XO Communications®

BUSINESS CONTINUITY & TODAY'S "ALWAYS-ON" BUSINESS ENVIRONMENT

www.xo.com

Services: VoIP ▪ Voice ▪ Network ▪ Internet & Hosted IT

XO Communications

BUSINESS CONTINUITY & TODAY’S “ALWAYS-ON” BUSINESS ENVIRONMENT

Table of Contents

Crisis Management & Business Continuity

As the floods along the Red River in North Dakota and Manitoba receded in the spring of 2009, officials began to estimate the costs of clean up, and the costs of lost revenue to local businesses. Several cities were endangered, including Winnipeg, Grand Forks, and Fargo. One early tally estimated lost business revenue just in Fargo, a city with less than 91,000 residents, at more than $100million.1

As terrible, destructive and costly as natural disasters like floods, hurricanes, tornados, earthquakes and wildfires are, they are relatively infrequent occurrences. But disruptions to daily living and business operations occur every day. Typically, disruptions are due to carelessness or accident, but some are deliberate. Although it's impossible to ensure that natural or man-made disruptions will never impact a particular person or business, there are a number of actions that can be taken to reduce the risk level and provide a means of rapid recovery. This is the objective of sound business continuity management practices.

BUSINESS CONTINUITY MANAGEMENT (BCM)

Fundamentally, business continuity management is a set of coordinated plans and actions that mitigate and/or negate the adverse effects natural and man-made events have on key business operations.

Most companies already engage in business continuity management practices to some degree. For instance, in the U.S., occupants of large buildings are required by law to practice fire drills at regular intervals. These drills help to protect employees who work inside the building, and can also help to protect the building and its contents. Good business continuity management practices are necessary to reduce the impact of a wide range of threats. They focus on protecting and preserving employees, facilities, and key resources, including essential company information housed in storage arrays, servers and personal computers.

The success of many companies' ongoing operations depends on continuous access to key IT assets, which are usually accessed via network resources. Additionally, the ongoing functionality of important business operations, like call centers, can greatly depend upon both highly available IT and network infrastructures. To help meet these needs, XO Communications offers a broad portfolio of business continuity services. They include network protection, data and information protection, applications protection, and disaster mitigation services – all of which will be discussed in a later part of this white paper.

TYPES OF RISK TO BUSINESS CONTINUITY

Three main types of threat that can impede the continuity of business operations include those that inhibit the use of key company buildings and facilities, risks that that limit the ability of employees to work at those facilities, and threats that hamper the usefulness of key IT and network resources. Without adequate preparation, each of these critical company resources is vulnerable to natural and man-made disasters:

Facilities

The impact of natural events, like fire, floods and hurricanes can make it impossible to access a building for a prolonged period of time. Man-made events can also impede access to the worksite. In 2009, for more than a day, protests in London essentially closed the financial district, even to people who work there.[2]

Workforce

Consider these scenarios—in recent years, terrorists disrupted train, subway and bus routes schedules in major cities, making it impossible for commuters to travel to work. Of broader and longer lasting impact is a pandemic—to minimize casualties, the government could prohibit the congregation of people (at places of work and elsewhere) for extended periods of time.

IT Infrastructure

Security breaches or the unavailability of key IT and network managers can diminish the usefulness of critical business information located in data and network hubs. Without sufficient backup power, brownouts and blackouts in the electrical grid can crash servers, LAN and WAN connectivity. Natural and man-made events can damage key facilities, and thus render IT and network infrastructure inoperable. When considering the underlying causes of business interruptions, only 3 out of 100 are caused by acts of nature. In contrast, 32% of the business interruptions are caused by human error, and 65% are caused by malfunctions in IT and communications hardware, software or services. Approximately 11% of IT and network-related malfunctions are directly caused by computer viruses.[3]

Regulation

Some regulations, like Sarbanes- Oxley, have broad scope and far-reaching impact on business continuity and disaster recovery planning. Among other provisions, it mandates that publicly-held companies engage in certain business continuity practices, particularly pertaining to data storage and archival. In some industries, possible risks to their business operations are so great, and their potential impact so pervasive that specific regulations have been enacted to minimize their existence and effect. For instance the Health Insurance Portability and Accountability Act (HIPAA), Federal Energy Regulatory Commission (FERC), Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standard (PCI DSS), the Basel II Accord and the Graham-Leach-Bliley Act each contain requirements designed to assure the continuation of key business operations in particular industries.

