Managing Risks in an Increasingly Automated Customer Contact Center

By Thomas Phelps IV, Michael Thomas and Leonard Kiing
Managing Risks in an Increasingly Automated Customer Contact Center

As enterprises implement customer relationship management (CRM) strategies to focus on customer service, retention and acquisition, customer contact centers (call centers) have increased in strategic importance. Forward-looking executives have leveraged these contact centers with enabling technologies to provide additional services to customers. Customer account inquiries and other transactions that previously involved a live agent can now be efficiently accomplished by Web or telephone self-service applications.

However, the complexity of these innovative technologies, coupled with the automation of customer interactions, significantly increases operational and financial risk. The growing complexity of contact center systems, networks and self-service applications increases the probability of failures resulting in customer service problems and reduced contact center performance and availability. Because of the growing reliance on contact centers, senior executives should be aware of the risks and resulting impact of contact center failures and inefficiencies even over short periods of times. An effective risk mitigation program requires that the operational integrity of contact centers be closely monitored through a rigorous program of automated testing.

Recent studies have shown that the primary reason customers choose to stop doing business with a particular company is poor customer service. Companies competing for the attention of and loyalty from today’s consumer must continue to improve the quality of the customer’s experience with the contact center. Today, the customer’s attention span is shorter than ever. Customers have more choices, easier access to information, and higher expectations of service and availability.
A steady, lifetime customer revenue stream could hinge upon a single interaction that quickly changes a customer’s perception and satisfaction with the business. The era of e-business decreases customer’s switching costs to a level where a competitor’s products are just a click away. The moment a contact center or Web site fails to deliver expected information or slows in the transaction process, the customer looks elsewhere.

Customer relationship management (CRM) strategies and the Internet have spawned the evolution of traditional agent-intensive inbound call centers into highly automated, technology-enabled customer contact centers. Call center interactions that previously required agent intervention are now fully automated. Self-service Web applications, Interactive Voice Response (IVR) and Computer Telephony Integration (CTI) systems enable customers to connect to a contact center, access their account and complete a transaction without speaking with an agent.
Web-enabled content and transactions now provide self-service capabilities for customers who want to research, compare and purchase products or services over the Internet. Driven in part to meet customers’ expectations for multimedia channels of interaction and to facilitate e-business transactions, companies are implementing new capabilities — Voice over Internet Protocol (VoIP), chat and email — into their legacy call centers.

Enabling self-service transactions provides economic benefits — it decreases agent costs and allows the most common transactions to be performed quickly and efficiently. However, automation increases business risks by hiding problems customers may have accessing or using automated applications. Given the volume of calls in self-service applications, many organizations will not know if calls are being blocked, dropped, misrouted, or queued for an unacceptable period — until it’s too late. Organizations may not know until hours or days later that customers received busy signals or were routed incorrectly, or that the wrong prompts or applications were playing.

Without supervisors and agents involved in the customer interaction with the contact center, the company may not have immediate visibility to operational issues and dissatisfied customers. Self-service applications remove the human control that provided companies with assurance over the quality of the customer’s experience.

As senior executives leverage the latest e-business, CRM and telephony technologies to gain a competitive advantage, they should also be aware of the financial and operational risks that could impact the business. Integrating contact center systems, networks and self-service applications to automate transactions and provide additional services are important contact center enhancements. However, they also increase the probability of contact center operational failures and undiscovered customer service problems. A failure with one multimedia access channel could cause a chain reaction of failures with other multimedia access channels. For example, a recent brokerage Web site outage caused customers to inundate the company’s contact center with phone calls. The customers who got through the busy signals experienced wait times exceeding ten minutes.
Service disruptions caused by contact center system failures or other operational issues could significantly impact revenue. An audit of one high-tech manufacturing company revealed that each hour of interrupted telephone service could cost the company $1 million in lost revenue. In some industries with low switching costs such as financial services or the travel industry, highly publicized, negative events dilute brand equity and cause customer churn. When adding up marketing and sales costs to acquire profitable new customers, the total cost of a single lost call or failed Web transaction could be considerable.

Major operational risks in contact center operations include:

- Call handling errors or Web site errors,
- Network performance/availability issues,
- Implementation issues from inadequate application testing, and
- Outsourcing issues.

