How to Ensure **IT Resiliency** and **Business Continuity**

Consolidated Communications
In the past, organizations focused on how quickly they could recover from unexpected IT outages. Creating a disaster recovery plan became a must-have strategy for minimizing downtime and its detrimental effects on the business. Today, however, successful businesses are concentrating their energies on business continuity – ensuring that critical systems and information remain connected and available across all company locations at all times.

The idea behind business continuity is to keep your operations running, regardless of disruptive events. These events could be any number of things that cause an equipment component to fail or data center facility to lose power.

This white paper will focus on a number of relevant topics related to business continuity, including:

- What Causes Data Center Outages?
- The Impact of Power Outages
- What Can Your Organization Do to Prevent Downtime?
- How to Choose the Right Data Center for Business Continuity

Because data centers handle mission-critical operations, they need to remain available on a continuous basis. The following information will help you understand the importance of protecting your data center infrastructure to maintain business continuity.
Many IT managers believe the bulk of power outages result from natural disasters. And, because natural disasters may be rare events in many locations, these managers may erroneously believe their data and equipment are relatively safe. However, this line of thinking doesn’t match reality.

In a 2013 study by the **Ponemon Institute**, 83% of participants knew the root cause of an unplanned outage. As it turns out, natural disasters were not among the top reasons. Instead, the study reported the most frequently cited root causes of data center outages were uninterruptible power supply (UPS) battery failure (55%), UPS capacity exceeded (46%) and human error (48%). In addition, 52% of the respondents believed most, if not all, of the unplanned outages could have been avoided by investing in better equipment, improving security and/or increasing the business continuity budget.

No doubt an unplanned outage is one of the worst things that can happen to a data center. Many unforeseen circumstances, including natural disasters and even acts of terrorism, can cause outages. However, research indicates the majority of data center outages are caused by one or more of the following factors:
- **Human Error** – A mistake can happen if an unauthorized person is granted access to a room housing sensitive IT equipment. For example, what if the janitor accidentally unplugged a server to run the vacuum or someone accidentally hits the EPO (Emergency Power Off) button? In addition, authorized IT personnel also make mistakes. It’s not uncommon for a technician to cause an outage. In addition to the findings in the Ponemon Institute study cited earlier, an article in *Data Center Journal* found human error results in more outages each year than network or facility design issues.

- **Lack of Tested Procedures** – A good number of data center managers have not developed formal operational procedures to manage the complexities inherent in data center facilities. In addition, they fail to test these procedures on a regular basis.

- **Insufficient Maintenance** – Maintenance of emergency backup equipment, such as replacing UPS batteries, is critical to ensuring business continuity. However, data center staff often lack properly developed procedures indicating when and how equipment should be maintained.

- **Lack of Redundancy** – Without redundancy, you are at risk for a single point of failure. Yet, many data centers do not house multiple back-up systems at each site, such as generators, UPS, and cooling systems.
• **Generator Performance** – If commercial power becomes unavailable, emergency power systems need to manage the computer loads, air conditioning, telecom operations, emergency lights and other electrical requirements. Typically, a centralized UPS is configured to sense a power interruption and switch to battery backups. At the same time, the UPS communicates with the backup generator, which comes online and assumes the electrical load. However, if the generator is not sufficiently sized or does not have enough available fuel, continuous operations cannot be guaranteed.

• **Capacity Limits** – An increased demand for IT applications typically requires additional servers and/or greater rack densities. However, the existing IT infrastructure, including cooling systems, may not be able to support this growth. When IT demand outgrows the supporting infrastructure the risk of downtime significantly increases.

• **Power Anomalies** – Power quality can vary across utilities, yet many data center operators don’t invest in the equipment necessary to minimize inconsistencies. Power disruptions, including spikes and surges, can be common occurrences in data centers.

• **Physical Security Breaches** – Data centers housing mission-critical operations may not have the necessary access controls in place. Some facilities house servers in areas that are open to the public, increasing the risk of an inadvertent or purposeful breach.

• **Location Concerns** – The location of your data center can have a significant impact on how frequently you experience power outages. Some locations are more susceptible to floods, weather, seismic activity, power grid problems and other risk factors. In addition, a secondary disaster recovery site located near your primary site will be subjected to the same risks.

• **Building Issues** – When designing a facility, some data center operators don’t consider the location of functional areas or actual capacity requirements. For example, housing critical equipment near bathrooms increases the risk of flooding. In addition, lack of capacity in air conditioning systems can lead to equipment overheating.

• **Insufficient Budget Resources** – According to the Ponemon Institute’s research, many large companies spend 2% to 4% of their dedicated IT budgets on preventing outages. Without this investment, organizations are at greater risk to incur losses associated with IT infrastructure failure.
CHAPTER 2:  
The Impact of Power Outages

POWER DISRUPTIONS OR EQUIPMENT FAILURES CAN CAUSE A WIDE RANGE OF CONSEQUENCES IN A DATA CENTER

As a result, your facility may suffer from a partial or complete shutdown, sub-par operation, unacceptable performance of data center equipment, damaged equipment and more.

