Are You Managing the Risk for Your Call Center?

By David Richert, CPA, CITP, CIA, CISA, CQA

Call centers are utilized to a great extent in the media and entertainment industry. Companies focused on information, communication and entertainment delivery, like cable, digital and other high-speed service providers, rely heavily on call centers to serve as the front line of their companies.

Call centers manage phone calls, emails and letters for technical assistance, requesting answers about bills or types of service, or a variety of other inquiries. This frontline support can be a key source of goodwill or frustration.

As businesses grow, management often makes economic and strategic decisions to contract with a third party and outsource their call centers. Call centers can reduce support costs by reducing payroll expenses and redundant work, by easing the means to meet regulatory requirements and by streamlining processes.

Key business objectives of a call center can include revenue generation (sales, collections, and retention), efficiency (cost effective operations) and customer satisfaction (strong brand image).

Further, some types of contact are governed by laws around data privacy, how quickly inbound calls are answered, and outbound telemarketing calls (“do-not-call” lists).

Controls to Ensure Privacy

One of the more daunting challenges facing companies relying on call centers is consumer privacy and the protection of personally identifiable information.

In many cases, access to your customer accounts can be gained with little more than these six pieces of information:

- Social Security number/account number;
- Mother’s maiden name; date of birth; name; address; and phone number.

Given the confidential nature of this information, it’s critical for you to ask what assurance your call center provider has in place for effective controls. Where is the information stored? How is it accessed? And, how is it preserved only within the call center?

Availability of the call center to service your customers is another key support function; you may have a service level agreement (SLA), but how successful is your call center vendor in meeting this benchmark?

With call centers occupying such a critical role in your business, management should seek some form of assurance around the performance of this outsourced activity.

Approaches to Risk

As companies increase the volume of activity outsourced to third parties, there’s an increased need for assessing the risk related to those services. There are several approaches to take to manage this risk:

- Include necessary parameters in the service level agreements with the third party.
- Perform a risk assessment on the service provider.
- Rely on a report on selected risks at the service provider.

Regardless of the approach taken, the following are the typical risks to focus on:

- Security — The outsourced system is protected against unauthorized physical or logical access.
- Availability — The outsourced system is available as agreed. This can include technology outage risk (data, circuit, software).
- Processing Integrity — The outsourced system processing is complete, accurate, timely, and authorized. This can include quality of staffing.
- Confidentiality — Information designated as confidential is managed as such.
- Privacy — Personally identifiable information that is collected, retained, disclosed and/or destroyed is managed.
- Regulatory — This can include FTC and FCC rules and/or Fair Debt Collections Practices Act.

SOC 2 Reports

With regard to reports, recently released information from the American Institute of CPAs describes a new Service Organization Controls Report (SOC 2) as one designed “to meet the needs of a broad range of users that need to understand internal control at a service organization as it relates to security, availability, processing integrity, confidentiality and privacy.”

A SOC 2 report provides valuable information users need to assess and address the risks associated with an outsourced service. These reports can play an important role in organizational oversight, vendor management programs, internal corporate governance and risk management processes, and regulatory oversight.

Managing the reputational and regulatory risks of a call center service provider is key and will provide you added comfort over the confidentially and availability related to your customer information.

David Richert, CPA, is a manager with RubinBrown LLP in St. Louis specializing in IT controls and financial services. He was an adjunct professor of accounting at St. Louis Community College and is a member of the MSCPA Information Technology Committee. David can be reached at david.richert@rubinbrown.com.