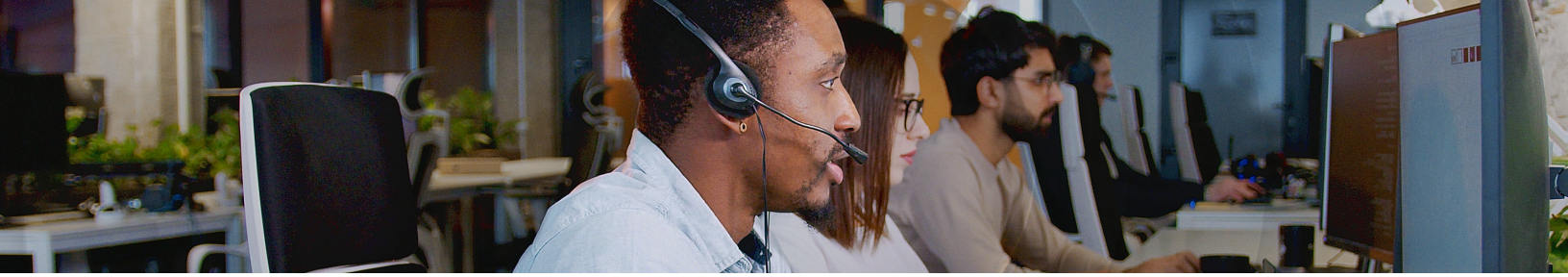
LIVEVOX

The Changing Face of Business Continuity & Disaster Recovery in the Modern Contact Center Environment

Presented by the creators of the contact center platform purpose-built for agents.

info@livevox.com | 844.207.6663 | livevox.com



INTRODUCTION

An Ounce of Prevention

Given all the pressing demands on your time and resources, it's easy to see why contact center business continuity and disaster recovery (BCDR) planning can take a backseat to more urgent matters in the here and now. But if the last time you reviewed your plan was before the COVID-19 pandemic, you likely have considerable gaps that may leave your contact center vulnerable to risk and financial loss.

You must still be prepared for traditional causes of outages or system strain, such as severe weather events, data breaches, seasonal spikes in volume or workload (e.g., holiday shopping events, annual sales, open enrollment), or even successful marketing promotions. However, the pandemic exposed numerous shortcomings in companies' BCDR plans, including how to:

- Adapt to constantly evolving circumstances (aka the "new normal")
- Support employee health, safety, and mental wellness throughout a prolonged period of uncertainty
- Navigate supply chain disruptions and their impact on operations, staff, and customers
- Maintain service delivery during widespread staff shortages

While the pivot to working from home kept businesses afloat over the past two years, hybrid and remote-work environments add a new layer of risk that needs to be addressed, such as new communication and collaboration tools, and cybersecurity risks from poorly secured home networks, computer equipment, and IoT devices.

With new and expanding risks threatening your contact center environment, how can you prepare for the unexpected? Let's start by considering the impact and causes of unplanned downtime.

CHAPTER 1

The Cost of Unplanned Downtime Is Rising

In the digital age, when your system goes down, your business goes with it. The impact of service disruptions on your customers, employees, brand reputation, and bottom line can be staggering. Most large and mid-sized enterprises (91%) estimate the cost of a single hour of downtime to be over $300,000 due to lost business, productivity disruptions, and remediation efforts.[1]

Costs are expected to continue rising along with the growth of ecommerce, digital channels, and distributed workforces. ITIC research has found that **hourly downtime costs increased 32% between 2014 and 2021**.[2] Research by IBM Security and Ponemon Institute reported a **10% increase in the average cost of a data breach** from 2019-2021, with lost business constituting the biggest portion of the costs (38%).[3]

The environment businesses operate in has changed considerably over the past decade and even more rapidly since 2019. As a result, contact center leaders are having to think differently about how they store and protect customer data. Traditional views of disaster recovery are evolving—it's not just about backup and recovery anymore.

