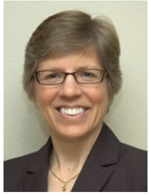
Contact Center Technology Monitoring

Monitoring allows companies to detect outages and issues for quick resolution, and enables effective planning for prevention and optimization going forward.

By Lori Bocklund, Strategic Contact

Contact Center pipeline

Pipeline Articles
www.contactcenterpipeline.com



Lori Bocklund
Strategic Contact

We all use tools to monitor important elements of our personal world in ways that we never did before: GPS and text messaging on the kids' phones, home security systems with remote notification and control, apps to follow activity with your favorite sports teams or stocks, and updates about your flights or financial accounts. Now you can—and need to—do the same things with your contact center technology. We have better tools and plenty of reasons to be tuned in to what's happening and use the information to define actions to prevent issues or optimize going forward.

A Little History Helps Define the Present

In the past, companies didn't need to monitor their contact center technology. We lived in a world of rock-solid reliability with fully redundant systems, automatic failover, and little downtime (planned or unplanned). Upgrades and other management and maintenance tasks were infrequent and handled with expectations of "five 9s" of reliability. Equipment vendors and network providers monitored their respective solutions, often clearing alarms on their proprietary systems and networks before anyone knew there was a problem to solve.

There used to be a clear division between IT and telecom. IT focused on data systems and the associated networks, and telecom addressed voice-related systems. As such, the corporate Network Operations Center (NOC) didn't see alarms and track outages for the PBX, much less the specialized contact center applications. Telecom may have provided some monitoring, but for the most part they got involved if things went wrong.

Our High-Tech World

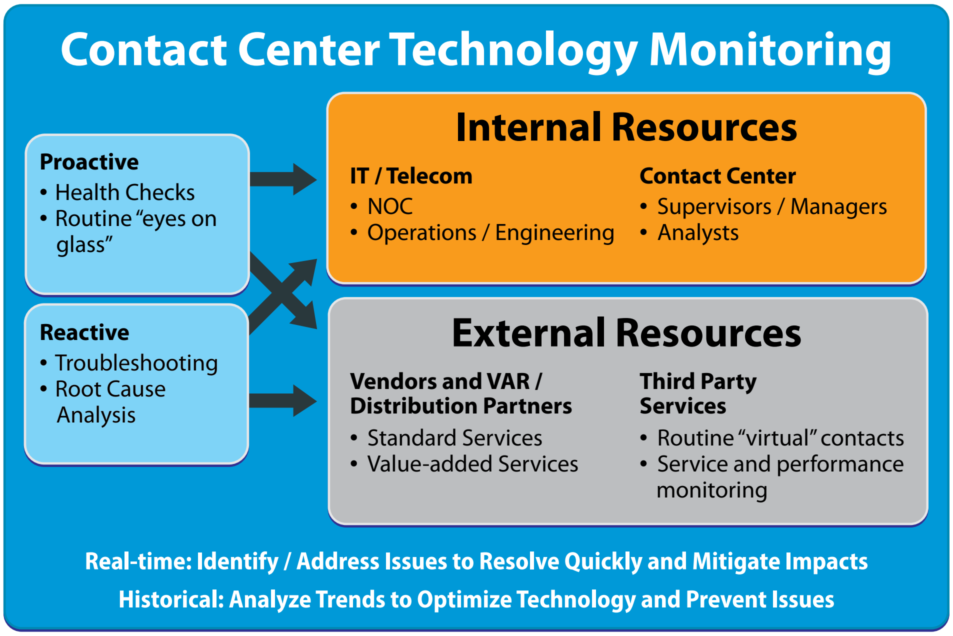
Things have changed. Contact center technology sits in data centers, running on standard servers (and even virtual machines), with standard operating systems and databases. With increased adoption of Voice over IP (VoIP) and remote data centers, centers have added a lot of voice traffic to a Wide Area Network (WAN) infrastructure that was originally built for data. Since monitoring tools can capture information about all of this technology, centers should be able to rely on "standard" IT support. Unfortunately, all too often that isn't happening. To make matters worse, today's technology seems to have less of a guarantee of performance; more things can (and do) go wrong. Moreover, the broad range of applications and integrations in the typical center increases complexity and diversity. The combination of all of these factors makes it challenging to achieve a stable, reliable, "healthy" environment.

It's time to bring contact center technology into the world of monitoring and focus on its unique needs and characteristics. That may mean 24x7 operations. It most certainly means the infrastructure, applications and network need to be "up" whenever the center is open. And it means monitoring with tools, people and processes that deliver the specialized expertise and focus on the center.