However, the real impact comes in the form of additional costs. In the Ponemon Institute’s studies on downtime costs, the research organization identified several core process-related activities that can incur significant expenditures during an outage. These costs include:

- **Detection cost** – Discovering and investigating the incident.
- **Containment cost** – Preventing an outage from spreading.
- **Recovery cost** – Bringing networks and core systems back online.
- **Response cost** – Determining all after-the-fact incidental costs associated with recovering from the disruption.
- **Equipment cost** – Purchasing new equipment and repairing and refurbishing existing equipment.
- **IT productivity loss** – Including the lost time and related expenses of downtime.
- **User productivity loss** – Assessing the lost time and related expenses of end-user downtime.
- **Third-party cost** – Hiring contractors, consultants and other specialists to help resolve unplanned outages.
- **Lost revenues** – Calculating the total revenue loss from customers and potential customers because they could not access core systems.
- **Business consequences** – Factoring in the total economic loss attributed to reputation damage, customer churn, and lost business opportunities.
In many instances IT managers fail to account for the total economic impact of unplanned outages. The true cost of downtime is typically under estimated, therefore, organizations are unaware of the crippling financial consequences. The following eye-opening statistics were calculated from the 2013 Ponemon Institute study:

**Downtime costs the average company in the U.S. nearly $8,000 per minute, a 41% increase over the previous 2010 statistics.**

![Downtime Costs $8,000 per minute](image1)

![Average Outage $505,502 per incident](image2)

Outage costs range from $38,969 to $1,017,746 per organization, with an overall average cost of $505,502 per incident, depending on outage duration and facility size. Here is a breakdown of the average costs associated with particular types of outages:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT equipment failures</td>
<td>$750,326</td>
</tr>
<tr>
<td>UPS system failures</td>
<td>$687,700</td>
</tr>
<tr>
<td>Water, heat or cooling equipment failures</td>
<td>$489,100</td>
</tr>
<tr>
<td>Backup generator failures</td>
<td>$463,890</td>
</tr>
<tr>
<td>Weather-related downtime</td>
<td>$395,065</td>
</tr>
<tr>
<td>Personnel errors</td>
<td>$298,099</td>
</tr>
</tbody>
</table>
The average cost of activity categories associated with downtime include:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business disruption</td>
<td>$179,827</td>
</tr>
<tr>
<td>Lost revenue</td>
<td>$118,080</td>
</tr>
<tr>
<td>End-user productivity</td>
<td>$92,226</td>
</tr>
<tr>
<td>IT productivity</td>
<td>$42,530</td>
</tr>
<tr>
<td>Detection</td>
<td>$22,347</td>
</tr>
<tr>
<td>Recovery</td>
<td>$20,884</td>
</tr>
<tr>
<td>Equipment costs</td>
<td>$9,063</td>
</tr>
</tbody>
</table>

Most every organization in the study had at least one outage in the past two years, averaging 2.48 complete shutdowns with an average duration of 107 minutes.

Only 37% of study participants believed they had ample resources and planning in place to maintain full data center functionality during an outage.
Although it’s impossible to completely eliminate outages, you can take steps to mitigate the consequences of downtime and ensure business continuity. Here are proven ways to minimize the losses that can result from an unexpected outage:

• **Develop a Comprehensive Plan** – Your IT leadership team must adequately address the impact to your data center facility, equipment and business operations. To resolve power outages in a timely manner, emergency procedures are necessary to minimize detrimental consequences. These procedures should list the steps to be taken during any given type of emergency.

• **Maintain All Systems Regularly** – Many experts believe regular maintenance of your data center systems is the most important strategy for ensuring high availability. This includes regularly testing primary and backup power systems under a full electrical load, conducting frequent inspections, following manufacturer recommendations and benchmarking performance over time. If you test your infrastructure quarterly or even annually, you’ll be much better prepared to minimize the effects of an unplanned outage.

• **Update Maintenance Procedures** – Comprehensive maintenance documentation is essential to all data center operations. Data centers are dynamic environments with new systems and infrastructure components being added all the time. When these additions take place, you need to update your documentation accordingly.
• **Train On-site IT Staff** – Access to trained personnel is a core requirement if you want to avoid outages due to human error. Your IT staff should be well-versed in their day-to-day responsibilities, but also trained to respond quickly in worst-case scenarios. This is especially critical if you contract with a third-party for data center maintenance. For example, if you rely on your equipment manufacturers to provide the necessary expertise in a power emergency, you may experience a much longer recovery time. You want trained, knowledgeable personnel available before, during and after an outage. Prepared people can be your most important data center asset.

• **Automate Routine Tasks** – Performing tasks, such as configuring and managing systems, should be automated whenever possible. Eliminating manual operations reduces outages caused by human error.

• **Locate Systems in Secure Locations** – To prevent unauthorized access, you should locate your primary and backup power systems in secure areas. Your facility must also include sophisticated access control systems to ensure that only authorized personnel gain entry. Using a secure, hardened data center environment to store your servers will help keep your core operational programs up and running.

• **Create a Secondary Data Center** – Ideally, you should have a secondary, geographically-diverse data center so that if something happens in one location, your IT operations can failover to the alternate data center.

