TECH LINE
by LORI BOCKLUND

CONTACT CENTER PIPELINE
AUGUST 2017

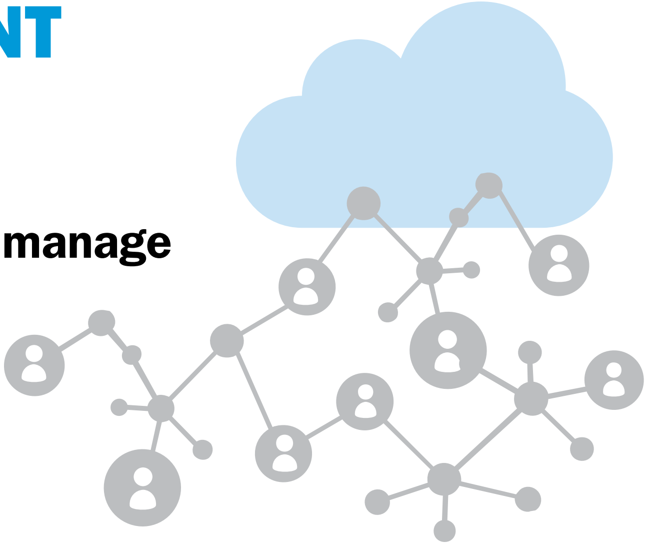
BUILDING A RESILIENT CONTACT CENTER

"A few minutes outage can leave the center playing catch up on service level (and perhaps, customer satisfaction) all day. If minutes turn into hours, or become too frequent, where will customers turn for assistance?"

Contact Center
pipeline

BUILDING A RESILIENT CONTACT CENTER

Don't take reliability for granted. Intentionally seek, implement and manage solutions to achieve your goals.



BY Lori Bocklund, Strategic Contact

In the era of "five nines" of reliability, contact center leaders didn't worry too much about the resiliency of their technology: It was always up. But with all the changes and permutations of technology, reliability can't be taken for granted. You need to intentionally seek, implement and manage solutions to achieve your goals.

Simple availability calculations (**SEE TABLE 1**) drive the point home. Traditional technology commitments of 99.999% availability yield about five minutes of downtime a year. If you don't pay attention today, you might actually sign up for tens of minutes of downtime per month! Contact center and IT leaders, along with vendor partners, must play a role in ensuring that the proper level of redundancy and resiliency are in place to deliver the right customer experience and protect the brand the center represents.

Mission Criticality Demands Resiliency

Several factors have elevated the need for improved contact center resiliency. Delayed technology investments come home to roost when a formerly reliable machine starts to have bad days, or an unexpected peak impacts system performance. A center may have contracted for cloud services without considering reliability or how the vendor will stand behind its offering, and found out too late that the performance wasn't what was expected. Complex architectures, whether premise or cloud, can introduce multiple vendors and single points of failure, leading to finger-pointing rather than rapid resolutions and root-cause analysis. And when customers can't reach the center, they've got a rather large stage on which to vent their frustrations.

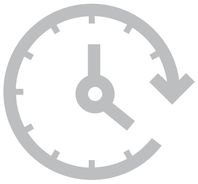
Centers are increasingly aware of the need to "fix" these issues but don't always have the time, resources and funding to do so. If your center is mission critical and you aspire to be "best-in-class" (or remotely close to it), resiliency is an imperative, not an option.

Defining Requirements

While it might be tempting to say everyone should buy five nines of reliability and every vendor should offer it, the reality is not that simple. High-performing, resilient solutions require a substantive investment in technology along with the people to set up and maintain the monitoring, troubleshooting and remediation protocols. Bigger organizations have more resources and focus on these issues (and, perhaps, have more to lose). But smaller companies need to consider it, too. There are some good options to do so, as we'll demonstrate in the cloud section of this article. Financial services and utilities can be viewed as leaders in striving for resilience. Heathcare, retail, manufacturing, and others

TABLE 1: How Much Downtime Can You Afford?

Contact center technology traditionally delivered a rock-solid 99.999% ("five nines") reliability. This table reflects some of the percentages we've seen for today's solutions. Think about how much downtime your center can endure.



	DOWNTIME EQUIVALENT	
Availability %	**Hours/Year**	**Minutes/Month**
99.800%	17.52	87.6
99.900%	8.76	43.8
99.950%	4.38	21.9
99.980%	1.75	8.76
99.990%	0.88	4.38
99.999%	0.09	0.438

follow closely behind. Finding cost-effective solutions feels easier if you have multiple sites, but you still must focus on the technology and where it resides.

As a starting point to defining *your* requirements, consider what would happen if you lost your contact center technology for minutes, hours or more. Maybe you think you can endure a short blip, but consider what happens next. A few minutes outage can leave the center playing catch up on service level (and perhaps, customer satisfaction) all day. If minutes turn into hours, or become too frequent, where will customers turn for assistance? What would the impact be on other channels or departments? Who would hear about it, and how? Would you risk losing business—whether short-term sales, or longer term loyalty? Would your customer take to the "airwaves" of social media, risking brand damage? You get the idea.

Smart leaders consider many factors in defining resiliency requirements. They work with IT to define scenarios and how redundancy and resiliency can prevent and mitigate the more likely ones.

Start with the voice and data networks, seeking to eliminate single points of failure in connectivity to carriers and your LAN, WAN, Internet, MPLS, etc. Chances are you need some resiliency built into your core routing and reporting. Most think of voice first, but centers increasingly need to consider other media as well. That can be more complicated if different solutions route the various media versus an integrated routing and reporting engine.

Most workforce optimization tools (WFM, QM, etc.) don't need to be redundant, but think about how long you can be without them. If you're large, you probably can't live too long without your WFM without risking some serious inefficiencies. Those with regulatory or compliance demands need to ensure recordings are always captured and perhaps backed up or duplicated in real-time.

