Contact Center Pipeline

BUSINESS CONTINUITY/ DISASTER RECOVERY

BY LORI BOCKLUND,
STRATEGIC CONTACT, INC.

IS YOUR CENTER *REALLY* RESILIENT?

Self-Assess and Take the Next Step in Resiliency Readiness.

SEPTEMBER 2022

ILLUSTRATION PROVIDED BY NAKIGITSUNE-SAMA ADOBE STOCK

IS YOUR CENTER *REALLY* RESILIENT?

SELF-ASSESS AND TAKE THE NEXT STEP IN RESILIENCY READINESS.

BY LORI BOCKLUND, STRATEGIC CONTACT, INC.

Formal Business Continuity and Disaster Recovery (BC/DR) planning has always been a very important aspect of contact centers' success. In the May 2020 issue of this esteemed publication, I showed how Covid and the move to work-from-home (WFH) provided a clear rationale for making preparedness mission-critical. *Resiliency* was the theme of the day, and still is, more than two years later.

You may have some well-earned pride in all you have done in your center since Covid hit. Kudos for managing the work-from-home transition and keeping on-site staff safe. You deserve badges for handling unpredictable volume swings and fluctuating handle times. You may still be earning your stripes dealing with high turnover and hiring challenges. Maybe you transitioned to a cloud-based solution or boosted self-service through chat bots or voice bots. Way to go! All these things build resiliency cred.

Yet, I still have this lingering feeling that centers invoke a *tactical, reactive* practice than one steeped in strategic, proactive thinking. So, this article starts with a three-step call to action:

1. Take the little self-assessment I outline. If you answer yes to each question, go read something else! Assuming you don't come out of that thinking, "We're good!"...
2. Identify what you need to do to close the gaps in your plans, and...
3. Go fill those gaps!

> ***I STILL HAVE THIS LINGERING FEELING THAT CENTERS INVOKE A TACTICAL, REACTIVE PRACTICE THAN ONE STEEPED IN STRATEGIC, PROACTIVE THINKING.***

SO, YOU WANT SOME "HOW TO?"

I thought you might meet me here! If you got to this point, that means you have some opportunities to boost your resiliency preparedness. There is no better time than today to get started!

My first contribution to helping you with your planning is my May 2020 article, which you can find here.[1] That article outlines all kinds of things to consider for building a resiliency plan. It even includes a link to an outline to get you started!

I also want to provide some top considerations because BC/DR is not what it used to be, and you can't look at it like you always did. Many centers are using cloud solutions, whether as a fundamental shift in sourcing strategy or for select applications. Cloud solutions change the roles and responsibilities for technology and processes. It is very important to rethink plans based on the advantages cloud offers for resiliency,

[1]See May 2020 Contact Center Pipeline article, "A NEW ERA CALLS FOR A NEW LEVEL OF RESILIENCY" https://www.contactcenterpipeline.com/Article/a-new-era-calls-for-a-new-level-of-resiliency

RESILIENCY SELF-ASSESSMENT

Assess your center's resiliency by answering these questions:

- Do we have some level of site agility, through work-from-home, multiple sites, and/or partners?
- Do we have redundancy for all our "mission critical" systems and networks? If so, do they failover automatically or do we have a clear plan for how to invoke failover?
- Do we have a way to route our calls to available resources under various scenarios of issues and outages? Do we have built-in routing configurations for "typical" scenarios and processes ready to invoke for less common but possible scenarios?
- Do we have clear plans for what to do if we are significantly understaffed (due to volume increases, and/or various system, facility, and/or staffing issues)?
- For any of these scenarios, do we have documented guidelines for when our plans are invoked (e.g., how long an issue must last before we do something), how we take action, who is responsible to do what (including notifications), how we test it is working, how we return to "normal," and how we keep our plans up to date?
- Are those plans up-to-date based on our *current state* for technology, agent locations, and processes?

and the realities of relinquishing control for managing infrastructure (including network connectivity and carriers) and applications, potentially introducing new types and frequency of issues.