CALL CENTER OVERVIEW

A quick overview of how calls are routed through a traditional call center will facilitate an understanding of operational risks. Traditional call centers include Automatic Call Distributors (ACD), Interactive Voice Response (IVR) systems and Computer Telephony Integration (CTI) systems.
The Automatic Call Distributor (ACD) processes each call and routes it to the Interactive Voice Response (IVR) system, or queues it for distribution to an agent. The IVR prompts callers with a series of menu choices. Working in tandem with the IVR and ACD, the Computer Telephony Integration (CTI) system accesses databases for caller account information and automatically processes the call without agent intervention. When callers “zero out” for human intervention, the CTI system provides caller account information to the agent in the form of “screen pops.”
IVR CALL FLOWS

Based on digits selected by the caller, IVRs route calls through pre-programmed call flows using conditional branching. As additional menus are added, the conditional branches become increasingly complex. For example, a typical banking customer might navigate through at least four menus and spend two minutes on a call. If each menu has six options, calls could be routed through any one of the 1296 unique call flows that involves CTI and other telephony systems.

ELAPSED TIME

PRESS
1 for ATM locator
2 to open an account
3 for account information
0 for a service rep

20 Seconds

Please enter social security no.
Please enter password

55 Seconds

PRESS
1 for savings information
2 for checking information
3 for line of credit information

65 Seconds

PRESS
1 for balance information
2 for checks paid and withdrawals
3 for deposits

80 Seconds

Listen to balance information

120 Seconds

CALL TERMINATED
COMMON CALL HANDLING ERRORS

The following major types of errors illustrate the gamut of potential failures in automated telephony systems.

Blocked Calls
A common call handling error is blocked calls. Busy or out-of-order telephone trunks block calls when customers try to dial an inbound toll-free number. Unless trunks are actively monitored, managers may not be aware that calls cannot reach their contact centers.

Dropped Calls
Calls can also be accidentally dropped due to system failures once when the call reaches the contact center. A financial services customer may spend several minutes navigating four IVR menus for an automated banking system. After selecting the correct digits to hear her checking account balance, a customer may hear silence and have the call dropped because the CTI or IVR application failed to connect to the mainframe database.

Misdirected Calls
A similar situation occurs when calls are misdirected. A customer may call an airline reservation hotline and navigate IVR menus to reach a domestic travel agent. Because of programming errors in the IVR call flow, the customer is connected to the automated flight departures and arrivals menu and is not allowed to “zero out” to reach an agent.

Database Access
A common call handling error that causes network congestion and customers to disconnect their calls is lengthy access times to account information. Fast access to mainframe databases is critical in CTI and IVR applications. Customers encountering longer than average wait times for balance inquiry information or other automated transactions may “zero out” to talk with an agent.
Most organizations have business continuity or disaster recovery plans that address contact center availability in mission critical operations. However, these same organizations may not have adequate controls to monitor availability and quickly identify slow or failed applications and systems.

Traditional system and network monitoring tools used in network operations centers cannot find many of the problems that can potentially impact today's contact center. For example, system and network monitoring tools cannot identify busy trunks. They cannot identify if the wrong prompts are playing or if calls are being disconnected. They have trouble finding application slowdowns or response time problems that negatively impact customer service levels.

In addition, contact center systems are increasingly distributed across different geographical regions. Without appropriate monitoring controls, it may take hours to recognize and isolate IVR or other system and application failures resulting in thousands of lost calls.

Many organizations monitor each system, network connection, or application independently without consideration for monitoring the total end-to-end performance of a customer call. A performance degradation of any one system or network link could impact the performance of the entire customer transaction but may not be sufficient, in itself, to trigger an alarm with traditional system and network monitoring tools. For example, organizations that purchase extra trunk capacity for an investor hotline in anticipation of a spike in call volume, but run a CTI application on an aging computer with 32 MBs of memory, will have serious customer service problems. As enterprises add additional services by implementing new telephony systems and applications, the risk of creating additional points of failure increases geometrically.
IMPLEMENTATION ISSUES

Inefficient, inadequate or nonexistent testing of CRM, e-business and CTI/IVR applications is the root cause of most implementation issues. For example, many companies implement IVR changes without comprehensively testing call routing features. When testing is performed, companies typically perform inadequate manual tests. Only a few people are employed to interact with the IVR and identify programming errors or network routing issues based on the voice prompt responses. Since these manual tests do not check all possible call flows or simulate real world conditions, applications and systems may fail from incorrect configurations or inadequate engineering.

OUTSOURCING ISSUES

Some companies outsource either part or all of their contact center operations to control costs, manage seasonal variances in call volume, or focus on core competencies. Although service level agreements typically include key performance indicators and remedies, they may not provide senior executives with assurance that the metrics reported by the outsource service provider truly reflect the customer’s actual service experience.

MANAGING CONTACT CENTER RISKS

To minimize business risks, senior executives should embed comprehensive risk processes into their contact center business activities and drive risk management responsibilities down to all organizational layers. A risk assessment will help align the objectives, risks and control processes within the organization. Questions to ask include:

- What are the business objectives?
- How do contact center technology initiatives support these objectives?
- What are the risks that could influence the achievement of these objectives?
- What current controls exist to monitor and mitigate these risks?
By aligning risks with business objectives and identifying appropriate control processes, senior executives take a proactive approach to risk management instead of reacting to unmanaged risk when it becomes a problem. An example of a reactive approach is when organizations, without further review, automatically increase trunk capacity after hearing customer complaints about busy signals.

