How Proactive Business Continuity Can Protect and Grow Your Business

A CenturyLink White Paper
How Proactive Business Continuity Can Protect and Grow Your Business

For most companies, business continuity planning is instantly equated with disaster recovery – the reactive ability of a business to continue its operations following an unplanned disruption. However, the new imperative for business continuity is the optimization of business efficiency. As a result, the reactive mindset around business continuity has evolved to include proactive and preventative planning, as shown in Figure 1 below, that provides an additional benefit beyond disaster recovery and resiliency. Rather than waiting for an outage, proactive business continuity practices create a networking platform that monitors even minor degradations and other dynamic changes in a network’s operations. Taking this approach, companies deploy a resilient platform for business communications that transcends traditional business continuity by accomplishing goals in four key areas:

- Security – Plan for potential vulnerabilities and deploy solutions that maximize flexibility without sacrificing security.
- Reliability – Keep critical business functions running 24/7/365.
- Adaptability – Develop continuity plans built for today but ready for future business needs.
- Efficiency – Ensure continuity of networks and operations in the most efficient way.

The result is a networking platform that is not only resilient but continually optimizes operations to protect and support the growth of a business. Small to medium-size businesses are prime beneficiaries of this approach. With smaller IT staffs to handle patches, upgrades and disaster recovery planning, they are more susceptible to severe business-impacting events. As a result, they are often challenged to keep costs low while delivering high levels of customer service.

This paper summarizes how businesses can employ this planning strategy and how this optimization can yield substantial benefits during the normal course of operations – not just during a disaster or outage.

centurylink.com/business
Changing the Focus of Business Continuity

Today many businesses operate on the premise that business continuity plans are a necessary expense or insurance to mitigate the rare events that create business outages. While this is prudent, it misses an opportunity to use some of the same technology and planning process to become a revenue generator versus a cost center. In Japan, post-World War II businesses used the word “kaizen” to refer to a philosophy of continual improvement across every aspect of a business’ operations. A proactive approach to business continuity is similar in that it’s designed to make constant improvements in business communications as the dynamics of the network change, and becomes part of the organization’s culture.

Rather than waiting for full outages or disasters, this methodology recognizes that minor changes and degradations in the data network can be identified before they become major issues. It also provides continual opportunities to make adjustments to improve performance, security, and reliability.

The core of a sound business continuity strategy involves detailed planning to understand what components of the business are mission-critical, what events are likely to disrupt operations, and what preventative measures can be applied so the number of business-impacting events is greatly reduced or eliminated. Instead of creating and maintaining a separate business continuity planning function, organizations should integrate this planning into their existing business planning cycle. This ensures that opportunities for improvements are recognized and integrated into the business. Figure 2 below illustrates the continual, iterative process of business continuity planning, which can be integrated into an enterprise’s regular business planning process.

Figure 2: The iterative process of business continuity planning can be integrated into existing business planning, helping drive efficiencies throughout the business and becoming part of the organizational culture.

centurylink.com/business
Business continuity planning includes identifying the resources – people, communication systems, facilities, and IT infrastructure – that are required for the business to function, as well as developing a plan to ensure they run without interruption. Integrating business continuity into standard business planning drives efficiency through many aspects of business operations.

Some of the principles applied in proactive business continuity include:

- Event mitigation – Use of a distributed security model that enables remote offices, partners and workers to collaborate securely, but also proactively monitors, detects, and mitigates breaches or attacks.
- Full resource utilization – Utilize redundant capacity and infrastructure in running everyday business, and make use of features like Class of Service so mission-critical applications are prioritized and overall efficiency is improved.
- Planned resiliency – Build in resiliency as part of the core network; proactively anticipate failure in a network by dynamically accessing alternate routes on demand.
- Virtualization – Distribute communications, data, and computing resources across locations to improve reliability.

These principles help a business evolve from being reactive to a proactive stance.

Four Cornerstones of Proactive Business Continuity

Sound business continuity planning consists of developing strategies to meet goals in four key areas: Security, Reliability, Adaptability and Efficiency. Only when the business requirements of a company are fully understood can planners effectively develop the corresponding IT requirements in these four areas.

