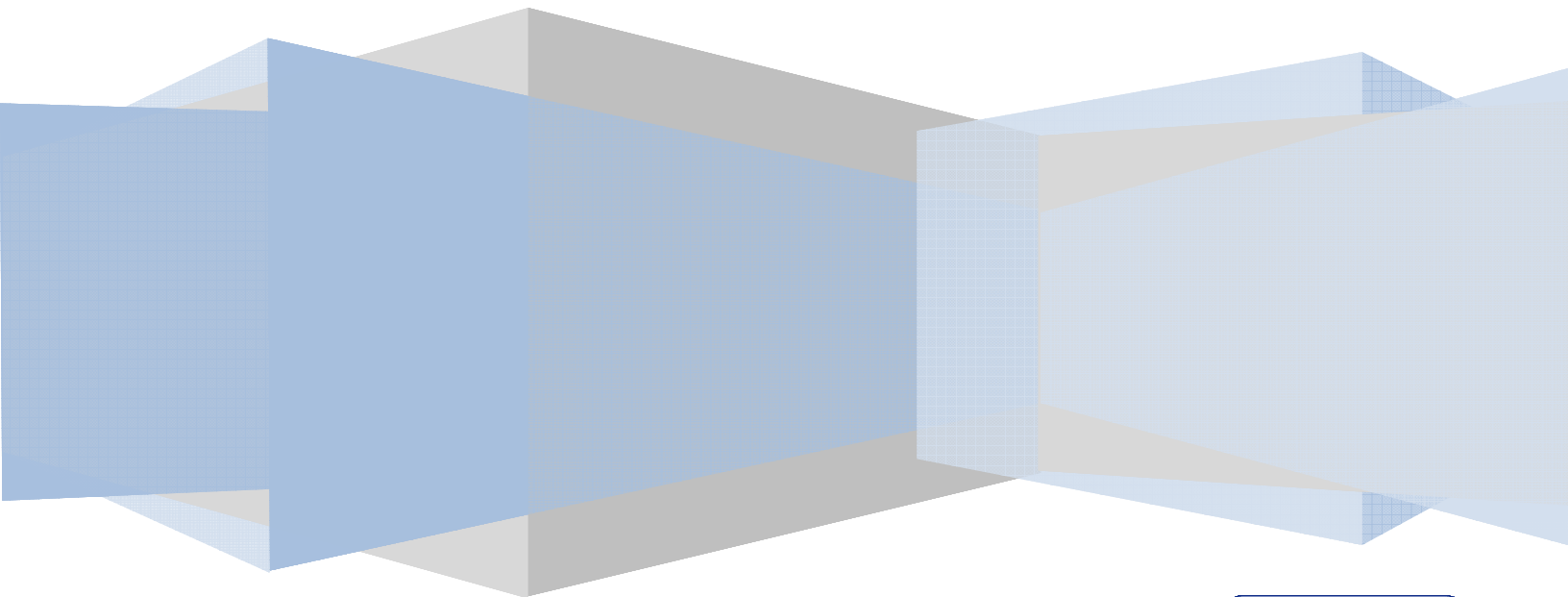


A BTS Technologies White Paper

Are You Absolutely Sure Your Critical Data is Secure?

Learn What You Can Do To Protect Your Company From the Threat!

Terry W. Mayfield





Every Company Needs a Business Continuity Plan

Today's business environment is pressing business owners and managers to reexamine the threats that could cause business interruption. Organizations of all sizes are generating and depending on larger amounts of data that must be readily available and easily accessible. Consequently, companies have to effectively manage more infrastructure resources, including servers, networks, and storage, to ensure data is protected in a timely manner while at the same time providing adequate performance and capacity and securing data for access when needed.

