"The more you rely on outsourcers to handle your contacts, the more you need to be on top of it." p.2

THE SECRETS TO TECHNOLOGY SUCCESS

LESSONS LEARNED FROM THE TRENCHES.

By Lori Bocklund, Strategic Contact Inc.

CONTACT CENTER PIPELINE
SMART INSIGHTS AND PRACTICAL ADVICE FOR THE CONTACT CENTER
www.contactcenterpipeline.com blog.contactcenterpipeline.com

By Lori Bocklund
Strategic Contact Inc.

@StratContact

TOO OFTEN TODAY, THE PURSUIT OF TECHNOLOGY IS DRIVEN BY SPEED AND CONSTRAINED BY RESOURCES—IN-HOUSE AND ON THE VENDOR SIDE. Experience shows this to be a bad combination and certainly not a recipe for success. This article will look at key lessons from technology projects with these all-too-common challenges with the hope that they give you a leg up on implementation, testing, monitoring and support on your next endeavor.

Implementation and Testing

Getting implementation right takes time, well-structured plans and commitment from the contact center, IT, vendors and/or their partners. Input from all parties that touch the technology, directly or indirectly, gets you off on the right foot. Ongoing engagement in the project ensures proper representation on both the technical (IT) and functional (users) fronts. The first flag goes up if IT views the contact center technology project (whether premise or cloud-based) as secondary, offering only partial engagement. For best results, they must remain key and committed project team members throughout.

As you build the plan, ensure enough time to test, revise and test again; ideally, plan for three complete rounds. Rare is the project that gets everything right the first time, whether due to solution complexity, diverse sites or groups, multiple vendors, or numerous systems and integrations. Vendors do not typically plan for multiple rounds because they want to show you a good timeline (and admit it, you pressure them for it!) and move onto the next project. You need to be the realist in overall timeline planning and communicate up and down the chain of command. You may also need to be the advocate to avoid changing multiple variables and systems at once—testing becomes more difficult and implementation success less likely.

Be clear on vendor role through the Statement of Work (SOW) and what they will do for testing, which is usually limited. You will likely have greater testing (and test plan) responsibility, so plan accordingly. Most projects do not plan for comprehensive testing. The vendor will do some basic component testing, and may have network testing as a prerequisite to ensure that the environment is ready for the new solution. Beyond that, you need System Integration Testing (SIT) and User Acceptance Testing (UAT) at a minimum—the former requiring significant involvement from your IT, the latter from your CC team members. UAT success depends on a detailed plan (that is not easy to create) and thorough execution, so make sure you know who is doing what and commit the time and resources the plan demands.

Add business continuity/disaster recovery testing for automatic failover procedures where possible. Unlike the past, systems do fail and do need to switch over to the backup instance. Add stress/load testing where appropriate, which is more likely for a premise solution and if you have major peaks. Our *Pipeline* Tech Line article, "Contact Center Technology Testing" (July 2012), provides much more detail on planning for and executing adequate testing.

Keep in mind that, if you set unrealistic expectations and shortcut these tests, you risk failure of implementation or failure to deliver on time—or both! You never want to be cutting over an untested system or one with known issues just to meet a timeline.

As consultants, we are often the ones bringing reality to schedules and pointing out testing can't be done in one week, or that the network connectivity needs a 90-day lead time at a minimum, and could be six months. Another key issue we often have to tackle is committing enough staff for UAT and doing a thorough job of testing paths, documenting outcomes, and fixing things—then testing again. And it's not just call flows that need testing—it's email routing and handling, supervisor tools (reports, scorecards, administration, etc.), quality monitoring

The more you rely on outsourcers (who are increasingly using cloud-based systems) to handle your contacts, the more you need to be on top of it. You cannot take a hands-off approach.

and more. Another differentiator we see is that the best-run projects plan resource time commitment for weeks, not days, after cutover. If possible, plan to have the vendor come back a couple months after implementation to provide refresher training and optimize use. It requires more time and money, but it can enhance value and performance of the system.

When the solution involves multiple vendors, they may have differing views of the best architecture and approach. If not engaged up front, vendors may try to redesign after the fact to meet their needs. We have seen vendors trying to change the design at or after cutover. Establish the fundamental architecture in advance and socialize it with all involved—Carrier (see the sidebar on page 5 for more about this critical player), PBX, ACD, Outsourcer, and any others such as CRM or performance tool vendors. Engage them in the plans for testing and cutover activities as well. Ensure that procedures are in place for agreement (and signoff if possible) by all players—i.e., we all agree this is what we're implementing, how we're going to do it, who is doing what.