Consider this:

95%
of organizations have had to rethink data protection due to the sudden emergence of work-from-home.[4]

Malware and ransomware attacks are so pervasive that organizations must provide protection from them and ensure recovery[5]:

43%
of organizations suffered unrecoverable data within the past 12 months.

63%
of organizations have suffered a data-related business disruption within the past 12 months.

Over 60%
of failures result in at least $100,000 in total losses.[6]

What Causes Downtime?

Companies often don't realize how much their BCDR needs have evolved. While most operations plan for disruptions to the power supply and communications caused by severe weather and natural disasters, unplanned downtime is much more likely to be caused by **everyday human error**.

The Uptime Institute estimates that human error plays some role in about two-thirds of all outages, most commonly caused by staff failing to follow procedures (50%) or because the procedures themselves are faulty (35%).[7]

Security hacks are another top source of unplanned downtime. Unlike outages caused by human error, phishing scams, ransomware, and data breaches are targeted and, therefore, can be much more costly and destructive to your business.

Similarly, **cybersecurity risks related to remote work** have been increasingly widespread since the sudden scramble to send agents home. IT has been challenged with ensuring that employees adequately secure their PCs, laptops, phones, and tablets while at home. And hybrid work arrangements can pose an even more significant threat since employees' devices can potentially bring malware back to the office, putting the company's network at risk every time they connect.

CHAPTER 2

Is It (Past) Time to Review Your BCDR Plan?

Developing and maintaining a comprehensive BCDR plan is a demanding and resource-intensive activity. It's easy to see why so many businesses adopt a "set it and forget it" approach to disaster recovery.

But allowing your strategy to get stuck on the back burner because of time constraints can be disastrous for your operation. Contact centers have complex processes and systems, and many blindspots that are easily overlooked.

And the pace of change is accelerating: Customers' expectations and demands are rapidly evolving, staff turns over, new channels are added, new software releases and upgrades, and cybercriminals are becoming more cunning. It's a good idea to review your plan frequently (i.e., quarterly, biannually) to ensure you're addressing all of the changes in your business, staff, systems, and emerging security threats.

Regularly reviewing your BCDR plan will not only ensure that your operation is aligned with current and future business needs, you'll be prepared to respond quickly and effectively when the next negative event occurs.

The following checklist provides key questions to help guide your team in its BCDR review and planning efforts:

Is Your BCDR Up to Date?

- ❑ **When was your BCDR plan reviewed last?**
  - ❑ Do you have regularly scheduled reviews?
  - ❑ Is the frequency adequate for your business? (Depending on your business and environment, you may need to schedule quarterly reviews, bi-annually, or at least once a year.)
- ❑ **Have you considered all the possible threats and discussed what you would do to address each one?**
  - ❑ Have any new risks emerged since the last review?
- ❑ **Have you estimated how long it will take your operation to recover from an incident or outage, including new risks?**
- ❑ **Have you calculated the cost of downtime for your contact center and the financial impact on the organization?**
- ❑ **Have you identified and prioritized mission-critical processes, systems, applications, personnel, and other resources?**
  - ❑ Have you also determined interdependencies with other business functions?
- ❑ **How will customer interactions be routed during a system outage or disruptive event?**
- ❑ **Do your current policies and processes for data retention and storage adhere to the latest compliance regulations and standards?**
- ❑ **Is supplier and vendor information up to date?**
- ❑ **Have there been any personnel changes that affect the makeup of the BCDR team?**
- ❑ **When is the plan invoked? Are the specific triggers and guidelines documented? How is the team notified?**
- ❑ **Have specific BCDR roles and responsibilities been established so each team member understands what to do in an emergency?**
- ❑ **Do you have multiple contact information for each team member, and is it up to date?**
- ❑ **When was the last time the BCDR plan was fully tested?**

If you haven't ticked off all the boxes on your checklist, you may be leaving your operation vulnerable to new potential threats. The risk landscape is continuously evolving; plans should be frequently analyzed and updated based on recent events and predictions. And while no plan is entirely foolproof, staying consistent in your efforts will help you be prepared to handle any new challenges that come your way.

