**Risk Management & Disaster Recovery**

* **The identification, analysis, control and communication of risks in the business world are concerns every company faces!**

**What you do to face these risks is up to you.  Who you hire to help control the risks is where we come in!**

* **Why go it alone, when you can have network engineers and IT experts ready to help your staff that are already trained in implementation methods**
* **Risk Management can be achieved for a fraction of the cost of partnering with major security vendors, and all it takes is one phone call to us!**
	+ **Businesses face Risks every day!  Some risks are unseen, others refuse to be noticed!**
	+ **Internet hackers taking advantage of little known exploits are**
		- **randomly seeking out vulnerable server operating systems and**
		- **targeting your network right now. Are you protected?**

**Some** ***risks* are obvious such as physical damages from flood, fire or natural disasters, others are not obvious!**

* + **The truth is, there is no such thing as being 100% invulnerable, but there are certainly measures that can be taken to reduce risks. Not every company is in a position to manage them independently and we would be less than truthful if we stated that even our own networks are impervious to all forms of risk.**
* **But, by competing in a global marketplace for PC market share, we have learned a lot along the way.**
* **It takes more than wishful thinking to prevent problems, it requires action!**
	+ **These days it takes a full time team of internet engineers & security specialists and more than old fashioned luck to keep your business network up and running.**
		- **If you think in this world of technology that you can go it alone, think again! If you're looking for help in determining how to better manage your risk then we suggest you call us!**
		- **By allowing us to help serve and protect your network needs, you get access to not only our own expertise in risk management, you get the benefit of our partners knowledge base and training experience**
* **When Disaster Strikes..., Will you be Ready?**
* **The related concept of business continuity involves insuring that an organization's critical business processes, including those utilizing IT systems, can be maintained in the event of a disaster.**
	+ **Does your company have what it takes?**
	+ **All good IT disaster recovery plans consider the three main components of operations which are Data, Systems & People.**
* **Of prime concern with IT disaster prevention, planning, and recovery today you must consider the following;**
	+ **Cost - comprehensive disaster recovery is extremely expensive**
	+ **Testability - disaster recovery plans that look great on paper but are technically unproven will likely fail in practice**
* **Overemphasis on the back office - without the people and the client-side infrastructure available, business still can't be done**
	+ **Some of the considerations of our disaster recovery  plans include use of all of the following and more;**
	+ **Network Backups**
	+ **Mirroring & Replication**
	+ **Replication & Imaging**
	+ **Failover Clustering**
	+ **Survivability - It's more than having what it takes to get by in a disaster, it's continuing to thrive in the event of one!**
* **In the IT field, disaster recovery involves a series of actions to be taken in the event of major unplanned outages to minimize their adverse effects.**
	+ **Disasters can result from events such as;**
		- **Hacker attacks**
		- **Computer viruses**
		- **Electric power failures**
		- **Underground cable cuts & failures**
		- **Fire, flood, earthquake, and natural disasters Mistakes in system administration**
* **It takes Partners - We've Got them!**
	+ **That's why we make proud mention of our dedicated partnership alliances with multiple worldwide vendors, because without them our own risks would be nearly unmanageable.**
* **Failure Mode and Effects Analysis: Examines each potential failure condition in a system to determine the severity of the impact to the system.**
* ***HAZOP (Hazard and Operability): Examines process and engineering intentions to assess the potential hazards that can arise from deviations from design specifications.***
	+ ***Historical Analysis: Examines frequency of past incidents to determine the probability of a condition recurring.***
	+ ***Human-Error Analysis: Examines the possible impact of human intervention and error on a system.***
	+ ***Probabilistic Risk Assessment: Examines the probability that a combination of events will lead to a particular condition.***
	+ ***Tree Analysis: A family of analysis methods, such as event tree, attack tree, management-oversight tree and fault tree, that focuses on processes or a sequence of events that may lead to a particular condition.***
* **Prevention - It hardly ever is thought about until "after" the fact - (when it's needed least)!**

**Don't let Disasters render you helpless!**

* **For those events that can't be prevented, an IT disaster recovery plan takes into account the need to;**
* **Notify any affected parties so that they can take action as needed when and where they are needed most**
* **Isolate the affected systems so that damage cannot spread**
* **Repair the critical affected systems so that operations can be resumed**
* **Detect the possible outages or other disaster effects as quickly as possible**

**Disaster Plans - Before you need one... Get one!**

* **Some of the considerations of our disaster recovery plans may include use of all of the following and more**

**Hot Sites**

* **A hot site is a commercial disaster recovery service that allows a business to continue computer and network operations in the event of a computer or equipment disaster**
	+ **For example, if an enterprise's data processing center becomes inoperable, that enterprise can move all data processing operations to a hot site**
* **A hot site has all the equipment needed for the enterprise to continue operation, including office space and furniture, telephone jacks, and computer equipment**

**Cold Sites**

* **A cold site is a similar type of disaster recovery service that provides office space, but the customer provides and installs all the equipment needed to continue operations**
	+ **A cold site is less expensive, but it takes longer to get an enterprise in full operation after the disaster.**

**Typically, a business has an annual contract with a company that offers hot and cold site services with a monthly service charge**

**Online Backups**

* **Some disaster recovery services offer** [**backup**](https://web.archive.org/web/20080719163709/http%3A/searchstorage.techtarget.com/sDefinition/0%2C%2Csid_gci211633%2C00.html) **services so that all company data is available regardless of whether a hot site or cold site is used**
	+ **If an enterprise must use a hot or cold site, there are usually daily fees and other incidental fees in addition to the basic service charge**