Keep in mind, these best practices don't just apply to new implementations; they can improve changes to architecture, configuration, major upgrades and more.

Monitoring

Monitoring is perhaps the most neglected or overlooked key to success, yet it is increasingly important with current multivendor, complex, cloud/hosted solutions.

Your first line of defense is exploring the monitoring the vendor provides through your due diligence process. Explore what and how they monitor, what information their Network Operations Center (NOC) receives, how the NOC is staffed (24x7?), what processes they use when seeing an issue, what visibility you will have to system health, etc. Your second line of defense is filling gaps with your own monitoring or third-party services. For example, you could use a call-testing service (dial through call flows and show results), or have people check key numbers and flows each day to ensure routing is working, especially for flows with menus and messages that change or have many conditional paths. Set up test accounts for self-service and test them periodically. One little related annoyance we see that compounds all this monitoring is poor number management, which can lead to issues or perceived ones on numbers that nobody has been keeping track of or are not sure how they are used, by whom (or even if they are used), and where they route. Put good processes in place to assign, track and monitor all numbers and email addresses coming into your center, and reinforce them with all groups impacted, including IT and marketing.

Keep in mind that these keys to success apply whether your solution is premise- or cloud-based. The approach will differ on who is monitoring what and the levels of accountability, which are covered in your next line of defense, good Service Level Agreements (SLAs). And remember that SLAs are only useful if there is someone holding the vendor accountable to them. Most require you to formally claim remediation: They will not automatically say, "We missed, here is the credit we owe you." Also keep in mind that SLAs aren't enough on their own. Back to the testing and monitoring, you aren't just looking for remediation, you're looking for a solid system that stays up and working and if it has a problem, someone is responding and resolving it in a timely manner (more on support below).

The more you rely on outsourcers (who are increasingly using cloud-based systems) to handle your contacts, the more you need to be on top of it. You cannot take a hands-off approach. The same things apply to testing, monitoring and SLAs. We see companies using outsourcers, not just for "butts in seats," but also for cloud solutions for their in-house staff. This approach can be great for reducing IT's burden, but it puts more eggs in one basket, so you better make sure it's a really good basket!

Support

They just don't make 'em like they used to, and they just don't support 'em like they used to either. It's hard to get good help (with deep knowledge, discipline, communication skills, etc.), have enough help, and have good processes in place for issue identification (including proactive monitoring per

above), resolution, root- cause analysis, etc. In spite of the popularity of ITIL for vendors and in-house IT, and best intentions for stellar responsiveness, we see support being a pain point in many cases. (Information Technology Infrastructure Library, ITIL, provides a set of best practices processes for technology support and delivery to effectively meet business user needs.)

Define what it will take to support the new systems as part of your implementation planning. Consider vendor and IT roles and responsibilities. Avoid finger-pointing and gaps in responsibilities by establishing clear accountabilities with the vendors and defining any new processes and procedures for IT. Start with assignment of the Tier 1 role and define the steps and contact points for initiating a trouble ticket, acknowledging receipt, performing initial analysis, and engaging the right resources to resolve the issue (including Tier 2).

Unfortunately, in spite of the best planning efforts, we've seen a variety of support issues including lack of responsiveness, not understanding severity and impact, no follow through, and accountability issues. Sometimes a quick response to a request falls flat with a dearth of analysis, or "paralysis by analysis" and no one taking charge and pursuing what is really happening and how to fix it. "We'll work on it and let you know" is sometimes the response—albeit an unacceptable one. What can appear as stall tactics puts the onus on the customer—e.g., get us more examples, see if it's still happening, we don't see it so you will need to provide us with X—and deflects the situation temporarily, but again, unsatisfactorily. When multiple vendors are involved in providing a single solution (e.g., ACD plus Network Carrier), one vendor (more likely for cloud solution) or IT (more likely for premise solution) must take overall responsibility for the entire solution and lead the troubleshooting and resolution process.