CHAPTER 3

Business Continuity Challenges for Hybrid Workforces

Hybrid work models are quickly becoming the norm for organizations. While there is no doubt that the flexibility a hybrid arrangement provides can increase your contact center's ability to maintain service delivery during a crisis, it also comes with a unique set of challenges and risks that your business continuity plan must take into account.

Who Is Available, When, and Where?

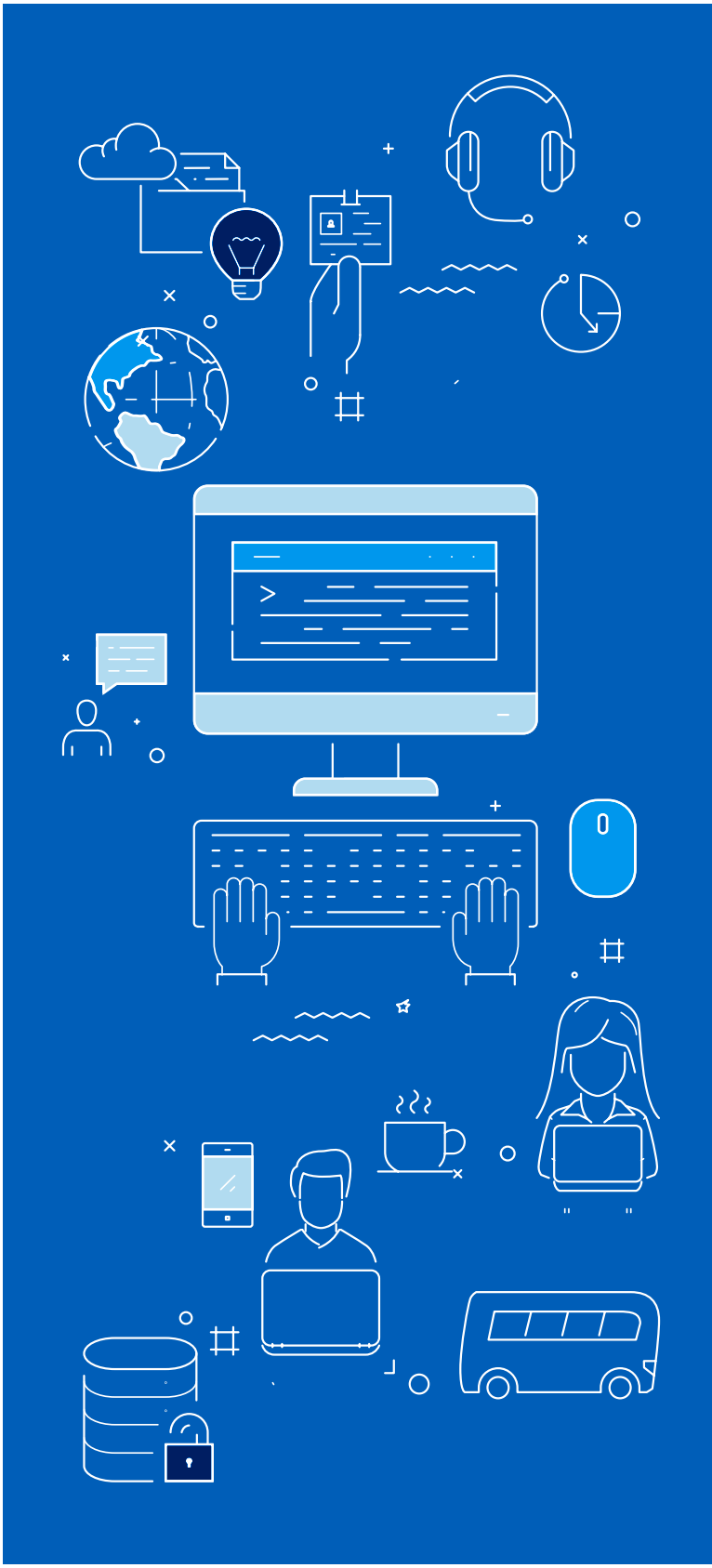
When managing a distributed workforce, you must be ready for a broad range of possibilities, including severe weather or a widespread power outage that could take many of your work-from-home agents offline. Will the affected agents be required to return to the contact center facility or go to an alternate site with backup power?

