



Is your POS ready for a Disaster?

BROWNSTONE TECHNOLOGY SOLUTIONS

Volume 3, Issue 1

March 2011

Are you prepared for disaster?



Are you prepared for disaster? Not the kind that occurs every day such as the fresh food going bad, a cash drawer shortage or the POS terminal freezing, but rather a real disaster. Are you ready for a POS server failure? An office fire that destroys your POS server(s)? A power surge that knocks all of your POS workstations off-line and corrupts your database? A burglary that includes your POS server(s)?

Disaster recovery for your POS system is something that we all think about but often fail to follow up on. When a real disaster strikes, you need to be prepared in order to get your business back-on-line. Proper disaster recovery planning can be the difference between being

back in business quickly or closing down for good.

A good disaster recovery plan includes a minimum of several elements including:

Notification - An effective recovery from a disaster first requires notification that there is a disaster. Some type of alert software should be used to notify the appropriate person when a server experiences problems, and specifically when a server goes off line. This notification will allow the appropriate personnel to check on the server which unfortunately may result in determining there has been a complete failure. Many operating systems and databases have this type of alert capability.

Same Computer Backup - A backup of your POS database should be done each day, at a minimum, and maintained on a different drive, on the same computer. This allows for quick recovery in case of a localized problem with the

database. This backup should be conducted at prescheduled intervals. Typically this backup can be automated.

Different Computer Backup - Much like the backup to the same computer a backup of the POS database should be done at least daily. This computer will also need to contain the operating system for the POS in order to recover and use the database if needed. This backup should be conducted at prescheduled intervals. Typically this backup can be automated.

Off-Site Backup - An entire backup of your POS system, its operating system, database and all related components should be done off-site on a predetermined schedule. There are several ways to conduct off-site backups:

Tape - A backup may be done on tape and the tape should be secured off-site. The drawback to this type of backup is that a person has to be responsible for

Disaster recovery plan includes several elements:

- NOTIFICATION
- SAME COMPUTER BACKUP
- DIFFERENT COMPUTER BACKUP
- OFF-SITE BACKUP
- RECOVERY PLAN

Inside this issue:

ARE YOU PREPARED FOR DISASTERS?	1-2
NEW TWITTER PAGE	2
HOW TO CHOOSE A POS SYSTEM THAT IS RIGHT FOR YOUR BUSINESS?	3
SAFETY & SOCIAL NETWORKING SITES	3
COMPANY INFORMATION	4

Is your POS ready for a Disaster?

Are you prepared for disaster?

and remember to exchange tapes and move them off-site.

Backup To An Off-Site Computer - Backups may be done to a computer located at another location. This computer may be owned by the establishment or a service that provides backups at another location, usually a datacenter that specializes in backups. The drawback to this type of backup is an off-site backup must have access to the on-site computer on a predetermined schedule.

When determining how often to conduct off-site backups remember that all data between backups will be lost in case of a disaster. So if you backup monthly you could lose up to one month's data, backup weekly and you can lose one weeks data and so

on. This does not just include sales, this also includes menu changes, price changes, etc.

Recovery Plan - By far the most important part of the disaster recovery plan is the recovery plan itself. Some of the questions that a recovery plan must include are:

1. Who will be in charge of the recovery efforts?
2. Who will physically do the recovery of hardware and software?
3. Do you have backup hardware to use? If not, where will it come from?
4. What are the contact points and communication plan?

It is critical that the recovery plan is in writing, and that all parties involved have a clear understanding of their roles. The recovery plan should be

reviewed on a regular basis to ensure it is up-to-date and accurate.

Nobody wants to think about the possibility of their POS system suffering a major failure but at the same time everyone must be prepared for the possibility. Make sure you have a comprehensive disaster recovery plan for your location just in case that worst case scenario does happen.



When a real disaster strikes, you need to be prepared in order to get your business back-on-line.

Twitter.com/pos_systempros

Brownstone Technology Solutions announced the launch of its new Twitter page to increase its accessibility to current clients. BTS plans to utilize this social media strategy to distribute news about its new point-of-sale software, BPOS, to provide support and advice to its current customers, and to establish a brand for BPOS.

The Twitter page can be found at: http://twitter.com/pos_systempros. Tweets will be sent out daily, and "followers" will be able to gain access to cutting-edge information about the new software. Current customers will also be able to obtain information about special deals and promotions regarding the new software.

All clients will receive a letter in the mail with this information, as well as an email reminding them to "follow" BPOS on Twitter.



How to choose a POS system that is right for your business?

Choose a system that is right for you and meets your business needs. Analyze and prioritize your needs:

- Reduce Costs
- Monitor Staff Schedules and Associated Costs
- Monitor Sales In Real-Time
- Monitor Your Inventory
- Meet Your Bottom Line Goals
- Simplify Training

Compare quotes & analyze the following:

- Review Line Item Descriptions
- Training Costs
- Support Costs and Terms
- Review the Implementation Timeline
- Understand Total System Costs

Implement an effective system. Ensure the supplier provides:

- Site Preparation
- Detailed Project Management Outline
- Training Schedules; both Managers and Staff
- System Support



Posiflex KS7315 Fan-Free Cel-M 1.8, 2GB RAM, 160GB HDD, POS Ready

Safety & Social Networking Site

Participation on social networking sites can have some serious safety ramifications, so what can you do to safely use social networking sites?

1. Password security - Use strong password security. Always use at least three of the following characters in your password - uppercase letters, lowercase letters, numbers, special characters such as *. In addition always use at least 6 to 8 characters in your password and NEVER use birthdates, kid's names, pet's name, parent's names or birthdates, city born in, etc.
2. Privacy statements/policies - Read the privacy statement and policies associated with the site. This will be downloadable on their homepage. Make sure the site does not retain private information once you delete your account. Make sure you are aware of when they can and cannot release any of your information to a third party without your consent.
3. Research security breaches - Search the site on the three major Internet search engines and see if they have a history of security issues. Simply search the name of the site and "security breaches" and "release of information."
4. Screen what you say - Be careful what you say. Never say anything you would not say in a public place like a store or restaurant. Never say anything that you do not want heard by the people listed above.
5. Screen pictures and video - Never post any picture anywhere on the site (public or private) that you do not want seen by your boss, significant other, parents, co-workers, etc. Never associate a full name with a picture as this makes it very easy to search for. Remember, once pictures and videos are released in the public domain they can never be taken back.
6. Be careful what you allow others to post - Be careful what information you allow your friends and family to have if you know they "love to post everything" on a social networking site. If they post it you run the same disclosure risks as if you post it yourself.
7. Remember, this is PUBLIC domain - Every time you are going to say or post something just remember that you are in the public domain of the Internet and this information may very well follow you for the rest of your life and be accessible to hundreds of millions of people.

Social networking sites can be a great ways to meet people, share information and gain knowledge, but you must also be aware of the potential privacy and security risks, as well as the potential ramifications and the action you need to take in order to avoid these issues.





Service | Quality | Innovation

BROWNSTONE TECHNOLOGY SOLUTIONS

2625 Manhattan Beach Blvd.
Suite 100
Redondo Beach, CA 90278
Phone 310.297.3605
Toll Free 800.241.6808
Fax 310.297.3609
www.brownstonets.com



Brownstone Technology Solutions provides a variety of products and services related to point-of-sale (POS) systems, video surveillance systems, network services and related training. BTS products and services are designed for the hospitality and retail industries.

BTS specializes in integrated systems for the restaurant & bar, hotel & motel and retail industries.



2625 Manhattan Beach Blvd.
Suite 100
Redondo Beach, CA 90278