Protecting the Enterprise

Business Continuity: Why Now?

Business processes that revolve around digitally held data are vulnerable to human error, insecure external service providers, and data links to third parties. In the US, four to five federal disasters and up to 150,000 system break-ins occur each year. These and other disruptions cause loss of revenue, assets, and stock value and drive regulatory liability and recovery costs. The impact of just one hour of downtime is staggering.

Business Continuity Snapshot

Definition. Business continuity is a fundamental objective to keep vital information-intensive business processes available, within a predetermined tolerable risk threshold, to avoid disruptions and to recover from unforeseen circumstances. Business continuity is comprised of three approaches to protecting against unpredictable business threats: continuity planning, risk management and recovery preparedness. Continuity planning minimizes impacts, risk management reduces the likelihood of potential crises, and recovery preparedness enables recovery from crisis situations.

Benefits. Depending on the criticality of the application, solutions range from zero downtime to recovery within hours or days.

Costs. A fully redundant network system can cost up to 3.5 times the cost of a basic system. However, not all applications and processes require that level of investment. Overall, one quarter of companies plan to spend at least $500,000 on business continuity IT initiatives, comparable to the number spending significantly on CRM.

Less quantifiable but equally devastating losses include customer dissatisfaction and desertion, customer service failure, damage to reputation, brand and market credibility, and lowered productivity. For example, interrupted supply chain processes can result in obstructed views of demand and production, leading to excess or obsolete inventory, customer loss due to shortages, and market share loss to competitors who are more responsive.

Executed through a range of processes and technologies, business continuity helps to maintain availability for business’ critical information-intensive, application-enabled business processes that typically include Customer Relationship Management (CRM), Supply Chain Management (SCM), and Enterprise Resource Planning (ERP). These software- and network-dependent processes enable the relationships companies have with customers, suppliers, employees and partners.
Research suggests critical implementation of business continuity strategies is currently lacking in the following areas:

• Nearly one-third of organizations have no manual alternatives to their digitized data and processes.5
• One third of companies say they will lose data or operational efficiency in the event of a disaster because of insufficient planning and investment in business continuity.
• Most large businesses have a disaster recovery plan, but few plans extend and link into security and high availability to encompass all aspects of business continuity.
• A majority of senior executives think that their existing IT networks are not well-equipped to meet the array of business challenges they face over the next two years.6

However, driven by the increasingly digital and direct nature of business process and the intense expectations of customers, shareholders, employees, suppliers, and regulatory agencies for continuous operation, businesses must rapidly understand and act on the imperative for continuity planning policy and technology.5 They must make the assets that carry out business process – people, systems, and networks – invulnerable to concentrated attack and able to recover quickly and locally to change. Regulatory and industry-led efforts are now underway in such places as the financial industry, in which a market like the NYSE, that transacts over $40 billion per day in stocks of over 2,500 companies, must be protected from systemic risk.7 (See Box: Regulatory and Industry-Led Efforts Driving Business Continuity)

Regulatory and Industry-Led Efforts Driving Business Continuity

1. Financial institution proposals hint at upcoming regulations. The Federal Reserve, the Office of the Comptroller for Currency, and the SEC published a draft white paper in August 2002 on “Sound Practices to Strengthen Resilience of the US Financial System.” The paper lays out four key steps: identifying critical activities in support of critical markets; determining recovery/resumption objectives (targeting two to four hours after an event); maintaining sufficient out-of-region staff, equipment, and data within robust infrastructure; and routinely using or testing the recovery/resumption arrangements8.

2. Sarbanes-Oxley Act of 2002 accelerates the disclosure obligations of public companies. This broad auditing, financial disclosure, and corporate governance law increases reporting requirements and accelerates timetables, driving data availability and freshness needs. A lengthened statute of limitations on securities fraud drives storage requirements and recovery.

3. Health Care Insurance Portability and Accountability Act (HIPAA) of 1996 ensures privacy of personal data. This law led to security standards for healthcare providers to protect against unauthorized electronic access of health information using safeguards for storage, maintenance, transmission, and access.

Business Continuity Decisions and Considerations

Business processes within an enterprise differ in terms of their overall business value and the required performance level of the underlying application and infrastructure. Grouping processes into three categories, as shown in the chart below, is useful for selecting the right levels of business continuity:

• Some business-essential applications, online training for example, are essential long term but present little immediate vulnerability to the enterprise and may not require significant business continuity support.
• Business-critical applications might include financial, payroll, and some inventory systems that, while critical, can tolerate some short amount of downtime without jeopardizing the enterprise.
• Mission- or market-critical applications include customer-affecting and revenue-generating applications like CRM and SCM. Many businesses require zero downtime for their mission-critical applications.
Based on the required performance level and business value of the application, businesses need to mitigate risk, protect mission critical data, meet regulatory requirements, and invest wisely. Businesses often conduct an application and networking readiness assessment to guide business continuity solutions by focusing on seven key criteria:

1. Most critical business processes, applications and services
2. Impact of potential disruption
3. Continuity needs across security, availability, and recovery
4. Continuity plan testing
5. Mandated customer/partner performance or service levels
6. Current or emerging regulatory requirements
7. ROI analysis across operational, end user, and financial performance

Additional considerations and nuances of the assessment, based on observed shortfalls for many business continuity strategies in place today, include:

- Vendor reliability and contracting
- Plan/policy update and maintenance
- Risk analysis of data centers, business processes and applications (e.g., over-consolidation)
- Discreet IT asset identification and workspace recovery needs
- Risk analysis of external business partners

Across all these business continuity considerations, the network is fundamental. The management of the interconnections among applications, systems, and network infrastructures is crucial to delivering optimal business continuity solutions.