What "Monitoring" Means for the Contact Center

Monitoring contact center technology first and foremost means having real-time visibility into availability, functionality, and performance. Through monitoring, companies can detect issues and ensure the appropriate resources can react to any current or pending situation. The result is quick resolution and impact mitigation or prevention. Here are some examples of monitoring to keep the "finger on the pulse" for the contact center:

Monitoring Spans a Variety of Roles and Responsibilities, **Figure 1,** ***below***



Contact Center Technology Monitoring

Proactive
- Health Checks
- Routine "eyes on glass"

Reactive
- Troubleshooting
- Root Cause Analysis

Internal Resources

IT / Telecom
- NOC
- Operations / Engineering

Contact Center
- Supervisors / Managers
- Analysts

External Resources

Vendors and VAR / Distribution Partners
- Standard Services
- Value-added Services

Third Party Services
- Routine "virtual" contacts
- Service and performance monitoring

Real-time: Identify / Address Issues to Resolve Quickly and Mitigate Impacts

Historical: Analyze Trends to Optimize Technology and Prevent Issues

- System elements are working—network connections are live, systems or processes respond when pinged.

- Functions are working properly, achieving the expected outcome—routing paths deliver contacts, integration interfaces ensure systems are talking to each other.

- Specific performance elements are within "acceptable" range—for things like VoIP (packet loss, delay, jitter, Mean Opinion Score), servers (utilization of key elements, such as memory, processor, disk), and integration (response time on lookup from the IVR or desktop).

Engaged, proactive monitoring, such as health checks, ensures that things are working right each day or hour, and increases the likelihood of reliable, "normal" operation. For example, best-in-class companies will routinely test calls on all critical toll-free numbers, dialing into IVRs or menus. Some manually dial, some use in-house tools (e.g., Empirix Hammer), some use third-party services (e.g., IQ Services). They monitor trunk group and IVR port utilization. They test transactions on the website, submit test email or chat inquiries, or simulate application inquiries to assess response times.

Monitoring also enables effective planning and optimizing to prevent issues. For example, capacity planners can keep a close watch on utilization reports for trunks and processors to trigger budget requests when certain thresholds are met.

What to Monitor

Many companies only start monitoring contact center technology after issues occur. Better to proactively identify what to monitor for your particular environment, starting with core, mission-critical, customer-facing functions and applications. Identify things like your main toll-free numbers, ACD system (infrastructure and apps), IVR and website as "critical" in Service Level Agreements (SLAs) with IT and vendors. IT should already be monitoring your core business applications and infrastructure (e.g., things like customer information systems, order or claim processing applications, etc.), but if they're not, get those on the list, as well. Explore what network infrastructure monitoring already occurs and define any unique needs tied to VoIP, remembering that voice has very different performance needs than data (think speed over accuracy). You should also consider anything else that is mission critical and could impact operations, such as call recording, if you have compliance requirements. You should also monitor the elements that provide these functions—servers, gateways, routers and switches, for starters.

Monitoring applications such as WFM and QM may not be necessary since you can live without them for a few hours or days. However, it's a good thing to do once you establish strong monitoring structure (people, process and technology). You can build on the existing approach as you add more applications and infrastructure.

Who Should Monitor

The resources to carry the monitoring burden vary depending on architecture, sourcing, size, staff availability, and of course, funding.

If you have a NOC, they can provide monitoring support such as "eyes on glass," Tier 1 ticket creation based on monitoring outcomes, and escalation for help when monitoring shows an issue (real-time or trending). Lacking a NOC, look to other IT operations and engineering functions to tap the right tools and take action based on monitoring results.

Vendors and their partners can still play a role, and many offer value-added monitoring services. You will need to carefully define their role and how it fits with what IT is doing to avoid overlap, redundancy, or worst case, competing interests. Ideally, the vendor/distributor tools and services close gaps on internal monitoring. Cloud (or hosted) solutions and managed services providers remove some of the burden from in-house resources. That option becomes especially attractive when there aren't enough IT resources and/or monitoring tools aren't funded (see Table 1).

Sourcing Alternatives Impact Monitoring, **Table 1, *below***

Contact Center Technology Sourcing Option and Characteristics	Monitoring Advantages	Monitoring Considerations
Cloud-based/Hosted Solutions ◗ Vendor provides technology in their data centers ◗ Network may be vendor-provided or yours ◗ Connects to your premise and/or remote positions	◗ Vendor has responsibility for reliability and availability ◗ A good vendor will have strong monitoring tools, resources and processes that are included in the solution ◗ Little burden on your internal resources (IT or CC) to monitor technology	◗ Carefully select vendor, reviewing monitoring capabilities as part of due diligence • With managed service, define monitoring as part of their responsibilities ◗ Use strong SLAs to ensure monitoring delivers reliability, responsiveness and optimization ◗ Carefully address any accountabilities between vendor, internal IT, and technology or network providers
Managed Services ◗ Vendor provides resources to manage technology ◗ Technology may reside in vendor's facilities or yours (and be yours or theirs) ◗ Network may be vendor-provided or yours	◗ Shifts IT burden to vendor, including monitoring and associated response and optimization ◗ A good vendor will have strong monitoring tools, resources and processes as part of their service offering ◗ Added value may include 24x7 monitoring of all mission-critical applications	

Contact Center leaders or support functions (e.g., analysts) may get involved in monitoring on some platforms, leveraging visibility into how technology is performing. They can call toll-free numbers, IVR scripts, etc. Or, they may use third parties, such as IQ Services, to provide monitoring independent of what IT does. These services help address the contact center's desire to have more direct involvement in technology optimization.