Organizations that embrace a proactive approach build controls and risk management processes into their activities. For example, a travel agency’s objective is to reduce the amount of time agents spend on the phone and save money on network and agent costs. The company develops a new application that automatically retrieves a business customer’s travel profile based on the originating telephone number — shaving approximately 15 seconds from each call. A key risk to increasing agent productivity is that the agents do not understand how to use the new application, or the application does not work correctly. The controls would be to test the application prior to deployment, monitor the end-to-end network performance and implement a training program for all agents.

A comprehensive quality assurance program proactively mitigates financial and operational risks associated with automated self-service applications. A typical program involves customer satisfaction surveys, pro-active, real-time monitoring controls and change management controls. Customer satisfaction surveys would allow a customer to exit out of an automated call flow to provide direct feedback on the call to an agent. Monitoring controls assure senior executives that the systems, applications and the network are functional and meeting customers’ quality of service expectations.
Examples of change management controls include:

- Software is tested to detect programming errors,
- Software is tested to ensure it operates as intended in a live environment,
- Modifications made subsequent to initial testing are retested,
- Systems and applications are backed up prior to installation,
- Implementations are authorized and signed-off by management,
- Application features are documented, and
- Users are trained on the software.

The weakest area for many companies in implementing a quality assurance program is change management controls. Many applications such as IVRs are not tested before they are implemented. Other applications are tested manually by a few employees, which does not provide assurance that the application will function properly when processing thousands of calls or that the tests are performed consistently. The solution to change management testing control weaknesses is to use automated testing tools. Automated testing using automated call generators and other sophisticated tools allow complex call flows to be completely tested in a simulated production environment prior to actual deployment in the contact center.

Change management controls should involve the following three application tests using automated test tools:

- Functional testing of new applications,
- Load and stress testing of call center components, and
- Regression testing of software before implementation into a production environment.
Functional tests ensure the features and functions of a new application are working as designed. Load and stress tests determine the specific conditions where the software will fail and identifies system, network, and application bottlenecks. Automated testing tools provide features for varying the load on the application. An application that supports 48 simultaneous calls may not scale up to support 96 simultaneous calls. Regression tests occur prior to deployment and ensure that recent software changes do not contain any bugs.

With the increasing complexity and number of contact center applications, manual testing performed on individual systems may not identify critical problems that would surface in a production environment. In-service testing, or monitoring, creates an effective monitoring control by simulating the customer’s experience with an automated self-service application. It tests the end-to-end call flow by placing test calls that duplicate the real-world actions of customers.

An automated test tool that is connected to telephone lines calls an inbound contact center, or connects to a Web server, and interacts with the contact center like a real customer. The test tool can be programmed to run every fifteen minutes on a 24/7 schedule. It provides vital information on call handling or transaction errors such as network and system delays, call misrouting and dropped calls. In the case of a system or network failure, in-service testing can quickly pinpoint the source of the failure.
SUMMARY

An increasing number of customer interactions with the contact center are now automated by self-service applications, including Web sessions and Interactive Voice Response (IVR) transactions. Companies may be exposed to operational and financial risks because of the complexity of innovative contact center technologies, the growing number of potential failure points, and the reduced number of agent interactions that previously provided assurance over the customer’s experience.

To mitigate these business risks, senior executives should embed comprehensive risk management processes into their contact center business activities and identify appropriate controls. Critical to this is a comprehensive quality assurance program that leverages automated testing tools to provide strong controls over change management, and monitoring of contact center systems and applications; in particular, customer self-service systems and applications.

The author, Thomas Phelps IV, is a manager in the Technology Practice of PricewaterhouseCoopers (PwC). Along with call center and cost management client service responsibilities, he is the West region lead for telecommunications security. Thomas is a frequent presenter on telecom security issues to IT audit groups such as ISACA. He has developed and instructed several PricewaterhouseCoopers’ telecom classes. Thomas can be reached at (213) 236-3577 and via email at Thomas.Phelps@us.pwcglobal.com.

Leonard Kiing and Michael Thomas, CCNA, CPA, contributed to this white paper. Leonard is a manager in PwC’s Technology Practice and is the West region call center lead. He can be reached at (415) 498-7590 or via email at Leonard.Kiing@us.pwcglobal.com. Mike is an associate in PwC’s Technology Practice. He has extensive experience in the assessment and remediation of enterprise telecom cost management, PBX security and network technologies and processes.