When calling teams back to the contact center, your recovery time objective (RTO) will need to consider **how long it will take team members to get to the site**.

For instance:

- **How far will each agent have to travel?**
- **Do they use public transportation?**
- **What are the average commute times where they live?**

Processes with a very low RTO may require an alternative recovery strategy. For instance, if your RTO is an hour or less and most of your agents cannot travel to the facility within that amount of time, customer calls may need to be temporarily routed to a location that is outside the affected area.



How Secure Are Your Agents at Home?

Employees are typically the weakest link in a company's cybersecurity program. It's not surprising that remote workers became the primary target of criminals during the pandemic, driving a 238% increase in cyber attacks.[8]

Work-from-home agents, especially those new to remote work, often lack proper training in cybersecurity protocols and best practices. For instance, home-based employees often overlook the security risk posed by wireless routers. Most people don't bother to change the default password after setting it up, and they share the password with friends, neighbors, or guests.

Providing explicit instructions on the proper setup and management of work devices, which services to use, and how to use them is the first step toward mitigating security risks among remote agents.

Remote workers also often introduce unsanctioned technology into their work environment. This presents considerable security risks since personal devices may have outdated operating systems and nonessential apps (e.g., social media, file sharing, games, etc.) that can increase the company's exposure to malware and other cyber threats.

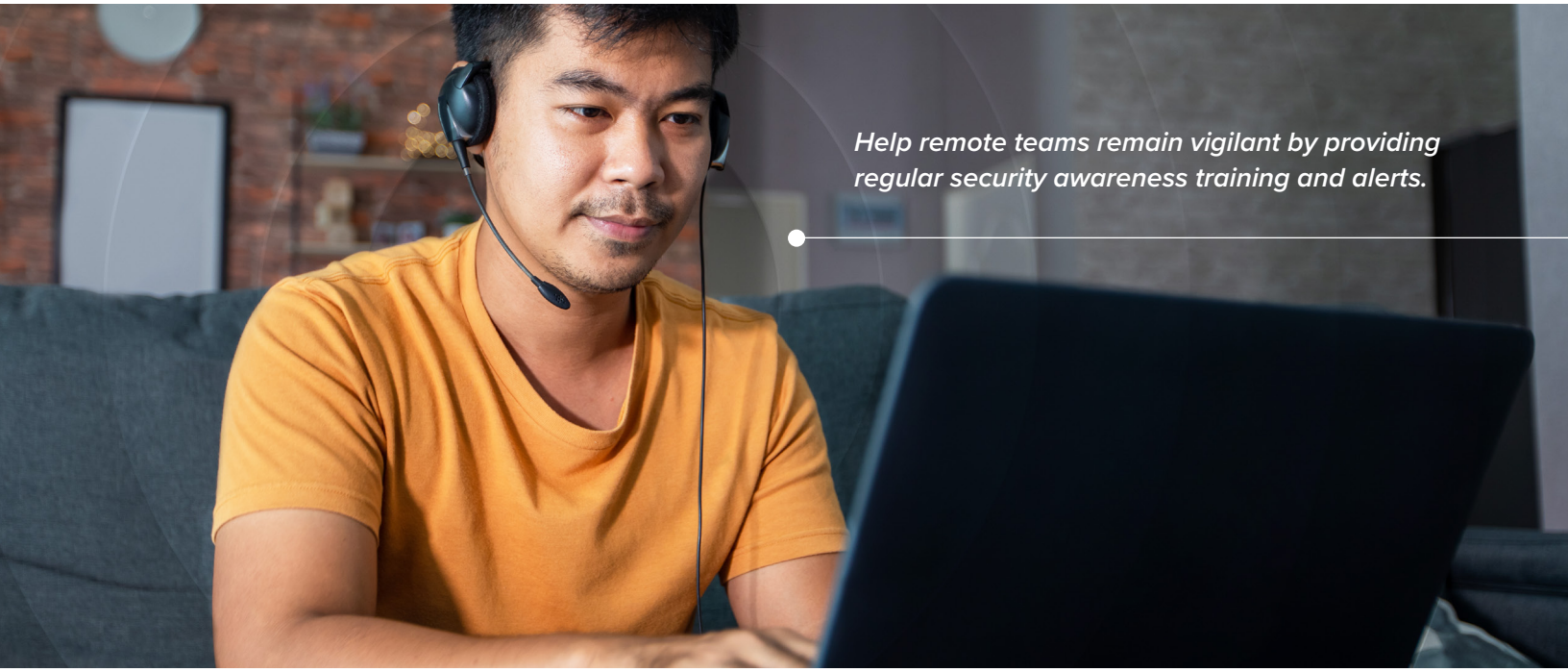
Even if you provide remote agents with work equipment, be sure to instruct them to use only company-provided devices to access company systems and only from approved access points (and preferably via a virtual private network), or they may be tempted to log in using their personal devices on an unprotected network, exposing the company to a man-in-the-middle attack in which a hacker can intercept the team member's communication or data.