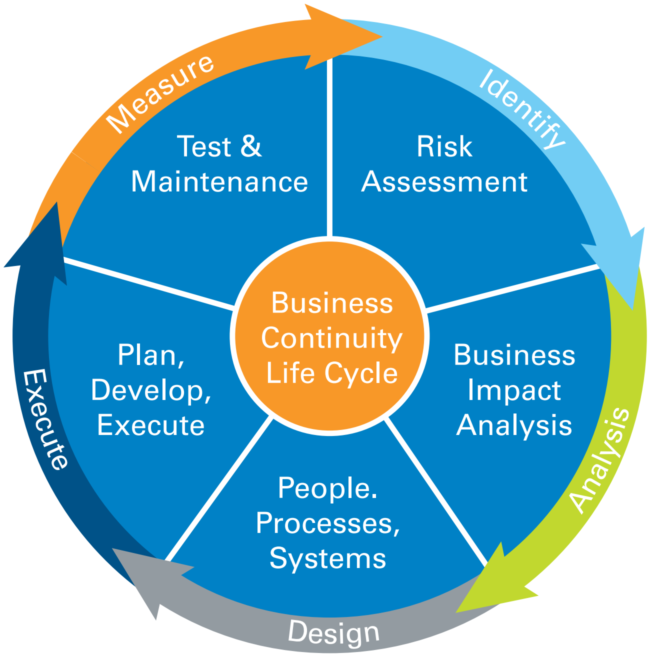

Figure 1: Business Continuity Life Cycle

ELEMENTS OF BUSINESS CONTINUITY PLANNING

Key components of a business continuity plan include documentation of the business operations that are included in the continuity strategy, their threats and regulatory requirements, and mediation and remediation activities. The plan identifies the resources and personnel which compose the business continuity team. These can be internal resources and personnel, and/or external ones. It also contains information on the ROI of each business continuity action. If certain internal or external company locations are designated to act as alternate locations for some business continuity activities, this must also be documented. Finally, to ensure continuity in the planning process over time, some companies may elect to include an appendix that lists business operations that were excluded from the continuity plan, and the reason for their exclusion. **Figure 1** shows the Business Continuity Life Cycle that businesses can use to conceptualize their approach to business continuity planning.

EFFECTIVE BUSINESS CONTINUITY PLANNING STRATEGIES

Effective business continuity strategies rank the potential effects of various threats to ongoing business operations. They also employ both proscriptive and prescriptive remediation techniques, and use business case framework to assess and compare risk and remediation costs:

Rank Risk

Each organization should identify its key business activities and determine how long they can be forgone without adversely impacting the company or its customers. In addition to ranking these events by time, they also must be ranked by their financial impact. When combined, companies use these two factors to assess high-medium-low risks. For instance, an event that has immediate impact but is financially small poses low risk and thus also has a low recovery objective.

Employ Both Risk Avoidance and Remediation Tactics

To optimize the effectiveness of a business continuity plan, effective strategies typically contain both proscriptive and prescriptive elements.

- ***Proscriptive.*** To maximize agent productivity, it's fairly common for companies with large call center operations to deploy them in diverse geographic regions, and to use IT and network technology to route or transfer calls between the centers. Proscriptively, if employees can't get to their normal workplace during a blizzard, agents in other centers can handle their calls. This essentially brunts virtually all of the adverse impact to customers.
- ***Prescriptive.*** Companies that employ just- in- time inventory practices can be vulnerable to disruptions experienced by primary shippers. Some of these businesses have made advanced arrangements to obtain critical inventory via alternate shippers. A delay in receiving inventory will occur, but it won't be as disruptive as if no plans had been made.
- ***Proscriptive and Prescriptive.*** Many organizations back up critical IT data and processes, often in more than one location. Such a strategy contains both risk avoidance and business recovery elements.