Some vendors, such as Interactive Intelligence, include monitoring functionality for things like port utilization with their end-user administrative interface. With the right permissions, a contact center manager or analyst can find out if trunks are routinely busy, resulting in blocked calls. Or, they may see if the IVR ports are running at high utilization, risking that calls more readily spill over into live-agent handling, impacting service levels and costs. When the center gets more involved in monitoring, you need to define the degree to which users can go in and administer systems (as opposed to contacting IT or the vendor). They may have limited ability to make changes as a response to the monitoring they see, for example, changing routing or tweaking a script.

How to Monitor

When it comes to the "how" of monitoring, start by defining your monitoring strategy and plans for making it happen. Consider both proactive and reactive activity, real-time and historical perspectives. The best monitoring environments have strong governance, clear expectations, and routine outcomes that engage key members of IT and the contact center. Accountability is much easier to assign (and embrace) with the proper tools, processes and resources in place.

On the proactive front, you need to define who is doing what, when, using what tools or resources to ensure a consistent routine. For example, define the health checks to be done each morning before the center opens. Is someone in IT doing it, or will you rely on contact center resources or a third party for some of them? Similarly, you'll need to define who/what/when using what tools or resources for the "eyes on glass" monitoring. Is it the NOC? Vendors? Third parties? Staff in the Center? Some combination?

Every center should look at enterprise tools used in the NOC for other monitoring first. They may have tools such as Solarwinds that get SNMP data from other systems and applications. Since many contact center technology solutions now leverage SNMP, you may be able to go further, faster leveraging existing tools. Coordinate with vendors to see which solutions are compatible with SNMP and which require another means to monitor the system's health. Some vendors partner with specialty providers for monitoring. For example, Interactive Intelligence provides monitoring tools and options for their systems, and Path Solutions delivers network monitoring for those who need it, ensuring good, reliable quality VoIP conversations. Such tools also help with one of the biggest issues with monitoring: good documentation. Path Solutions tools quickly detect and map the entire network. This documentation is an invaluable resource for monitoring as well as troubleshooting and optimization.

When something's wrong, monitoring tools, processes, and resources play a key role in resolving the issue and identifying the root cause to prevent future occurrences. This level of readiness is invaluable to a mission-critical center, as it means quick resolution and (hopefully) minimal customer impact. Define who will do what, using what tools or resources, when monitoring unearths an issue, and how it fits with your overall trouble ticket and troubleshooting process. If the NOC is where monitoring occurs, tie into the tools and those who use them through good communication processes. Conduct trouble-ticket root-cause analysis reviews to refine monitoring efforts. And tie the reactive tools and processes into what you are doing on the proactive side to help you be ready. Then use monitoring results for strategic planning, trending, configuration optimization and trouble resolution

One final consideration is tying your monitoring strategy into your testing strategy—particularly routine testing, including heartbeat calls. The line between monitoring and testing is very gray here; it's all part of what you do to make sure that things are working right, thereby preventing or mitigating issues. (To read more about technology testing, see "Contact Center Technology Testing," *Pipeline*, July 2012.)

Who's Looking Out for You?

You probably don't ignore where your kids are or what they're doing, and likely feel like you can't live without your "monitoring" tools and processes. (Ever forget or lose your phone?!) While your contact center technology is not nearly as dear as your kids, it shouldn't be ignored either. Today, there are great tools and services—affordable and well suited to fit into your enterprise and contact center technology strategies—to help you make monitoring a routine part of your daily work life.

Lori Bocklund is Founder and President of Strategic Contact.

✉ lori@strategiccontact.com
☎ (503) 579-8560

Best Practices for Effective Monitoring

Here are some quick tips on best practices for effective monitoring of your contact center technology:

- Maintain an accurate inventory for the network, systems infrastructure and applications.
- Define monitoring strategy and protocols:
  - ❍ What's monitored and why
  - ❍ Who receives what information, when, via what channels
  - ❍ What are acceptable monitoring results
  - ❍ Who responds, how fast, when something is not normal
- Secure the tools and/or services to meet the defined requirements and objectives
- Assign contact center technology monitoring responsibilities to qualified resources
- Establish baseline performance metrics and define thresholds for action (using Service Level Agreements where possible)
- Perform health checks proactively and routinely
- Capture outcomes for routine reporting, trending, correlation, planning and optimization
- Evolve monitoring practices with environment changes and updates

Want to learn more? Visit **www.goo.gl/lpoe2** for testing and monitoring best practices.

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

Online Resource

This issue is available online at: Oct 2012, Contact Center Pipeline

http://www.contactcenterpipeline.com/CcpViewIndex.aspx?PubType=2

Pipeline Publishing Group, Inc. PO Box 3467, Annapolis, MD 21403
(443) 909-6951 | info@contactcenterpipeline.com