• **Implement Adequate Redundancies** – In addition to housing important resources in multiple locations, business continuity requires high levels of redundancy within each location. You want backup sources for power, connectivity and cooling, as well as the technical support necessary to manage it. Because equipment failure is inevitable and the costs of an outage are substantial, 451 Research believes organizations should invest in redundancy.

• **Ensure Clean Power** – Sophisticated IT equipment requires consistently clean power. However, power coming from commercial sources often needs to be conditioned and filtered. Because power quality can vary greatly, data center managers must invest in equipment that minimizes power anomalies such as voltage and frequency fluctuations, sags, spikes, surges, brownouts, and blackouts.
Selecting a data center colocation service provider to house computer systems, networking and other technology components is a complex and critical decision for any organization. With the right provider, you can improve the reliability of your IT infrastructure and minimize the risk of an unplanned outage. When choosing a provider, you should consider these factors:

• **Location** – An off-site data center should be located in an area with a low risk of natural disasters, minimal adverse weather conditions, an adequate transportation infrastructure, and more.

• **Reliability** – The data center should eliminate points of failure by integrating multiple levels of redundancy. Be sure to check the provider’s track record on outages, availability and service level history, as well as its maintenance procedures.

• **Commercial Power** – A resilient data center will provide diverse power feeds from utilities into the facility. If one feed is compromised, another feed can keep operations running.

• **Network Availability** – Access to a reliable network and high-speed connectivity is a major benefit for businesses.

• **Physical Security** – The right data center provider will implement multiple levels of physical security inside and outside the facility. External physical security measures, such as barriers, reduce the likelihood of vandalism or break-in while sophisticated access control and monitoring systems can prevent unauthorized access to secure areas.

• **Staff Expertise** – The best data center providers will employ experienced, knowledgeable and highly skilled IT staff. The right solution will offer support staff around-the-clock, every day of the year.
• **Scalability** – Should you need more space, power or bandwidth, a highly scalable data center will be able to deliver a solution to meet your short- and long-term growth requirements. You can’t risk disrupting your operation during space reconfigurations.

• **Facility Amenities** – For the comfort, safety and productivity of your IT staff, you should evaluate the facility’s features. Since your employees may be required to work long hours at the data center, they will appreciate customer accommodations, such as workspaces and conferencing facilities.

This list is by no means comprehensive. However, it provides a good foundation for evaluating the data center colocation facilities that will best meet your business continuity requirements. Your final selection of a provider will depend on your unique business model, IT infrastructure and the priorities established by key stakeholders in your company.
CHAPTER 5:

Why Consolidated Communications?

NETWORK.

Consolidated Communications, Inc. (CCI) is a leading provider of business communications technology throughout the country. CCI combines the unique benefit of an expansive fiber network across 24 states with local, responsive support to deliver powerful, customer-focused solutions to the organizations we serve. Businesses rely on CCI to help them stay competitive and productive while also keeping their data safe and secure. As a customer, you can count on CCI to help you:

- Enhance productivity
- Meet business goals
- Improve efficiency
- Extend IT resources and expertise
- Gain peace of mind
- Simplify technology

RELIABLE.

If five nines are important to your business, then CCI is the provider you should trust. CCI delivers reliable, consistent data communications systems that keep your business up and running at all times. With more than 36,000 fiber route miles, our network is the most extensive in the nation and our systems are monitored and managed 24/7/365.
LOCAL.

CCI maintains a local presence in every market we serve. Businesses are backed by professional support staff around the clock so that if a problem arises, we’re there to fix it for you. We’re also committed to our communities. With more than a century of service, Consolidated Communications has forged a strong legacy and tradition of philanthropy. Whether it’s through donations that bring technology into classrooms, events that support critical community needs or programs that feed hungry children in the community, we are proud to be a leader in giving back to the communities we serve.

MORE THAN A NETWORK.
THE SERVICE PROVIDER YOU’VE BEEN LOOKING FOR.

We can do much more for your organization than provide data transport and availability at the desired speeds to all your locations. We can help you use technology in smart ways that improve operations and save you time and money. With Consolidated Communications, you can focus more on running your organization, and use your IT staff more strategically, by outsourcing some or all of your IT operations, from routine to complex. For example:

1. **Converge voice and data onto a single network.** CCI’s VoIP services deliver a modern business-class phone system with mobile- and cloud-based features. We offer two VoIP options: Hosted PBX and SIP Trunking. Both options simplify network requirements, provide access to enhanced features and lower operational costs.

2. **Use data center colocation for savings and protection.** We’ve already made the capital investment in a physically secure, state-of-the-art data center, so you don’t have to. Experience ultimate peace of mind by working with Consolidated Communications for your primary data center or secondary site for redundant computer operations and data backup. If you experience a serious failure or disaster at the office, your organization can stay up and running with the right solution.

3. **Free up your resources and rely on CCI expertise to extend your IT team.** We have skilled personnel to help you with remote-hands tasks at our data center. With our experienced Advanced Services team at your fingertips, your IT staff has more time to develop new applications and address strategic priorities.

consolidated.com | 844.YOUR.CCI