Understand Total BCM Return on Investment (ROI)

Companies will develop and execute plans based on the level of risk to ongoing business operations, recovery objectives, *and* their avoidance and mitigation costs. In the inventory example above, the company implemented processes to reduce, not eliminate, the impact of disruptions with primary shippers who supply critical inventory. In theory, the company could employ other methods to reduce the risk of running out of inventory, including stocking large reserves on premises. But it has calculated that the costs involved in such possible solutions outweigh the risk and costs of its preferred approach

Key Stakeholders

The plan lists by name and function each member of the business continuity team, their contact information and alternates. The plan also contains information on their performance metrics. Without the involvement of key executives, a business continuity strategy runs the risk of being nothing more than a document that gathers dust. Good contingency plans assume that key executives won't be able to fulfill their normal duties during a crisis, and designates and trains alternates.

Training

Key internal and external personnel and their alternates must be trained on the business continuity strategy and plan, and their roles in fulfilling its objectives. This includes key executives. The company should conduct drills to familiarize personnel with plan enactment, and to identify, remediate and re-test any weaknesses in the plan.

XO Business Continuity Services

To help companies assure that key business operations that depend on highly available IT and network resources aren't impacted by natural and man-made crises, XO Communications offers a broad range of services that can help protect IT applications, company data and networks.

XO NETWORK PROTECTION SERVICES

When considering business continuity management practices, most companies assume the focus of their IT infrastructure protection efforts will be on data network preservation and restoration. And for small, medium and large companies across diverse industries, this often is the case. However, some companies' key business operations also depend upon the continuous availability of voice services. Companies with contact centers that support inbound or outbound sales, or customer service, are clear examples. It won't take very long for a company to begin to lose revenue if its customers can't communicate with contact center representatives during normal business hours. In addition, employee access to internal resources, like IT help desk or HR, can also depend on voice services. Particularly in emergencies like hurricanes or tornados, these can be vital resources for affected employees, and thus for the ongoing operation of the business.

Many smaller businesses, or those with one primary location, may assume that network protection services are only needed by medium and large companies—that it's unlikely that a single site won't have access to the network for any lengthy period of time. But if a backhoe mistakenly takes out the main electrical or communications links into a building, that business location will be off the grid for at least several hours, and probably much longer. And just like some man-made threats, many natural events, like fire, tornado and flood, can render a site unusable for days, weeks or months. Thus in some cases, companies with only one main business location are more vulnerable to business continuity threats than are larger companies with several main business sites.

Companies who are interested in assuring network continuity will find that XO has a very broad portfolio of services designed to protect both voice and data networks. And since these networks connect to IT resources through network access and premises equipment like routers, XO offers a range of services to protect these assets as well. They include:

Voice Network Resiliency Services

XO offers a range of services to support inbound and outbound calling requirements:

Inbound Call Re-Routing
XO offers several different automatic call re-routing features designed to protect important inbound calls and contact center applications. In addition, some companies make extensive use of Interactive Voice Response (IVR) applications for use internally, or for use by customers, suppliers and key partners. XO provides hosted voice XML services that can be deployed on a dedicated server in XO's hosting center. For customers who are interested in minimizing costs, XO also offers hosted voice XML service on a shared platform. To assure availability, XO's resources are housed in multiple data centers deployed across the U.S.

Outbound Call Re-Routing
For some companies, their business continuity requirements dictate the preservation of both incoming and outgoing call connectivity. XO provides features to support this—for both traditional PSTN calls and VoIP calls.

Administration
XO provides customers with a broad range of tools to administer and manage their voice protection services as they need to, on a round the clock basis. These self-service tools include basic touch tone access and web-based access.

Data Network Resiliency Services

Good business continuity practices attempt to balance the costs of implementing data network continuity practices against the importance of the activity to continuing operations, and the likelihood a problem will occur. Different companies, even in the same industry, may have different cost/risk profiles. To meet a wide range of needs, XO offers a broad array of data network protection services:

Fixed Wireless Access Diversity
To ensure the ultimate in access diversity and availability, XO's Nextlink broadband fixed wireless access service can be used to backup any type of dedicated access that is connected to either voice or data services, or both.

Landline Access Diversity
At a customer's request, XO will deploy diversely routed landline access from its point of origin at the customer premises to its network node and beyond. To ensure the highest levels of continuity of key data-oriented business applications, customers may employ either landline or fixed wireless access diversity in conjunction with IP or MPLS load sharing or multi-homing networks.

Multi-Homing Networks
Companies who are interested in ensuring uninterrupted data network connectivity between select sites can use techniques like load sharing or multi-homing on both XO's MPLS IP-VPN and dedicated Internet access services.