With agents in multiple locations, not dependent on corporate facilities, you have a new level of built-in agility. However, you need a mini-resiliency plan for each agent in their home office, even if IT is supplying the computer. WFH is only as good as the technology the agents have – including their home router, WIFI, and Internet Service Provider (ISP). You need to adapt to many different situations and prepare them to be resilient on their own!

CLOUD SOLUTION CONSIDERATIONS

Network: We see three different models for carrier management and each introduces different considerations for how you manage issues:

1. The cloud provider is the carrier
2. The cloud provider uses one or more 3rd parties as the carrier
3. You choose to "bring your own carrier" (BYOC) and continue to manage it

If you are paying the cloud solution vendor to provide carrier services (options 1 and 2), it is important to understand if they use multiple carriers (in option 2) or what level of diversity they have (option 1) so they can reroute. You could be totally reliant on them. It is better to know ahead of time than get frustrated or surprised in the middle of an issue.

> ***BC/DR IS NOT WHAT IT USED TO BE, AND YOU CAN'T LOOK AT IT LIKE YOU ALWAYS DID.***

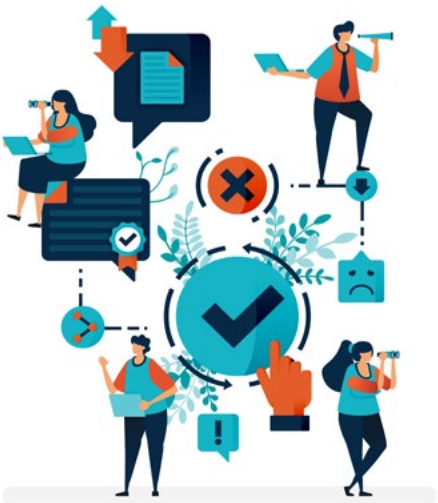
If you choose the BYOC option, you are weighing the tradeoffs of finger-pointing risk versus level of control you have. While you can still do multi-carrier, make sure your IT team has the resources to oversee it. You should also engage with your cloud CC solution provider to understand how they resolve issues when the problem is (or may be) with the carrier(s) that your company manages.

Routing: When designing routing, make sure you consider atypical scenarios such as emergency closure, no staffing during normal hours, or even excessive queue conditions. You can set up decision trees to automatically route to a message, self-service, or other resources. Pre-record messages for these circumstances and define the process for (trained) staff to put them into action. (And make sure they have a "cheat sheet" to remember all the steps!) With a cloud solution, you should be able to set these up so contact center resources can do the changes and not have to rely on IT or the vendor. If you must rely on IT, identify priority and time response commitments; don't let it fall into a ticket queue without rapid response, or get stuck waiting for someone who knows how to act on it!

Reliability Expectations: Historically, we are accustomed to "five 9s" of reliability: 99.999% uptime, or less than 5 minutes of downtime per year. With cloud solutions, you may fall short of that in the SLAs and/or in the operational reality. Thus, your planning needs to consider the risks of lower levels, such as 99.99% for your mission critical voice routing. Other applications, such as cloud-based bots/IVR could be even lower (such as 99.9%).[2]

SLAs: SLAs are a critical part of the commitment cloud solution vendors make to the market and to your center's operational reliability. Read the SLAs carefully, understand the vendor's commitment to keep things working and respond when they are not, and provide you some remediation if they fail. If the solution is being delivered by one of their partners, understand the roles and responsibilities they have in tandem with the vendor. Ask for performance history, because an SLA may under- or overstate performance, and you want to understand the track record. Talk to references, because their experience is a very important reflection of reality. You may have a limited ability to negotiate a higher SLA or pay a premium for the privilege, but you need to know what to expect and prepare for it.

Finally, know that an SLA is generally only as good as your commitment to hold the vendor accountable to it. You may need to track downtime and manage the remediation process. Worst case, your accounting of the performance is your ticket to get out of a contract if a vendor is not serving your interests well.