Help remote teams remain vigilant by providing regular security awareness training and alerts. Make sure remote team members know how to report suspicious emails and are informed whenever new phishing attacks surface. Cybersecurity awareness training is not a once-and-done event; it should become a regular part of your team's discussions.

How Will You Monitor and Support Remote Workers' Mental Wellness?

While agents enjoy the flexibility that working from home offers, blurred lines between work and personal lives contribute to higher stress among remote workers. A BCDR event can further amplify anxiety and stress leading to burnout and long-term health issues like cardiovascular disease, depression, and sleep and eating disorders, among other problems.

Unlike their on-premise teammates, managers have a harder time identifying issues or personal crises in agents who work from home. It's essential to include a process for monitoring the mental health of your agents. Provide both online and in-person social activities to allow remote workers to connect with their teams, as well as coaching and mental wellness training.



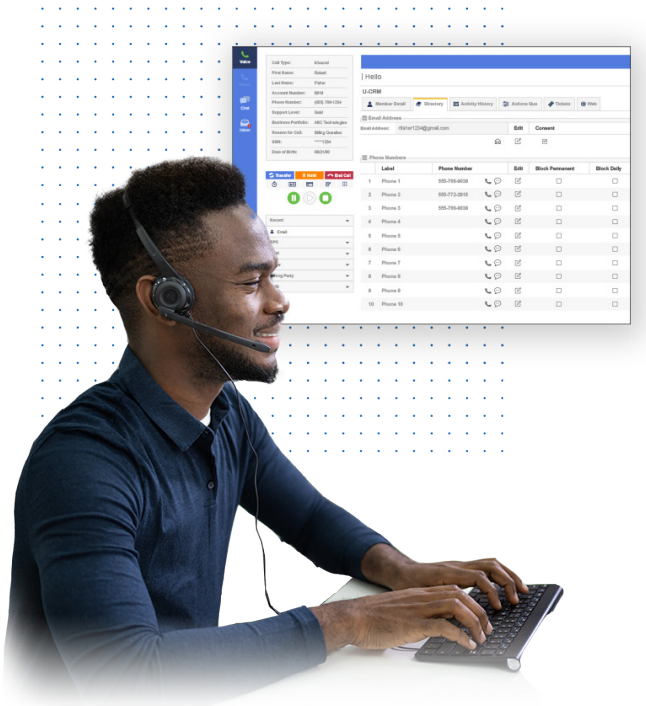
CHAPTER 4

Why Resilience Is Critical in the Modern Contact Center Environment

No doubt the pandemic served as a wake-up call to businesses to prepare for the unexpected and that proactively updating and expanding the BCDR plan is paramount. Not surprisingly, a study by global consultancy firm Mercer in 2020 found that more than half (51%) of companies worldwide had no plans or protocols to manage a global emergency like COVID-19.[9] And, just over 27% of companies said they had no business continuity plan in place, while nearly 24% said they were drafting one.