Support success again starts with clarity on who is doing what (with the key vendor, or their subs, and your in-house responsibilities), which is partially covered in your due diligence in selecting the vendor, but also in SOWs and SLAs, and in putting processes in place. You need to drive accountability in ticket follow through and living up to SLAs. Understand the vendor's processes and use them well—submitting tickets, classifying them (you can usually declare the level yourself based on your view of the impact), getting an acknowledgement, getting updates with committed time frames. Follow through on resolution and closure as well as Root Cause Analysis (RCA) because the vendor may not do that to a great enough degree to meet your needs, especially if you need to answer to leadership, have the full story on what happened, and feel confident it won't happen again. RCA should also involve solid documentation in case the problem reoccurs, such as a new release that doesn't contain the fix.

While it's not always an option, and may not be the best option for a number of reasons, fewer vendors minimizes complexity in your overall solution and therefore its support. Everyone likes the "one neck to choke" concept. Every integration between different vendors is a point where responsibility is shared. Shared responsibility can mean no responsibility.

The Road to Success

The keys to success are at odds with some of today's common project drivers. You want to go fast, without enough resources, but in reality you need to take time and commit resources (yours and the vendors'), and probably phase in functionality. From the due diligence to cutover through ongoing management of your system, active involvement and proactive engagement from a wide-ranging team will serve you well.

LORI BOCKLUND is Founder and President of Strategic Contact.

lori@strategiccontact.com

TOP LESSONS LEARNED FOR TECHNOLOGY SUCCESS

IMPLEMENTATION AND TESTING	MONITORING	SUPPORT
Build realistic timelines that provide adequate testing, including resolution and retesting	Ensure tools and/or services are in place to monitor system health and, ideally, call flows	Explore support processes, resources and SLAs in depth during vendor due diligence
Conduct thorough testing with SIT and UAT at a minimum	Structure processes (and assign resources, if done internally) for routine monitoring, analysis of results and changes, if needed	Follow vendor (or internal IT) trouble ticket processes whenever there is an issue
Involve all players—CC, IT, all vendors—in implementation, including agreement on design and architecture, and testing	Don't assume cloud, managed services or outsourcers means you have no monitoring responsibility	Manage vendor/IT on resolution (outcome and time), Root Cause Analysis (RCA), and Service Level Agreements (SLAs)

THE CARRIER CHALLENGE

Technology implementations are very dependent on the "carrier" or vendor that provides network connectivity and services (MPLS, ISDN, SIP, etc.). Increasingly, this vendor is not a direct contract but is engaged through a cloud vendor. Whether your IT is contracting the carrier or another vendor is, there may be multiple carriers involved to cover the geography and/or upstream from your carrier. One vendor may have multiple subcontracts. The resulting lack of comprehensive monitoring and support can lead to no accountability or ability to pinpoint an issue and get it resolved.

Because the buyer can lack direct control and SLA accountability (and the vendor you have an SLA with may have a clause not holding them accountable for carrier issues), you need clarity, whether it is with the cloud vendor or your IT, on who holds agreements with whom, and what those agreements provide. Ask questions about monitoring visibility—for you, the cloud vendor, or managed services vendor—testing resources, support resources and processes, SLAs, etc.

The carrier challenge highlights the importance of testing as defined in SOWs and executed during implementation end-to-end, with involvement of all vendors including carriers. And as highlighted elsewhere in this article, allow time for additional testing after things are fixed, if things change, you make additions, etc.

The carrier challenge also highlights the importance of SLAs, and the reality of the compromises you may face. You need to at least know what your risks are even if you can't get the ideal SLA commitment. Then, you also need strong backup plans that address what you will do if the carrier has an issue and it is not resolved quickly.

CONNECT WITH PIPELINE


@SusanHash • @CCPipeline


youtube.com/ccPipeline


linkd.in/17M5rKM

About Contact Center Pipeline

Contact Center Pipeline is a monthly instructional journal focused on driving business success through effective contact center direction and decisions. Each issue contains informative articles, case studies, best practices, research and coverage of trends that impact the customer experience. Our writers and contributors are well-known industry experts with a unique understanding of how to optimize resources and maximize the value the organization provides to its customers.

To learn more, visit: www.contactcenterpipeline.com


Download complete issues, articles, white papers, and more at http://bit.ly/14bq01k

PIPELINE PUBLISHING GROUP, INC. | PO Box 3467, Annapolis, MD 21403 • (443) 909-6951 • info@contactcenterpipeline.com

Copyright ©2015, Pipeline Publishing Group, Inc. *All rights reserved.*
Reproduction of Contact Center Pipeline in whole or in part is expressly prohibited without prior written permission from the publisher.