<table>
<thead>
<tr>
<th>Business Needs</th>
<th>Business Continuity Strategies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td><strong>Adopt layered security model</strong></td>
</tr>
<tr>
<td></td>
<td>- Employ MPLS VPNs for corporate WAN security</td>
</tr>
<tr>
<td></td>
<td>- Use Secure Internet Access for distributed locations</td>
</tr>
<tr>
<td></td>
<td>- Fend off distributed denial of service attacks with carrier Ethernet and MPLS</td>
</tr>
<tr>
<td><strong>Reliability</strong></td>
<td><strong>Tap into Ethernet services for backup</strong></td>
</tr>
<tr>
<td></td>
<td>Built-in redundancy</td>
</tr>
<tr>
<td></td>
<td>Keep business running</td>
</tr>
<tr>
<td></td>
<td>Early intervention</td>
</tr>
<tr>
<td><strong>Adaptability</strong></td>
<td><strong>Use MPLS to prioritize delay-sensitive applications</strong></td>
</tr>
<tr>
<td></td>
<td>Deploy new applications quickly with IP Convergence</td>
</tr>
<tr>
<td></td>
<td>Scale instantly with Ethernet</td>
</tr>
<tr>
<td></td>
<td>Automatically reroute traffic with MPLS</td>
</tr>
<tr>
<td><strong>Efficiency</strong></td>
<td><strong>Utilize secondary or redundant circuits for everyday business</strong></td>
</tr>
<tr>
<td></td>
<td>Deploy two hot sites that fail over to each other</td>
</tr>
<tr>
<td></td>
<td>Tap into MPLS VPNs for IP Convergence</td>
</tr>
</tbody>
</table>

*Figure 3: Sound business continuity planning consists of developing strategies to meet needs in four key areas.*

centurylink.com/business
Security
The nature of business mandates distribution of data, processing and people, but this landscape is constantly shifting. Today’s businesses are highly dynamic in nature as the network access of partners, suppliers, customers, and employees are in a constant state of change. As a result, security configurations and policies struggle to keep up with this dynamic environment. This leaves organizations at risk of disruptions due to unintended internal security vulnerabilities or external threats such as Distributed Denial of Service (DDoS) attacks and other intrusions, which are a growing cause of business interruptions and outages.

In this environment, IT security planning shifts from a perimeter-based design that is used when all resources are centralized to an architecture that provides distributed security at the periphery of a network. This approach to security is layered and establishes hardware-based defenses in the datacenter, software defenses at the periphery, and network-based firewalls that together provide higher levels of security.

MPLS VPNs for Corporate WAN Security
MPLS VPNs are purpose-built to provide secure access to a corporate WAN on a nationwide basis. MPLS VPNs apply labels to data packets to establish label-switching paths between destinations. The labeling scheme is not publicly visible and the traffic is therefore isolated, reducing any chance of interception by potential attackers. The Layer-3 routing schemes are maintained by a service provider who pre-programs the network with failover routes to be used in the event of an outage or other threat that compromises a connection. The MPLS routing tables maintained by the service provider reroute traffic over different paths or to a failover facility, with complete transparency to end users. This inherent failover capability provides resiliency in the event a security compromise makes a primary route unusable. For those with more stringent requirements, MPLS VPNs can operate using additional encryption through the use of SSL or IPSec.

Secure Internet Access for Distributed Locations
Secure Internet Access is another way to ensure that locations in a distributed network have a safe connection to the Internet. Deployment of a hardware-based firewall ensures that a company’s connection to the Internet is not visible and prevents unauthorized intrusion from the public Internet to the private LAN behind it. The Achilles heel of firewalls is a rule set that establishes what type of traffic can enter and leave the LAN. This set of policies is established by an administrator and can be fairly complex and demanding from a maintenance standpoint. Since many remote locations lack onsite IT personnel, many companies outsource firewall management to a service provider who handles deployment, integration and ongoing maintenance along with Internet access. This managed services approach to Secure Internet Access can lower the total cost of ownership while ensuring that the firewall is always properly configured and able to block threats from the Internet.

Ethernet and MPLS for Fending Off DDoS Attacks
Finally, with the use of carrier Ethernet services and MPLS, businesses can scale networks to multiple Gbps, well beyond the SONET speeds of OC-3 (155 Mbps). Through a brute-force strategy, this approach can help companies weather a DDoS attack while attacks are identified and traffic is blocked.

Sound business continuity planning assumes there will be failures of software, hardware, and transport. Yet planning and managing a system that proactively anticipates failure and dynamically adjusts to it is challenging.
Reliability
Sound business continuity planning assumes there will be failures of software, hardware, and transport. Yet planning and managing a system that proactively anticipates failure and dynamically adjusts to it is challenging. Managed Network Services provide the ability to gain not just assurance in the face of an outage but ongoing optimization of communications. For many companies, the reliability of voice and data communications is achieved by maintaining a backup set of dedicated lines for use in the event the primary set fails. While effective, this approach doubles operating costs as having a backup dedicated line is typically the same cost as the primary line. Depending on the network architecture those costs could be multiplied as a company could require several backup lines for separate voice and data connection. A more economical approach can be found in the use of Ethernet services for WANs.

Ethernet Services for Backup
Ethernet services provide businesses the opportunity to use Ethernet to form point-to-point connections to be used in the event a primary link fails. Of course, preserving a backup copy of data is critical for resiliency. Because Ethernet is typically priced more economically than dedicated lines, it is an excellent choice for creating redundant circuits that connect to an alternate set of servers. This can be accomplished by using the Ethernet circuit as a backup to infrastructure operated by the company, or alternatively, the backup infrastructure is maintained by the service provider in a co-location facility.