If your IVR carries a heavy workload (e.g., financial services, utilities), you probably want some redundancy and geographic diversity on the ports. CRM or a core system may be mission critical for some, as it is important to track contact records and not risk losing that history. This one can be tricky if it is the system of record. When it is down, other solution availability can become moot if agents can't address customer needs anyway. So, it may be the starting point to form the baseline of center availability.

Vendor Questions in the Pursuit of Resiliency

If you are embarking on a vendor evaluation and want to consider redundancy and resiliency, here are some key questions to ask. Choose the pertinent ones based on the sourcing approach and the vendor's scope. And if the solutions aren't the vendor's responsibility, ask your IT department!

- Where are the data centers (DCs)? How diverse are they? (e.g., geography, power grids)
- Who owns/provides the DCs? (Vendor or third party or infrastructure/platform provider)
- How are the DCs secured? Address physical and network access.
- What network connectivity options do they offer? (Address carriers, physical paths, failover, etc.)
- What are the single points of failure? What options are offered to minimize risks?
- Does the system transition to backup automatically? Or does transition require manual activity? (and if so, who does what?)
  - Is the data duplicated?
  - Do agents have to login again?
- Are calls in progress maintained? Are calls in queue maintained?
- What are the SLAs? Remediation?

Remember, you need to dive into what a vendor means, as definitions can vary and you know what happens if you assume!

Looking to the Cloud

Many people look to cloud solutions to get the resiliency they need. They don't want to be "in the data center business" and may lack the expertise, resources and/or facilities needed.

As we've pointed out in other Tech Line articles, "cloud" can be delivered in various ways, so looking to the cloud to address resiliency must take into account the approach and service offered. True cloud solutions can offer redundancy and failover services; however, not all vendors have this built in or part of a standard offer. You may "get what you pay for" when choosing a low-cost option. An alternative approach is a private cloud or hybrid model with a dedicated platform with geo-redundancy. In these scenarios, you have more control but, of course, it is not the lowest cost alternative. Regardless, you need to consider the network connectivity (e.g., between your site and the cloud solution) and a variety of elements in the architecture and vendor support processes to ensure your needs are met. And whether premise solution or cloud, you need to define what is onsite and what is in the data center. Decisions can include gateways for carrier network termination and recording servers and storage.

Another enticing option is managed services, putting the technology and its management into a vendor's hands. But managed services itself may not provide more resiliency. It's still a question of architecture and service level agreements (SLAs). Managed services could speed recovery time (and make someone else responsible for it) if you are concerned about internal IT resource availability and processes.

Regardless of sourcing strategy, proper SLAs that include the target uptime, response times under various scenarios, escalation processes (timing and resources), resolution targets, and remediation are the crucial pieces of the resiliency puzzle. Without "dollar-and-cents" remediation, any SLA becomes a statement of good intentions, not a commitment to reliability and resiliency. Some vendors offer no remediation, so decide in advance if remediation is a "deal breaker" and pursue solution options accordingly.

Pursuing Best Practices

Beyond the SLAs, "best practices" start with geo-redundancy across two (or more) data centers that are not vulnerable to the same issues for storms or other natural events, or major network or power outages. The provider offers data center expertise (directly or through a third party) that includes hardened, secure facilities, with biometrics for access.

Core functionality is duplicated and delivered in true "active/active" mode, with duplicated data and automated failover. A caution is in order here, as vendor definitions can vary. "Active/standby" may be called "active/active" but not include proactive data sharing. You must assess what it means and if it meets your needs.

Ideally, the network and server capacity can handle the entire load in one location in the event of a failure. Full redundancy of network connectivity can be hard to achieve and require cost and value tradeoffs. The perfect scenario includes different carriers and different entry points into a single data center or dual centers with diverse carrier paths. You must look beyond carrier brands as the physical trunks and paths can be the same. Internet Service Provider (ISP) redundancy can be particularly important for cloud-based solutions that depend on Internet connectivity. The net of all these variables is network connectivity can be the Achilles heel, and IT's overall resiliency architecture and BC/DR plans may play an overarching role in the contact center options.

Let's not forget (easily neglected) testing in the pursuit of best practices. You need to routinely (e.g., annually or biannually) test failure scenarios and the abilities of the systems and network, as well as human process execution. If you have a full BC/DR plan, testing for the center may be part of it. Too few companies have strong and comprehensive BC/DR plans that account for the center's specific requirements. A resiliency project can help bring this need into focus. If you are pursuing a cloud solution, make sure periodic testing is part of the vendor's routine (see **THE SIDEBAR** for other questions to ask of vendors).

If you are single site, you may be wondering if you can still get resiliency. The answer is a qualified yes. For example, you could have a dual processor (A/B) at that site, employ third-party data centers that are geo-redundant (even if both serve the same site), or consider disaster recovery services. Some cloud vendors are seizing this opportunity with low-cost "insurance policy" licensing that lets you kick into backup mode on their technology when needed.

Protect Your Center, Customers and Company

The first step on the path to resiliency is to assess your current state and define your desired state, gaps and how you will address them. Identify single points of failure and other vulnerabilities. Define the level of resiliency you need and the associated requirements. Decide if you will enhance what you have, or replace (and enhance) it. Then you must consider sourcing strategy, recognizing that resiliency is just one factor in that big decision. Define the roles of your vendor along with internal IT and contact center roles.

Once you have a new resiliency plan and solutions in place, operate with best practices. Manage vendors (or IT) and hold them accountable. Routine tests will give you the confidence that when something happens, you are ready to protect the needs of your center, company and customers. ◉

Lori Bocklund is Founder and President of Strategic Contact. (lori@strategiccontact.com)

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