Business Continuity / Disaster Recovery

J. Michael Lam, VP Premier Technical Services

Avoid Being a Statistic

- 93% of companies who lost their data for 10 days or more as a result of a disaster filed for bankruptcy within one year

- 50% of businesses that found themselves without data management for 10 days or more filed for bankruptcy immediately

- 70% of all businesses that have a major fire go out of business within five years, 30% fail within one year

- An estimated 25 percent of businesses do not reopen following a major disaster

- 70 percent of small firms that experience a major data loss go out of business within a year

Source: National Archives and Records Administration

What Happens Next?

Of companies experiencing catastrophic data loss:

- 43% of companies never reopened
- 51% of companies closed within 2 years
- 80% of companies that do not recover from a disaster within one month are likely to go out of business.
- 75% of companies without business continuity plans fail within three years of a disaster
- Companies that aren't able to resume operations within ten days are not likely to survive

Of those businesses that experience a disaster and have no emergency plan, 43 percent never reopen; of those that do reopen, only 29 percent are still operating two years later.

Are You Prepared?

- According to an AT&T Survey of 100 Chicago firms (revenues <$10M), 81 have DR plans, but only 43% have fully tested their plans within the last 12 months and 12% admitted they have never tested their business continuity plans .When Hurricane Earl, was a major hurricane, hit the East Coast of the U.S. many enterprises will find that their Business continuity plans were not adequately tested.

- Critical data centers, with backup generators, facilities and fuel supplies, are now built to continue operating during storms. The same can't be said for the small business that rely on their computing servers, desktops, and laptops.

- Last year there were only three hurricanes in U.S. waters last year, and none of them brought hurricane force winds over land in this country. In 2009, there were an average of 236 power outages a month in the U.S. Through July of 2010, the average had increased to 273 a month.

What if your Email is down?

- Comcast customers had been unable to receive e-mail for at least 24 hours beginning Wednesday, an inconvenience that sparked anger and calls for government oversight of the nascent broadband industry.

- A representative for the company said the outage was caused by problems with its e-mail distribution servers. Initially customers could neither send nor receive e-mail, but since late Thursday customers had been able to send but not receive, the representative said.

- The outage persisted into Friday morning, according to a customer-support representative, and the system was clogged as Thursday's incoming e-mails were being distributed.

- Over 900,000 email accounts affected.

- 24+ hours for resolution.

Laws and regulations that may mandate having a disaster recovery plan (or indirectly require one) include:

- The Foreign Corrupt Practices Act of 1977.
- Internal Revenue Service (IRS) Law for Protecting Taxpayer Information.
- Food and Drug Administration (FDA) mandated requirements.
- Homeland Security and terrorist prevention.
- Pandemic (Bird Flu) prevention.
- ISO 9000 certification.
- Requirements for radio and TV broadcasters.
- Contractual obligations to customers, business partners.
- Document protection and retention laws, including the FRCP (the Federal Rules of Civil Procedure).
- Personal identity theft laws and insurance.
- GLB (Gramm-Leach-Bliley act).
- DMCA (Digital Millennium Copyright Act).
- FMA (Financial Management and Accountability act).
- FERPA (Family Education Rights and Privacy Act).
- CFAA (Computer Fraud and Abuse Act).