When used to connect a TDM or IP PBX to a Session Internet Protocol (SIP) Gateway to enable Voice over IP (VoIP), Ethernet also becomes a viable choice as a failover for voice communications. For networks that opt to combine voice and data through IP Convergence, a single Ethernet circuit can serve as backup for both voice and data communications.

Adaptability
Rather than just reacting to a large-scale outage, proactive business continuity dynamically adapts to network conditions. While this adaptability provides uptime during an outage, it also delivers the benefit of constant improvement of communications that ultimately drives business performance. One way this is accomplished is through the unique labeling scheme used in MPLS. Label switching provides the ability to create Class of Service (CoS) classifications. Through that approach, delay-sensitive applications such as voice and video can be prioritized in the event that network conditions degrade. This adaptation to changing network conditions is done dynamically and is transparent to the end user.

Another example of adaptability is in the ability to quickly deploy new applications to maintain a competitive edge. Web applications, voice, and video have all migrated to IP as a standard transport. Industry-wide, innovations are developed on IP sooner and businesses can gain competitive advantages more quickly on an IP converged network.

Ethernet services also deliver adaptability in the way they can scale from Mbps to Gbps. Unlike leased lines, this gives businesses the ability to always have enough capacity on tap so they are never victims of their own success. A final example of adaptability is found in the inherent ability of MPLS to automatically reroute traffic over different paths or to a failover facility, completely transparently to end users.
Case Study: City of Lorain Achieves Business Continuity

CenturyLink has worked with many organizations of varying sizes to help them meet the goals outlined in the four sections above. One example of a successful business continuity strategy is demonstrated in the City of Lorain, the 10th largest city in Ohio, 30 miles outside Cleveland.

Lorain’s IT team manages critical data and networking systems for police, fire, city departments and utility functions. The city had poorly performing databases, along with issues with the performance and the availability of network access. The IT department needed to centralize data while making it available in a highly secure manner. In addition to data networking requirements, Lorain had mission-critical voice networking requirements as 911 services need to be always available.

CenturyLink deployed a solution that relied on a Metro Ethernet network to enable high-speed access to data as well as the interconnection of an IP-based PBX handling over 300 phones. CenturyLink’s design for Lorain deployed clustered databases, mirroring data to create fully redundant, readily accessible primary and backup databases. To secure the infrastructure, CenturyLink deployed a managed firewall solution to identify and eliminate viruses before they caused disruptions.

Efficiency

Organizations can tap into a few options when it comes to ensuring efficient operations. The first is the way that secondary or redundant circuits are used. Many enterprises relegate these to standby mode. However, by utilizing them for everyday business, organizations can increase capacity and provide users with better access. The same approach can be used in the case of site redundancy. Instead of deploying one primary and one secondary data center, deploy two hot sites that fail over to each other. This strategy allows the organization to efficiently use all resources and proactively build in redundancy as an integrated part of the business, rather than as an adjunct process.

IP Convergence also offers opportunities for efficiencies. IP convergence strategies combine voice, video, and data and simplify business continuity by making uniform use of IP for all applications. It delivers an additional benefit of making more efficient use of resources for multiple applications, rather than maintaining separate networks for voice, video and data for each, which duplicates time, effort, and cost. The standard use of IP helps companies centralize management and better control costs while improving collaboration and the adoption of new business applications.

VoIP is a frequently cited example of convergence as it enables businesses to cut costs by interspersing digitized voice packets with IP data packets. When voice traffic is idle, data uses that capacity and when voice traffic picks up, it is prioritized over data. Businesses can standardize on a single Mbps model for both voice and data and make more efficient use of the uniform transport.

Yet with the promise of IP Convergence come the challenges. The migration to an all-IP network may prove difficult for businesses that operate a wide mix of protocols such as Frame Relay, ATM, and legacy connections. These separate networks with their individual billing schemes and management systems can more than duplicate management effort and costs. MPLS VPNs provide the ability to encapsulate the varying protocols in “labels,” creating a uniform transport method for all of a company’s traffic. The result is that businesses use fewer resources and operate at a lower cost per Mbps when using an all-IP infrastructure. Adding and moving locations, supporting remote users, and increasing capacity are all simplified.
Summary

Business continuity planning should be part of a business’ regular planning processes, and embedded into the organization’s culture. Companies need to look past the response to an outage to include ongoing optimizations that reduce the chance of a business-impacting event while also improving the overall operations of a business.

CenturyLink’s suite of services is designed to address the four areas of security, reliability, adaptability, and efficiency, the key elements of a business continuity solution. The result is a networking platform that not only sustains operations during outages but also drives efficiency into the enterprise, continually optimizing operations to proactively prevent any degradation in service. By adopting this approach, numerous organizations have achieved their business continuity goals while driving efficiency in the process.

For more information about how CenturyLink can help you with your business continuity planning, contact your CenturyLink representative at 1-866-345-0814.

Or view our case studies at centurylink.com/stronger.