloud service providers.

Gyft, of course, is not alone. Dozens of retailers have had cybersecurity breaches, and retail isn't the only hot spot. Cybersecurity breaches occur across all industries. Organizations that use service providers often give them access to sensitive data and information systems. All it takes is one service provider with poor cybersecurity practices to cause a cybersecurity breach.

If that happens, the damage could extend to your business, your employees, and your customers.

So how can you assess and manage service provider risk?

Point B's Approach

It's no longer enough to focus just on your organization's data and information systems. You also need to know about the cybersecurity practices of your service providers. We're not alone in saying so—executive leadership and boards are increasingly asking organizations to perform due diligence on service providers.

The good news is that you can reduce the risk by using an effective service provider risk management program. At Point B, we've identified the four major components that any good service provider risk management program should include:

- ✓ Leadership support for mandatory risk assessment of service providers
- ✓ Right-to-audit cybersecurity practices clause in service providers' contracts
- ✓ A short questionnaire to quickly assess the cybersecurity practices of service providers
- ✓ A risk scoring tool to prioritize risks

Details on each of the components follow.

Copyright © 2016 Point B. All rights reserved.

Leadership support for risk assessment

When you put a service provider risk management program in place, support from senior management is a must. Leadership needs to make it clear that risk management is a priority—and then they need to put their money where their mouth is by making resources and budget available for it.

In addition, it's important to create an organization-wide policy that calls for the annual assessment of your service providers. Include all current and prospective providers who process, transmit or store your organization's sensitive data or who access your information systems.

Right-to-audit clause

Start including a right-to-audit clause in contracts with your service providers. That gives you the right to assess your service provider's cybersecurity practices as they relate to your business. When you include that clause in a contract, it sets the tone with your service providers, letting them know that you take cybersecurity seriously. It also gives them incentive to respond to your questions.

It's also a good idea to review your existing contracts with service providers. Older contracts can be modified to include the right-to-audit clause.

Cybersecurity practices questionnaire

Requiring your provider to complete a questionnaire is a quick and effective way to find out if their cybersecurity practices have major gaps—like not encrypting stored sensitive data. The questionnaire also gives you the chance to identify areas where you might need to follow up or dig more deeply.

When you're developing your questionnaire, base it on best practices for cybersecurity—the Center for Internet Security's Critical Security Controls is a good option. Try to keep the questionnaire short, preferably under 50 questions. That increases the chances that your provider will get it back to you within a reasonable amount of time. Focus on the cybersecurity controls that are most relevant to service providers, like encryption of stored data, system patching, privilege management and security incident detection & response.

More sophisticated service providers may respond to your questions by giving you a third-party assessment, such as an SSAE16 report. Such assessments are performed by third party experts and their reports are often full of useful information.

Risk-scoring tool

Develop a risk-scoring tool so that you can quantify the level of risk (e.g. high, medium, low) you have with each provider, based on their cybersecurity practices. Base the tool on the factors that are most important and relevant to your organization: how much sensitive information is stored at a service provider, for example, or whether the provider will have access to your information systems.

For current service providers, focus your mitigation efforts on those the tool identifies as high risk.

For prospective service providers found to be high or medium risk, ask the tough question: is the service they provide worth the risk?

The Bottom Line

Service providers increasingly pose a risk to organizations; such risk must be regularly assessed and managed. Doing so can reduce that risk to a reasonable level and help satisfy your leadership and board of directors that you've done everything possible to safeguard your organization from a cybersecurity breach.

Creating a service provider risk management program requires some upfront time and effort, but in the long run, it's an excellent way for organizations to reduce their overall risk.

About Point B
Point B is a management consulting firm that helps clients develop strategic insights and translate them into impact. Point B's Organizational Change Management program helps clients drive sustainable change through deep understanding of their business culture, processes, and goals.

 Copyright © 2016 Point B. All rights reserved.