High-Bandwidth Network Transport Solutions
Companies with very large file transfer requirements, or who are in heavily regulated industries like healthcare or financial services, will be interested in using high-bandwidth dedicated private line services to construct fully redundant, geographically diverse networks between large data centers. XO's private line services use a variety of state-of –the-art WAN technologies, including Ethernet and wavelength services.

Collocation
XO makes its highly secure, carrier grade environment with redundant power supplies available to customers for collocation. Although some companies use co-location as a backup to premises-based web and applications servers, others who want to totally eliminate the threat posed by access unavailability will co-locate key servers in XO's data centers.

Applications Performance Management
These begin with XO's three tiers of application performance management tools, which customers can use to spot and remediate potential problems in their MPLS-based networks before they do any damage.

Remote VPN

Companies who want to ensure that employees can access important computing resources without interruption will employ Internet VPN backup services, which are available on a broadband or dial-up basis.

Figure 2 summarizes the different types of data network and CPE diversity and the levels of protection they provide. **Figure 3** outlines the risks and costs trade-off for certain types of data network protection.

Capability	Medium Protection	High Protection	Very High Protection
Wireless Access as Backup			✓
Full Access Diversity		✓	
Redundant Access, Single Router	✓		
Redundant Access, and Multiple Routers		✓	
Redundant Access with Diverse Network Gateways			✓
Diverse Carriers			✓
Collocation Only	✓		
Collocation with Access Diversity		✓	
Collocation with Hardware and Access Diversity			✓

Figure 2: Protecting Access and CPE Levels of Protection

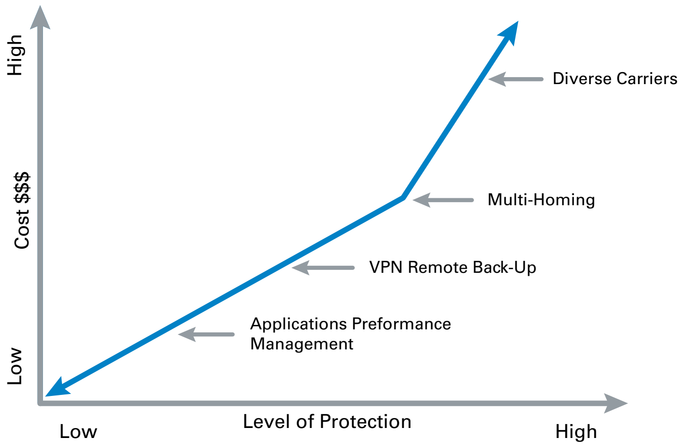

Figure 3: Risk/Cost Trade-Off for Data Protection Options

XO INFORMATION PROTECTION SERVICES

Irrespective of where they are housed, key IT and network resources must be protected against security and survivability threats. XO offers both premises-based managed services and hosted services to help protect your organization's information. They include:

Managed Backup

XO's state of the art remote backup service combines WAN and remote access resources with the resources of XO's cloud computing platform to deliver a round the clock, highly automated, efficient, cost-effective and scalable service that protects data housed in popular software like Oracle databases and Microsoft Exchange, and across a wide variety of operating systems commonly deployed in servers, desktop PCs and notebooks. By employing 128-bit AES encryption, the service is highly secure. Finally, it provides easy to use web-based tools for customers to manage and retrieve stored data.

Email Filter and Authentication

For customers that house email in their own servers, XO offers a Perimeter email Protection (PEP) service that stops spam and filters viruses before they arrive at the server. It also prevents other types of malicious behavior, including phishing, DDOS, secondary attacks, and directory harvesting. This service, developed by XO, is identical to the one employed in XO's hosted Exchange and web hosting services, and works with all major brands of email software. Critical to any business continuity strategy is planning for email server unavailability. Should the server be unable to receive email for a period of time, PEP will store up to 5 days of incoming email at no charge, and deliver it to the customer's email server as soon as it has been restored. Introduced in 2006, XO's PEP service includes companies in IT, professional services and retail industries.

Managed Security Solutions

In addition to email filtering and authentication, XO offers a very scalable, managed security solution which includes an Internet firewall service that can be located either on the customer's premises or in the XO network. The latter approach can be cost effective because it assures that access trunks are utilized only for authorized applications and users, and don't experience congestion caused by security breaches. XO's Cisco-certified managed firewall service was introduced more than ten years ago and is used by many industries, including finance, healthcare and retail. XO also offers a service that bundles managed firewall with managed VPN services.