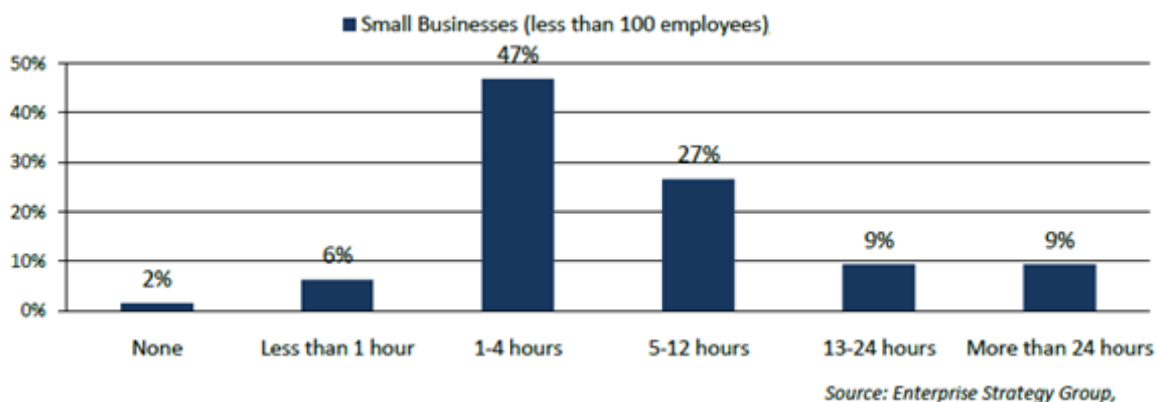
Many risks are unavoidable, but if your company does not have a business continuity plan to protect your critical data then you are **extremely vulnerable** to unexpected downtime and data loss due to viruses, hackers, equipment failure, or even human error. This means you are probably thinking that business interruptions only happen to the other guy, but would never happen to you.

Ignoring Thorough Business Continuity Planning can be Very Dangerous. Here's why:

Studies show that 93% of businesses that lost their computer network for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster, and 50% of businesses that found themselves without a way to restore or reconstruct their data for this same time period, filed for bankruptcy immediately.

But even if you don't experience this level of catastrophe, you can still end up losing a considerable amount of productive work and man hours due to a system crash, virus, power outage, or even human error. Not to mention the money it will take to restore your system.

The table below shows the number of hours that businesses can be down before they begin to experience revenue loss or damage to business operations.





BTS Technologies

Even more mind-boggling is the fact that these business interruptions could have been prevented. How?

Today's digital technology and the internet enable information to be protected both on site and at remote data centers. Therefore, if an event should occur your business can keep running as if nothing happened, or down time can be greatly reduced.

Business continuity planning is a growing concern. Experts are attributing this primarily to business owners and managers coming to the realization that operating without a viable continuity solution in place is simply a risk they are not willing to take. The pace of today's business environment is faster than it has ever been, and business owners cannot afford to lose their valuable data.

All businesses face a certain degree of risk, but most savvy business owners and managers are looking to eliminate unnecessary risks as well as uncertainty. Business continuity solutions provide business owners and managers with a safety net that enables organizations to continue to operate without anyone noticing a network interruption. Whether a natural disaster, virus attack, power outage, or human error, a business continuity plan provides businesses with the assurance that they need to compete in today's markets.

Tape Backup: There is a Better Way

Historically, the data backup method for most companies has been to backup vital information on a data tape and let an employee such as an IT manager take it home for safe keeping. It's a simple and cheap plan. But you get exactly what you pay for. The problems with tape backup are well known; companies have been dealing with them for decades.

- **Tape backup requires a significant investment.** Tape hardware and backup software are expensive, as is the labor required to set up and maintain them.
- **Tape is physically delicate and easily compromised by environmental factors** such as heat, humidity and magnetic interference, and tape cartridges must be replaced every 6 to 12 months.
- **Tape sensitivity contributes to high failure rates;** with analysts estimating that 40 percent of tape restores fail.