While ensuring that your contact center is prepared to maintain its processes, coordinate your people response, and recover technology is absolutely essential, **the long-term effects of the pandemic have prompted more companies to favor business resilience over continuity**.

The truth is, you need both.



So how do business continuity and resilience differ? The International Organization for Standardization (ISO) refers to **business continuity** as an organization's ability to continue to deliver its products and services at acceptable levels following a business disruption.[10]

On the other hand, **resilience** is defined by Gartner as: "The ability of an organization to resist, absorb, recover, and adapt to business disruption in an ever-changing and increasingly complex environment to enable it to deliver its objectives, and rebound and prosper."[11]

In other words, your contact center doesn't merely continue to operate during a crisis; it improves, grows stronger, and progresses to a more successful state.

Let's consider resilience in pandemic terms using the shift to remote work as an example. Contact centers not only had to overcome numerous challenges during the first months of working from home to ensure continued service delivery, they quickly adapted to this new way of working by adopting remote tools and management approaches. Many have since expanded staffing models to include hybrid work and more flexible schedules to ensure that their operations can survive similar disruptions in the future.

Resilience and High Availability for an Always-On World

Even better than recovering quickly is the ability to resist disruption in the first place. It's easy to see why organizations that provide always-on services and data access for customers are now emphasizing resiliency over recovery, and are looking to achieve high availability in the cloud. A high-availability program ensures that the contact center platform is reliable and will operate continuously, even in the event of an outage or failure.

While high availability and disaster recovery (DR) have become part of the larger conversation about business resilience, the concepts are frequently confused. For instance, when people refer to redundancy and disaster recovery, they're often really talking about high-availability capabilities.

High availability and disaster recovery are related, but they have different meanings, approaches, and impacts on service delivery. Here are three important distinctions when it comes to improving your contact center's resiliency.

1. How much downtime is acceptable?

Disaster recovery is a reactive process that takes place after an event has occurred. DR planning focuses on restoring the system to an operational state when that system is rendered inoperative. The loss of service depends on how quickly the DR plan can be executed and the system restored (think hours, days, or even weeks).

High availability is about prevention, eliminating single points of failure to reduce the probability of system outages. If there is an outage, data center redundancy delivers seamless failover for minimal disruption to the operation. With high availability, there is generally no loss of service.

2. Does your plan account for rare scenarios, everyday errors, or both?

Disaster recovery planning tends to focus on catastrophic events like hurricanes, floods, or earthquakes. When it comes to resiliency planning, certainly every company should be prepared to recover from natural disasters and even a global pandemic. However, keep in mind that it's the everyday events that cause the majority of disruptions. Human error and security breaches are the top causes of outages, according to ITIC.[12] Resilience focuses on proactively minimizing the potential for outages related to these more routine events.