Understanding the Fundamentals of Networking

Sufficient capacity, route diversity, redundancy, and service level guarantees are the basic networking performance requirements and business continuity “table stakes”. Working with a service provider founded on network reliability, that possesses a high level of network expertise and breadth of capabilities, is the surest way to develop sound business continuity functionality. Service provider basic requirements include:

- Financial flexibility and strength to invest in servicing customers
- Track record of meeting backup/recovery metrics including recovery time, data integrity, and recovery point
- Comprehensive, system-by-system extended SLA coverage
- Ability to participate in regular reviews and updates to business continuity plans
- Efficient network provisioning (a majority of companies make changes annually to their WAN to accommodate shifts in business continuity strategy)
Businesses seeking to maximize business continuity effectiveness turn to service providers that continuously raise the bar on the basics, and provide even greater value through coordinating multiple network capabilities and providing multiple options. Raising the bar on the basic requirements means meeting several additional requirements, including:

- Truly diverse routing and geographic redundancy built in, not just deployed in SONET rings or switches, and extending to the local loop with Ethernet and optical choices
- VoIP within the network for more robust and recoverable voice communications
- Integrated network and data center asset ownership for complete control and monitoring
- Ability to handle new standards-based storage protocols that assist with networking-enabled real-time data replication

Businesses increasingly leverage new networking capabilities to extend highly reliable connectivity and comprehensive information storage to more business processes and more value chain members. These higher-value network capabilities include:

- Network designs that are optimized around application performance requirements
- Bandwidth that is deployed dynamically when applications need it
- Error correlation that pinpoints application-impacting performance issues

Only 20% of Global 2000 organizations have business continuity plans effective enough to ensure a strong likelihood of the enterprise surviving a disaster without lasting adverse impacts. Given this, business continuity decisions are both critical and strategic. Selecting a service provider capable of backing effective, high-value, holistic solutions with networking expertise is an imperative for most major enterprises. (See Box Four Reasons Using Third Party-Providers Makes Sense)

### Four Reasons Using Third-Party Providers Makes Sense:

1. **Business continuity solutions are critical, but “non-core” to most businesses** — using third parties for business continuity allows companies to deploy their own IT resources onto more strategic and “core” development work.

2. **Using third parties often provides the solution to rapidly changing IT environments and continuity needs** that, addressed in-house, would drive slow, expensive change efforts.

3. **Resident business continuity expertise, and the availability of additional professional services resources, allows third parties to speed the delivery of business continuity solutions.**

4. **In many cases, consolidating network infrastructure under one network service provider is a powerful approach to achieve higher reliability through reduced complexity, fragmentation, and inefficiency and increased end-to-end monitoring.**

### How Do Companies “Do” Business Continuity?

Until recently, business continuity strategies were self-governing and characterized by a focus on disaster recovery, reactive interventions, and periodic impact analysis. Strategies today tend to be industry- or regulatory-driven and incorporate sophisticated disaster mitigation, proactive interventions, and continuous impact analysis. This paradigm shift has heightened the need for powerful networking solutions in both disruption avoidance and recovery strategies.
**Continuity Planning:** To avoid disruption, businesses reengineer processes, establish procedures, and train employees in ways that minimize risks. They develop security policies that encompass partners and suppliers because so many processes extend outside the enterprise. They invest in technology safeguards like high availability and redundancy that bolster networks. And, they use technologies like clustering, Storage Area Networks (SANs), and software management that fit with their disruption avoidance strategy. Most critically, businesses requiring the highest levels of business continuity employ network technology like real-time fail over and monitoring tools and processes that make performance highly visible and predictable.

**Recovery Preparedness:** To recover and minimize loss from disruption, businesses also reengineer processes, establish integrated and automated procedures, and train employees through disaster simulations in preparation for recovery. Businesses prepare to steer through disruptions by adopting disciplined and interdependent management and planning that provide adaptability, responsiveness, and local autonomy. They identify which data are the most important to keep the business running smoothly in order to maximize recovery efforts. They develop IT contingency plans for disasters, but also for day-to-day glitches, unexpected traffic peaks, intrusion, and recurring application problems. They back up and standardize IT assets so recovery can proceed rapidly without interoperability or sourcing issues.

**AT&T: Business Continuity Networking Partner of Choice**

The AT&T business continuity portfolio offers options for security, availability, and recovery across the infrastructure and applications layer. AT&T integrates all of these elements into a “best practices” strategy to keep businesses up and running – and to plan for a way to recover business functions quickly if something unexpected does happen.

AT&T services, like business risk analysis, security audits and recommendations, help companies establish the appropriate levels of protection for their enterprise. Protecting business processes using network solutions is an AT&T strength. For over 100 years, AT&T has set the industry standards for network reliability: it operates highly reliable ATM, Frame, and IP networks that underpin application-enabled business processes. AT&T’s approach to business continuity coordinates its many networking capabilities to bring the most appropriate protection and greatest value to business. On top of its networking reliability foundation, AT&T delivers integrated services that cover all crucial aspects of business continuity, from resiliency at the device, network, application, and transaction level, to data loss prevention and restoration, to security.

Taking an enterprise-wide view of a company’s networking environment is a key element of AT&T’s overarching approach to helping its 4 million business customers secure their business processes. And, AT&T’s investment in disaster recovery and

![Figure 2 – Mission-Critical Applications Demand High-Performance Networking](image-url)
ongoing disaster recovery training demonstrate unparalleled commitment and best practices to providing the most effective business continuity services available. AT&T can assist in analyzing, designing, deploying and managing a comprehensive enterprise business continuity solution to meet your business application and process infrastructure requirements.

Sources:


For more information about AT&T’s Business Continuity portfolio of services, visit www.att.com/business.