- **Tapes themselves are subject to loss or theft**, and may be in the possession of an employee or vendor unable to reach a recovery site.
- **Tape is seldom encrypted**, compounding the destructive impact of tape theft. Very few people encrypt backup tapes. This creates security vulnerability because they rely only on the security of the off-site rotation process to secure the data.
- **The tape backup process is inconvenient**. Tape backup can involve downtime, known as ‘backup windows’, since the system being backed up cannot be used during the process. Given the ever-increasing demand for around the clock data access, it gets harder and harder for companies to complete nightly backups within the time window provided. In many cases, it is so hard to complete the backup that the once-nightly backup goal often slips to every other night for many machines.
- **The tape backup and restore process is inconsistent**. In a survey of 500 IT departments, as many as 20% of routine nightly backups fail to capture all data. Among participants of another survey, 40% of IT managers were unable to recover data from a tape when they needed it. The odds were high that neither the tape backup nor the restore would work at the critical moment. This is a significant concern for corporations that are regulated by industry or government requirements as they can face the risk of being out of compliance if they cannot produce required data when they need it.
- **Tape backup is unable to achieve an acceptable recovery point objective (RPO)** – the point in time to which system data can be recovered should disaster strike. Periodic tape backup guarantees hours of lost data in the event of a disaster. Suppose, for example, that a critical system fails anytime today; the most recent data that can be recovered is yesterday's data, which will be at least twelve hours old. The later in the day disaster strikes, the older the recoverable data will be. In addition, recovering from a disaster, any data not backed up is lost for good – unless it can be recreated.
- **Traditional tape-based backup solutions have fallen behind and are no longer meeting backup/restore requirements**. Historically, organizations have performed their backups to tape and carried a copy of these tapes off-site. However, installed disk capacity has grown faster than tape performance, Add the demands of 24x7 Web operations and ecommerce-based applications, and the need to supplement traditional backup and recovery methods becomes obvious.



BTS Technologies

There was a time when tape-based backup was widely believed to be the only feasible backup solution for SMBs. But tape backup is no longer the only realistic solution and cost-effective alternate solutions are coming to the forefront. As a result of this shift, enterprises are re-evaluating their tape backup solutions. When evaluated on such criteria as total cost of ownership, scalability, data security, automation, reliability, ease of data restoration, required length of backup window, and server virtualization, it becomes obvious that alternate solutions have much to offer.

Fortunately, advances in technology have made the data continuity process easier to manage. Solutions such as BTS's **SleepEZ** Data Continuity Service protects your critical data by combining all of the software and hardware needed to meet the requirements of a comprehensive data continuity solution. The **SleepEZ** solution removes the uncertainty of tape backups and provides a high level of data protection for business-critical data.

The SleepEZ Service: A Comprehensive Data Protection Solution

- **Proactive Monitoring of your Network 24/7/365:** We'll be able to predict and prevent problems before they even arise. This service can save thousands of dollars by PREVENTING an expensive disaster from happening!
- **Frequent Backups:** A complete image of servers covered by **SleepEZ** is stored and is updated every 15 minutes. The 15-minute incremental backups are saved for 3 days; a daily backup for 1 month; a monthly backup for one year. A copy of the most recent daily backup is copied offsite every night and stored in 2 different data centers on opposite sides of the continental U.S.
- **Standby Server:** A network attached storage device (NAS) is installed in your equipment room. A complete image of servers covered by **SleepEZ** is stored on the onsite NAS device. Servers covered by **SleepEZ** can be virtualized on the NAS device in the event of a server failure. You have the ability to restore to a virtual server or dissimilar hardware configuration for ease of recovery after a disaster; e.g. hardware failure.
- **Data Integrity Monitoring:** Not only will we make sure your system is actually backing up every night, but we'll make sure the data is not corrupted and can be recovered in the event of a disaster. Backups are tested and verified on a monthly basis.



BTS Technologies

- **Rapid Recovery:** Servers covered by **SleepEZ** can be virtualized on the NAS device in the event of a server failure. Downtime is reduced to hours instead of days. In the event of a catastrophic loss of facility a new NAS can be imaged at the offsite data center and shipped overnight to help get your servers up and running the moment temporary office space is located.
- **A NO-Hassel, NO Questions, NO Problem, “Cancel the Service” Guarantee:** Sign up and use our **SleepEZ** service for 3 months. Put us to the test. If you don’t feel we’ve helped you make your network much more secure, and greatly reduced the chance of a network disaster give us a call and say, “this is not really working for us.”

Is the SleepEZ Service Right for Your Company?

Contact Terry Mayfield by phone (205-290-8424) or email (terrym@askbts.com) He can discuss your data protection requirements and review your network storage to customize the **SleepEZ** solution for your company.