[2]See August 2017 Contact Center Pipeline article, "BUILDING A RESILIENT CONTACT CENTER," for a table of downtimes tied to availability percentages.
https://www.contactcenterpipeline.com/Article/building-a-resilient-contact-center

All Hands on Deck scenarios: Many companies have an "All hands on deck" element to their resiliency plans. People working in other departments who transferred out of the center may pitch in, or you may tap trainers and quality team members. These are great resources to add a level of staffing agility. However, you need to understand how the configuration and licensing works with your cloud provider so that these people can be added quickly without breaking the bank. For example, make sure you don't have an agreement that requires you to pay for named licenses that sit idle, or one that the license counts (named or concurrent) can only go up, never down. If you need resiliency seasonally or a few days each month, you may need to negotiate a specific structure that accommodates that flexibility.

Dev/Test/Sandbox environments: Your IT department may have development, test, "sandbox," and/or quality assurance (QA) environments for core systems (like CRM, customer information systems, etc.) and may want to set up something similar with your contact center solutions. Perhaps they want to be able to test routing and integration, or self-service applications such as IVRs and bots. These can be important elements for resiliency.

Talk with your vendor(s) or prospective vendors about these environments and how they handle licensing and version management. You may choose to create a separate instance of your environment ("organization" or URL) or just configure different numbers and agents for routing. You will also need a process to transition a test environment into production.

Testing: Testing the platform resiliency overall is the cloud vendor responsibility, not yours. (Don't assume you can invoke a test!) Explore this topic with the vendor so you understand what they routinely do to assure your network and system can failover successfully. This subject may be of even greater interest when the vendor uses third-party data centers and servers, such as Microsoft, Google, or Amazon infrastructure. And looping back to the carrier discussion, network failover testing depends on who the carrier(s) are and what level of control you have.

> ***WITH AGENTS IN MULTIPLE LOCATIONS, NOT DEPENDENT ON CORPORATE FACILITIES, YOU HAVE A NEW LEVEL OF BUILT-IN AGILITY.***

WORK-FROM-HOME CONSIDERATIONS

Technical support: Every home-based agent relies on the PC, the applications, and the network access in their house. If anything is down or performing poorly, or they aren't sure what to do, they can't move to another desk or get some help at their side quickly. So, the first day of onboarding and every day thereafter (no matter what shift they work!), they need great technical support and clear guidelines for how to get it.

Support must include a quick and easy way to share the desktop (e.g., through Teams, Zoom, Google, etc.) to get help from IT, Supervisors, the CC help desk, or peers. It should include ways to test network performance. Technical support may even need some new guidelines around shipping out new PCs or ancillary devices, such as monitors, headsets, or phones.

Discussions with IT need to address the reality that an agent with a technology issue is of little use. You'll need clarity on the support they (or the third party they contract) will provide and the hours they are willing to staff. The boundaries around what IT will or won't address with network issues also need to be clearly defined. Nobody likes to hear, "Call your local ISP." That is a ticket to delay in getting an agent back to handling contacts. Your training may need a new module on basic technical support so an agent can more comfortably do their part to help troubleshoot and solve problems. You may also want to provide WIFI hotspots or define other locations (including a trek into the office) where agents can go when they have issues.

USE OF THIRD PARTIES TO AUGMENT STAFF RESILIENCY

WFH is not the only site diversity model. Many companies use third parties to augment their staff, and they can play an important role in providing backup support in many situations. An outsourcer could play a routine overflow role and be prepared to handle additional volume if you have an event. They need trained staff, and enough of them, to be of use. In addition, you need great knowledge management (KM) tools and processes, and your routing strategies need to be very clearly defined and configured to move the right volume to the right place(s). There is no value in overflowing to a backup that is just a different holding place!

I have also written previously about the intrigue of "gig workers" as a staff augmentation opportunity. Leaders love the idea, and it can fit in the right circumstances – e.g., high digital channel use, passionate consumers or business peers that want to help others, great Knowledge Management. Many success stories have been published for things like technology support, consumer goods, and B2B services. The theme of using it routinely, not just in a pinch, surfaces again. If this approach might be a fit for you, explore it for day-to-day support and you will have a new level of agility in your toolkit.