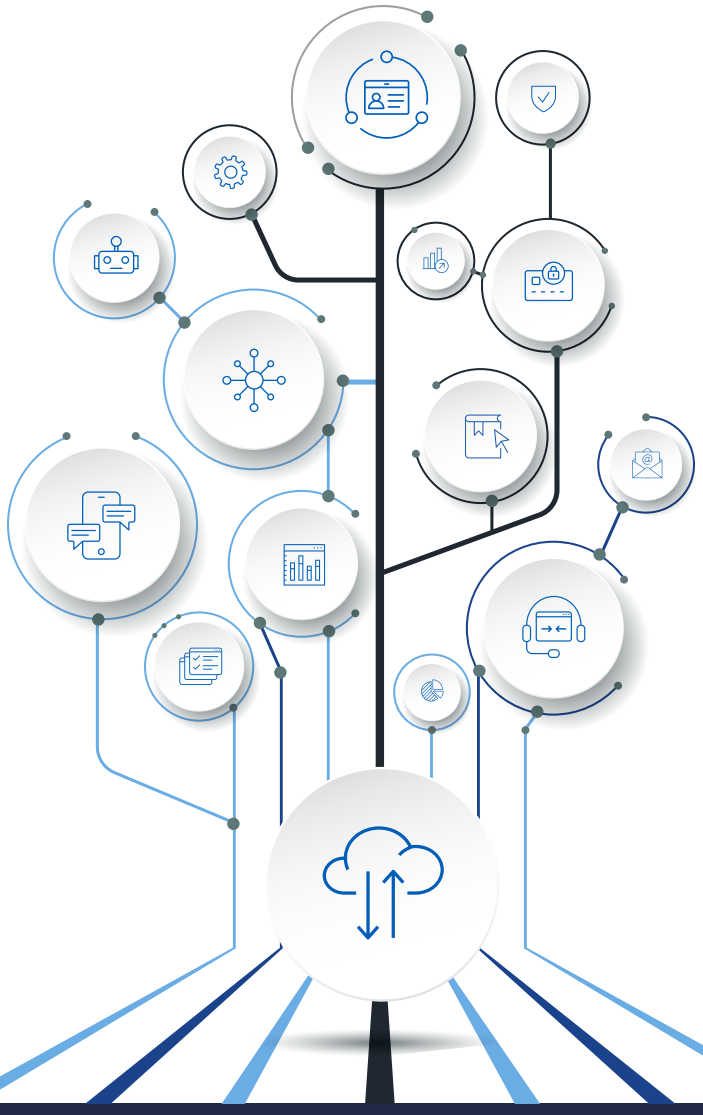
3. Does your organization have the budget and resources to maintain a redundant system?

The more redundancy required, the higher the price tag due to added hardware and resources needed for failover. For instance, high availability requires sophisticated processes, including duplicating data across multiple sites to guarantee the main data center is functional all of the time.

Disaster recovery, on the other hand, usually involves less expensive technology and fewer resources since it focuses more on restoring operations after a catastrophe. For these less critical applications and systems, replication between various sites may not be necessary and backups are often enough for restoring information after a disruption.

Although a redundant solution can be expensive to build and maintain, the potential harm of unexpected system downtime on customer loyalty, agent productivity, and revenue should not be ignored. Without a reliable platform, you can't deliver the consistent service experiences that are expected today.

Fortunately, **cloud computing has revolutionized the IT industry**, and with its growing popularity comes a decrease in cost for high-availability systems. The capability to make cloud environments more scalable than ever before makes it possible for organizations of all sizes to reap the rewards from these highly reliable resources.



Develop a Resilience Plan to Transition from Survival to Growth

Because today's contact centers are navigating an unpredictable, dynamic business environment, it is essential to have a comprehensive plan to address short-term outages and extended disruptions while ensuring optimal conditions for the operation to transition from survival to growth.

The following steps will help you to get started:

- **Establish a resiliency team** composed of members from both IT and operations, defining each member's role in detail.
- **Ensure resiliency team members are well-versed in the different aspects of the plan.** Provide cross-training to lessen reliance on any one key individual and thus ensure a successful outcome.
- **Identify and assess external and internal risks**, such as natural disasters, power outages, cyber threats, etc., prioritized by likelihood and impact on the business.
- **Create a process for monitoring both existing and potential threats** and responding to any incidents that occur.
- **Ensure that mission-critical systems and networks are well-protected with redundancy.** Can they fail over automatically, or is there a strategy to activate the failover process?
- **Identify all stakeholders who need to be notified** in case an incident occurs, and contingency plans for communicating with them quickly.
- **Develop a list of third-party services that could supplement the contact center's capabilities**, such as cloud-based applications, backup sites, satellite offices for staff, and BPOs.
- **Define organization-wide communication** and collaboration requirements. Where will agents and supervisors access information and updates regarding their return to work or if they need to report elsewhere (i.e., work from home, satellite office, etc.)?
- **Define training and development needs** for extended disruptions, such as shifting company services or policies, how best to handle customer inquiries and complaints, and strategies for adjusting agent workflows or schedules.
- **Plan for fluctuations in demand and staffing.** How will you handle increased volume, spikes in workload, and staffing challenges?
- **Refine workforce models and practices.** Is your workforce location-dependent (i.e., required to be on-site), fully remote, or hybrid? Your plan must include contingency plans for scheduling, training, workflow, and management practices for each staffing model.
- **Frequently review and adjust to any new difficulties that arise.** Utilize your resilience to fix the business setbacks you initially experienced while strategically adding elements to ensure continued success in this rapidly changing landscape. Embrace these changes as they are vital to achieving long-term growth and prosperity.

By including these steps in your contact center's resiliency planning, you can ensure that your operation will survive and thrive, no matter what challenges it faces.

CONCLUSION

Don’t Leave It to Chance

The global marketplace is constantly changing—and so are the dangers that threaten your business. Leaving your contact center BCDR strategy to chance is too high a risk for any organization that wants to stay competitive.

Good leadership is essential in a time of ongoing uncertainty. With forward-thinking BCDR plans in place and focusing on resilience, contact center leaders will be better positioned to help their operations adapt to a rapidly evolving landscape.

Cloud infrastructure is essential in realizing BCDR. When it comes to keeping your contact center up and running, prevention is better than cure. With a high-availability solution in place and a proactive CCaaS partner committed to reliability and preventing outages from happening in the first place, you may never need to activate your disaster recovery plan.

Learn how LiveVox can enhance your contact center’s resilience with our high-availability infrastructure and industry-leading end-to-end Service Level Agreement. **Contact our Solutions Consulting team to tailor a solution to fit your business needs. Talk to an expert at (844) 387-3066.**

About LiveVox

LiveVox (Nasdaq: LVOX) is a next generation contact center platform that powers more than 14 billion omnichannel interactions a year. By seamlessly unifying blended omnichannel communications, CRM, AI, and WEM capabilities, the Company’s technology delivers exceptional agent and customer experiences, while helping to mitigate compliance risk. With more than 20 years of cloud experience and expertise, LiveVox’s CCaaS 2.0 platform is at the forefront of cloud contact center innovation. The Company is headquartered in San Francisco, with international offices in Medellin, Colombia; and Bangalore, India. To stay up to date with everything LiveVox, follow us at @LiveVox, visit livevox.com or call one of our specialists at (844) 207-6663.

Footnotes:

1 https://techchannel.com/IT-Strategy/09/2021/cost-enterprise-downtime
2 https://techchannel.com/IT-Strategy/09/2021/cost-enterprise-downtime
3 https://www.ibm.com/downloads/cas/OJDVQGRY
4 https://www.zerto.com/wp-content/uploads/2021/04/IDC-White-Paper-The-State-of-Data-Protection-and-Disaster-Recovery-Readiness-2021.pdf
5 https://www.zerto.com/wp-content/uploads/2021/04/IDC-White-Paper-The-State-of-Data-Protection-and-Disaster-Recovery-Readiness-2021.pdf
6 https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening
7 https://journal.uptimeinstitute.com/outages-understanding-the-human-factor/
8 https://www.alliancevirtualoffices.com/virtual-office-blog/remote-work-statistics-costs/
9 https://www.me.mercer.com/newsroom/covid-19-companies-have-no-business-continuity-plan-to-combat-coronavirus-outbreak.html
10 https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en
11 https://www.gartner.com/smarterwithgartner/cios-ask-3-questions-before-updating-strategy-post-pandemic
12 https://itic-corp.com/itic-poll-human-error-and-security-are-top-issues-negatively-impacting-reliability/