Is this your plan???
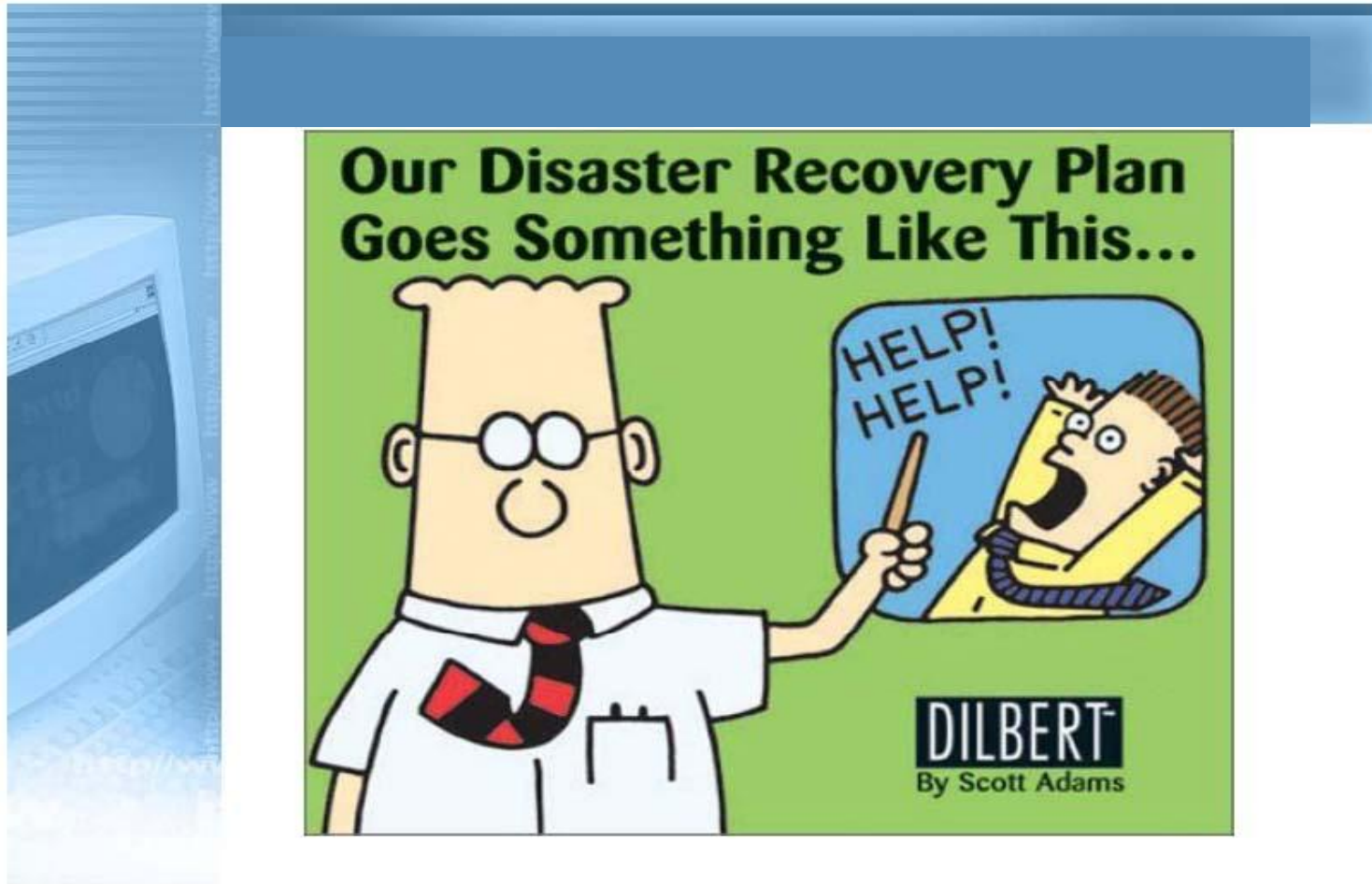
- What is……a "disaster"

- A **disaster** is a perceived tragedy, being either a natural calamity or man-made catastrophe. It is a hazard which has come to fruition. A hazard, in turn, is a situation which poses a level of threat to life, health, property, or that may deleteriously affect society or an environment.

- In contemporary academia, disasters are seen as the consequence of inappropriately managed risk. These risks are the product of hazards and vulnerability.

Is Your Businesses Prepared?

- This all might seem so obvious, that it is hard to conceive of any small business that does not frequently back up its key data. The SBA tells all small business owners: "Make back-up copies of all tax, accounting, payroll and production records and customer data on computer hard drives, and store the records at an offsite location at least 100 miles away. Important documents should be saved in fireproof safe deposit boxes." It all seems so obvious, yet a national Harris Interactive survey of 597 computer users, as reported in Realty Times found:

- One in four users frequently back up digital files, even when 85 percent of computer users say they are very concerned about losing important digital data.

- Thirty-seven percent of the survey's respondents admitted to backing up their files less than once per month.

- Nine percent admitted they have never backed up their files. More than 22 percent said backing up information is on their to-do list, but they seldom do it!

Deltaville – Less than 200 miles away

Deadliest Year for Tornadoes in Virginia

- 2011 has become the second deadliest year for tornadoes in Virginia since 1950, when the National Weather Service began tracking such data.

- Initial reports say more than 400 private homes and businesses were damaged, but that number likely will increase because some of the hardest-hit areas still haven't finished sorting out the losses.

- Businesses also suffered severe losses, including a hose-and-belt manufacturing plant that is a total loss. Washington County is working to find another location for the facility and its 170 jobs.

- Inspections found the most powerful storm in the regional outbreak struck in Virginia's Shenandoah Valley, ripping a 33-mile path across Rockingham and Shenandoah counties in the northern end of the valley.

The devastation that was Hurricane Katrina is still fresh in our minds and the calamitous results can still be seen not just in New Orleans but across the Gulf Coast. Katrina generated the largest single loss in the history of insurance – $40.6 billion and more than 1.7 million claims – across six states

Louisiana, Mississippi, Alabama, Florida, Tennessee, and Georgia.