UPDATE YOUR THINKING ON RESILIENCY

Here's a quick check list to get you started on your new and improved plan:

BC/DR CONSIDERATION	TRADITIONAL THINKING	CLOUD IMPACT	WFH IMPACT
RISK SCOPE	· Technology · People/Staffing · Facilities	· CC Technology in the cloud is in the hands of the vendor for BC/DR	· People can work from home (or anywhere!) – reduces reliance on facilities and processes around relocation
IT SCOPE	· Network · Systems · Power · Desktops	· IT may only be responsible for network and core systems (not CC technology), and basic infrastructure for in-house facilities/ systems	· IT must provide remote agent support – with hours to match and rapid response · IT likely won't support the home agent's internet service ("call your ISP")
DEVELOPING PLANS	· IT develops full technology plan – for enterprise, and (hopefully) for contact center · CC should develop the people and process elements of resiliency plans	· IT plans must address how they (or the CC) manage the vendor(s), and what they control vs. the vendor controls	· Some plans will be easier (e.g., less reliance on facilities) but they don't all go away · Consider facilities plans that could impact homes (e.g., widespread power or ISP outage)
TESTING	· Test failover – at implementation, and routinely (e.g., annual)	· Failover is controlled by the vendor – no need (or likely, ability) to test	· Should add performance testing for new agents (at a minimum) and have ability to test when any changes or issues
MAINTAINING PLANS	· Perform routine updates (e.g., annually) · Update when any specific changes occur	· IT – does this for the core systems but not any CC systems in the cloud	· CC – does this for the people/ process elements and must consider any lessons learned or changes for WFH
OTHER PLAN ELEMENTS	· Rerouting · Message updates · Service reduction tolerance (impact, duration) · Alternate site(s) or relocation · System failover (e.g., to backup servers) · System replacement · Roles and responsibilities	· Staff can work anywhere – no "rerouting" or site considerations · Vendor has responsibility to failover, reroute, rehome, transition to backup, replace, restore	· Much of the typical actions may be transparent to WFH agents – but don't forget to keep them informed, and make sure they know how to let the right people know if they notice a problem!

Policies: The policies for WFH are as important as the practices when it comes to resiliency. Proactively define "what happens if" for a variety of situations – like those just discussed under technical support. For example, most companies won't provide local ISP support. The agent must deal with that, and they may not want to, feel incapable to do what is asked of them, or end up waiting a day or two (or more!) for a service call. So, then what? Are they paid during that time? Do they have to come into the office after X hours? If it's a PC issue, how quickly can you get them a backup PC, and what do they do in the meantime? Policies include what the agent must do, what IT or the center leadership must do, and the related HR issues, such as do you keep paying them (and for how long).

All Hands on Deck scenarios: If you have one of those "all hands on deck" strategies that tap WFH, it is not just a technology planning item. Make sure it is clear how to notify people and what they need to do to jump in and help. And then make sure they have all the (remote) support they need!

Communication: Speaking of notifications, an always important part of resiliency planning, it is not quite the same when you have a WFH environment. Mobile phones become a key path for communication under various technology issues. And no matter what the scenario, make sure there is active, visible communication (not passive things like email) to keep the team informed of what is happening *right now*!

Lori Bocklund is President of Strategic Contact, an independent consulting firm that helps companies optimize the value of their customer contact technology and operations.
Email: lori@strategiccontact.com

PREMIUM CONTENT + RESPECTED CONTRIBUTORS FOR CONTACT CENTER PROFESSIONALS

ENABLING A NEW GENERATION OF CX AND EX PROFESSIONALS to create successful customer management strategies, develop cutting-edge technologies, refine the skills necessary to advance their career, and build a culture that advances the contact center within the organization—that's what we do.

Since 2009, **Contact Center Pipeline** has leveraged the insight of today's notable CX and EX thought–leaders, along with our advisory board, expert magazine authors, blog contributors, and industry insiders; keeping our audience ahead of the trends transforming the contact center and customer sales, service, and support industries, improving outcomes, and the way companies engage with their customers.

Contact Center Pipeline Magazine is published monthly digitally and in print. For more information and to subscribe, visit our website.

Contact Center Pipeline

INSIGHT AND INSPIRATION FOR CONTACT CENTER PROFESSIONALS