Dedicated Web Hosting

Companies with mission-critical web applications, including e-commerce, are very interested in assuring their high survivability and availability. To support this, XO developed its own patented clustered web hosting platform. Types of industries that use XO's hosted e-commerce service include IT services, professional services and retail.

XO DISASTER MITIGATION SERVICES

Since it's not possible to prevent all crises from affecting business operations, XO also offers a range of services to mitigate their ill effect and help ensure organizations can maintain communications with employees, customers and partners during a disaster. These include:

Teleworking Services

These include tools to support both voice and data applications, enabling employees to work virtually from any location. To protect against the unavailability of key IT and network resources housed in particular facilities, XO offers network-based web conferencing, audio conferencing, voicemail and email services. In addition, by using XO Anywhere service, employees can turn any phone into their XO office phone line because the service operates independently of PBXs or key systems (these can be unavailable in the event of a facilities-related emergency). XO's VPN remote access service, discussed in an earlier section, can be used to connect remote employees to a particular location to still access its computing resources.

Multi-Media and Outbound Notification Services

Employees who are part of the business continuity team must be able to communicate with each other, and with other employees, as soon as an emergency occurs. Organizations may also need to communicate with people in other companies, with customers, or with key emergency services personnel. XO Connect, a multimedia notification service, supports the broadcast of messages across a variety of media, including text messages, email and voice calls. XO's Interactive Voice Response (IVR) services can also be used to support a company's employee notification requirements.

"Always- On" Business Environments Require Strong Business Continuity Partners

In today's "always-on" business environment, creating and implementing a business continuity and disaster recovery plan is critical in order to:

- ***Protect revenue,*** ensure employee productivity and protect your company's ability to serve its customers without interruption.
- ***Ensure compliance*** with government mandated regulations and industry guidelines that require your company to implement and maintain business continuity plans; and
- ***Proactively protect*** your company's IT infrastructure against many types of events that can negatively impact your business. Given their increasing frequency, these safeguards extend to protecting your company from security threats to IT and network resources.

XO Communications has one of the nation's largest and most technologically advanced nationwide networks. Its architecture provides a unique balance between cost effectiveness and requirements to maximize performance and availability With XO Communications as your business continuity partner, you can have solutions that deliver bottom line benefits to help you:

- Protect Your Network
- Protect Your Information & Data
- Mitigate Disruption

Objective	XO Service	Benefit
Protect My Network	Wireless Network Resiliency	Provides back-up connection via high-speed broadband wireless connections
	Dedicated Internet Access Redundancy and Re-Routing	Ensure availability of applications and access with back-up or shared IP ports when primary IP port is unavailable
	MPLS IP-VPN	High-performance private wide area network solution for primary or as "always-on" back-up network
	High-Bandwidth Network Transport	Provides additional layer of network resiliency with Ethernet and wavelength services for connecting locations and data centers
	Collocation	Provides secure back-up facilities for data center operations
	Applications Performance Management	Proactive monitoring of applications and network performance so issues can be better anticipated
	Voice Re-Routing and Redundancy Services	Ability to re-route inbound large call volumes to alternate locations or phone numbers
Protect My Information	MPLS IP-VPN	Ensures data traffic transmitted across network does not touch the public Internet
	Managed Security	Protection for data against outages from hacking and viruses
	Managed Backup	Data back-up to remote location with full restore back to primary data center
	Perimeter Email Protection	Filters and scans email to reduce spam and viruses and backs up email after an outage
	Web Hosting	Facilitates ongoing web operations during an outage because server is hosted by XO
Mitigate Disruption	Teleworking	Allow employees to work anywhere with unified communications, conferencing, remote VPN and hosted email services
	Notification Services	Provides voice and multi-media communication tools for notifying employees, customers and partners in the event of an outage

Services may not be available in all areas.

References

1. "Bill Rolls in for Red River Flooding", Minnesota Public Radio, April 6, 2009
2. "G20 Protests: Riot Police Clash with Demonstrators", the Guardian, April 1, 2009.
3. "Techniques, Tips and Technologies for Business Continuity Planning", Computer Associates webinar, 2004.