Katrina Disaster

- Approximately 81,000 businesses in Louisiana were damaged by hurricanes Katrina and Rita last year, according to the Census Bureau. Mary Lynn Wilkerson, director of the Louisiana Small Business Development Centers says the number was greater, 110,000 businesses in Louisiana were destroyed or severely impacted.

- Although 75 percent have since reopened their doors, around 18,700 have closed permanently since the storms, according to the Louisiana Recovery Authority19. Two-thirds of those not reopening have are classified as small business.

- We lost over 60 percent of our small businesses," says Doug Gurley, state director of the Mississippi Small Business Development Center

A Disaster Is Not Just Weather Related

- For a small, growing or even medium sized business a disaster can be caused by a hurricane or a tornado, by a fire, or simply by a wrong keystroke. One study shows that 50 percent of data loss is caused by **USER** error. But no matter how it is caused, a loss of data, or access to data for any kind of extended period, inevitably means a loss of revenue, a loss of productivity, a loss of reputation, and increased costs.

- A frozen pipe that bursts on a weekend might not be detected until you open for business on Monday morning; long after the resulting flood has destroyed inventory, equipment, floors or walls. Disasters that threaten a business can happen anywhere at any time. Some rather startling statistics that are generally accepted in the data recovery field and reported by the University of North Carolina's Information Technology Service:

Loss of Data is a DISASTER

- A hard drive crashes every 15 seconds
- 2,000 laptops are stolen or lost every day
- 32% of data loss is caused by human error
- 31% of PC users have lost all of their PC files to events beyond their control.
- 25% of lost data is due to the failure of a portable drive.
- 44% of data loss caused by mechanical failures
- 15% or more of laptops are stolen or suffer hard drive failures
- 1 in 5 computers suffer a fatal hard drive crash during their lifetime.
- 40% of Small and Medium Sized Businesses don't back up their data at all.
- 60% of all data is held on PC Desktops and laptops

What do YOU need to do

- Business continuity planning begins with assessing how potential risks to your business will impact your ability to deliver products and services

- Start by defining what those risks are so you can look into ways to mitigate them. You can't plan for everything, but you should be aware of the risks that are statistically likely to happen to you, based on factors such as geography. The odds of a hurricane hitting a company on the coast of Florida are very high. The odds of one hitting Tulsa, Oklahoma, are very low." You should also look around your workplace for smaller physical risks, like having a hot plate near paper, a potential fire hazard.

- Define your backup strategies, implement and protect your data and your customers sensitive data.

- The KEY is to be redundant. Arrange backup vendors or suppliers to provide you with critical resources and materials. List of vendors with pre-approvals on equipment.

WHAT DO YOU need to do

- Make sure you have a technology recovery plan, and that you have backed up important IT data like customer records and corporate documents. Back them up more than once, and arrange a secure, off-site storage location. Make sure the appropriate people have knowledge of relevant passwords and codes, and that you have backup tech vendors arranged.

- Make sure you have contact information for all critical staff (staff that you need to rebuild your infrastructure). Remember their home may be lost or as simple as they are out of town on an remote island. Who is your next point of contact.

- It's a good idea to appoint someone (possibly yourself if you're a small business owner) to coordinate the efforts to create a business continuity plan, but a successful plan requires feedback and input from all parts of an organization. Never try to create a plan in a vacuum, You need a dynamic group to get people together talking about exactly what they do and how they do it.

WHAT DO YOU NEED TO Do

- The document itself is the product of all this planning, analysis and input. It's your Bible when disaster strikes, so make sure it's clear, concise and simple enough for any employee to understand. It should address the basic questions of what are you going to do, where are you going to do it from, who is going to do it, and what resources, support, equipment, and facilities do you need to do that.

- Make sure the document includes all the information you've gathered so far: supplier contact information, backup suppliers, employee contact information, the roles and responsibilities of key employees, major client contact information, backup equipment and IT data, and the place of the off-site recovery location. It should also establish a timeframe for getting this done, in order of priority. For example, it should clearly spell out what's accomplished within the first hour, within the first day, and within the first week.

WHAT DO YOU NEED TO DO!!!

- Creating a plan that allows your organization to stand up against a major disaster or disruption is a gradual process. You can't be perfect right out at the start, You need to create an expectation of continuous improvement and realize it's not just a project, but a long term goal. It is a simple concept, but the devil's in the details and the execution.

- Test Your Plan

- Contingency planning is a living and breathing document, as your business changes it must change.

Now What ??

Review
Design
Implement
Test

Thank You / Questions?

J. Michael Lam, Vice President