Does Your Plan Protect You From Loss…?

What do you when all your information technology stops working? Businesses large and small have essential data that is vital to the survival and continued operation of their business. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be catastrophic. A very high percentage of companies that suffer from a disaster event and weren't properly prepared found themselves out of business within 6 months. A plan for data backup and restoration of electronic information is crucial for all business sizes.

Small Business Cyber Security Statistics

- 43 percent of cyber-attacks target small business.
- Only 14 percent of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.
- 60 percent of small companies go out of business within six months of a cyber-attack.
- 48 percent of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest.

As cyber criminals continue to target small businesses, owners and employees need to know how to protect themselves and also have plans in place for when it inevitably does occur. A step-by-step recovery plan consists of the precautions to minimize the effects of a disaster so your organization can continue to operate or quickly resume mission-critical functions. Recovery strategies should be developed for all IT systems, applications and data,

including networks, servers, desktops, laptops, wireless devices, data and connectivity. If you already have a plan, how confident are you that the plan will actually work? Recovery plans are only as good as their testing. Testing identifies deficiencies and provides opportunities to fix problems before a disaster occurs. Since IT systems and technologies are constantly changing, testing also helps ensure a disaster recovery plan is up to date.

Develop a Disaster Recovery Plan or Find Out If Your Plan is sufficient and meets business recovery requirements. Infrastructure Assessment by qualified providers is key to finding week spots or vulnerability in your strategy. Don't wait for a Disaster to strike to find out if you are prepared. Top 10 Reasons to take a closer look at your plan:

1) Many organizations experience a failure of some kind in any given year, and most of those businesses will go under in just over a year after that extended outage or Disaster and Recovery. IT downtime have costed an estimated $27 Billion dollars in lost revenue within the last 10 years. Your Organization can not afford not to have the right disaster recovery plan in place to protect data and business operations. Your customers a expect your company's products and services to be available 24/7/365. Downtime means a lack of availability to your customers and a loss of revenue to competitors.

2) In an always on business world, your customers expect to have access 24/7. Downtime means a lack of availability to your customers and a loss of business. You need the right technologies to provide the proper level of continuity and protection from outages related to disaster or production operations.

3) Downtime and lost data can impact business operations, reputation with your customers. This can Negatively impact the view of your company which can lead to loss of trust that can result in a large amount of lost revenue from your customers. Many small and medium sized enterprises don't have a sufficient DR plans in place to protect data and business operations. Most are not even doing regular recovery tests to make sure the plan is sound. Are you taking chances with your business and creating **High Risk of loss**?

4) Natural disasters have cost the global economy Trillions of dollars since the early 2000's. Virtually every region of the world is vulnerable natural disasters like fire, flood, Power Failures, Earthquakes, hurricane's or tornado. A disaster of any of these types can be severely business impacting and have a cost of thousands to millions of dollars for some organizations.

5) You can buy the best technology available but that does not mean you are protected from loss or service interruption. Roughly 95% of IT professionals have had experience with hardware or applications failures of some kind that effected business operations during the course of their career.

6) Roughly 70% of web users report abandoning a company website for a competitor's due to problems such as latency with site operations. When a website goes down, online shoppers will not wait for the unknown time period that the site is down before they go else ware to spend their money for Products and Services. If you aren't protecting your company site your leave the door right open to revenue loss to competing products and services.

7) 60% of Business' and Corporations need to produce DR reports for things such as compliance. Disaster Recovery plans and technologies helps protect data and retain data required by regulation. Data Loss and inability to recovery can lead to serious legal problems with regulatory standards set by the government.

8) A large portion of Business's were immediately put out of business by a “major loss” of data, and almost half of them permanently closed their doors within two years leaving roughly a 10% rate of survival.

9) Are you running duplicate sites, multiple servers, all to ensure if something happens to one you have another? Multi-site Recovery Plans can be complex and really difficult to execute if the plan is too hands on and lacks automation.

10) People make mistakes. 80% of unplanned outages are due to ill-planned changes made by administrators and 60% of availability and performance errors are the result of errors in configuration